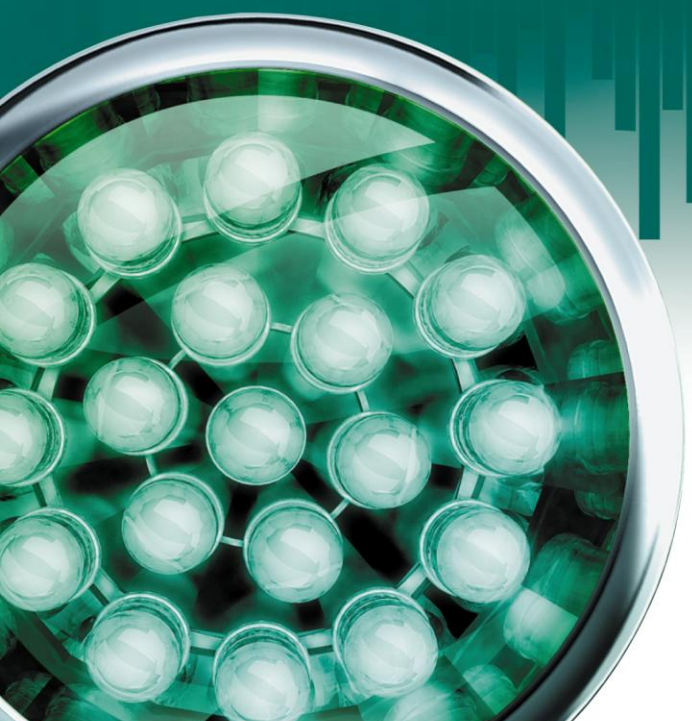
Kaspersky PURE

MANUEL DE L'UTILISATEUR

VERSION DE L'APPLICATION : 9.1



KASPERSKY lab

Chers utilisateurs !

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

Attention ! Ce document demeure la propriété de Kaspersky Lab ZAO (puis dans le texte 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, en tout ou en partie, est passible de poursuites civiles, administratives ou judiciaires conformément aux lois de la France.

La copie sous n'importe quelle forme et la diffusion, y compris la traduction, de n'importe quel document sont admises uniquement sur autorisation écrite de Kaspersky Lab.

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

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

Kaspersky Lab ne pourra être tenue 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. La responsabilité de Kaspersky Lab en cas de dommages liés à l'utilisation de ces textes ne pourra pas non plus être engagée.

Ce document reprend des marques commerciales et des marques de service qui appartiennent à leurs propriétaires respectifs.

Date d'édition : 14.09.2010

© 1997–2010 Kaspersky Lab ZAO. Tous droits réservés.

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

CONTENU

CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB 12

PRESENTATION DU GUIDE 18

Dans ce document 18

Conventions 20

SOURCES D'INFORMATIONS COMPLEMENTAIRES 21

Sources d'informations pour une aide autonome 21

Discussion sur les logiciels de Kaspersky Lab dans le forum en ligne 22

Contacter le service commercial 22

Communication avec le Groupe de rédaction de la documentation 22

KASPERSKY PURE 23

Distribution 23

Organisation de la protection du réseau domestique 24

Service pour les utilisateurs enregistrés 26

Configurations logicielle et matérielle 27

INSTALLATION ET SUPPRESSION DE L'APPLICATION 28

Installation de l'application 28

Étape 1. Rechercher d'une version plus récente de l'application 29

Étape 2. Vérification de la configuration du système par rapport à la configuration requise 30

Étape 3. Sélection du type d'installation 30

Étape 4. Lecture du contrat de licence 30

Étape 5. Règlement d'utilisation de Kaspersky Security Network 30

Étape 6. Sélection du dossier d'installation 31

Étape 7. Sélection des composants à installer 31

Etape 8. Recherche d'autres logiciels antivirus éventuellement installés 32

Etape 9. Désactivation du pare-feu de Microsoft Windows 32

Etape 10. Préparation de l'installation 32

Etape 11. Installation 33

Etape 12. Activation de l'application 33

Etape 13. Analyse des données 33

Etape 14. Enregistrement de l'utilisateur 33

Etape 15. Fin de l'activation 34

Etape 16. Restriction de l'accès à l'application 34

Etape 17. Sélection du mode de protection 35

Etape 18. Configuration de la mise à jour de l'application 35

Etape 19. Sélection des menaces identifiées 36

Etape 20. Analyse du système 36

Etape 21. Fin de l'Assistant 36

Première utilisation 37

Modification, réparation ou suppression de l'application à l'aide de l'Assistant d'installation 38

Étape 1. Fenêtre d'accueil du programme d'installation 38

Étape 2. Sélection de l'opération 38

Étape 3. Fin de la réparation, de la modification ou de la suppression du logiciel 39

ADMINISTRATION DE LA LICENCE....40
Présentation du contrat de licence....40
Présentation de la licence....40
Présentation du code d'activation....41
Consultation des informations sur la licence....41
INTERFACE DE L'APPLICATION....43
L'icône dans la zone de notification de la barre des tâches....43
Menu contextuel....44
Fenêtre principale de Kaspersky PURE....45
Protection de l'ordinateur....47
Mes Sauvegardes....49
Mon Contrôle Parental....50
Fenêtre Mon Gestionnaire de mots de passe....50
Icône dans la zone de notification....51
Menu contextuel de Mon Gestionnaire de mots de passe....51
Fenêtre de la base des mots de passe....52
Fenêtre de configuration des paramètres....53
Bouton de lancement rapide....53
Extensions et modules externes....54
Index....54
Fenêtre de configuration des paramètres de l'application....54
Fenêtre de notification et messages contextuels....55
LANCEMENT ET ARRET DE L'APPLICATION....57
Activation et désactivation du lancement automatique....57
Lancement et arrêt manuels de l'application....57
ÉTAT DE LA PROTECTION DU RESEAU DOMESTIQUE....58
Diagnostic et suppression des problèmes dans la protection de l'ordinateur....58
Activation / désactivation de la protection de l'ordinateur....59
Suspension de la protection....60
Utilisation du mode de protection interactif....60
RESOLUTION DES PROBLEMES TYPES....62
Procédure d'activation de l'application....63
Procédure d'achat ou de renouvellement d'une licence....63
Que faire en cas d'affichage de notifications....64
Procédure de mise à jour des bases et des modules de l'application....64
Procédure d'analyse des secteurs importants de l'ordinateur....65
Procédure de recherche de virus dans un fichier, un dossier, un disque ou un autre objet....66
Procédure d'exécution d'une analyse complète de l'ordinateur....67
Procédure de recherche de vulnérabilités sur l'ordinateur....67
Vérification à distance de l'état de la protection des ordinateurs du réseau domestique....68
Procédure de protection des données personnelles contre le vol....69
Protection contre le phishing....69
Mon Clavier virtuel....70
Mon Gestionnaire de mots de passe....71
Mes Coffres-forts....72
Que faire si vous pensez que l'objet est infecté par un virus....73
Procédure de restauration d'un objet supprimé ou réparé par l'application....74

Que faire si vous pensez que votre ordinateur est infecté 74
Copie de sauvegarde des données 75
Comment restreindre l'accès aux paramètres de Kaspersky PURE 77
Comment restreindre l'utilisation de l'ordinateur et d'Internet pour différents comptes utilisateur 78
Procédure de création du disque de dépannage et utilisation de celui-ci 78
Création d'un disque de dépannage 78
Démarrage de l'ordinateur à l'aide du disque de dépannage 80
Que faire avec un grand nombre de messages non sollicités 80
Consultation du rapport sur la protection de l'ordinateur 82
Procédure de restauration des paramètres standards d'utilisation de l'application 82
Transfert des paramètres de l'application sur un autre ordinateur 83
CONFIGURATION ETENDUE DE L'APPLICATION 84
Protection de l'ordinateur 85
Analyse de l'ordinateur 85
Recherche de virus 86
Recherche de vulnérabilités 93
Mise à jour 93
Sélection de la source de mises à jour 95
Programmation de l'exécution de la mise à jour 96
Annulation de la dernière mise à jour 97
Analyse de la quarantaine après la mise à jour 98
Utilisation du serveur proxy 98
Lancement de la mise à jour avec les privilèges d'un autre utilisateur 99
Antivirus Fichiers 99
Activation et désactivation de l'Antivirus Fichiers 100
Arrêt automatique de l'Antivirus Fichiers 101
Constitution de la zone de protection 101
Modification et restauration du niveau de protection 102
Modification du mode d'analyse 103
Utilisation de l'analyse heuristique 103
Technologie d'analyse 104
Modification de l’action à réaliser sur les objets découverts 104
Analyse des fichiers composés 104
Optimisation de l'analyse 105
Antivirus Courrier 106
Activation et désactivation de l'Antivirus Courrier 107
Constitution de la zone de protection 107
Modification et restauration du niveau de protection 108
Utilisation de l'analyse heuristique 109
Modification de l’action à réaliser sur les objets découverts 109
Filtrage des pièces jointes 109
Analyse des fichiers composés 110
Analyse du courrier dans Microsoft Office Outlook 110
Analyse du courrier dans The Bat! 111
Antivirus Internet 111
Activation et désactivation de l'Antivirus Internet 113
Modification et restauration du niveau de protection 113
Modification de l’action à réaliser sur les objets découverts 114

Blocage des scripts dangereux 114
Analyse des liens par rapport aux bases d'URL de phishing ou suspectes....114
Utilisation de l'analyse heuristique 115
Optimisation de l'analyse....115
Module d'analyse des liens 116
Composition d'une liste d'adresses de confiance 117
Antivirus IM 117
Activation et désactivation de l'Antivirus IM....118
Constitution de la zone de protection 118
Sélection de la méthode d'analyse 118
Anti-Spam 119
Activation et désactivation de l'Anti-Spam....121
Modification et restauration du niveau de protection 121
Entraînement d'Anti-Spam 122
Analyse des liens dans les messages....125
Identification du courrier indésirable sur la base des expressions et des adresses. Composition des listes125
Régulation des seuils d'indice de courrier indésirable....130
Utilisation d'indices complémentaires pour le filtrage du courrier indésirable....131
Sélection de l'algorithme d'identification du courrier indésirable....131
Ajout d'une remarque à l'objet du message 132
Filtrage des messages sur le serveur. Gestionnaire de messages 132
Exclusion des messages Microsoft Exchange Server de l'analyse 133
Configuration du traitement du courrier indésirable par les clients de messagerie 134
Anti-bannière....136
Activation et désactivation de l'Anti-bannière 136
Sélection des méthodes d'analyse 137
Composition des listes d'adresses de bannières autorisées ou interdites....137
Exportation et importation des listes d'adresses 137
Contrôle des Applications 139
Activation et désactivation du Contrôle des Applications 139
Répartition des applications selon les groupes 140
Consultation de l'activité des applications 141
Modification du groupe de confiance....141
Règles du Contrôle des Applications....142
Protection des ressources du système d'exploitation et des données personnelles 145
Défense Proactive....147
Activation et désactivation de la Défense Proactive 147
Composition d'un groupe d'applications de confiance....148
Utilisation de la liste des activités dangereuses 148
Modification d'une règle de contrôle de l'activité dangereuse 148
Retour à l'état antérieur aux actions du programme malveillant....149
Protection du réseau....149
Pare-feu 151
Prévention des intrusions....154
Analyse des connexions cryptées 157
Surveillance du réseau....159
Configuration des paramètres du serveur proxy 159
Composition de la liste des ports contrôlés....159
Zone de confiance 161

Composition de la liste des applications de confiance 162
Création de règles d'exclusion 162
Exécution des applications en environnement protégé 163
Lancement d'une application en Environnement protégé 163
Composition de la liste des applications à exécuter dans l'environnement protégé 164
Création de raccourcis pour le lancement d'applications 165
Purge des données de l'environnement protégé 165
Utilisation du dossier virtuel 166
Quarantaine et dossier de sauvegarde 167
Conservation des objets de la quarantaine et de la sauvegarde. 167
Manipulation des objets en quarantaine 168
Mes Sauvegardes 170
Création de l'espace de sauvegarde 170
Connexion d'un espace de sauvegarde créé antérieurement 171
Purge de l'espace de sauvegarde 171
Suppression de l'espace de sauvegarde 172
Création d'une tâche de copie de sauvegarde 172
Lancement de la sauvegarde 173
Restauration des données 173
Recherche des copies de sauvegarde 174
Consultation des données de la copie de sauvegarde 175
Consultation du rapport sur les événements 176
Mon Contrôle Parental 177
Configuration du Contrôle Parental de l'utilisateur 178
Activation et désactivation du contrôle 178
Enregistrement et chargement des paramètres de Mon Contrôle Parental 179
Représentation du compte utilisateur dans Kaspersky PURE 180
Durée d'utilisation de l'ordinateur 180
Lancement des applications 180
Durée d'utilisation d'Internet 181
Consultation de sites 181
Téléchargement 181
Mode de recherche sécurisée 182
Communication à l'aide de clients de messagerie instantanée 182
Communications dans les réseaux sociaux 184
Transfert d'informations confidentielles 185
Recherche de mots clés 185
Consultation des rapports sur les actions de l'utilisateur 185
Mes Coffres-forts 187
Création et connexion d'un coffre-fort déjà créé 187
Interdiction et autorisation de l'accès aux données du coffre-fort 188
Ajout de fichiers au coffre-fort 189
Configuration des paramètres du coffre-fort 189
Création d'un lien pour accéder rapidement au coffre-fort 190
Mon Réseau 191
Configuration de l'administration à distance 191
Recherche de virus et de vulnérabilités dans le réseau domestique 192
Mise à jour à distance sur les ordinateurs du réseau 192
Activation/désactivation des composants de la protection sur les ordinateurs du réseau 193

Administration à distance de Mon Contrôle Parental 194
Lancement de la copie de sauvegarde sur les ordinateurs du réseau 194
Administration à distance des licences sur les ordinateurs du réseau 195
Mon Gestionnaire de mots de passe 196
Gestion de la base de mots de passe 198
Accès à la base de mots de passe 198
Ajout de données personnelles 199
Utilisation des données personnelles 207
Recherche de mots de passe 208
Suppression de données personnelles 208
Importation / exportation de données 209
Copie de sauvegarde/restauration de la base de mots de passe 210
Configuration des paramètres de l'application 212
Assistant de Configuration des paramètres 213
Utilisation d'un Identifiant par défaut 213
Comptes favoris 214
URL ignorées 215
URL de confiance 215
Touches de raccourci 216
Emplacement du fichier de la base de mots de passe 216
Création d'une nouvelle base de mots de passe 217
Emplacement de la copie de sauvegarde 218
Sélection du mode de cryptage 219
Verrouillage automatique la base de mots de passe 220
Modification du mode d'authentification de Mon Gestionnaire de mots de passe 220
Autorisation à l'aide d'un périphérique USB ou Bluetooth 221
Modification du Mot de passe principal 221
Navigateurs compatibles 222
Administration des modèles des notes personnelles 222
Affichage du bouton d'accès rapide 223
Définir la durée de conservation d'un mot de passe dans le Presse-papiers 224
Notifications 224
Fonction d'activation par double-clique 225
Création de mots de passe fiables 225
Utilisation d'une version portable de Mon Gestionnaire de mots de passe 226
Création et connexion de la version portable 227
Synchronisation de la base de mots de passe 228
Performances et compatibilité avec d'autres applications 229
Sélection des catégories de menaces identifiées 229
Technologie de réparation de l'infection active 230
Répartition des ressources de l'ordinateur pendant la recherche de virus 230
Paramètres de l'application en cas d'utilisation du mode plein écran. Mode jeux 231
Économie d'énergie en cas d'alimentation via la batterie 231
Autodéfense de Kaspersky PURE 231
Activation et désactivation de l'autodéfense 232
Protection contre l'administration externe 232
Apparence de l'application 233
Eléments actifs de l'interface 233
Graphisme de Kaspersky PURE 233

Kiosque d'informations 234
Mes Outils d'optimisation 235
Suppression permanente des données 236
Suppression des traces d'activité 237
Nettoyage du disque 238
Configuration du navigateur 240
Rapports 241
Composition du rapport pour le composant sélectionné 242
Filtrage des données 242
Recherche d'événements 243
Enregistrement du rapport dans un fichier 244
Conservation des rapports 244
Purge des rapports 245
Entrées relatives aux événements non critiques 245
Configuration de la notification sur la disponibilité du rapport 245
Notifications 246
Activation et désactivation des notifications 246
Configuration des modes de notification 246
Participation au Kaspersky Security Network 248

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE KASPERSKY PURE 249
Virus d'essai EICAR et ses modifications 249
Test de la protection du trafic HTTP 250
Test de la protection du trafic SMTP 251
Vérification de l'exactitude de la configuration d'Antivirus Fichiers 251
Vérification de l'exactitude de la configuration de la tâche d'analyse antivirus 252
Vérification de l'exactitude de la configuration de la protection contre le courrier indésirable 252

CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE 253
Mon Espace Personnel 253
Assistance technique par téléphone 254
Création d'un rapport sur l'état du système 254
Création d'un fichier de trace 255
Envoi des rapports 255
Exécution du script AVZ 257

ANNEXES 258
Etats de l'abonnement 258
Utilisation de l'application au départ de la ligne de commande 259
Activation de l'application 260
Lancement de l'application 261
Arrêt de l'application 261
Administration des composants de l'application et des tâches 261
Recherche de virus 263
Mise à jour de l'application 265
Annulation de la dernière mise à jour 266
Exportation des paramètres de protection 266
Importation des paramètres de protection 267
Obtention du fichier de trace 267
Consultation de l'aide 268
Codes de retour de la ligne de commande 268

Liste des notifications Kaspersky PURE 269
La réparation de l'objet est impossible 269
Serveur de mises à jour inaccessible 270
Un objet malveillant a été identifié 270
Un objet dangereux a été découvert dans le trafic 271
Objet suspect détecté 271
Une activité dangereuse a été découverte dans le système 272
Détection de processus cachés 273
Une tentative d'accès à la base de registres système a été découverte 273
Une activité réseau de l'application a été découverte 274
Un nouveau réseau a été découvert 274
Une tentative de phishing a été découverte 275
Lien suspect découvert 275
Découverte d'un certificat incorrect 276
Restriction sur la durée d'utilisation de l'application 276
Une procédure spéciale de réparation est requise 276
Le fichier existe déjà 276
GLOSSAIRE 277
KASPERSKY LAB 286
INFORMATIONS SUR LE CODE TIERS 287
Code d'application 287
AGG (ANTI-GRAIN GEOMETRY) 2.4 289
BISON PARSER SKELETON 2.3 289
BOOST 1.30.0, 1.39.0, 1.43.0 290
BZIP2/LIBBZIP2 1.0.5 290
EXPAT 1.2, 2.0.1 290
FASTSCRIPT 1.9 290
GECKO SDK 1.8 290
INFO-ZIP 5.51 290
LIBJPEG 6B 291
LIBNKFM 2.0.5 292
LIBPNG 1.2.8, 1.2.29 292
LIBSPF2 1.2.9 292
LIBUNGIF 3.0 293
LIBXDR 293
NDIS INTERMEDIATE MINIPORTDRIVER SAMPLE 294
NDIS SAMPLE NDIS LIGHTWEIGHT FILTER DRIVER 294
NETWORK CONFIGURATION SAMPLE 294
OPENSSL 0.9.8D 294
PCRE 3.0, 7.4, 7.7 295
PROTOCOL BUFFER 296
QT 4.6.1 297
RFC1321-BASED (RSA-FREE) MD5 LIBRARY 302
TINICONV 1.0.0 302
WINDOWS TEMPLATE LIBRARY 7.5 308
WINDOWS TEMPLATE LIBRARY 8.0 310
ZLIB 1.2, 1.2.2 310
Autres informations 311

INDEX 312

CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB

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

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

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

1. Définitions

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

2. Concession de la Licence

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

Logiciel à environnements multiples ; Logiciel à langues multiples ; Logiciel sur deux types de support ; copies multiples ; packs logiciels. Si vous utilisez différentes versions du Logiciel ou des éditions en

différentes langues du Logiciel, si vous recevez le Logiciel sur plusieurs supports, ou si vous recevez plusieurs copies du Logiciel de quelque façon que ce soit, ou si vous recevez le Logiciel dans un pack logiciel, le nombre total de vos Ordinateurs sur lesquels toutes les versions du Logiciel sont autorisées à être installées doit correspondre au nombre d'ordinateurs précisé dans les licences que vous avez obtenues auprès du Titulaire des droits, *sachant que,* sauf disposition contraire du contrat de licence, chaque licence acquise vous donne le droit d'installer et d'utiliser le Logiciel sur le nombre d'Ordinateurs stipulé dans les Clauses 2.2 et 2.3.

2.2. Si le Logiciel a été acquis sur un support physique, Vous avez le droit d'utiliser le Logiciel pour la protection du nombre d'ordinateurs stipulé sur l'emballage du Logiciel.
2.3. Si le Logiciel a été acquis sur Internet, Vous pouvez utiliser le Logiciel pour la protection du nombre d'Ordinateurs stipulé lors de l'acquisition de la Licence du Logiciel.
2.4. Vous ne pouvez faire une copie du Logiciel qu'à des fins de sauvegarde, et seulement pour remplacer l'exemplaire que vous avez acquis de manière légale si cette copie était perdue, détruite ou devenait inutilisable. Cette copie de sauvegarde ne peut pas être utilisée à d'autres fins et devra être détruite si vous perdez le droit d'utilisation du Logiciel ou à l'échéance de Votre licence ou à la résiliation de celle-ci pour quelque raison que ce soit, conformément à la législation en vigueur dans votre pays de résidence principale, ou dans le pays où Vous utilisez le Logiciel.
2.5. Vous pouvez transférer la licence non exclusive d'utilisation du Logiciel à d'autres personnes physiques dans la limite du champ d'application de la licence qui Vous est accordée par le Titulaire des droits, à condition que son destinataire accepte de respecter les conditions générales de ce Contrat et se substitue pleinement à vous dans le cadre de la licence que vous accorde le Titulaire des droits. Si Vous transférez intégralement les droits d'utilisation du Logiciel que vous accorde le Titulaire des droits, Vous devrez détruire toutes les copies du Logiciel, y compris la copie de sauvegarde. Si Vous êtes le destinataire du transfert d'une licence, Vous devez accepter de respecter toutes les conditions générales de ce Contrat. Si vous n'acceptez pas de respecter toutes les conditions générales de ce Contrat, Vous n'êtes pas autorisé à installer ou utiliser le Logiciel. Vous acceptez également, en qualité de destinataire de la licence transférée, de ne jouir d'aucun droit autre que ceux de l'Utilisateur final d'origine qui avait acquis le Logiciel auprès du Titulaire des droits.
2.6. À compter du moment de l'activation du Logiciel ou de l'installation du fichier clé de licence (à l'exception de la version de démonstration du Logiciel), Vous pouvez bénéficier des services suivants pour la période définie stipulée sur l'emballage du Logiciel (si le Logiciel a été acquis sur un support physique) ou stipulée pendant l'acquisition (si le Logiciel a été acquis sur Internet) :
- Mises à jour du Logiciel par Internet lorsque le Titulaire des droits les publie sur son site Internet ou par le biais d'autres services en ligne. Toutes les Mises à jour que vous êtes susceptible de recevoir font partie intégrante du Logiciel et les conditions générales de ce Contrat leur sont applicables ;
- Assistance technique en ligne et assistance technique par téléphone.

3. Activation et durée de validité
3.1. Si vous modifiez Votre Ordinateur ou procédez à des modifications sur des logiciels provenant d'autres vendeurs et installés sur celui-ci, il est possible que le Titulaire des droits exige que Vous procédiez une nouvelle fois à l'activation du Logiciel ou à l'installation du fichier clé de licence. Le Titulaire des droits se réserve le droit d'utiliser tous les moyens et toutes les procédures de vérification de la validité de la Licence ou de la légalité du Logiciel installé ou utilisé sur Votre ordinateur.
3.2. Si le Logiciel a été acquis sur un support physique, le Logiciel peut être utilisé dès l'acceptation de ce Contrat pendant la période stipulée sur l'emballage et commençant à l'acceptation de ce Contrat.
3.3. Si le Logiciel a été acquis sur Internet, le Logiciel peut être utilisé à votre acceptation de ce Contrat, pendant la période stipulée lors de l'acquisition.
3.4. Vous avez le droit d'utiliser gratuitement une version de démonstration du Logiciel conformément aux dispositions de la Clause 2.1 pendant la seule période d'évaluation correspondante (30 jours) à compter de l'activation du Logiciel conformément à ce Contrat, *sachant que* la version de démonstration ne Vous donne aucun droit aux mises à jour et à l'assistance technique par Internet et par téléphone. Si le Titulaire des droits fixe une autre durée pour la période d'évaluation unique applicable, Vous serez informé(e) par notification.
3.5. Votre Licence d'utilisation du Logiciel est limitée à la période stipulée dans les Clauses 3.2 ou 3.3 (selon le cas) et la période restante peut être visualisée par les moyens décrits dans le Manuel de l'utilisateur.
3.6. Si vous avez acquis le Logiciel dans le but de l'utiliser sur plus d'un Ordinateur, Votre Licence d'utilisation du Logiciel est limitée à la période commençant à la date d'activation du Logiciel ou de l'installation du fichier clé de licence sur le premier Ordinateur.
3.7. Sans préjudice des autres recours en droit ou équité à la disposition du Titulaire des droits, dans l'éventualité d'une rupture de votre part de toute clause de ce Contrat, le Titulaire des droits sera en droit, à

sa convenance et sans préavis, de révoquer cette Licence d'utilisation du Logiciel sans rembourser le prix d'achat en tout ou en partie.
3.8. Vous vous engagez, dans le cadre de votre utilisation du Logiciel et de l'obtention de tout rapport ou de toute information dans le cadre de l'utilisation de ce Logiciel, à respecter toutes les lois et réglementations internationales, nationales, étatiques, régionales et locales en vigueur, ce qui comprend, sans toutefois s'y limiter, les lois relatives à la protection de la vie privée, des droits d'auteur, au contrôle des exportations et à la lutte contre les outrages à la pudeur.
3.9. Sauf disposition contraire spécifiquement énoncée dans ce Contrat, vous ne pouvez transférer ni céder aucun des droits qui vous sont accordés dans le cadre de ce Contrat ou aucune de vos obligations de par les présentes.
3.10. Le détenteur des droits se réserve le droit de limiter la possibilité d'activation en dehors de la région dans laquelle le logiciel a été acquis auprès du détenteur des droits et/ou de ses partenaires.
3.11. Si vous avez acheté le logiciel avec un code d'activation valide pour la localisation de la langue parlée dans la région où il a été acquis auprès du détenteur des droits ou de ses partenaires, vous ne pouvez pas activer le logiciel avec le code d'activation prévu pour la localisation d'une autre langue.
3.12. En cas de restrictions précisées dans les clauses 3.10 et 3.11, vous trouverez des informations concernant ces restrictions sur l'emballage et/ou le site Web du détenteur et/ou de ses partenaires.

4. Assistance technique
4.1. L'assistance technique décrite dans la Clause 2.6 de ce Contrat Vous est offerte lorsque la dernière mise à jour du Logiciel est installée (sauf pour la version de démonstration du Logiciel).
Service d'assistance technique : http://support.kaspersky.com

5. Recueil d'informations
5.1. Conformément aux conditions générales de ce Contrat, Vous consentez à communiquer au Titulaire des droits des informations relatives aux fichiers exécutables et à leurs sommes de contrôle pour améliorer Votre niveau de protection et de sécurité.
5.2. Pour sensibiliser le public aux nouvelles menaces et à leurs sources, et dans un souci d'amélioration de Votre sécurité et de Votre protection, le Titulaire des droits, avec votre consentement explicitement confirmé dans le cadre de la déclaration de recueil des données du réseau de sécurité Kaspersky, est autorisé à accéder à ces informations. Vous pouvez désactiver le réseau de sécurité Kaspersky pendant l'installation. Vous pouvez également activer et désactiver le réseau de sécurité Kaspersky à votre guise, à la page des options du Logiciel.
Vous reconnaissez par ailleurs et acceptez que toutes les informations recueillies par le Titulaire des droits pourront être utilisées pour suivre et publier des rapports relatifs aux tendances en matière de risques et de sécurité, à la seule et exclusive appréciation du Titulaire des droits.
5.3. Le Logiciel ne traite aucune information susceptible de faire l'objet d'une identification personnelle et ne combine les données traitées avec aucune information personnelle.
5.4. Si vous ne souhaitez pas que les informations recueillies par le Logiciel soient transmises au Titulaire des droits, n'activez pas ou ne désactivez pas le réseau de sécurité Kaspersky.

6. Limitations
6.1. Vous vous engagez à ne pas émuler, cloner, louer, prêter, donner en bail, vendre, modifier, décompiler, ou faire l'ingénierie inverse du Logiciel, et à ne pas démonter ou créer des travaux dérivés reposant sur le Logiciel ou toute portion de celui-ci, à la seule exception du droit inaliénable qui Vous est accordé par la législation en vigueur, et vous ne devez autrement réduire aucune partie du Logiciel à une forme lisible par un humain ni transférer le Logiciel sous licence, ou toute sous-partie du Logiciel sous licence, ni autoriser une tierce partie de le faire, sauf dans la mesure où la restriction précédente est expressément interdite par la loi en vigueur. Ni le code binaire du Logiciel ni sa source ne peuvent être utilisés à des fins d'ingénierie inverse pour recréer le programme de l'algorithme, qui est la propriété exclusive du Titulaire des droits. Tous les droits non expressément accordés par la présente sont réservés par le Titulaire des droits et/ou ses fournisseurs, suivant le cas. Toute utilisation du Logiciel en violation du Contrat entraînera la résiliation immédiate et automatique de ce Contrat et de la Licence concédée de par les présentes, et pourra entraîner des poursuites pénales et/ou civiles à votre encontre.
6.2. Vous ne devrez transférer les droits d'utilisation du Logiciel à aucune tierce partie sauf aux conditions énoncées dans la Clause 2.5 de ce Contrat.
6.3. Vous vous engagez à ne communiquer le code d'activation et/ou le fichier clé de licence à aucune tierce partie, et à ne permettre l'accès par aucune tierce partie au code d'activation et au fichier clé de licence qui sont considérés comme des informations confidentielles du Titulaire des droits, et vous prendrez toutes les mesures raisonnables nécessaires à la protection du code d'activation et/ou du fichier clé de licence, étant

entendu que vous pouvez transférer le code d'activation et/ou le fichier clé de licence à de tierces parties dans les conditions énoncées dans la Clause 2.5 de ce Contrat.
6.4. Vous vous engagez à ne louer, donner à bail ou prêter le Logiciel à aucune tierce partie.
6.5. Vous vous engagez à ne pas vous servir du Logiciel pour la création de données ou de logiciels utilisés dans le cadre de la détection, du blocage ou du traitement des menaces décrites dans le Manuel de l'utilisateur.
6.6. Le Titulaire des droits a le droit de bloquer le fichier clé de licence ou de mettre fin à votre Licence d'utilisation du Logiciel en cas de non-respect de Votre part des conditions générales de ce Contrat, et ce, sans que vous puissiez prétendre à aucun remboursement.
6.7. Si vous utilisez la version de démonstration du Logiciel, Vous n'avez pas le droit de bénéficier de l'assistance technique stipulée dans la Clause 4 de ce Contrat, et Vous n'avez pas le droit de transférer la licence ou les droits d'utilisation du Logiciel à une tierce partie.

7. Garantie limitée et avis de non-responsabilité
7.1. Le Titulaire des droits garantit que le Logiciel donnera des résultats substantiellement conformes aux spécifications et aux descriptions énoncées dans le Manuel de l'utilisateur, *étant toutefois entendu* que cette garantie limitée ne s'applique pas dans les conditions suivantes : (w) des défauts de fonctionnement de Votre Ordinateur et autres non-respects des clauses du Contrat, auquel cas le Titulaire des droits est expressément dégagé de toute responsabilité en matière de garantie ; (x) les dysfonctionnements, les défauts ou les pannes résultant d'une utilisation abusive, d'un accident, de la négligence, d'une installation inappropriée, d'une utilisation ou d'une maintenance inappropriée ; des vols ; des actes de vandalisme ; des catastrophes naturelles ; des actes de terrorisme ; des pannes d'électricité ou des surtensions ; des sinistres ; de l'altération, des modifications non autorisées ou des réparations par toute partie autre que le Titulaire des droits ; ou des actions d'autres tierces parties ou Vos actions ou des causes échappant au contrôle raisonnable du Titulaire des droits ; (y) tout défaut non signalé par Vous au Titulaire dès que possible après sa constatation ; et (z) toute incompatibilité causée par les composants du matériel et/ou du logiciel installés sur Votre Ordinateur.
7.2. Vous reconnaissez, acceptez et convenez qu'aucun logiciel n'est exempt d'erreurs, et nous Vous recommandons de faire une copie de sauvegarde des informations de Votre Ordinateur, à la fréquence et avec le niveau de fiabilité adaptés à Votre cas.
7.3. Le Titulaire des droits n'offre aucune garantie de fonctionnement correct du Logiciel en cas de non-respect des conditions décrites dans le Manuel de l'utilisateur ou dans ce Contrat.
7.4. Le Titulaire des droits ne garantit pas que le Logiciel fonctionnera correctement si Vous ne téléchargez pas régulièrement les Mises à jour spécifiées dans la Clause 2.6 de ce Contrat.
7.5. Le Titulaire des droits ne garantit aucune protection contre les menaces décrites dans le Manuel de l'utilisateur à l'issue de l'échéance de la période indiquée dans les Clauses 3.2 ou 3.3 de ce Contrat, ou à la suite de la résiliation pour une raison quelconque de la Licence d'utilisation du Logiciel.
7.6. LE LOGICIEL EST FOURNI " TEL QUEL " ET LE TITULAIRE DES DROITS N'OFFRE AUCUNE GARANTIE QUANT À SON UTILISATION OU SES PERFORMANCES. SAUF DANS LE CAS DE TOUTE GARANTIE, CONDITION, DÉCLARATION OU TOUT TERME DONT LA PORTÉE NE PEUT ÊTRE EXCLUE OU LIMITÉE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS ET SES PARTENAIRES N'OFFRENT AUCUNE GARANTIE, CONDITION OU DÉCLARATION (EXPLICITE OU IMPLICITE, QUE CE SOIT DE PARLA LÉGISLATION EN VIGUEUR, LE " COMMON LAW ", LA COUTUME, LES USAGES OU AUTRES) QUANT À TOUTE QUESTION DONT, SANS LIMITATION, L'ABSENCE D'ATTEINTE AUX DROITS DE TIERCES PARTIES, LE CARACTÈRE COMMERCIALISABLE, LA QUALITÉ SATISFAISANTE, L'INTÉGRATION OU L'ADÉQUATION À UNE FIN PARTICULIÈRE. VOUS ASSUMEZ TOUS LES DÉFAUTS, ET L'INTÉGRALITÉ DES RISQUES LIÉS À LA PERFORMANCE ET AU CHOIX DU LOGICIEL POUR ABOUTIR AUX RÉSULTATS QUE VOUS RECHERCHEZ, ET À L'INSTALLATION DU LOGICIEL, SON UTILISATION ET LES RÉSULTATS OBTENUS AU MOYEN DU LOGICIEL. SANS LIMITER LES DISPOSITIONS PRÉCÉDENTES, LE TITULAIRE DES DROITS NE FAIT AUCUNE DÉCLARATION ET N'OFFRE AUCUNE GARANTIE QUANT À L'ABSENCE D'ERREURS DU LOGICIEL, OU L'ABSENCE D'INTERRUPTIONS OU D'AUTRES PANNES, OU LA SATISFACTION DE TOUTES VOS EXIGENCES PAR LE LOGICIEL, QU'ELLES SOIENT OU NON DIVULGUÉES AU TITULAIRE DES DROITS.

8. Exclusion et Limitation de responsabilité
8.1. DANS LA MESURE MAXIMALE PERMISE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS OU SES PARTENAIRES NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES DE TOUT DOMMAGE SPÉCIAL, ACCESSOIRE, PUNITIF, INDIRECT OU CONSÉCUTIF QUEL QU'IL SOIT (Y COMPRIS, SANS TOUTEFOIS S'Y LIMITER, LES DOMMAGES POUR PERTES DE PROFITS OU

D'INFORMATIONS CONFIDENTIELLES OU AUTRES, EN CAS D'INTERRUPTION DES ACTIVITÉS, DE PERTE D'INFORMATIONS PERSONNELLES, DE CORRUPTION, DE DOMMAGE À DES DONNÉES OU À DES PROGRAMMES OU DE PERTES DE CEUX-CI, DE MANQUEMENT À L'EXERCICE DE TOUT DEVOIR, Y COMPRIS TOUTE OBLIGATION STATUTAIRE, DEVOIR DE BONNE FOI OU DE DILIGENCE RAISONNABLE, EN CAS DE NÉGLIGENCE, DE PERTE ÉCONOMIQUE, ET DE TOUTE AUTRE PERTE PÉCUNIAIRE OU AUTRE PERTE QUELLE QU'ELLE SOIT) DÉCOULANT DE OU LIÉ D'UNE MANIÈRE QUELCONQUE À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISATION DU LOGICIEL, À L'OFFRE D'ASSISTANCE OU D'AUTRES SERVICES OU À L'ABSENCE D'UNE TELLE OFFRE, LE LOGICIEL, ET LE CONTENU TRANSMIS PAR L'INTERMÉDIAIRE DU LOGICIEL OU AUTREMENT DÉCOULANT DE L'UTILISATION DU LOGICIEL, EN RELATION AVEC TOUTE DISPOSITION DE CE CONTRAT, OU DÉCOULANT DE TOUTE RUPTURE DE CE CONTRAT OU DE TOUT ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE, LA FAUSSE DÉCLARATION, OU TOUTE OBLIGATION OU DEVOIR EN RESPONSABILITÉ STRICTE), OU DE TOUT MANQUEMENT À UNE OBLIGATION STATUTAIRE, OU DE TOUTE RUPTURE DE GARANTIE DU TITULAIRE DES DROITS ET DE TOUT PARTENAIRE DE CELUI-CI, MÊME SI LE TITULAIRE DES DROITS OU TOUT PARTENAIRE A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES. VOUS ACCEPTEZ QUE, DANS L'ÉVENTUALITÉ OÙ LE TITULAIRE DES DROITS ET/OU SES PARTENAIRES SONT ESTIMÉS RESPONSABLES, LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES SERA LIMITÉE AUX COÛTS DU LOGICIEL. LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES NE SAURAIT EN AUCUN CAS EXCÉDER LES FRAIS PAYÉS POUR LE LOGICIEL AU TITULAIRE DES DROITS OU AU PARTENAIRE (LE CAS ÉCHÉANT). AUCUNE DISPOSITION DE CE CONTRAT NE SAURAIT EXCLURE OU LIMITER TOUTE DEMANDE EN CAS DE DÉCÈS OU DE DOMMAGE CORPOREL. PAR AILLEURS, DANS L'ÉVENTUALITÉ OÙ TOUTE DÉCHARGE DE RESPONSABILITÉ, TOUTE EXCLUSION OU LIMITATION DE CE CONTRAT NE SERAIT PAS POSSIBLE DU FAIT DE LA LOI EN VIGUEUR, ALORS SEULEMENT, CETTE DÉCHARGE DE RESPONSABILITÉ, EXCLUSION OU LIMITATION NE S'APPLIQUERA PAS DANS VOTRE CAS ET VOUS RESTEREZ TENU PAR LES DÉCHARGES DE RESPONSABILITÉ, LES EXCLUSIONS ET LES LIMITATIONS RESTANTES.

9. Licence GNU et autres licences de tierces parties

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

10. Droits de propriété intellectuelle

10.1. Vous convenez que le Logiciel et le contenu exclusif, les systèmes, les idées, les méthodes de fonctionnement,la documentation et les autres informations contenues dans le Logiciel constituent un élément de propriété intellectuelle et/ou des secrets industriels de valeur du Titulaire des droits ou de ses partenaires, et que le Titulaire des droits et ses partenaires, le cas échéant, sont protégés par le droit civil et pénal, ainsi que par les lois sur la protection des droits d'auteur, des secrets industriels et des brevets de la Fédération de Russie, de l'Union européenne et des Etats-Unis, ainsi que d'autres pays et par les traités internationaux. Ce Contrat ne vous accorde aucun droit sur la propriété intellectuelle, en particulier toute marque de commerce ou de service du Titulaire des droits et/ou de ses partenaires (les " Marques de commerce "). Vous n'êtes autorisé à utiliser les Marques de commerce que dans la mesure où elles permettent l'identification des informations imprimées par le Logiciel conformément aux pratiques admises en matière de marques de commerce, en particulier l'identification du nom du propriétaire de la Marque de commerce. Cette utilisation d'une marque de commerce ne vous donne aucun droit de propriété sur celle-ci. Le Titulaire des droits et/ou ses partenaires conservent la propriété et tout droit, titre et intérêt sur la Marque de commerce et sur le Logiciel, y compris sans limitation, toute correction des erreurs, amélioration, mise à jour ou autre modification du Logiciel, qu'elle soit apportée par le Titulaire des droits ou une tierce partie, et tous les droits d'auteur, brevets, droits sur des secrets industriels, et autres droits de propriété intellectuelle afférents à ce Contrat. Votre possession, installation ou utilisation du Logiciel ne transfère aucun titre de propriété intellectuelle à votre bénéfice, et vous n'acquerrez aucun droit sur le Logiciel, sauf dans les conditions expressément décrites dans le cadre de ce Contrat. Toutes les reproductions du Logiciel

effectuées dans le cadre de ce Contrat doivent faire mention des mêmes avis d'exclusivité que ceux qui figurent sur le Logiciel. Sauf dans les conditions énoncées par les présentes, ce Contrat ne vous accorde aucun droit de propriété intellectuelle sur le Logiciel et vous convenez que la Licence telle que définie dans ce document et accordée dans le cadre de ce Contrat ne vous donne qu'un droit limité d'utilisation en vertu des conditions générales de ce Contrat. Le Titulaire des droits se réserve tout droit qui ne vous est pas expressément accordé dans ce Contrat.
10.2. Vous convenez de ne modifier ou altérer le Logiciel en aucune façon. Il vous est interdit d'éliminer ou d'altérer les avis de droits d'auteur ou autres avis d'exclusivité sur tous les exemplaires du Logiciel.

11. Droit applicable ; arbitrage
11.1. Ce Contrat sera régi et interprété conformément aux lois de la Fédération de Russie sans référence aux règlements et aux principes en matière de conflits de droit. Ce Contrat ne sera pas régi par la Conférence des Nations Unies sur les contrats de vente internationale de marchandises, dont l'application est strictement exclue. Tout litige auquel est susceptible de donner lieu l'interprétation ou l'application des clauses de ce Contrat ou toute rupture de celui-ci sera soumis à l'appréciation du Tribunal d'arbitrage commercial international de la Chambre de commerce et d'industrie de la Fédération de Russie à Moscou (Fédération de Russie), à moins qu'il ne soit réglé par négociation directe. Tout jugement rendu par l'arbitre sera définitif et engagera les parties, et tout tribunal compétent pourra faire valoir ce jugement d'arbitrage. Aucune disposition de ce Paragraphe 11 ne saurait s'opposer à ce qu'une Partie oppose un recours en redressement équitable ou l'obtienne auprès d'un tribunal compétent, avant, pendant ou après la procédure d'arbitrage.

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

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

14. Informations de contact du Titulaire des droits

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

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

© 1997-2010 Kaspersky Lab ZAO. Tous droits réservés. Le Logiciel et toute documentation l'accompagnant font l'objet de droits d'auteur et sont protégés par les lois sur la protection des droits d'auteur et les traités internationaux sur les droits d'auteur, ainsi que d'autres lois et traités sur la propriété intellectuelle.

PRESENTATION DU GUIDE

Ce document est un manuel d'installation, de configuration et d'utilisation de Kaspersky PURE 9.1 (par la suite, Kaspersky PURE). Ce document est prévu pour un large public. L'utilisateur de l'application doit posséder des connaissances de base sur l'utilisation de l'ordinateur : connaissance de l'interface du système d'exploitation Windows, maîtrise des principales tâches, maîtrise des logiciels les plus utilisés pour le courrier électronique et Internet, par exemple Microsoft Office Outlook et Microsoft Internet Explorer.

Objectif de ce document :

- Aider l'utilisateur à installer lui-même l'application sur l'ordinateur, à l'activer et à réaliser une configuration optimale qui tient compte de ses besoins ;
- Offrir un accès rapide aux informations pour répondre aux questions liées à l'application ;
- Présenter les autres sources d'informations sur l'application et les méthodes pour obtenir une assistance technique.

DANS CETTE SECTION

Dans ce document 18

Conventions 20

DANS CE DOCUMENT

Le Guide de l'utilisateur de Kaspersky PURE contient les principaux paragraphes suivants :

Sources d'informations complémentaires

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

Kaspersky PURE

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

Installation

Cette section contient les instructions qui vous aideront à installer l'application sur l'ordinateur et à actualiser la version précédente de l'application. Cette rubrique aussi décrit comment supprimer l'application de l'ordinateur.

Administration de la licence

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

Interface de l'application

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

Lancement et arrêt de l'application

Cette rubrique explique comment lancer et arrêter l'application.

Etat de la protection de l'ordinateur

Cette rubrique contient des informations qui permettront de confirmer si l'ordinateur est protégé ou si sa sécurité est menacée. Elle explique également comment supprimer les menaces qui se présentent. Cette rubrique explique aussi comment activer ou désactiver la protection ou la suspendre temporairement pendant l'utilisation de Kaspersky PURE et présente les différents modes de protection.

Résolution des problèmes types

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

Configuration étendue de l'application

La rubrique offre une présentation détaillée de chaque composant de l'application et des informations sur la configuration pour une protection souple et des plus efficaces.

Validation de la configuration de l'application

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

Contacter le service d'assistance technique

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

Annexes

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

Glossaire

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

CONVENTIONS

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

Tableau 1. Conventions

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

SOURCES D'INFORMATIONS COMPLEMENTAIRES

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

DANS CETTE SECTION

Sources d'informations pour une aide autonome 21

Discussion sur les logiciels de Kaspersky Lab dans le forum en ligne 22

Contacter le service commercial 22

Communication avec le Groupe de rédaction de la documentation 22

SOURCES D'INFORMATIONS POUR UNE AIDE AUTONOME

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

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

Page du site de Kaspersky Lab

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

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

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

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

Service d'assistance interactive

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

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

Aide électronique

La distribution de l'application reprend le fichier d'aide complète et contextuelle. Il contient les informations sur la gestion de la protection de l'ordinateur : consultation de l'état de la protection, analyse de divers secteurs de l'ordinateur, exécution d'autres tâches. En plus, dans le fichier d'aide contextuelle et complète vous pouvez trouver les informations sur chaque fenêtre de l'application : description des paramètres qui figurent dans chacune d'entre elles et liste des tâches exécutées.

Pour ouvrir le fichier d'aide, cliquez sur le bouton **Aide** dans la fenêtre qui vous intéresse ou sur la touche **F1** du clavier.

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

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

Une fois que vous avez accédé au forum, vous pouvez consulter les sujets publiés, écrire vos commentaires, créer de nouveaux sujets ou lancer des recherches.

CONTACTER LE SERVICE COMMERCIAL

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

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

COMMUNICATION AVEC LE GROUPE DE REDACTION DE LA DOCUMENTATION

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

KASPERSKY PURE

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

DANS CETTE SECTION

Distribution 23

Organisation de la protection du réseau domestique 24

Service pour les utilisateurs enregistrés 26

Configurations logicielle et matérielle 27

DISTRIBUTION

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

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

- Une enveloppe cachetée contenant le cédérom d'installation avec les fichiers du logiciel et la documentation au format .pdf.
- La documentation en version "papier" présentée par les documents suivants : Manuel de l'utilisateur et Démarrage rapide.
- Contrat de licence (dépend de la région).
- La carte d'activation contenant le code d'activation et les instructions d'activation de l'application (dépend de la région).

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

Lisez attentivement le contrat de licence !

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

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

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

Si vous achetez Kaspersky PURE en ligne, vous copiez le logiciel depuis le site Internet de Kaspersky Lab. Cette distribution, outre le logiciel, reprend également ce manuel. Le code d'activation est envoyé par courrier électronique après le paiement.

ORGANISATION DE LA PROTECTION DU RESEAU DOMESTIQUE

Kaspersky PURE garantit la protection complexe de votre réseau domestique. La notion de protection complexe désigne la protection de l'ordinateur, la protection des données et la protection des utilisateurs, ainsi que l'administration à distance des fonctions de Kaspersky PURE sur tous les ordinateurs du réseau.

Pour exécuter les tâches de la protection complexe, différents modules fonctionnels sont prévus dans Kaspersky PURE.

Protection de l'ordinateur

Les composants de protection sont prévus pour garantir la protection de l'ordinateur contre les menaces connues ou nouvelles, contre les attaques de réseau et les escroqueries, contre les messages non sollicités et autres informations indésirables. Chaque type de menaces est traité par un composant de la protection particulier (cf. description des composants dans cette section). Il est possible d'activer et de désactiver les composants indépendamment les uns des autres et de configurer leur fonctionnement de la manière qui vous convient.

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

La *mise à jour* des bases et des modules logiciels utilisés dans le fonctionnement de l'application est requise pour que Kaspersky PURE garantisse l'actualité de la protection.

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

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

La protection de votre ordinateur en temps réel est garantie par les composants de la protection :

Antivirus Fichiers

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

Antivirus Courrier

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

Antivirus Internet

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

Antivirus IM

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

Défense Proactive

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

Contrôle des Applications

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

Pare-feu

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

Surveillance du réseau

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

Prévention des intrusions

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

Anti-Spam

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 identifiés sont marqués par un objet particulier. Il est possible également de configurer Anti-Spam pour le traitement du courrier indésirable (suppression automatique, enregistrement dans un répertoire spécial, etc.).

Anti-Phishing

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

Anti-bannière

Anti-bannière bloque les messages publicitaires situés sur des bannières spéciales dans l'interface de divers programmes installés sur votre ordinateur ou sur Internet.

Protection des informations

Afin de protéger les données contre la perte, l'accès non autorisé ou le vol, vous pouvez utiliser les fonctions Mes Sauvegardes, Mon Gestionnaire de mots de passe et Mes Coffres-forts.

Mes Sauvegardes

Les données enregistrées sur l'ordinateur peuvent se perdre ou être endommagées pour toute une série de raisons telles que l'action d'un virus, la modification ou la suppression par un autre utilisateur, etc. Afin d'éviter de perdre des informations importantes, il est primordial de réaliser fréquemment des copies de sauvegarde des données.

Mes Sauvegardes permettent de créer des copies des données dans l'espace de sauvegarde spécial sur un support choisi. Il faut pour ce faire configurer une tâche de copie de sauvegarde. Les copies de sauvegarde des fichiers sélectionnés sont créées dans l'espace de sauvegarde après l'exécution manuelle ou programmée de la tâche. Le cas échéant, il sera possible de restaurer la version requise du fichier enregistré. Ainsi, une copie de sauvegarde régulière offre une sécurité complémentaire pour les données.

Mes Coffres-forts

Les données confidentielles enregistrées sous forme électronique requièrent une protection complémentaire contre l'accès non autorisé. Cette protection est garantie par l'enregistrement des données dans le coffre-fort crypté.

Le composant Mes Coffres-forts permet de créer des coffres-forts spéciaux cryptés sur le support amovible. Ces coffres-forts apparaissent dans le système sous la forme de disques amovibles virtuels. Pour accéder aux données dans le coffre-fort crypté, il faut saisir le mot de passe.

Mon Gestionnaire de mots de passe

A l'heure actuelle, la majorité des services et des ressources requièrent l'enregistrement de l'utilisateur et la saisie des données du compte utilisateur pour l'authentification. Pour des raisons de sécurité, il est déconseillé d'utiliser des noms d'utilisateur et des mots de passe identiques pour diverses ressources, voire de noter ces données. Finalement, l'utilisateur d'aujourd'hui n'est plus en mesure de retenir en mémoire ce volume important de données d'authentification. La problématique de la conservation fiable des mots de passe est pour cette raison d'actualité.

Mon Gestionnaire de mots de passe permet de conserver sous forme chiffrée diverses données personnelles (par exemple, noms d'utilisateur, mots de passe, adresses, numéros de téléphone et de carte de crédit). L'accès aux données est protégé par un mot de passe principal unique. Une fois que le mot de passe principal a été saisi, Mon Gestionnaire de mots de passe permet de remplir automatiquement les champs de différents formulaires d'autorisation. Ainsi, il suffit de se souvenir d'un seul mot de passe principal pour gérer tous les comptes utilisateur.

Mon Contrôle Parental

Pour protéger les enfants et les adolescents des menaces liées à l'utilisation d'Internet et de l'ordinateur, il existe la fonction Mon Contrôle Parental.

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

Mon Réseau

Souvent, le réseau domestique contient plusieurs ordinateurs, ce qui complique l'administration de la sécurité. La vulnérabilité d'un ordinateur menace tout le réseau.

Mon Réseau permet de lancer les tâches d'analyse antivirus et de mise à jour pour l'ensemble du réseau ou pour certains ordinateurs, d'administrer les copies de sauvegarde des données et de configurer les paramètres de Mon Contrôle Parental sur tous les ordinateurs du réseau directement depuis votre poste de travail. C'est ainsi que l'administration à distance de la sécurité de tous les ordinateurs appartenant au réseau domestique est organisée.

SERVICE POUR LES UTILISATEURS ENREGISTRES

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

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

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

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

CONFIGURATIONS LOGICIELLE ET MATERIELLE

Pour garantir le fonctionnement normal de Kaspersky PURE, l'ordinateur doit répondre aux exigences minimum suivantes :

Configuration générale :

- 500 Mo d'espace disponible sur le disque dur.
- Lecteur de cédérom (pour l'installation de Kaspersky PURE depuis un cédérom).
- Microsoft Internet Explorer 6.0 ou suivant (pour la mise à jour des bases et des modules de l'application via Internet).
- Microsoft Windows Installer 2.0.
- Souris.
- Connexion à Internet pour l'activation de Kaspersky PURE.

Microsoft Windows XP Home Edition (Service Pack 3), Microsoft Windows XP Professional (Service Pack 3), Microsoft Windows XP Professional x64 Edition (Service Pack 2)*:*

- Processeur Intel Pentium 300 Mhz ou supérieur (ou analogue compatible).
- 256 Mo de mémoire vive.

Microsoft Windows Vista Home Basic (32-bit/64-bit, Service Pack 2), Microsoft Windows Vista Home Premium (32-bit/64-bit, Service Pack 2), Microsoft Windows Vista Business (32-bit/64-bit, Service Pack 2), Microsoft Windows Vista Enterprise (32-bit/64-bit, Service Pack 2), Microsoft Windows Vista Ultimate (32-bit/64-bit, Service Pack 2) :

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

Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:

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

INSTALLATION ET SUPPRESSION DE L'APPLICATION

Cette section contient les instructions qui vous aideront à installer l'application sur l'ordinateur et à actualiser la version précédente de l'application. Cette rubrique aussi décrit comment supprimer l'application de l'ordinateur.

DANS CETTE SECTION

Installation de l'application 28

Modification, réparation ou suppression de l'application à l'aide de l'Assistant d'installation..... 38

INSTALLATION DE L'APPLICATION

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

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

Avant de lancer l'installation, il est conseillé de quitter toutes les applications en cours d'exécution.

- *Pour installer Kaspersky PURE sur votre ordinateur,*

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

La procédure d'installation de Kaspersky PURE depuis une version téléchargée via Internet est en tout point identique au processus d'installation depuis le CD.

DANS CETTE SECTION

Étape 1. Rechercher d'une version plus récente de l'application 29

Étape 2. Vérification de la configuration du système par rapport à la configuration requise 30

Étape 3. Sélection du type d'installation 30

Étape 4. Lecture du contrat de licence 30

Étape 5. Règlement d'utilisation de Kaspersky Security Network 30

Étape 6. Sélection du dossier d'installation 31

Étape 7. Sélection des composants à installer 31

Etape 8. Recherche d'autres logiciels antivirus éventuellement installés 32

Etape 9. Désactivation du pare-feu de Microsoft Windows 32

Etape 10. Préparation de l'installation 32

Etape 11. Installation 33

Etape 12. Activation de l'application 33

Etape 13. Analyse des données 33

Etape 14. Enregistrement de l'utilisateur 33

Etape 15. Fin de l'activation 34

Etape 16. Restriction de l'accès à l'application 34

Etape 17. Sélection du mode de protection 35

Etape 18. Configuration de la mise à jour de l'application 35

Etape 19. Sélection des menaces identifiées 36

Etape 20. Analyse du système 36

Etape 21. Fin de l'Assistant 36

Première utilisation 37

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

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

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

Si les serveurs de mises à jour hébergent une version plus récente, vous serez invité à la télécharger et à l'installer sur votre ordinateur. Il est conseillé d'installer une nouvelle version de l'application, parce que les améliorations sont

apportées à la nouvelle version. Ces améliorations permettent de protéger votre ordinateur d'une manière plus efficace. Si vous refusez d'installer la version plus récente, l'Assistant d'installation de la version actuelle sera lancé. Si vous décidez d'installer la nouvelle version, les fichiers de la distribution seront copiés sur l'ordinateur et l'Assistant d'installation de la nouvelle version sera lancé automatiquement. Pour connaître la suite de l'installation de la version plus récente, lisez la documentation de la version correspondante de l'application.

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

Avant d'installer l'application, le programme vérifie si le système d'exploitation et les paquets de mises à jour (Service Pack) installés correspondent à la configuration requise pour l'installation de Kaspersky PURE (cf. page 27). De plus, l'application vérifie la présence de la configuration requise ainsi que les privilèges pour l'installation du logiciel. Si une des conditions énumérées n'est pas remplie, le message de circonstance apparaîtra.

ÉTAPE 3. SELECTION DU TYPE D'INSTALLATION

Cette étape permet de choisir le type d'installation de Kaspersky PURE:

- *Installation express*. Si vous choisissez cette option (la case **Installation personnalisée** est décochée), l'application sera entièrement installée sur l'ordinateur selon les paramètres recommandés par les experts de Kaspersky Lab. L'Assistant d'installation vous soumet le texte du contrat de licence ainsi que les conditions d'utilisation de Kaspersky Security Network. L'application est ensuite installée.

- *Installation personnalisée*. Si vous choisissez cette option (la case **Installation personnalisée** est cochée), vous pouvez modifier les paramètres d'installation : choisir les composants à installer et désigner le dossier d'installation. Chaque composant installé sera configuré selon les paramètres de protection recommandés par les experts de Kaspersky Lab.

  L'installation personnalisée doit être réservée aux utilisateurs expérimentés.

Quel que soit le type d'installation sélectionné, à la fin de celle-ci vous pouvez activer Kaspersky PURE et configurer les paramètres de protection de l'application contre l'accès non autorisé.

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

ÉTAPE 4. LECTURE DU CONTRAT DE LICENCE

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

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

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

ÉTAPE 5. REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK

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

Lisez les dispositions relatives à l'utilisation de Kaspersky Security Network. Pour lire le texte complet du contrat, cliquez sur le bouton **Accord KSN complet**. Si vous êtes d'accord avec tous les points, cochez la case **J'accepte les conditions de participation à Kaspersky Security Network**.

Pour poursuivre l'installation, cliquez sur **Installer** (pour l'installation express) ou sur **Suivant** (pour l'installation personnalisée).

ÉTAPE 6. SELECTION DU DOSSIER D'INSTALLATION

Cette étape de l'Assistant d'installation est accessible uniquement lors de l'installation personnalisée de Kaspersky PURE (cf. page 30). Cette étape est sautée pendant l'installation standard et l'application est installée dans le dossier par défaut.

Cette étape permet de sélectionner le dossier dans lequel Kaspersky PURE sera installé. Le chemin d'accès suivant est proposé par défaut :

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

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

Prêtez attention aux restrictions suivantes :

- Il est interdit d'installer l'application sur des disques de réseau ou des disques amovibles ou sur des disques virtuels (créés à l'aide de l'instruction `SUBST`).
- Il est déconseillé d'installer l'application dans un dossier contenant des fichiers et d'autres dossiers car l'accès à ceux-ci pourrait être bloqué après l'installation pour la modification.
- Le chemin d'accès au dossier d'installation doit compter moins de 200 caractères et ne peut pas contenir les caractères suivants **/**, **?**, **:**, *****, **"**, **>**, **<** et **|**.

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

ÉTAPE 7. SELECTION DES COMPOSANTS A INSTALLER

Cette étape de l'Assistant d'installation est accessible uniquement lors de l'installation personnalisée de Kaspersky PURE (cf. page 30). Lors de l'installation standard, cette étape est passée et l'application est installée avec tous ses composants sur l'ordinateur.

Cette étape permet de sélectionner les composants de l'application qui seront installés sur l'ordinateur. Par défaut, tous les composants et le moteur de l'application sont sélectionnés.

Pour décider des composants à installer, vous pouvez lire la brève description du composant sélectionné proposées dans la partie inférieure de la fenêtre et voir l'espace requis sur le disque pour l'installation du composant en question.

Pour sélectionner un composant en vue d'une installation ultérieure, cliquez sur le signe à côté du nom du composant et choisissez l'option **Le composant sera installé sur un disque dur local.** Pour ne pas installer le composant, choisissez l'option **Le composant sera inaccessible.** N'oubliez pas qu'en décidant de ne pas installer un composant de Kaspersky Anti-Virus, vous vous exposez à toute une série de programmes dangereux.

Pour obtenir des informations détaillées sur l'espace disponible sur les disques durs de l'ordinateur, cliquez sur le bouton **Disque**. Les informations seront proposées dans la fenêtre qui s'ouvre.

Une fois que vous aurez opéré votre sélection, cliquez sur **Suivant**. Pour revenir à la liste des composants à installer, cliquez sur **Annuler**.

ETAPE 8. RECHERCHE D'AUTRES LOGICIELS ANTIVIRUS EVENTUELLEMENT INSTALLES

Cette étape correspond à la recherche d'autres logiciels antivirus installés, y compris d'autres logiciels de Kaspersky Lab, dont l'utilisation conjointe à celle de Kaspersky PURE pourrait entraîner des conflits.

Si de tels programmes existent sur votre ordinateur, leur nom apparaîtra à l'écran. Vous pourrez les supprimer avant de poursuivre l'installation.

Pour supprimer les applications antivirus découvertes, cliquez sur **Supprimer**.

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

ETAPE 9. DESACTIVATION DU PARE-FEU DE MICROSOFT WINDOWS

Cette étape de l'Assistant d'installation est proposée si Kaspersky PURE est installé sur un ordinateur doté d'un pare-feu Microsoft Windows actif et que le Pare-feu figure dans la liste des composants à installer.

Lors de cette étape de l'installation de Kaspersky PURE, vous êtes invité à désactiver le pare-feu du système d'exploitation Microsoft Windows. Kaspersky PURE propose le composant Pare-feu qui garantit une protection complète pendant l'utilisation d'Internet. Pour cette raison, il n'est pas nécessaire d'utiliser les outils de protection du système d'exploitation.

Si vous souhaitez utiliser le composant Pare-feu en guise de protection principale lors de l'utilisation d'Internet, cliquez sur **Suivant**. Le pare-feu de Microsoft Windows sera désactivé automatiquement.

Si vous souhaitez protéger votre ordinateur à l'aide du pare-feu de Microsoft Windows, sélectionnez l'option **Utiliser le pare-feu de Microsoft Windows**. Dans ce cas, Pare-feu sera installé mais sera désactivé pour éviter tout conflit.

ETAPE 10. PREPARATION DE L'INSTALLATION

Cette étape de l'Assistant d'installation est accessible uniquement lors de l'installation personnalisée de Kaspersky PURE (cf. page 30). Lors de l'installation standard, l'étape est ignorée.

Cette étape constitue la préparation finale pour l'installation de Kaspersky PURE sur votre ordinateur.

Si vous installez l'application pour la première fois, il est déconseillé de décocher la case **Protéger l'installation de l'application**. Si des erreurs se produisent durant l'installation de l'application, l'activation de la protection permet de réaliser une procédure correcte de remise à l'état antérieur à l'installation. Lors de la nouvelle tentative d'installation, il est conseillé de décocher la case.

En cas d'installation à distance de l'application sur un ordinateur via *Windows Remote Desktop*, il est conseillé de décocher la case **Protéger l'installation de l'application**. Si la case est cochée, la procédure d'installation peut ne pas être réalisée ou être réalisée de manière incorrecte.

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

Lors de l'installation de composants de Kaspersky PURE qui interceptent le trafic de réseau, les connexions réseau en cours seront coupées. La majorité des connexions interrompues seront rétablies après un certain temps.

ETAPE 11. INSTALLATION

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

L'Assistant de configuration de Kaspersky PURE est lancé automatiquement après l'installation.

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

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

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

ETAPE 12. ACTIVATION DE L'APPLICATION

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

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

Les options suivantes s'offrent à vous pour activer Kaspersky PURE :

- **Activer la version commerciale**. Choisissez cette option et saisissez le code d'activation (cf. section "Présentation du code d'activation" à la page 41) si vous avez acheté la version commerciale de l'application.
- **Activer la version d'évaluation**. Sélectionnez cette option si vous souhaitez installer une version d'évaluation du logiciel avant de décider d'acheter la version commerciale. Vous pouvez utiliser toutes les fonctionnalités de l'application pendant la période définie par la licence de la version d'évaluation. Après la date d'expiration de la licence, vous ne pourrez plus réutiliser une version d'évaluation.
- **Activer plus tard**. Si vous choisissez cette option, l'activation de Kaspersky PURE sera ignorée. L'application sera installée sur l'ordinateur mais certaines fonctions ne seront pas accessibles, par exemple la mise à jour (vous pourrez mettre l'application à jour une seule fois après l'installation), la création d'un coffre-fort crypté, les Mes Outils d'optimisation, etc. L'option **Activer plus tard** est accessible uniquement au premier lancement de l'Assistant d'activation, juste après l'installation de l'application.

ETAPE 13. ANALYSE DES DONNEES

Au cours de cette étape, Kaspersky PURE envoie les données au serveur d'activation pour l'analyse.

Une connexion à Internet est indispensable pour analyser les données.

ETAPE 14. ENREGISTREMENT DE L'UTILISATEUR

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

Si vous souhaitez pouvoir demander l'aide du Support technique de Kaspersky Lab, il faudra vous enregistrer.

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

ETAPE 15. FIN DE L'ACTIVATION

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

En cas d'activation de l'abonnement, les informations relatives à la durée de validité de la licence sont fournies en plus des informations sur l'état de l'abonnement (cf. page 258).

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

ETAPE 16. RESTRICTION DE L'ACCES A L'APPLICATION

Cette étape de l'Assistant de la configuration est accessible uniquement lors de l'installation personnalisée de Kaspersky PURE (cf. page 30). Lors de l'installation standard, cette étape est passée et l'application est installée sans restriction d'accès. Plus tard, vous pourrez activer cette restriction manuellement (cf. page 77) dans la fenêtre de configuration de l'application.

La restriction de l'accès à Kaspersky PURE permet d'éviter les tentatives de désactivation non autorisée de la protection ou de modification de la configuration des composants installés avec Kaspersky PURE.

La restriction de l'accès à l'aide d'un mot de passe peut être utile dans les cas suivants :

- si l'ordinateur personnel est utilisé par plusieurs personnes, y compris des personnes dont le niveau de connaissances informatiques varie ;
- si Kaspersky PURE protège plusieurs ordinateurs regroupés dans un réseau domestique ;
- s'il existe un risque de désactivation de la protection par des applications malveillantes.

Afin d'activer la protection, cochez la case **Activer la protection par un mot de passe** et saisissez les informations dans les champs **Mot de passe** et **Confirmation**.

Indiquez ensuite l'ampleur de la restriction :

- **Configuration de l'application** : l'utilisateur est invité à saisir le mot de passe lorsqu'il tente de sauvegarder les modifications des paramètres de Kaspersky PURE.
- **Administration de Mes Sauvegardes** : le mot de passe doit être saisi pour lancer la tâche de copie de sauvegarde.
- **Administration de Mon Contrôle Parental** : le mot de passe doit être saisi pour lancer les tâches de Mon Contrôle Parental.
- **Administration de la sécurité des ordinateurs du réseau domestique** : le mot de passe doit être saisi avant de modifier les paramètres de Kaspersky PURE via le réseau.
- **Arrêt de l'application** : l'utilisateur doit saisir le mot de passe s'il souhaite arrêter l'application

ETAPE 17. SELECTION DU MODE DE PROTECTION

Cette étape de l'Assistant de la configuration est accessible uniquement lors de l'installation personnalisée de Kaspersky PURE (cf. page 30). Dans le cadre de l'installation standard, cette étape est passée et l'application fonctionne par défaut selon le mode de protection automatique. Par la suite, vous pourrez sélectionnez le mode de protection manuellement (cf. page 60).

Sélectionnez le mode de protection offert par Kaspersky PURE.

Deux choix s'offrent à vous :

- *Automatique*. Lorsque des événements importants surviennent, Kaspersky PURE exécute automatiquement l'action recommandée par les experts de Kaspersky Lab. Lorsque l'application découvre une menace, elle tente de réparer l'objet et si cela est impossible, elle le supprime. Les objets suspects sont ignorés sans traitement. Des messages contextuels signalent les événements qui se produisent.

- *Interactif*. Dans ce mode, l'application réagit aux événements conformément à vos choix. Lorsqu'un événement qui requiert votre intervention se manifeste, l'application affiche des notifications offrant un choix d'actions.

La notification sur la découverte d'une infection active s'affiche à l'écran quel que soit le type de protection sélectionné.

ETAPE 18. CONFIGURATION DE LA MISE A JOUR DE L'APPLICATION

Cette étape de l'Assistant de la configuration est accessible uniquement lors de l'installation personnalisée de Kaspersky PURE (cf. page 30). Lors de l'installation standard, cette étape est passée et la mise à jour automatique est réalisée. Par la suite, vous pourrez sélectionnez le mode de mise à jour manuellement (cf. page 96).

La qualité de la protection de votre ordinateur dépend de l'actualité des bases et des modules du logiciel. Cette fenêtre de l'Assistant de configuration vous permet de sélectionner le mode de mise à jour et de la programmer :

- **Mise à jour automatique**. L'application vérifie, selon un intervalle déterminé, si un paquet de mise à jour se trouve dans la source. L'intervalle de vérification peut être réduit en cas d'épidémie et agrandi en situation normale. Si l'application découvre des nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur. Ce mode est utilisé par défaut.

- **Mise à jour programmée** (l'intervalle varie en fonction des paramètres de la programmation). La mise à jour sera lancée automatiquement selon l'horaire défini. La programmation est configurée dans la fenêtre qui s'ouvre à l'aide du bouton **Configuration**.

- **Mise à jour manuelle**. Vous lancez vous-même la procédure de mise à jour du logiciel.

N'oubliez pas que les bases des signatures des menaces et les modules de l'application qui font partie de l'installation peuvent être dépassés au moment de l'installation de Kaspersky PURE. Pour cette raison, nous vous conseillons d'obtenir les mises à jour les plus récentes Il suffit simplement de cliquer sur **Mettre à jour maintenant**. Dans ce cas, le programme recevra les mises à jour requises depuis les serveurs de mise à jour via Internet et les installera sur l'ordinateur.

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

Si vous souhaitez passer à la configuration des paramètres de la mise à jour (sélectionner la ressource d'où la mise à jour sera téléchargée, configurer le lancement de la mise à jour sous les privilèges d'un compte utilisateur distinct, etc.), cliquez sur **Configuration**.

ETAPE 19. SELECTION DES MENACES IDENTIFIEES

Cette étape de l'Assistant de la configuration est accessible uniquement lors de l'installation personnalisée de Kaspersky PURE (cf. page 30). Lors de l'installation standard, cette étape est passée et l'installation s'opère selon les paramètres par défaut. Par la suite, vous pourrez sélectionnez les menaces à découvrir manuellement (cf. page 229).

Cette étape vous offre la possibilité de sélectionner les catégories de menaces découvertes par Kaspersky PURE. Kaspersky PURE découvre toujours les programmes capables de nuire à votre ordinateur. Les virus, les vers et les chevaux de Troie appartiennent à cette catégorie d'applications.

ETAPE 20. ANALYSE DU SYSTEME

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

L'analyse des autres applications a lieu avant leur première exécution après l'installation de Kaspersky PURE.

ETAPE 21. FIN DE L'ASSISTANT

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

Dans certains cas, le redémarrage du système d'exploitation peut être requis. Si vous aviez coché la case **Lancer Kaspersky PURE** avant de quitter l'Assistant, l'application sera lancée automatiquement après le redémarrage. Si vous aviez décoché cette case, il faudra lancer l'application manuellement (cf. page 57).

PREMIERE UTILISATION

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

- Mise à jour les bases de l'application (cf. rubrique "Procédure de mise à jour des bases et modules de l'application" à la page 64).
- Recherche d'éventuels virus (cf. rubrique "Procédure d'exécution d'une analyse complète de l'ordinateur" à la page 67) et vulnérabilités.
- Vérifier l'état de la protection de l'ordinateur et, le cas échéant, éliminer les problèmes de protection (cf. rubrique "Diagnostic et suppression des problèmes dans la protection de l'ordinateur" à la page 58).

Le composant Anti-Spam, repris dans Kaspersky PURE, utilise un algorithme d'apprentissage automatique afin d'identifier les messages non sollicités. Lancez l'Assistant d'entraînement d'Anti-Spam afin de configurer le composant pour qu'il utilise votre courrier.

Afin de pouvoir restaurer rapidement les données en cas de perte, configurez la copie de sauvegarde (cf. rubrique "Copie de sauvegarde des données" à la page. 75).

Afin de protéger les données confidentielles contre l'accès non autorisé, créez des coffres-forts cryptés pour conserver les données (cf. la rubrique "Mes Coffres-forts" à la page 72).

Pour protéger les enfants et les adolescents contre les menaces liées à l'utilisation d'Internet, définissez des restrictions dans Mon Contrôle Parental (cf. rubrique "Comment restreindre l'utilisation de l'ordinateur et d'Internet pour différents utilisateurs" à la page 78).

MODIFICATION, REPARATION OU SUPPRESSION DE L'APPLICATION A L'AIDE DE L'ASSISTANT D'INSTALLATION

La réparation de l'application est utile si vous êtes confronté à certaines erreurs de fonctionnement suite à une mauvaise configuration ou à la corruption des fichiers de l'application.

La modification de la composition vous permet d'installer les composants manquants de Kaspersky PURE ou de supprimer ceux qui gênent votre travail ou qui sont inutiles.

- *Pour passer à la restauration de l'état d'origine de l'application ou à l'installation de composants de Kaspersky PURE qui n'avaient pas été installés à l'origine ainsi que pour supprimer l'application, procédez comme suit :*

  1. Introduisez le cédérom d'installation dans le lecteur pour autant que vous ayez installé le logiciel à l'aide de ce cédérom. Si vous aviez procédé à l'installation de Kaspersky PURE au départ d'une autre source (dossier partagé, répertoire du disque dur, etc.), assurez que le fichier d'installation se trouve toujours dans le répertoire et que vous y avez accès.

  2. Sélectionnez **Démarrer** → **Programmes** → **Kaspersky PURE 9.1** → **Modification, réparation ou suppression**.

Cette action entraîne le lancement du programme d'installation qui se présente sous la forme d'un Assistant. Examinons en détails les étapes indispensables à la réparation ou à la modification des composants de l'application ou à la suppression de celle-ci.

DANS CETTE SECTION

Étape 1. Fenêtre d'accueil du programme d'installation 38

Étape 2. Sélection de l'opération 38

Étape 3. Fin de la réparation, de la modification ou de la suppression du logiciel 39

ÉTAPE 1. FENETRE D'ACCUEIL DU PROGRAMME D'INSTALLATION

Si vous avez réalisé toutes les tâches nécessaires à la réparation ou à la modification de la composition de l'application, la fenêtre d'accueil du programme d'installation de Kaspersky PURE s'affichera. Afin de poursuivre, cliquez sur **Suivant**.

ÉTAPE 2. SELECTION DE L'OPERATION

Lors de cette étape, vous devez choisir l'opération que vous voulez exécuter sur l'application : vous pouvez modifier la sélection des composants, rétablir l'état d'origine des composants installés ou supprimer entièrement des composants. Pour exécuter l'action que vous voulez, il suffit de cliquer sur le bouton correspondant. La suite de l'Assistant dépend de l'action que vous avez choisie.

La modification de la composition de l'application est similaire à l'installation personnalisée qui vous permet de sélectionner les composants que vous voulez installer ou supprimer.

La réparation du programme s'opère sur la base de la composition actuelle. Tous les fichiers des composants installés seront actualisés et pour chacun d'entre eux, c'est le niveau de protection **Recommandé** qui sera appliqué.

Lors de la suppression de l'application, vous devrez sélectionner les données créées et utilisées par l'application que vous souhaitez sauvegarder. Pour supprimer toutes les données de Kaspersky PURE, sélectionnez l'option **Supprimer**

complètement l'application. Pour sauvegarder les données, vous devrez sélectionner l'option **Enregistrer les objets de l'application** et précisez quels objets exactement :

- *Informations relatives à l'activation* : fichier de licence indispensable au fonctionnement de l'application.
- *Base d'Anti-Spam* : base de données qui contribue à l'identification du courrier indésirable. Cette base contient des informations détaillées sur les messages qui, pour vous, sont considérés comme des messages non sollicités ou des messages utiles.
- *Objets de la quarantaine et de la sauvegarde*. Objets de la sauvegarde : copies de sauvegarde des objets supprimés ou réparés. Il est conseillé de sauvegarder ces objets en vue d'une restauration ultérieure. Objets de la quarantaine : objets qui sont peut-être infectés par des virus ou leur modification. Ces objets contiennent un code semblable au code d'un virus connu mais qui ne peuvent être classés catégoriquement comme un virus. Il est conseillé de les conserver car ils ne sont peut-être pas infectés ou il sera possible de les réparer après la mise à jour des bases de l'application.
- *Paramètres de la protection* : valeurs des paramètres de fonctionnement de tous les composants du logiciel.
- *Données iSwift et iChecker* : base contenant les informations relatives aux objets analysés dans le système de fichiers NTFS. Elle permet d'accélérer l'analyse des objets. Grâce à cette base, Kaspersky PURE analyse uniquement les objets qui ont été modifiés depuis la dernière analyse.
- *Données du dossier virtuel de l'environnement protégé* : données accessibles pendant l'utilisation dans l'environnement protégé et dans l'environnement normal.

Si un laps de temps important s'est écoulé entre la suppression d'une version de Kaspersky PURE et l'installation d'une autre, il est déconseillé d'utiliser la base iSwift et iChecker enregistrée de l'installation antérieur de l'application. En effet, pendant cet intervalle, un programme dangereux peut s'infiltrer et ses actions malveillantes pourraient ne pas être identifiées à l'aide de cette base, ce qui entraînerait l'infection de l'ordinateur.

Pour exécuter l'action sélectionnée, cliquez sur **Suivant**. La copie des fichiers nécessaires ou la suppression des composants et des données sélectionnés est lancée.

ÉTAPE 3. FIN DE LA REPARATION, DE LA MODIFICATION OU DE LA SUPPRESSION DU LOGICIEL

La progression de la réparation, de la modification ou de la suppression sera illustrée et vous serez averti dès que l'opération sera terminée.

En règle générale, la suppression requiert le redémarrage de l'ordinateur, indispensable pour tenir compte des modifications dans le système. La boîte de dialogue vous invitant à redémarrer l'ordinateur s'affichera. Cliquez sur **Oui** pour redémarrer immédiatement. Si vous souhaitez redémarrer l'ordinateur manuellement plus tard, cliquez sur **Non**.

ADMINISTRATION DE LA LICENCE

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

DANS CETTE SECTION

Présentation du contrat de licence 40

Présentation de la licence 40

Présentation du code d'activation 41

Consultation des informations sur la licence 41

PRESENTATION DU CONTRAT DE LICENCE

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

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

PRESENTATION DE LA LICENCE

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

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

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

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

Les services offerts dépendent du type de licence.

Les types de licence suivants existent :

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

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

  La licence d'évaluation est proposée avec la version d'évaluation de l'application. La licence d'évaluation vous permet de contacter le support technique uniquement pour les questions en rapport avec l'activation de l'application ou l'achat d'une licence commerciale. Une fois que la validité de la licence d'évaluation est écoulée, Kaspersky PURE arrête de remplir toutes ces fonctions. Pour continuer à utiliser l'application, il faut l'activer.

- *La licence commerciale* est une licence payante avec une durée de validité limitée (par exemple, un an) octroyée à l'achat de Kaspersky PURE. Un nombre défini d'ordinateurs sur lesquels Kaspersky PURE peut être installé avec cette licence est associé à chaque licence.

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

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

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

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

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

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

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

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

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

PRESENTATION DU CODE D'ACTIVATION

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

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

CONSULTATION DES INFORMATIONS SUR LA LICENCE

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

1. Ouvrez la fenêtre principale de l'application.

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

Cette fenêtre permet de lancer la procédure d'activation de l'application, d'acheter une nouvelle licence ou de prolonger la durée de validité de la licence en cours.

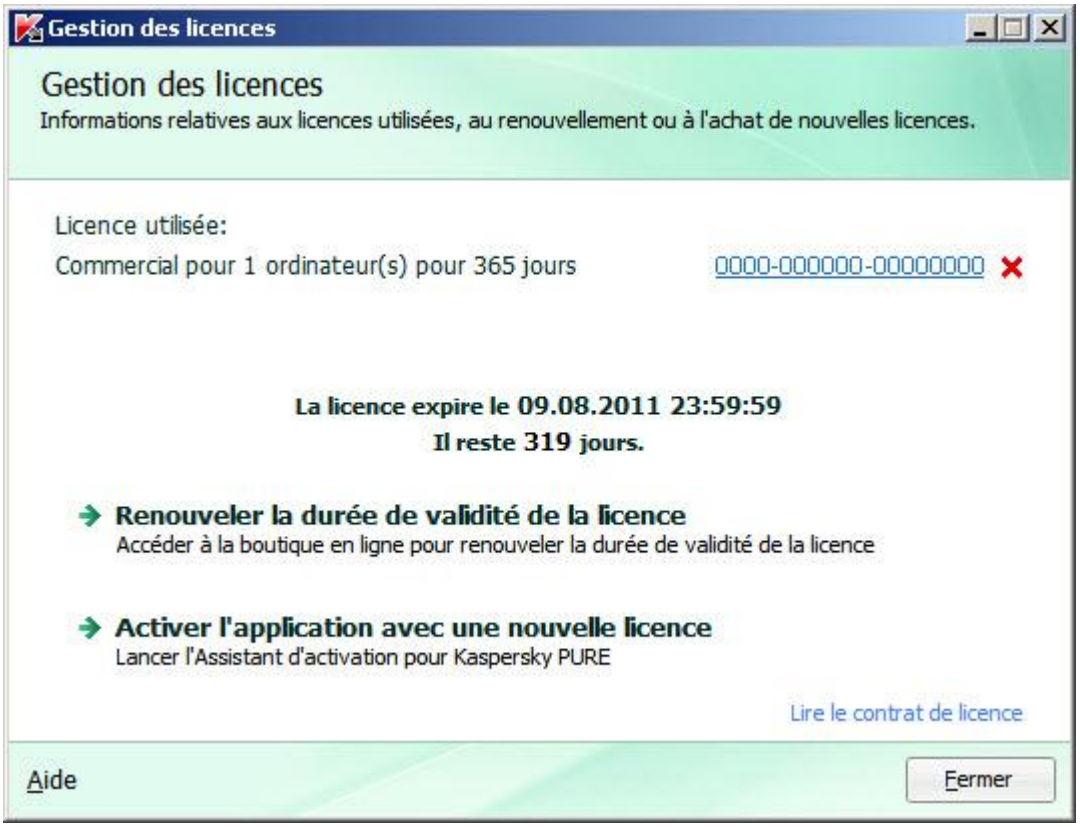


Illustration 1. Fenêtre Gestion des licences

INTERFACE DE L'APPLICATION

Ce chapitre présente les principaux éléments de l'interface de Kaspersky PURE.

DANS CETTE SECTION

L'icône dans la zone de notification de la barre des tâches. 43

Menu contextuel 44

Fenêtre principale de Kaspersky PURE 45

Fenêtre de configuration des paramètres de l'application 54

Fenêtre de notification et messages contextuels 55

L'ICONE DANS LA ZONE DE NOTIFICATION DE LA BARRE DES TACHES.

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

L'icône remplit les fonctions fondamentales suivantes :

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

Indication du fonctionnement de l'application

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

– analyse d'un message en cours ;

– analyse du trafic Web en cours ;

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

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

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

L'animation de l'icône est activée par défaut : par exemple, lors de l'analyse du message, l'icône miniature d'un message pulse sur le fond de l'icône de l'application, et lors de la mise à jour des bases de l'application, l'icône du globe tourne. Vous pouvez désactiver l'animation (cf. page 233).

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

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

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

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

L'icône permet d'ouvrir le menu contextuel (cf. page 44) et la fenêtre principale de l'application (cf. page 45).

- *Pour ouvrir le menu contextuel,*

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

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

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

L'icône apparaît dans la barre des tâches de Microsoft Windows lorsque des infos sont émises par Kaspersky Lab. La fenêtre de consultation des nouvelles (cf. page 234) s'ouvre d'un double-clique sur cette icône.

MENU CONTEXTUEL

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

Le menu de Kaspersky PURE contient les options suivantes :

- **Mise à jour** : lance le processus de mise à jour des bases et des modules de l'application.
- **Analyse complète** : lance l'analyse complète de l'ordinateur à la recherche d'éventuels objets malveillants (cf. page 67).
- **Recherche de virus** : lance la recherche d'éventuels objets malveillants dans les objets sélectionnés (cf. page 66).
- **Mon Clavier virtuel** : ouvre le clavier virtuel (cf page 70).
- **Kaspersky PURE** : ouvre la fenêtre principale de l'application (cf. page 45).
- **Configuration** : ouvre la fenêtre de configuration de l'application (cf. page 54).
- **Activation** : lance l'Assistant d'activation de Kaspersky PURE. Ce point du menu est visible uniquement si l'application n'a pas été activée.
- **A propos du programme** : ouvre la fenêtre contenant les informations relatives à l'application.
- **Suspension/Lancement de la protection** : suspend temporairement/active le composant de la protection en temps réel. Ce point du menu n'a aucune influence sur la mise à jour de l'application, ni sur l'exécution de la recherche de virus.
- **Suspendre/Activer Mon Contrôle Parental** : suspend temporairement/active le contrôle de tous les utilisateurs. Cette option du menu apparaît uniquement si le composant Mon Contrôle Parental est installé.
- **Bloquer le trafic de réseau/Débloquer le trafic de réseau** : bloque temporairement/rétablit toutes les connexions de réseau de l'ordinateur.

- **Quitter** : arrêt de Kaspersky PURE (si vous choisissez cette option, l'application sera déchargée de la mémoire vive de l'ordinateur).

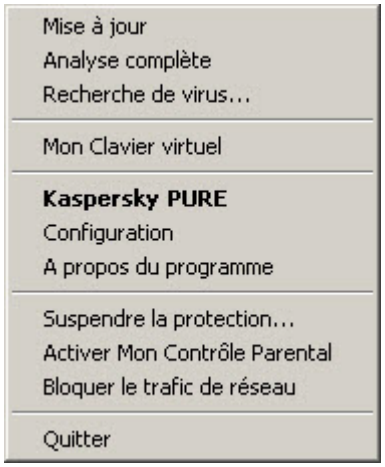


Illustration 2. Menu contextuel

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

Pour ouvrir le menu contextuel,

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

FENETRE PRINCIPALE DE KASPERSKY PURE

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

La fenêtre principale est scindée en trois parties.

- La partie supérieure reprend une évaluation globale de l'état de la protection de votre ordinateur.

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

Il faut remédier aux menaces pour la sécurité au fur et à mesure qu'elles se présentent (cf. rubrique "Diagnostic et suppression des problèmes dans la protection" à la page 58).

- La partie moyenne de la fenêtre permet d'accéder aux fonctions principales de l'application ainsi que de rétablir/suspendre la protection, rechercher la présence éventuelle de virus, lancer la copie de sauvegarde, etc. Les composants suivants de Kaspersky PURE se trouvent dans la partie supérieure de la fenêtre :

  - **Mes Sauvegardes** : création et conservation de copies de sauvegarde des fichiers, permettant une restauration de ceux-ci en cas de perte.

- **Ma Protection** : composants de la protection de l'ordinateur contre diverses menaces.
- **Mon Contrôle Parental** : restriction de l'accès des utilisateurs à l'ordinateur et à Internet.

- La partie inférieure de la fenêtre permet d'accéder aux fonctions complémentaires qui offrent une protection étendue et qui optimisent le fonctionnement du système. La partie inférieure de la fenêtre reprend les composants et les services suivants :
  - **Mes Outils d'optimisation** : optimisation du système et exécution de tâches spécifiques pour garantir la sécurité de l'ordinateur.
  - **Mon Clavier virtuel** : prévention de l'interception de données saisies à l'aide d'un clavier.
  - **Mon Réseau (cf. page** 191**) –** administration à distance de Kaspersky PURE.
  - **Mes Coffres-forts** : prévention de l'accès non autorisé aux données confidentielles.
  - **Mon Gestionnaire de mots de passe** : protection des données personnelles telles que les mots de passe, les noms d'utilisateur, les numéros de messagerie instantanée, les contacts, etc.

Illustration 3. Fenêtre principale de l'application

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

- **Configuration** : accès à la configuration des paramètres généraux de l'application (cf. page 54).
- **Aide** : ouvre l'aide de Kaspersky PURE.

- **Mon Espace Personnel** : accès à l'espace personnel de l'utilisateur (https://my.kaspersky.com/fr) sur le site du service d'Assistance technique.
- **Assistance technique** : ouvre la fenêtre contenant les informations relatives au système et les liens vers les sources d'informations de Kaspersky Lab (site du service d'assistance technique, forum).
- **Licence** : passe à l'activation de Kaspersky PURE et au renouvellement de la licence.

Vous pouvez changer l'apparence (cf. rubrique "Apparence de l'application" à la page 233) de Kaspersky PURE en créant et en utilisant vos propres éléments graphique et en choisissant la palette de couleurs.

PROTECTION DE L'ORDINATEUR

La fenêtre **Protection de l'ordinateur** est scindée en deux parties :

- La partie gauche de la fenêtre permet d'accéder rapidement à n'importe quelle fonction de l'application, au lancement de la recherche de virus ou de la mise à jour, etc.

Illustration 4. Partie gauche de la fenêtre Protection de l'ordinateur

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

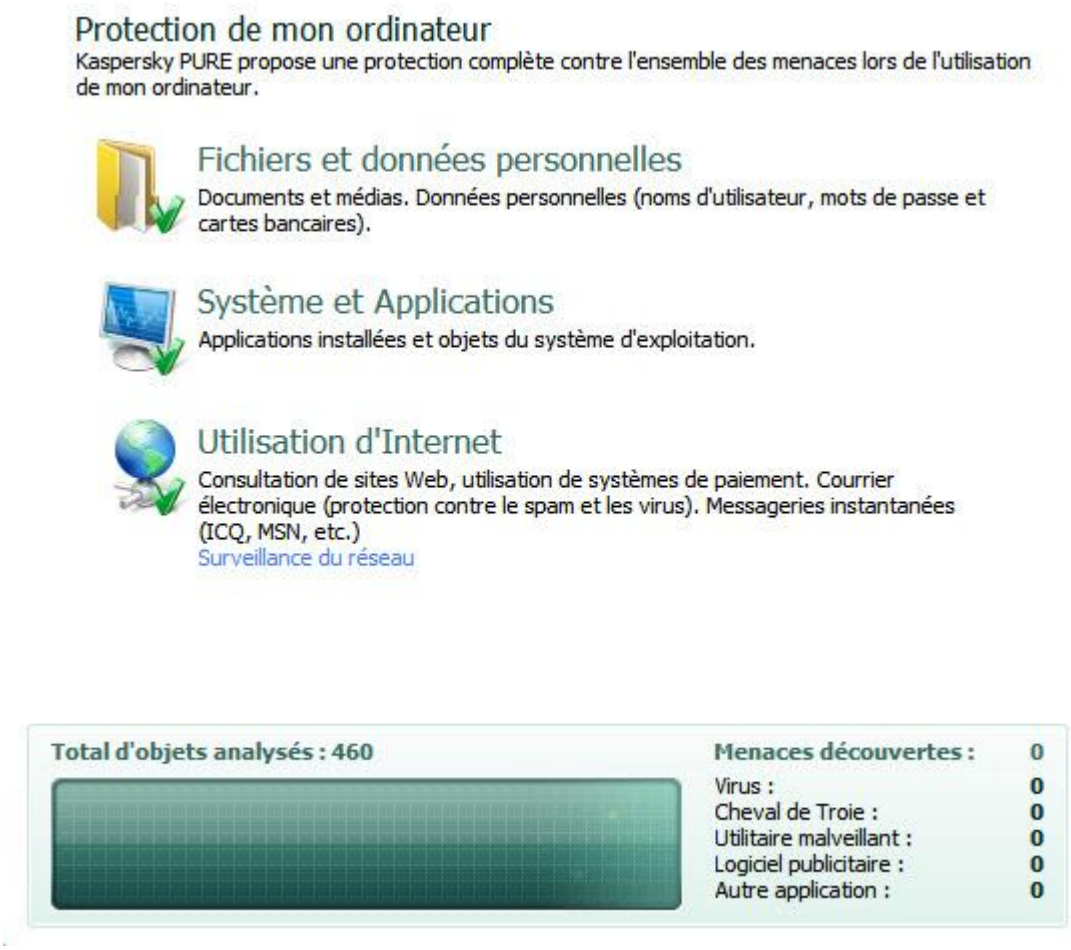


Illustration 5. Partie droite de la fenêtre Protection de l'ordinateur

Il est également possible d'utiliser les liens suivants :

- **Configuration** : ouvre la fenêtre de configuration des paramètres de la protection de l'ordinateur.
- **Quarantaine** : passe à la manipulation des objets placés en quarantaine.
- **Rapport** : passe à la liste des événements survenus pendant le fonctionnement de l'application.
- **Aide** : ouvre l'aide de Kaspersky PURE.

MES SAUVEGARDES

La fenêtre **Mes Sauvegardes** contient deux parties :

- la partie gauche permet de passer à l'utilisation des fonctions principales de Sauvegarde : administration des tâches de copie de sauvegarde et des espaces de sauvegarde ou restauration des données ;
- la partie droite de la fenêtre contient une liste des paramètres pour la fonction choisie dans la partie gauche.

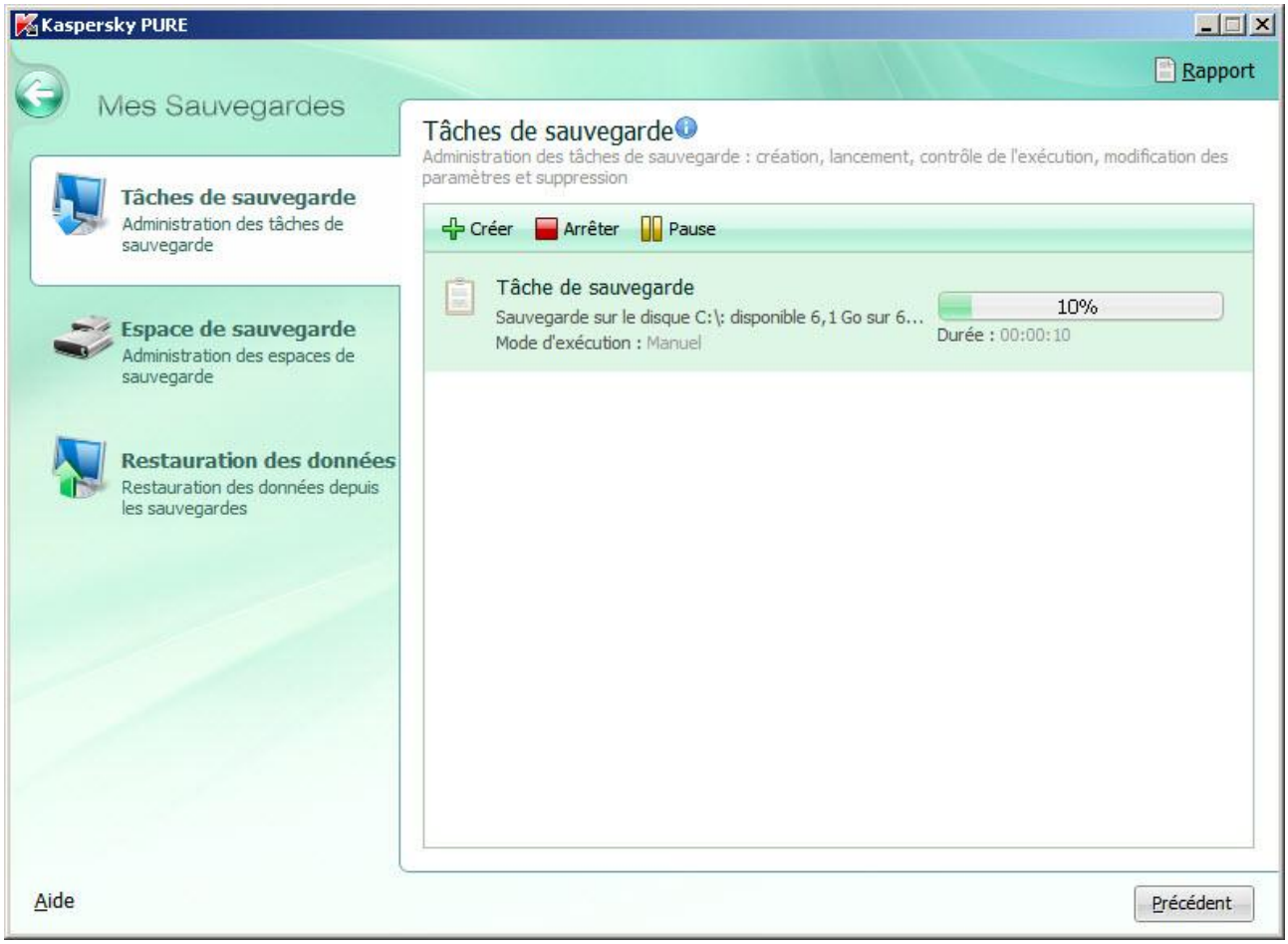


Illustration 6. Fenêtre principale du module Mes Sauvegardes

MON CONTROLE PARENTAL

La fenêtre **Mon Contrôle Parental** contient deux parties :

- la partie gauche de la fenêtre permet d'accéder aux fonctions principales de Mon Contrôle Parental telles que la configuration du contrôle pour les utilisateurs de l'ordinateur et la consultation des rapports ;
- la partie droite de la fenêtre contient une liste des paramètres pour la fonction choisie dans la partie gauche.

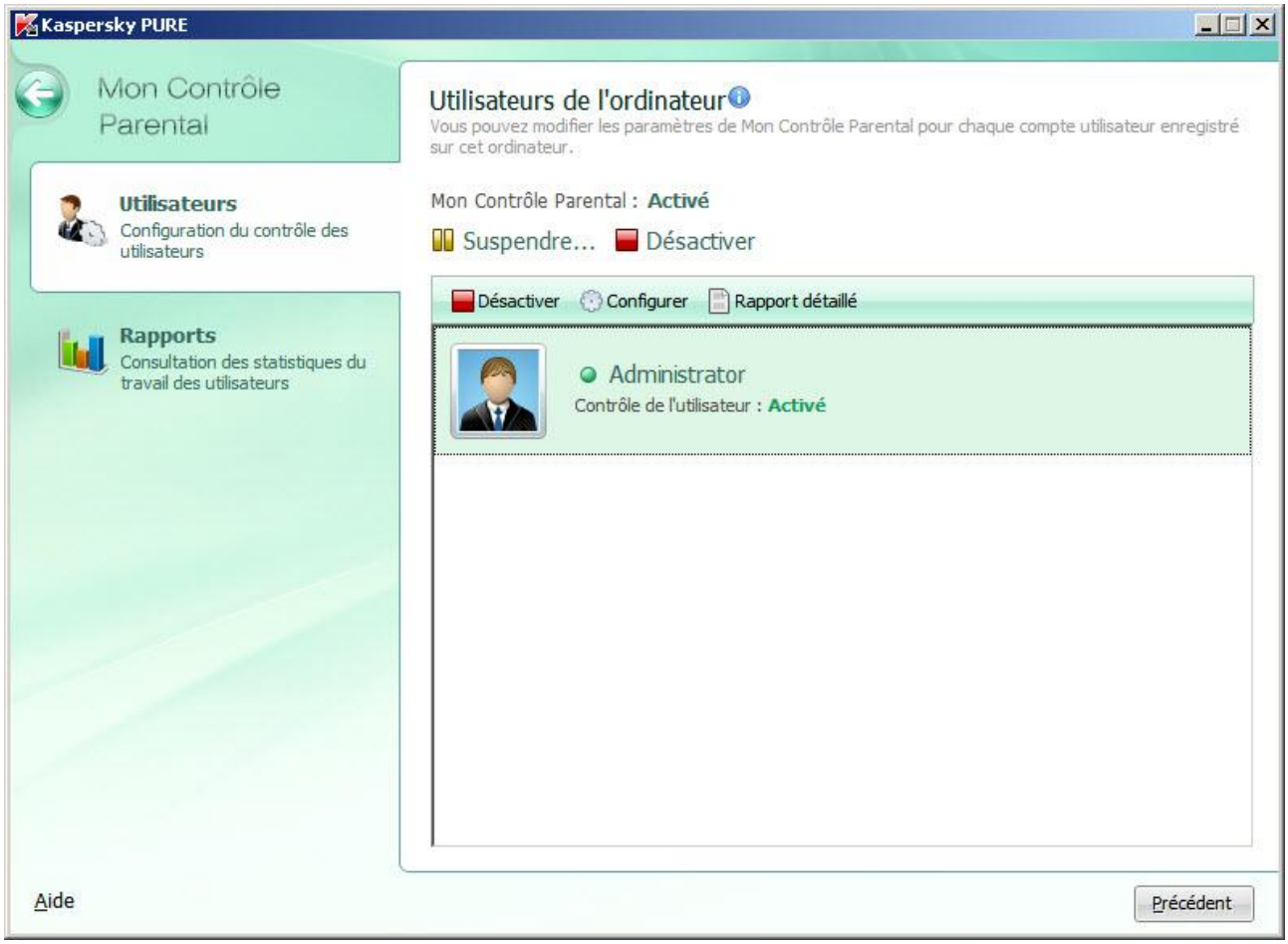


Illustration 7. Fenêtre principale du mode Mon Contrôle Parental

FENETRE MON GESTIONNAIRE DE MOTS DE PASSE

La fenêtre **Mon Gestionnaire de mots de passe** contient trois parties :

- Bouton de verrouillage/déverrouillage de la base de mots de passe (cf. page 198) ;
- Boutons d'accès rapide aux principales fonctions de Mon Gestionnaire de mots de passe : création d'un mot de passe, création d'identités, gestion de la base des mots de passe, configuration des paramètres de fonctionnement, de création et de synchronisation d'une version portable de Mon Gestionnaire de mots de passe (inaccessibles si la base de mots de passe est verrouillée).
- Bouton du générateur de mots de passe (cf. page 225).

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

- **Aide** : ouvre l'aide de Mon Gestionnaire de mots de passe ;

- **Précédent** : revient à la fenêtre principale de Kaspersky PURE (cf. page 45).

ICONE DANS LA ZONE DE NOTIFICATION

L'icône de lancement de Mon Gestionnaire de mots de passe apparaît dans la zone de notification de la barre des tâches de Microsoft Windows directement après son installation.

L'icône de Mon Gestionnaire de mots de passe prendra un des aspects suivants en fonction de la situation :

- Actif (vert) : Mon Gestionnaire de mots de passe est déverrouillé et l'accès aux données personnelles est autorisé ;

- Inactif (rouge) : Mon Gestionnaire de mots de passe est verrouillé et les données personnelles sont inaccessibles.

Cliquez sur l'icône pour accéder aux éléments suivants de l'interface :

- menu contextuel (cf. page 51) ;

- index de Mon Gestionnaire de mots de passe

MENU CONTEXTUEL DE MON GESTIONNAIRE DE MOTS DE PASSE

Le menu contextuel du gestionnaire de mots de passe permet d'exécuter les opérations principales et il propose les options suivantes :

- **Verrouiller / Déverrouiller** : autorisation/interdiction de l'accès à vos données personnelles.

- **Comptes** : accès rapide aux comptes utilisateur les plus souvent utilisés. Le nombre de comptes utilisateur dans la base de mots de passe apparaît entre parenthèses. La liste des comptes utilisateur les plus souvent utilisés est composée automatiquement. La liste est présente si son affichage dans le menu contextuel a été configuré (cf. page 214). Après la première exécution de l'application, la liste est vide car aucun compte n'a encore été utilisé.

- **Notes personnelles** : accès rapide aux notes personnelles. Le nombre de notes personnelles dans la base de mots de passe apparaît entre parenthèses.

- **Ajouter un Compte** : permet d'ajouter un nouveau compte utilisateur à Mon Gestionnaire de mots de passe.

- **Mon Gestionnaire de mots de passe** – passage à la fenêtre principale de l'application (cf. page 50).

- **Configuration** : raccourci vers la configuration des paramètres de l'application.

- **Version portable** : lance l'Assistant de création d'une version portable de l'application (cf. page 226).

- **Générateur de mots de passe** : création de mots de passe robustes (cf. page 225).

- **Aide** : ouvre l'aide de l'application.

- **Quitter** : quitte l'application (si vous choisissez cette option, l'application sera déchargée de la mémoire vive de l'ordinateur).

Si l'application n'est pas déverrouillée, l'accès à vos données personnelles sera interdit. Dans ce cas, le menu contextuel reprendra seulement les options suivantes : **Déverrouiller**, **Générateur de mots de passe**, **Aide** et **Quitter**.

Pour ouvrir le menu contextuel,

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

FENETRE DE LA BASE DES MOTS DE PASSE

La fenêtre de la base de mots de passe comporte trois parties.

- la partie supérieure de la fenêtre permet de sélectionner rapidement les fonctions de Mon Gestionnaire de mots de passe et d'effectuer les tâches de base ;
- la partie centrale de la fenêtre contient la liste de tous les comptes ainsi que les autres données personnelles. Elle permet également de gérer les informations personnelles ;
- la partie inférieure de la fenêtre contient les liens d'administration de la base des mots de passe.

Vous pouvez utiliser également le champ de recherche de la partie supérieure de la fenêtre. Le champ de recherche permet de trouver les informations souhaitées dans la base de mots de passe à l'aide de mots clés.

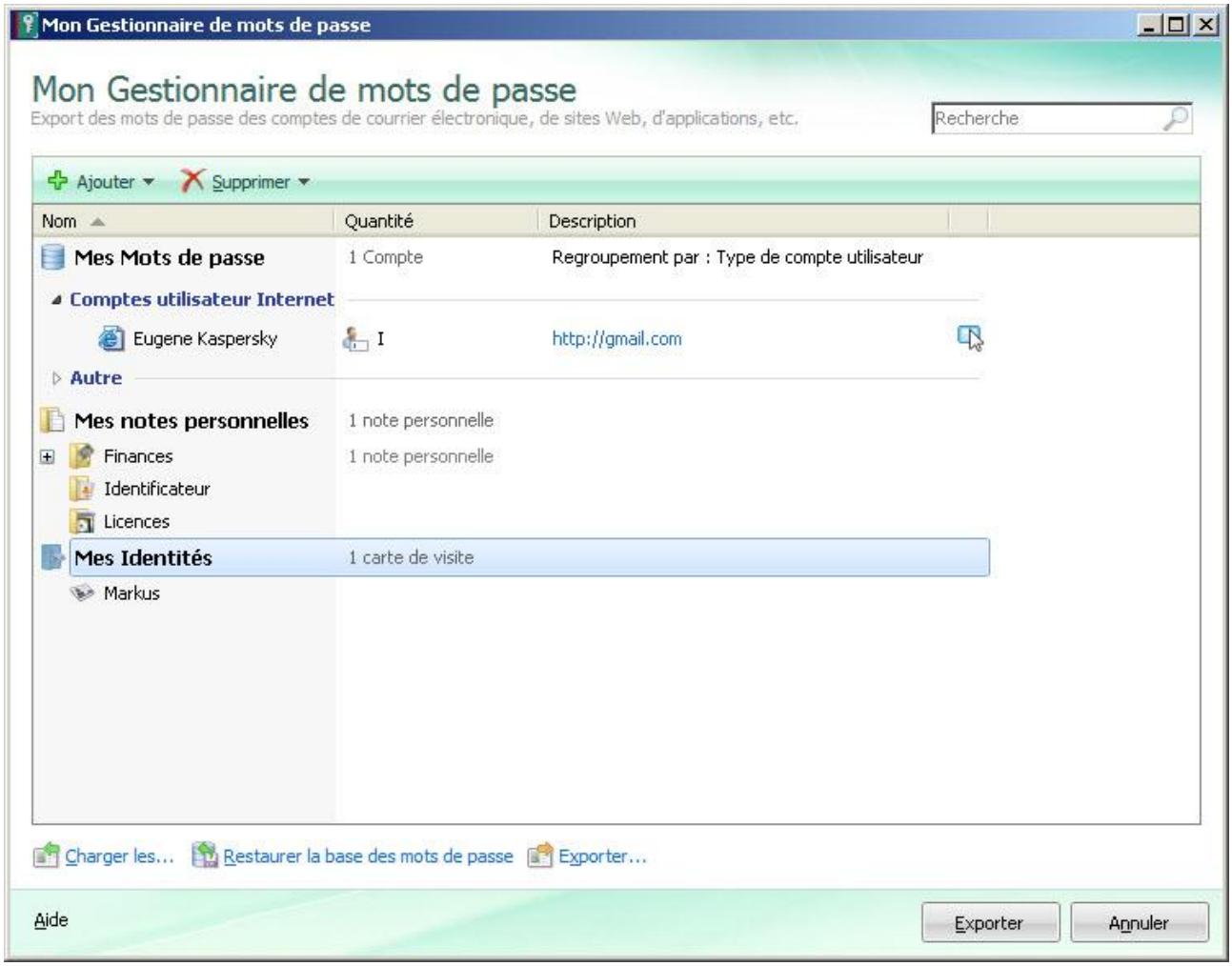


Illustration 8. Fenêtre de la base des mots de passe

FENETRE DE CONFIGURATION DES PARAMETRES

Vous pouvez ouvrir la fenêtre de configuration des paramètres de Mon Gestionnaire de mots de passe d'une des méthodes suivantes :

- depuis le (cf. page 51) : pour ce faire, sélectionnez l'option **Configuration** dans le menu contextuel de Mon Gestionnaire de mots de passe ;
- depuis la fenêtre de Kaspersky PURE**.** Pour ce faire, cliquez sur le bouton **Configuration**.

La fenêtre de configuration contient deux parties :

- La partie gauche de la fenêtre contient la liste des fonctions de l'application ;
- La partie droite de la fenêtre reprend les paramètres de la fonction, de la tâche, etc. sélectionnée.

BOUTON DE LANCEMENT RAPIDE

Le bouton de lancement rapide permet de manipuler vos données personnelles depuis la fenêtre de l'application ou depuis une page Web. Le bouton se trouve dans le coin supérieur droit de l'application.

Après avoir cliqué sur le Bouton d'accès rapide, un menu apparaît avec la liste des noms d'utilisateur associés au programme / à la page Web. Lorsque vous sélectionnez un Identifiant, Mon Gestionnaire de mots de passe complète automatiquement les champs d'autorisation en fonction des données stockées dans la base de mots de passe.

Le bouton de lancement rapide est actif si Mon Gestionnaire de mots de passe n'est pas verrouillé (cf. page 198). Cliquez sur le bouton pour réaliser une des opérations suivantes :

- **Ajouter un Compte** : permet d'ajouter un nouveau compte utilisateur.
- **Modifier le Compte** : permet d'ajouter un Identifiant/de modifier un compte utilisateur actif. L'option du menu apparaît si le compte utilisateur est activé
- **Comptes utilisateur Internet** : consultation de la liste de tous les comptes utilisateur pour Internet et ouverture de l'un d'entre eux. Le nombre de comptes utilisateur dans la base de mots de passe apparaît entre parenthèses.
- Liste des comptes utilisateur fréquemment utilisés : lancement d'un compte utilisateur de la liste. La liste est composée automatiquement sur la base de la fréquence d'utilisation des comptes utilisateur. La liste figure dans le menu si son affichage a été configuré (cf. page 214).
- **Identités** : ouverture de la liste des identités créées et sélection d'une identité pour remplir un formulaire.
- **Aide** : ouverture de l'aide du système.

Le bouton de lancement rapide est inactif si Mon Gestionnaire de mots de passe est verrouillé. Dans ce cas, le bouton ne permettra pas de réaliser des actions. Lorsqu'il est inactif, le bouton apparaît dans la fenêtre de l'application si les paramètres du Bouton d'accès rapide le spécifient (cf. page 223).

EXTENSIONS ET MODULES EXTERNES

Mon Gestionnaire de mots de passe dispose d'extensions (modules externes) qui s'intègrent aux applications exigeant une authentification. Vous pouvez installer indépendamment ces modules externes pour chaque Navigateur Internet que vous utilisez. Les modules externes installés garantissent l'accès aux fonctions de Mon Gestionnaire de mots de passe depuis l'interface de l'application/du navigateur Internet.

INDEX

L'index de Mon Gestionnaire de mots de passe permet de sélectionner rapidement l'application/la page Web en vue de la saisie automatique des données personnelles.

Pour utiliser le pointeur de Mon Gestionnaire de mots de passe, procédez comme suit :

1. Déplacez le curseur de la souris sur l'icône de Mon Gestionnaire de mots de passe dans la zone de notification de la barre des tâches et patientez quelques secondes.

2. Une fois que le pointeur de Mon Gestionnaire de mots de passe apparaît, déplacez-le dans la fenêtre de l'application/sur la page Web souhaitée. Mon Gestionnaire de mots de passe détermine automatiquement l'action pour l'application/la page Web sélectionnée.

FENETRE DE CONFIGURATION DES PARAMETRES DE L'APPLICATION

La fenêtre de configuration des paramètres de Kaspersky PURE permet de configurer les paramètres de fonctionnement de l'application dans son ensemble, de composants distincts de la protection, de l'analyse et de la mise à jour et d'exécuter d'autres tâches de configuration étendue (cf. page 84).

La fenêtre de configuration contient trois parties :

- La partie supérieure contient les catégories de tâches et les fonctions de Kaspersky PURE.

- La partie de gauche permet d'accéder aux tâches et aux fonctions de Kaspersky PURE dans la catégorie sélectionnée.

- La partie droite de la fenêtre contient la liste des paramètres pour la fonction ou la tâche de l'application choisie dans la partie gauche.

Il est possible d'ouvrir la fenêtre de configuration depuis la fenêtre principale (cf. page 45) ou depuis le menu contextuel (cf. page 44). Pour ouvrir la fenêtre de configuration, cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre ou choisissez l'option du même nom dans le menu contextuel de l'application.

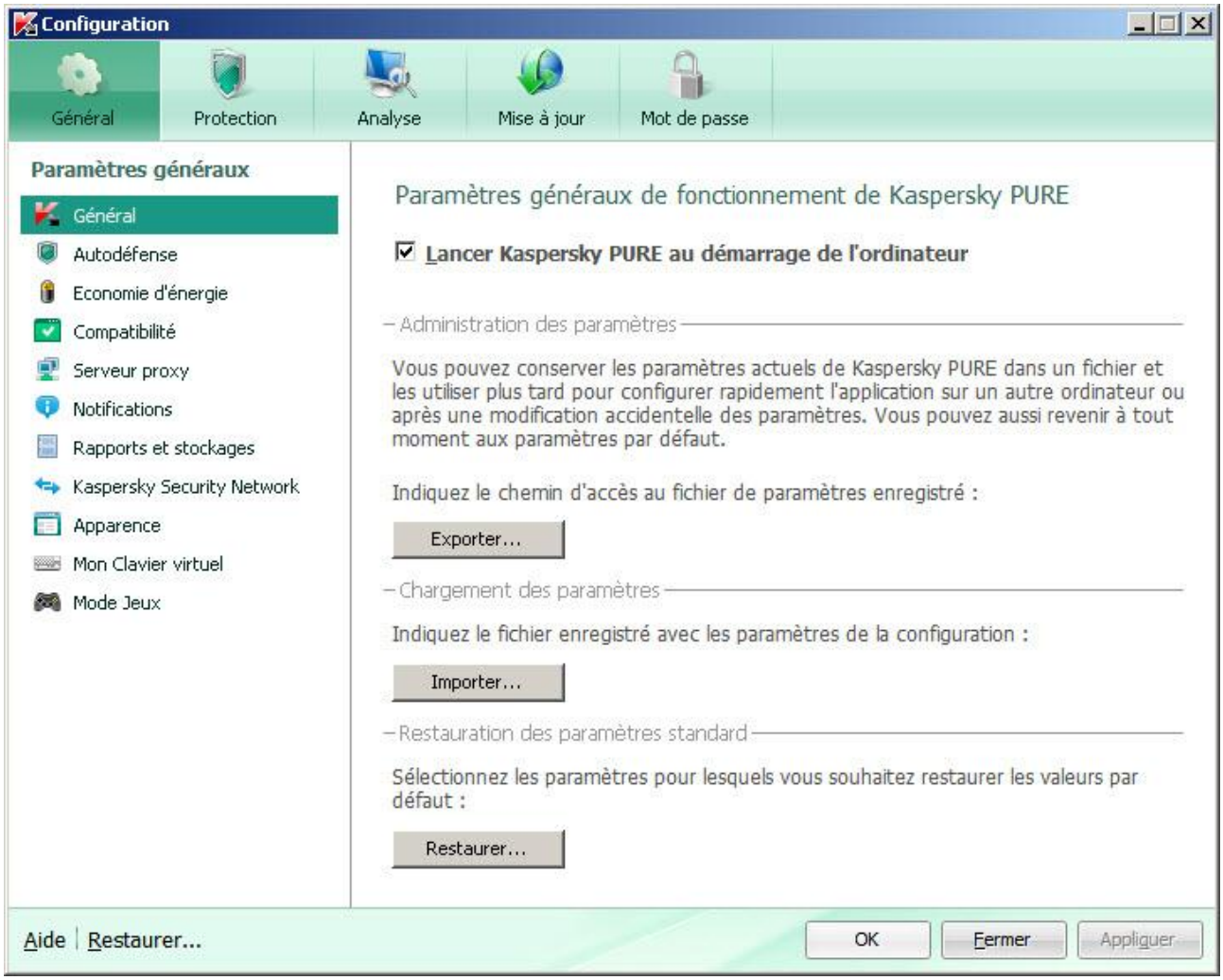


Illustration 9. Configuration des paramètres de Kaspersky PURE

FENETRE DE NOTIFICATION ET MESSAGES CONTEXTUELS

Kaspersky PURE vous signale les événements importants survenus pendant son fonctionnement à l'aide des *fenêtres de notification* et des *messages contextuels* qui apparaissent au-dessus de l'icône de l'application dans la zone de notification de la barre des tâches.

La fenêtre de notification de Kaspersky PURE s'affiche quand plusieurs actions sont possibles en rapport avec l'événement : par exemple, en cas de découverte d'un objet malveillant, vous pouvez bloquer l'accès à celui-ci, le supprimer ou tenter de le réparer. L'application vous propose de choisir parmi plusieurs options. La fenêtre de notification disparaît une fois que vous avez sélectionné une des actions proposées.

Illustration 10. Fenêtre notifications

Les messages contextuels de Kaspersky PURE s'affichent pour signaler des événements qui ne nécessitent pas obligatoirement une intervention. Certains messages contextuels contiennent des liens qui permettent d'exécuter l'action proposée (par exemple, lancer la mise à jour des bases ou activer l'application). Les messages contextuels disparaissent automatiquement de l'écran après l'affichage.

Illustration 11. Message contextuel

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

- Critiques : signalent des événements d'une importance capitale du point de vue de la sécurité de l'ordinateur (par exemple : découverte d'un objet malveillant ou d'une activité dangereuse dans le système). Les fenêtres de notification et les messages contextuels de ce type sont rouges.
- Importantes : signalent des événements potentiellement importants du point de vue de la sécurité de l'ordinateur (par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système). Les fenêtres de notification et les messages contextuels de ce type sont jaunes.
- Informatifs : signalent des événements qui ne sont pas critiques du point de vue de la sécurité. Les fenêtres de notification et les messages contextuels de ce type sont verts.

LANCEMENT ET ARRET DE L'APPLICATION

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

DANS CETTE SECTION

Activation et désactivation du lancement automatique 57

Lancement et arrêt manuels de l'application 57

ACTIVATION ET DESACTIVATION DU LANCEMENT AUTOMATIQUE

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

Pour activer le lancement automatique de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Général** dans la rubrique **Paramètres avancés**.
4. Dans la partie droite de la fenêtre, décochez la case **Lancer Kaspersky PURE au démarrage de l'ordinateur**.

LANCEMENT ET ARRET MANUELS DE L'APPLICATION

Kaspersky Lab déconseille d'arrêter Kaspersky PURE car, dans ce cas, l'ordinateur et les données personnelles qu'il contient seront menacés. Si une telle mesure s'impose vraiment, il est conseillé de suspendre la protection (cf. page 60) pour une période déterminée sans quitter l'application.

Il faut lancer Kaspersky PURE manuellement uniquement si vous avez désactivé le lancement automatique de l'application (cf. page 57).

Pour lancer l'application manuellement,

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

Pour quitter l'application,

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

ÉTAT DE LA PROTECTION DU RESEAU DOMESTIQUE

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

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

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

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

Cliquez sur le bouton **Corriger maintenant** pour ouvrir la fenêtre **État général de la protection** (cf. ill. ci-après) qui reprend des informations détaillées sur l'état de la protection de l'ordinateur et qui propose des options pour la suppression des problèmes et des menaces.

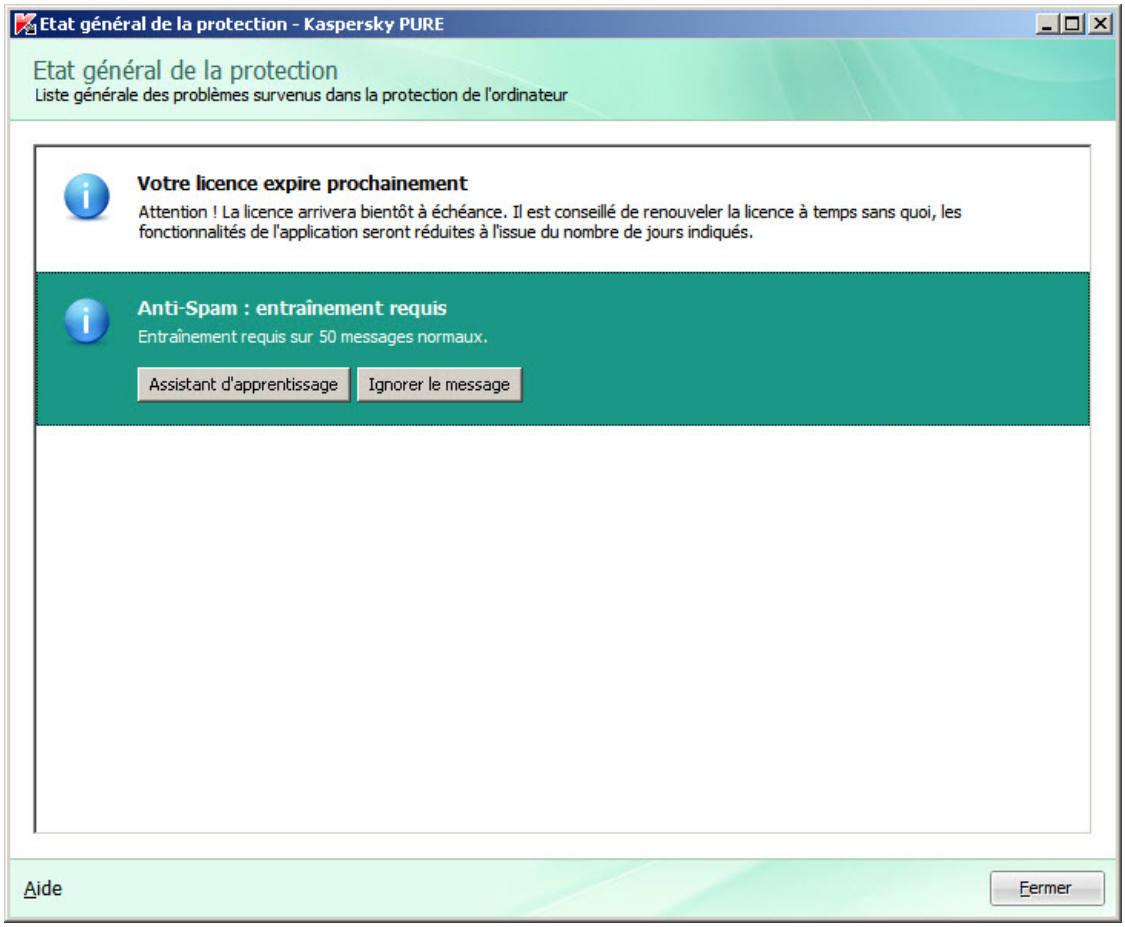


Illustration 12. Fenêtre État général de la protection

La fenêtre reprend la liste des problèmes de protection, notamment les écarts par rapport au fonctionnement optimum de l'application (par exemple, bases dépassées). Les actions suivantes sont proposées pour supprimer les problèmes et les menaces.

- Résolution immédiate. Cliquez sur le bouton avec l'action proposée pour passer directement à la résolution du problème. Il s'agit de l'action recommandée.

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

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

Pour que les messages masqués soient à nouveau affichés dans la liste générale, cliquez sur le bouton **Restaurer les messages dissimulés**, dans l'élément de la liste **Certains messages ont été ignorés**.

Vous pouvez analyser le niveau de protection du réseau domestique depuis le poste de travail de l'administrateur à l'aide de Mon Réseau (cf. rubrique "Vérification à distance de l'état de la protection des ordinateurs du réseau domestique" à la page 68).

ACTIVATION / DESACTIVATION DE LA PROTECTION DE L'ORDINATEUR

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

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

Les experts de Kaspersky Lab vous recommandent vivement de **ne pas désactiver la protection** car cela pourrait entraîner l'infection de l'ordinateur et la perte de données.

Cette action entraînera l'arrêt de tous ses composants. Les éléments suivants en témoignent :

- icône inactive (grise) de Kaspersky PURE (cf. rubrique "Icône dans la zone de notification de la barre des tâches" à la page 43) dans la zone de notification de la barre des tâches ;

- couleur rouge de l'indicateur de sécurité.

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

Pour désactiver complètement la protection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Protection de l'ordinateur**.
2. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
3. Dans la fenêtre qui s'ouvre, ouvrez la rubrique **Protection**.
4. Désélectionnez la case **Activer la protection**.

Pour activer ou désactiver à distance un composant de la protection, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Sélectionnez la rubrique **Ma Protection** dans la partie gauche de la fenêtre et dans la partie droite, cliquez sur le bouton portant le nom de la catégorie à protéger requise.

3. Dans la fenêtre **Composants de la protection** qui s'ouvre, activez/désactivez le composant de la protection souhaité d'un clic de la souris sur l'icône d'état située à droite du nom du composant.

SUSPENSION DE LA PROTECTION

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

Cette action suspend le fonctionnement de tous les composants de la protection en temps. Les éléments suivants permettent de confirmer la désactivation :

- Icône inactive (grise) de (cf. rubrique "Icône dans la zone de notification de la barre des tâches" à la page 43) dans la zone de notification de la barre des tâches ;

- Couleur rouge de l'icône d'état et du panneau de la fenêtre de protection de l'ordinateur.

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

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

1. Dans le menu contextuel (cf. section "Menu contextuel" à la page 44) de l'application sélectionnez **Suspension de la protection**.

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

   - **Suspendre pendant <intervalle> :** la protection sera restaurée à l'issue de l'intervalle désigné. Pour sélectionner la valeur, utilisez la liste déroulante.

   - **Suspendre jusqu'au redémarrage :** la protection sera activée après le redémarrage de l'application ou du système (pour autant que le mode de lancement de Kaspersky PURE au démarrage de l'ordinateur ait été activé).

   - **Reprendre manuellement** : la protection sera réactivée uniquement lorsque vous le déciderez. Pour activer la protection, cliquez sur le point **Lancement de la protection** dans le menu contextuel de l'application.

UTILISATION DU MODE DE PROTECTION INTERACTIF

Kaspersky PURE interagit avec l'utilisateur selon deux modes :

- *Mode de protection interactif*. Kaspersky PURE prévient l'utilisateur de tous les événements dangereux et suspects survenus dans le système. L'utilisateur doit lui-même prendre la décision d'autoriser ou d'interdire une action quelconque.

- *Mode de protection automatique*. Kaspersky PURE appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab lors d'événements dangereux.

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

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez la sous-section **Paramètres généraux**.

4. Dans le groupe **Protection interactive** de la partie droite de la fenêtre, décochez ou cochez les cases selon le mode de protection que vous avez sélectionné :

   - Pour installer le mode de protection interactif, décochez la case **Sélectionner l'action automatiquement** ;

   - Pour installer le mode de protection automatique, cochez la case **Sélectionner l'action automatiquement**.

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

RESOLUTION DES PROBLEMES TYPES

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

DANS CETTE SECTION

Procédure d'activation de l'application 63

Procédure d'achat ou de renouvellement d'une licence 63

Que faire en cas d'affichage de notifications 64

Procédure de mise à jour des bases et des modules de l'application 64

Procédure d'analyse des secteurs importants de l'ordinateur 65

Procédure de recherche de virus dans un fichier, un dossier, un disque ou un autre objet 66

Procédure d'exécution d'une analyse complète de l'ordinateur 67

Procédure de recherche de vulnérabilités sur l'ordinateur 67

Vérification à distance de l'état de la protection des ordinateurs du réseau domestique 68

Procédure de protection des données personnelles contre le vol 69

Que faire si vous pensez que l'objet est infecté par un virus 73

Procédure de restauration d'un objet supprimé ou réparé par l'application 74

Que faire si vous pensez que votre ordinateur est infecté 74

Copie de sauvegarde des données 75

Comment restreindre l'accès aux paramètres de Kaspersky PURE 77

Comment restreindre l'utilisation de l'ordinateur et d'Internet pour différents comptes utilisateur 78

Procédure de création du disque de dépannage et utilisation de celui-ci 78

Que faire avec un grand nombre de messages non sollicités 80

Consultation du rapport sur la protection de l'ordinateur 82

Procédure de restauration des paramètres standards d'utilisation de l'application 82

Transfert des paramètres de l'application sur un autre ordinateur 83

PROCEDURE D'ACTIVATION DE L'APPLICATION

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

Si vous n'avez pas activé l'application pendant l'installation (cf. page 33), vous pouvez le faire plus tard. Les notifications de Kaspersky PURE dans la zone de notifications de la barre des tâches vous rappelleront qu'il faut activer l'application.

Pour démarrer l'Assistant d'activation de Kaspersky PURE, réalisez une des opérations suivantes :

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

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

Examinons en détails les étapes de l'Assistant.

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

Assurez-vous que l'option **Activer la version commerciale** a bien été sélectionnée dans la fenêtre de l'Assistant d'activation, saisissez le code d'activation (cf. section "Présentation du code d'activation" à la page 41) dans le champ correspondant, puis cliquez sur le bouton **Suivant**.

Etape 2. Demande d'activation

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

Etape 3. Fin de l'Assistant

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

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

PROCEDURE D'ACHAT OU DE RENOUVELLEMENT D'UNE LICENCE

Si vous avez installé Kaspersky PURE sans licence, vous pourrez acheter celle-ci après l'installation de l'application. Quand la durée de validité de la licence approche de son échéance, vous pouvez la renouveler. Vous obtenez le code d'activation qui permet d'activer l'application.

Pour acheter une licence, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

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

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

Pour renouveler une licence, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Licence** situé dans la partie inférieure de la fenêtre.

La fenêtre **Gestion des licences** s'ouvre.

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

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

QUE FAIRE EN CAS D'AFFICHAGE DE NOTIFICATIONS

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

- Critiques : signalent des événements d'une importance capitale du point de vue de la sécurité de l'ordinateur (par exemple : découverte d'un objet malveillant ou d'une activité dangereuse dans le système). Les fenêtres de notification et les messages contextuels de ce type sont rouges.

- Importantes : signalent des événements potentiellement importants du point de vue de la sécurité de l'ordinateur (par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système). Les fenêtres de notification et les messages contextuels de ce type sont jaunes.

- Informatifs : signalent des événements qui ne sont pas critiques du point de vue de la sécurité. Les fenêtres de notification et les messages contextuels de ce type sont verts.

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

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

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

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

Pour maintenir la protection de votre ordinateur à jour, il est conseillé d'actualiser Kaspersky PURE directement après l'installation.

Pour lancer la mise à jour depuis le menu contextuel,

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 :

Ouvrez la fenêtre principale de l'application, dans la rubrique **Ma Protection**, cliquez sur le bouton **Lancement rapide des tâches**, puis choisissez l'option **Exécuter la mise à jour des tâches**.

PROCEDURE D'ANALYSE DES SECTEURS IMPORTANTS DE L'ORDINATEUR

L'analyse rapide désigne l'analyse des objets chargés au démarrage du système d'exploitation, l'analyse de la mémoire système, l'analyse des secteurs d'amorçage du disque, ainsi que l'analyse des objets ajoutés par l'utilisateur. L'analyse rapide est réalisée automatiquement lors de l'installation de Kaspersky PURE.

Vous pouvez lancer la tâche d'analyse express d'une des manières suivantes :

- via un raccourci créé (cf. page 93) au préalable ;
- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky PURE" à la page 45)
- .

Pour lancer la tâche de l'analyse rapide via un raccourci, procédez comme suit :

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

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

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

   Les informations relatives à l'analyse exécutées apparaissent :

   - Dans le groupe **Protection de l'ordinateur** de la fenêtre principale de l'application dans le champ **Analyse** ;
   - Dans la rubrique **Protection** de la fenêtre **Protection de l'ordinateur**, dans le groupe **Arrêter l'analyse rapide** ;
   - Dans la fenêtre **Analyse rapide** qui s'ouvre lorsque vous cliquez sur le lien **Fin** dans le groupe **Arrêter l'analyse rapide** ;
   - Dans le menu contextuel de l'icône de l'application (cf. page 44).

Pour arrêter l'analyse rapide, procédez comme suit :

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

PROCEDURE DE RECHERCHE DE VIRUS DANS UN FICHIER, UN DOSSIER, UN DISQUE OU UN AUTRE OBJET

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

- Via le menu contextuel de l'objet ;
- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky PURE" à la page 45).

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

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

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

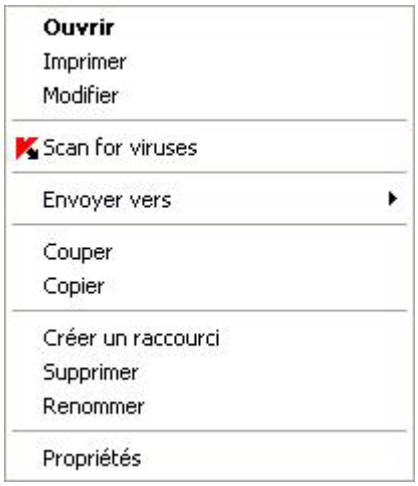


Illustration 13. Menu contextuel de l'objet dans Microsoft Windows

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

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Ma Protection**.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Dans la partie droite de la fenêtre, dans le groupe **Analyser les objets**, cliquez sur le lien **Ajouter**.
4. Dans la fenêtre **Sélection de l'objet à analyser** que s'ouvre, indiquez l'emplacement de l'objet que vous souhaitez soumettre à l'analyse antivirus.
5. Dans le groupe **Analyser les objets**, cochez les cases en regard des objets que vous souhaitez analyser.
6. Cliquez sur le bouton **Analyser les objets**.

   Les informations relatives à l'analyse exécutées apparaissent :

   - Dans le groupe **Protection de l'ordinateur** de la fenêtre principale de l'application dans le champ **Analyse** ;
   - Dans la rubrique **Protection** de la fenêtre **Protection de l'ordinateur**, dans le groupe **Arrêter l'analyse des objets** ;

- Dans la fenêtre **Analyse des objets** qui s'ouvre lorsque vous cliquez sur le lien **Fin** dans le groupe **Arrêter l'analyse des objets** ;
- Dans le menu contextuel de l'icône de l'application (cf. page 44).

Pour arrêter l'analyse des, procédez comme suit :

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

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

Vous pouvez lancer la tâche d'analyse complète d'une des manières suivantes :

- Via un raccourci créé (cf. page 93) au préalable ;
- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky PURE" à la page 45).

Pour lancer la tâche de l'analyse complète via un raccourci, procédez comme suit :

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

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

Ouvrez la fenêtre principale de l'application, dans la rubrique **Ma Protection**, cliquez sur le bouton **Lancement rapide des tâches**, puis choisissez l'option **Exécuter l'analyse complète**.

PROCEDURE DE RECHERCHE DE VULNERABILITES SUR L'ORDINATEUR

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

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

- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky PURE" à la page 45) ;
- Via un raccourci créé.

Pour lancer la tâche via un raccourci, procédez comme suit :

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

   Le processus d'exécution de la tâche sera affiché dans la fenêtre **Recherche de Vulnérabilités** qui s'ouvre.

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

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

   Le processus d'exécution de la tâche sera affiché dans la fenêtre **Recherche de Vulnérabilités** qui s'ouvre. Les vulnérabilités identifiées seront affichées sous les onglets **Vulnérabilités du système** et **Applications vulnérables**.

VERIFICATION A DISTANCE DE L'ETAT DE LA PROTECTION DES ORDINATEURS DU RESEAU DOMESTIQUE

Mon Réseau (cf. page 191) est le composant prévu pour l'administration à distance de Kaspersky PURE installée sur les ordinateurs du réseau domestique depuis le poste de travail de l'administrateur.

Vous pouvez analyser le niveau de protection du réseau domestique dans son ensemble ou consulter la liste des problèmes sur un ordinateur en particulier du réseau et régler certains d'entre eux à distance.

Pour obtenir des informations détaillées sur les problèmes au niveau de la protection du réseau et les supprimer, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure, cliquez sur **Mon Réseau**.
2. Au premier lancement, l'est ouvert automatiquement. Voici, en détails, les étapes de l'Assistant :
   a. Saisissez ou modifiez le mot de passe d'administration dans la fenêtre **Protection par mot de passe**.
   b. Sélectionnez le réseau pour l'administration à distance dans la fenêtre **Découverte du réseau**.
   c. Sélectionnez le mode de mise à jour des bases antivirus dans la fenêtre **Source des mises à jour**.
   d. Confirmez les paramètres sélectionnés dans la fenêtre **Résumé**.

   Lors des lancements suivants, il faudra saisir le mot de passe d'administrateur.
3. Dans la fenêtre **Mon Réseau** qui s'ouvre, cliquez sur l'icône de l'état ou sur le volet où elle se trouve.

   La fenêtre **Etat de la protection du réseau** qui s'ouvre reprend les problèmes actuels.

Pour obtenir la liste des problèmes pour un ordinateur du réseau local, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Réseau**.
2. Au premier lancement, l'est ouvert automatiquement. Voici, en détails, les étapes de l'Assistant :
   a. Saisissez ou modifiez le mot de passe d'administration dans la fenêtre **Protection par mot de passe**.
   b. Sélectionnez le réseau pour l'administration à distance dans la fenêtre **Découverte du réseau**.
   c. Sélectionnez le mode de mise à jour des bases antivirus dans la fenêtre **Source des mises à jour**.
   d. Confirmez les paramètres sélectionnés dans la fenêtre **Résumé**.

Lors des lancements suivants, il faudra saisir le mot de passe d'administrateur.

3. Dans la partie supérieure de la fenêtre **Mon Réseau** qui s'ouvre, choisissez l'ordinateur dont vous souhaitez afficher la liste des problèmes, puis cliquez sur le lien **Informations**.

4. Dans la partie droite de la fenêtre qui s'ouvre, sélectionnez l'option **Liste des problèmes**.

5. Dans la fenêtre **Etat de la protection** qui s'ouvre, vous verrez les problèmes actuels de l'ordinateur sélectionné.

PROCEDURE DE PROTECTION DES DONNEES PERSONNELLES CONTRE LE VOL

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

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

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

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

Le clavier virtuel et Mon Gestionnaire de mots de passe protègent les données contre l'interception des données au niveau du clavier.

Mes Coffres-forts est le composant chargé de la protection des fichiers contre l'accès non autorisé.

DANS CETTE SECTION

Protection contre le phishing 69

Mon Clavier virtuel 70

Mon Gestionnaire de mots de passe 71

Mes Coffres-forts 72

PROTECTION CONTRE LE PHISHING

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

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

L'Anti-Phishing, inclus dans l'Antivirus Internet, l'Antivirus Courrier et l'Antivirus IM, garantit la protection contre le phishing. Activez le fonctionnement de ces composants pour garantir l'efficacité maximale de la protection contre le phishing.

Pour activer le fonctionnement des composants de protection contre le phishing, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
4. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Antivirus Internet**.
5. Répétez les étapes 3 et 4 pour les composants **Anti-Spam** et **Antivirus IM (Chat)**.

   Les composants qui contiennent l'Anti-Phishing seront activés.

MON CLAVIER VIRTUEL

Au cours de l'utilisation de l'ordinateur, il arrive souvent qu'il faille saisir des données personnelles ou un nom d'utilisateur et un mot de passe. C'est le cas lors de l'enregistrement sur certains sites Internet, lors de l'achat dans des boutiques en ligne, etc.

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

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

Mon Clavier virtuel ne peut protéger vos données si le site nécessitant la saisie de ces données a été compromis car dans ce cas, les données tombent directement entre les mains des individus mal intentionnés.

Plusieurs programmes-espions peuvent faire des screenshots qui se transmettent automatiquement au malfaiteur pour qu'il analyse et qu'il puisse récupérer les données personnelles de l'utilisateur. Mon Clavier virtuel protège les données personnelles saisies contre l'interception par les screenshots.

Mon Clavier virtuel protége contre l'interception des données personnelles uniquement si les navigateurs Microsoft Internet Explorer et Mozilla Firefox fonctionnent.

Pour utiliser Mon Clavier virtuel, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Clavier virtuel**.
2. Saisissez les données requises en appuyant sur les touches du Mon Clavier virtuel. Assurez-vous que les données sont saisies dans le champ requis. Si vous appuyez sur les touches de fonction (**Shift**, **Alt** ou **Ctrl**) du Mon Clavier virtuel, le mode de saisie spécial est activé (ainsi, si vous appuyez sur la touche **Shift**, tous les caractères seront saisis en majuscules). Pour annuler un mode spécial, appuyez à nouveau sur la touche de fonction.

Le changement de la langue pour Mon Clavier virtuel se passe à l'aide de la combinaison des touches **Ctrl** + le clique sur **Shift** avec le bouton droit de la souris, ou **Ctrl** + le clique sur le **Left Alt** avec le bouton droit de la souris selon les paramètres installés.

MON GESTIONNAIRE DE MOTS DE PASSE

Mon Gestionnaire de mots de passe protège vos données personnelles (par exemple, les noms d'utilisateur, les mots de passe, les adresses, les numéros de téléphone et de carte de crédit).

Toutes les informations stockées sont cryptées dans une base de mots de passe dont l'accès est protégé au moyen d'un Mot de passe principal. Mon Gestionnaire de mots de passe établit un lien entre vos mots de passe et vos comptes et les applications Microsoft Windows ou pages Web dans lesquelles ils sont utilisés. Après avoir lancé la page Web ou l'application, Mon Gestionnaire de mots de passe introduit à votre place le mot de passe, l'identifiant et les autres données personnelles dans les champs correspondants. De cette manière, il vous suffit de retenir un seul mot de passe.

Pour utiliser Mon Gestionnaire de mots de passe pour le remplissage automatique des champs d'autorisation, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

2. Au premier lancement, l'Assistant de configuration de Mon Gestionnaire de mots de passe est ouvert automatiquement. Voici, en détails, les étapes de l'Assistant :

   a. Créez un mot de passe principal pour la protection de votre base de mots de passe dans la fenêtre **Mot de passe principal**.

   b. Sélectionnez le mode d'autorisation pour l'accès à votre base de mots de passe dans la fenêtre **Mode d'authentification**.

   c. Définissez la période à l'issue de laquelle Mon Gestionnaire de mots de passe sera automatiquement bloqué dans la fenêtre **Délai avant le blocage**.

   Il faudra saisir le mot de passe principal pour lancer à nouveau Mon Gestionnaire de mots de passe.

3. Dans la fenêtre qui s'ouvre cliquez sur **Ajouter le mot de passe**.

4. Dans la fenêtre de l'Assistant de création de compte utilisateur qui s'ouvre, sélectionnez le type de compte utilisateur (compte utilisateur Internet, compte utilisateur d'application ou mode utilisateur), puis cliquez sur **Suivant**.

   - Si vous avez choisi l'option compte utilisateur Internet ou d'application, indiquez le site Web ou l'application pour laquelle le compte utilisateur sera utilisé, puis cliquez sur **Suivant**.

   - Si vous avez sélectionné le mode utilisateur, sous l'onglet **Association** de la fenêtre qui s'ouvre, indiquez le chemin d'accès à l'application/à la page Web et définissez les paramètres d'utilisation du compte utilisateur.

5. Dans la partie supérieure de la fenêtre, dans le champ **Nom**, saisissez ou modifiez le nom du nouveau compte utilisateur.

6. Sous l'onglet **Identifiant**, introduisez l'Identifiant et le mot de passe.

7. Sous l'onglet **Modification avancée**, configurez si nécessaire les paramètres de remplissage des champs complémentaires de la page Web.

8. Sous l'onglet **Commentaires**, introduisez si nécessaire un texte complémentaire décrivant le compte. Pour afficher les commentaires dans les notifications après activation du compte, cochez la case **Afficher les commentaires dans les notifications**.

9. Fermez la fenêtre en cliquant sur le lien **OK**.

10. Lancez l'application/ouvrez la page Web pour laquelle le compte utilisateur a été créé.

    Le formulaire d'authentification sera automatiquement complété sur la base des données du Compte.

MES COFFRES-FORTS

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

Créez un coffre-fort, enregistrez-y les données, puis chiffrez ces données. Par la suite, pour accéder aux données du coffre-fort, il faudra saisir un mot de passe.

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

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Coffre-fort**.
  2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Créer...**.
  3. L'Assistant de création d'un coffre-fort crypté sera lancé. Voici, en détails, les étapes de l'Assistant :
     a. Saisissez le nom du coffre-fort, la taille et le mot de passe d'accès dans la fenêtre **Paramètres généraux**.
     b. Indiquez l'emplacement du fichier du coffre-fort dans la fenêtre **Source**.
     c. Sélectionnez la lettre du disque virtuel pour le déverrouillage du coffre-fort, définissez les paramètres complémentaires, si nécessaire, et confirmez la création du coffre-fort avec les paramètres indiqués dans la fenêtre **Résumé**.

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

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Coffres-forts**.
  2. Dans la fenêtre qui s'ouvre, sélectionnez le coffre-fort dans la liste, puis cliquez sur le bouton **Ouvrir**.

     Le coffre-fort s'ouvrira dans la fenêtre de l'Assistant Microsoft Windows.
  3. Enregistrez dans le coffre-fort les données qui doivent être cryptées.
  4. Dans la fenêtre **Mes Coffres-forts**, cliquez sur le bouton **Chiffrer les données**.

- *Pour pouvoir accéder aux données du coffre-fort, procédez comme suit.*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Coffre-fort**.
  2. Dans la fenêtre qui s'ouvre, sélectionnez le coffre-fort dans la liste, puis cliquez sur le bouton **Déchiffrer les données**.
  3. Dans la qui s'ouvre, saisissez le mot de passe d'accès au coffre-fort.
  4. Dans la fenêtre **Mes Coffres-forts**, cliquez sur le bouton **Ouvrir**.

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

Si vous pensez que l'objet est infecté par un virus, analysez-le d'abord à l'aide de Kaspersky PURE (cf. rubrique "Procédure d'analyse d'un objet distinct (fichier, dossier, disque)" à la page 66).

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

- Placer l'objet en *quarantaine*. Les objets placés en quarantaine ne constituent aucune menace pour votre ordinateur. Il se peut, après la mise à jour des bases, que Kaspersky PURE puisse identifier la menace et la supprimer.

- Envoyer l'objet au *Laboratoire d'étude des virus*. Les experts du laboratoire d'étude des virus étudieront l'objet pour voir s'il est vraiment infecté par un virus et ajouteront sur le champ la description du nouveau virus aux bases qui seront chargées par l'application lors de la mise à jour (cf. rubrique "Procédure de mise à jour des bases et des modules de l'application" à la page 64).

Un objet peut être placé en quarantaine de deux manières :

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

- Via le menu contextuel de l'objet.

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

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

2. Cliquez sur le lien **Quarantaine** situé dans la partie supérieure de la fenêtre qui s'ouvre pour ouvrir la fenêtre **Etat de la protection**.

3. Sous l'onglet **Menaces détectées**, cliquez sur le lien **Mettre en quarantaine**.

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

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

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

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

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

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

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

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

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

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

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

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Protection de l'ordinateur**.
2. Cliquez sur le lien **Quarantaine** situé dans la partie supérieure de la fenêtre qui s'ouvre pour ouvrir la fenêtre **Etat de la protection**.
3. Dans la liste déroulante située au-dessus de la liste des menaces de l'onglet **Menaces détectées**, choisissez l'élément **Neutralisées**.

   La liste des objets modifiés et réparés apparaît sous l'onglet **Menaces détectées**. Les objets sont regroupés par état. Pour afficher la liste des objets figurant dans un groupe, cliquez sur le bouton **+** situé à gauche du titre du groupe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'objet qu'il faut restaurer et choisissez l'option **Restaurer**.

QUE FAIRE SI VOUS PENSEZ QUE VOTRE ORDINATEUR EST INFECTE

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

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

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

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

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

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mes outils d'optimisation**.
2. Dans la fenêtre **Mes Outils d'optimisation** qui s'ouvre, cliquez sur le bouton **Réparation du système**.

Examinons en détails les étapes de l'Assistant.

Etape 1. Lancement de la restauration du système

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

Etape 2. Recherche des problèmes

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

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

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

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

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

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

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

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

Etape 4. Suppression des problèmes

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

Etape 5. Fin de l'Assistant

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

COPIE DE SAUVEGARDE DES DONNEES

La création de copies de sauvegarde en temps opportuns constitue la principale mesure de protection contre la perte de données importantes. Kaspersky PURE permet de réaliser automatiquement des copies de sauvegarde des données sélectionnées dans l'espace de sauvegarde choisi selon un horaire défini. Vous pouvez également réaliser la sauvegarde de manière ponctuelle.

Pour commencer, il faut créer l'espace de sauvegarde de copies de sauvegarde sur le disque sélectionné. C'est dans ce référentiel que les données de sauvegarde des fichiers requis seront créées. Il sera ensuite possible de configurer la

tâche de copie de sauvegarde (sélectionner les fichiers dont une copie de sauvegarde doit absolument être créée, programmer l'exécution automatique du lancement et configurer d'autres conditions de la copie).

Pour créer l'espace de sauvegarde de copies de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Espace de sauvegarde** et cliquez sur le bouton **Créer**.
3. Cette action lance l'Assistant de création de l'espace de sauvegarde de copies de sauvegarde. Voici, en détails, les étapes de l'Assistant :
   a. Sélectionnez le type de support qui sera utilisé pour le stockage dans la partie gauche de la fenêtre **Disque**.

      Pour la sécurité des données, il est conseillé de créer des stockages de données de sauvegarde sur des disques amovibles.

   b. Définissez un mot de passe pour protéger les données contre l'accès non autorisé dans la fenêtre **Protection** (le cas échéant).
   c. Limitez le nombre de version des fichiers qui seront présentes simultanément dans l'espace de sauvegarde ainsi que la durée de conservation des copies dans la fenêtre **Versions des fichiers** (le cas échéant).
   d. Saisissez le nom du nouveau référentiel et confirmez la création selon les paramètres définis dans la fenêtre **Résumé**.

Pour réaliser la sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Mes Sauvegardes** puis cliquez sur le bouton **Créer**.
3. L'Assistant de création d'une tâche de copie de sauvegarde est lancé. Voici, en détails, les étapes de l'Assistant :
   a. Dans la fenêtre **Contenu**, sélectionnez les objets pour lesquels les copies de sauvegarde seront créées.
   b. Dans la fenêtre **Stockage**, sélectionnez l'espace de sauvegarde dans lequel les copies de sauvegarde seront créées.
   c. Dans la fenêtre **Planification**, définissez les conditions d'exécution de la tâche.

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

   d. Saisissez le nom de la nouvelle tâche, puis cliquez sur le bouton **Terminer** dans la fenêtre **Résumé**.

Pour restaurer les données de la copie de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Restauration des données**.
3. Sélectionnez l'espace de sauvegarde qui abrite les copies de sauvegarde requises, puis cliquez sur le bouton **Restaurer les données**.
4. Dans la partie supérieure de la fenêtre **Restauration des données depuis la sauvegarde** sélectionnez l'archive dans la liste déroulante (ensemble de données conservées lors de l'exécution d'une tâche).

5. Sélectionnez les fichiers à restaurer. Pour ce faire, cochez la case en regard des fichiers requis. Pour sélectionner toutes les archives, cliquez sur le bouton **Tout sélectionner** en bas de la liste. Cliquez sur le bouton **Restaurer** dans la partie supérieure de la fenêtre.

6. Dans la fenêtre **Restauration** qui s'ouvre, sélectionnez l'emplacement de sauvegarde des fichiers à restaurer ainsi que la condition de conservation en cas d'équivalence des noms. Cliquez sur le bouton **Restaurer**.

   Les versions les plus récentes des fichiers sélectionnés seront restaurées.

COMMENT RESTREINDRE L'ACCES AUX PARAMETRES DE KASPERSKY PURE

Il se peut que l'ordinateur soit utilisé par plusieurs personnes possédant un niveau différent de maîtrise de l'informatique. L'accès illimité des utilisateurs à Kaspersky PURE et à ses paramètres peut entraîner une réduction du niveau de la protection de l'ordinateur dans son ensemble.

Pour limiter l'accès à l'application, vous pouvez définir un mot de passe et désigner les actions pour lesquelles il devra être saisi.

- modification des paramètres de fonctionnement de l'application ;
- administration de Mes Sauvegardes ;
- administration de Mon Contrôle Parental ;
- administration de la sécurité de Mon Réseau ;
- arrêt de l'application ;

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la rubrique **Mot de passe d'administrateur**, choisissez la sous-rubrique **Paramètres généraux**.
4. Dans la partie droite de la fenêtre, cochez la case **Activer la protection par mot de passe** dans le groupe **Protection par mot de passe** et remplissez les champs **Nouveau mot de passe** et **Confirmation du mot de passe**.
5. Dans le groupe **Zone d'action du mot de passe**, indiquez la zone qui sera soumise aux restrictions d'accès. Désormais, chaque fois qu'un utilisateur de votre ordinateur tentera d'exécuter les actions de Kaspersky PURE que vous avez sélectionnées, il devra saisir le mot de passe.

Pour modifier le mot de passe d'accès à Kaspersky PURE, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la rubrique **Mot de passe d'administrateur**, choisissez la sous-rubrique **Paramètres généraux**.
4. Dans la partie droite de la fenêtre, dans le groupe **Protection par mot de passe**, remplissez les champs **Ancien mot de passe**, **Nouveau mot de passe** et **Confirmation du mot de passe**.

COMMENT RESTREINDRE L'UTILISATION DE L'ORDINATEUR ET D'INTERNET POUR DIFFERENTS COMPTES UTILISATEUR

Directement après l'installation de Kaspersky PURE, aucune restriction n'est définie pour les utilisateurs de l'ordinateur. Afin de protéger les enfants et les adolescents contre les menaces liées à l'utilisation des ordinateurs et d'Internet, il faudra définir les paramètres de Mon Contrôle Parental pour tous les utilisateurs de l'ordinateur.

Si vous n'avez pas activé la protection par mot de passe lors de l'installation de l'application (cf. la rubrique "Etape 16. Restriction de l'accès à l'application" à la page 34), alors il est conseillé, au premier lancement de Contrôle Parental, de définir un mot de passe pour éviter les modifications non autorisées des paramètres du contrôle. Ensuite, vous pouvez activer Mon Contrôle Parental et configurer les restrictions d'utilisation de l'ordinateur et d'Internet pour tous les comptes utilisateur de l'ordinateur.

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

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Activer**.
4. Sélectionnez le compte utilisateur dans la liste des comptes pour lequel il convient de configurer les paramètres du contrôle puis cliquez sur le bouton **Configurer**.
5. Dans la partie gauche de la fenêtre qui s'ouvre, sélectionnez le type de restriction et définissez les paramètres du contrôle dans la partie droite de la fenêtre.

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

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

DANS CETTE SECTION

Création d'un disque de dépannage 78

Démarrage de l'ordinateur à l'aide du disque de dépannage 80

CREATION D'UN DISQUE DE DEPANNAGE

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

L'image du disque de départ, en fonction de laquelle le nouveau fichier est généré, peut être téléchargée du serveur de Kaspersky Lab, ou copiée depuis une source locale.

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

- Sous Microsoft Windows XP dans le dossier : Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP9\Data\Rdisk\ ;

- Sous Microsoft Windows Vista et Microsoft Windows 7 dans le dossier : ProgramData\Kaspersky Lab\AVP9\Data\Rdisk\.

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

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

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mes Outils d'optimisation**.

2. Dans la fenêtre **Mes outils d'optimisation** qui s'ouvre, cliquez sur le bouton **Disque de dépannage**.

Examinons en détails les étapes de l'Assistant.

Etape 1. Sélection de la source de l'image du disque

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

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

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

Etape 2. Copie (téléchargement) de l'image du disque

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

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

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

Etape 3. Mise à jour de l'image du disque

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

- la mise à jour des bases antivirus;

- la mise à jour des fichiers de configuration.

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

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

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

Etape 4. Fin de l'Assistant

Pour quitter l'Assistant, cliquez sur **Terminer**. Le fichier .iso obtenu peut être enregistré sur un CD/DVD et être utilisé pour le chargement ultérieur de l'ordinateur.

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

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

Le chargement du système d'exploitation requiert le CD-/DVD- contenant le fichier d'image de disque (iso) de dépannage.

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

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

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

QUE FAIRE AVEC UN GRAND NOMBRE DE MESSAGES NON SOLLICITES

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

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, cochez la case **Activer l'Anti-Spam**.
5. Dans le groupe **Niveau de protection**, le niveau de protection par défaut doit être **Recommandé**.

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

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

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

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

Examinons en détails les étapes de l'Assistant.

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

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

Etape 2. Sélection des répertoires contenant le courrier normal

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

Pour une sélection de Seulement les dossiers des comptes Microsoft Office Outlook et Microsoft Outlook Express (Windows Mail) sont accessibles.

Etape 3. Sélection des répertoires contenant le courrier indésirable

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

Pour une sélection de Seulement les dossiers des comptes Microsoft Office Outlook et Microsoft Outlook Express (Windows Mail) sont accessibles.

Etape 4. Entraînement d'Anti-Spam

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

Etape 5. Enregistrement des résultats de l'entraînement

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

- Ajouter les résultats de l'apprentissage à la base existante de l'Anti-Spam (choisissez l'option **Ajouter les résultats de l'apprentissage à la base existante de l'Anti-Spam**) ;

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

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

CONSULTATION DU RAPPORT SUR LA PROTECTION DE L'ORDINATEUR

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

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

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

   La fenêtre **Ma Protection** s'ouvre.

2. Le lien **Rapport** permet d'accéder à la fenêtre des rapports de Kaspersky PURE.

   Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** affiche les rapports sur l'utilisation de l'application sous la forme de diagrammes.

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

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

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

Vous pouvez toujours revenir aux paramètres recommandés de Kaspersky PURE. Ces paramètres sont les paramètres optimaux recommandés par les experts de Kaspersky Lab. La restauration des paramètres est exécutée par l'Assistant de configuration initiale de l'application.

Dans la fenêtre qui s'affiche, vous aurez la possibilité de définir les paramètres et les composants pour lesquels vous souhaitez les conserver ou non en plus de la restauration du niveau de protection recommandé.

La liste propose les composants de Kaspersky PURE dont les paramètres ont été modifiés par l'utilisateur ou assimilés par Kaspersky PURE durant l'entraînement des composants Pare-feu et Anti-Spam. Si des paramètres uniques ont été définis pour un composant quelconque, ils figureront également dans la liste.

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

Ces listes sont constituées pendant l'utilisation de Kaspersky PURE et tiennent compte des tâches individuelles et de l'exigence de sécurité. La constitution de telles listes prend en général beaucoup de temps et pour cette raison, nous vous recommandons de les conserver en cas de rétablissements des paramètres du programme à leur valeur d'origine.

Lorsque vous aurez quitté l'Assistant, tous les composants de la protection fonctionneront selon le niveau **Recommandé** et tiendront compte des paramètres que vous avez décidés de conserver lors de la restauration. De plus, les paramètres définis à l'aide de l'Assistant seront appliqués.

Pour restaurer les paramètres de protection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Général** dans la rubrique **Paramètres avancés**.

4. Dans la partie droite de la fenêtre, cliquez sur le bouton **Restaurer**.

5. Dans la fenêtre qui s'affiche, cliquez sur le bouton **Suivant**. Cette action entraîne le lancement de l'Assistant de configuration. Suivez les instructions affichées.

TRANSFERT DES PARAMETRES DE L'APPLICATION SUR UN AUTRE ORDINATEUR

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

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

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

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

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

Pour exporter les paramètres actuels de fonctionnement de Kaspersky PURE, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Général** dans la rubrique **Paramètres avancés**.

4. Dans la partie droite de la fenêtre, cliquez sur le bouton **Enregistrer**.

5. Saisissez le nom du fichier de configuration et précisez l'emplacement de la sauvegarde.

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

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Général** dans la rubrique **Paramètres avancés**.

4. Dans la partie droite de la fenêtre, cliquez sur le bouton **Télécharger**.

5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier à utiliser pour importer les paramètres de Kaspersky PURE.

CONFIGURATION ETENDUE DE L'APPLICATION

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

DANS CETTE SECTION

Protection de l'ordinateur 85

Mes Sauvegardes 170

Mon Contrôle Parental 177

Mes Coffres-forts 187

Mon Réseau 191

Mon Gestionnaire de mots de passe 196

Performances et compatibilité avec d'autres applications 229

Autodéfense de Kaspersky PURE 231

Apparence de l'application 233

Mes Outils d'optimisation 235

Rapports 241

Notifications 246

Participation au Kaspersky Security Network 248

PROTECTION DE L'ORDINATEUR

Les composants de la protection de l'ordinateur protège votre ordinateur contre diverses menaces, recherche la présence éventuelle de virus et de vulnérabilités dans les objets du système et assure la mise à jour des bases antivirus et des modules de l'application Kaspersky PURE.

DANS CETTE SECTION

Analyse de l'ordinateur 85

Mise à jour 93

Antivirus Fichiers 99

Antivirus Courrier 106

Antivirus Internet 111

Antivirus IM 117

Anti-Spam 119

Anti-bannière 136

Contrôle des Applications 139

Défense Proactive 147

Protection du réseau 149

Zone de confiance 161

Exécution des applications en environnement protégé 163

Quarantaine et dossier de sauvegarde 167

ANALYSE DE L'ORDINATEUR

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

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

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

DANS CETTE SECTION

Recherche de virus 86

Recherche de vulnérabilités 93

RECHERCHE DE VIRUS

Kaspersky PURE propose les tâches suivantes pour la recherche de virus :

- **Analyse des Objets**. Les objets sélectionnés par l'utilisateur sont analysés. L'analyse peut porter sur n'import quel objet du système de fichiers de l'ordinateur. Dans le cadre de cette tâche, vous pouvez configurer l'analyse des disques amovibles.
- **Analyse complète**. Analyse minutieuse de tout le système. Les objets suivants sont analysés par défaut : mémoire système, objets chargés au démarrage du système, sauvegarde, bases de messagerie, disques durs, disques de réseau et disques amovibles.
- **Analyse rapide**. L'analyse porte sur les objets chargés au démarrage du système d'exploitation.

Pour la tâche d'analyse complète et la tâche d'analyse express, il est déconseillé de modifier la liste des objets à analyser.

Chaque tâche d'analyse est exécutée dans une zone définie et peut être lancée selon un horaire défini. De plus, chaque tâche d'analyse se distingue par un niveau de protection (ensemble de paramètres qui exercent une influence sur le rapport entre performances et protection). Le mode de recherche des menaces à l'aide des signatures des bases de l'application est toujours activé par défaut. De plus, il est possible d'impliquer diverses méthodes et technologies (cf. page 90) d'analyse.

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

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

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

Ensuite, l'application affiche une notification (cf. page 246) sur la menace détectée et exécute l'action définie. Vous pouvez modifier l'action exécutée après la découverte d'une menace.

Si vous travaillez en mode automatique (cf. rubrique "Utilisation du mode de protection interactif" à la page 60), Kaspersky PURE appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants, il s'agit de l'action **Réparer. Supprimer, si la réparation est impossible**, pour les objets suspects : **Mettre en quarantaine**. Si vous utilisez le mode interactif (cf. rubrique "Utilisation du mode de protection interactif" à la page 60), l'application affiche un message après la découverte d'un objet dangereux et vous permet de choisir l'action à exécuter parmi la liste des actions proposées.

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

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

DANS CETTE SECTION

Modification et restauration du niveau de protection 87

Programmation de l'exécution de l'analyse 88

Composition de la liste des objets à analyser 88

Sélection de la méthode d'analyse 89

Sélection de la technologie d'analyse 90

Modification de l'action à exécuter après la découverte d'une menace 90

Lancement de l'analyse sous les privilèges d'un autre utilisateur 90

Modification du type d'objets à analyser 90

Analyse des fichiers composés 91

Optimisation de l'analyse 92

Analyse des disques amovibles à la connexion 92

Création d'un raccourci pour le lancement d'une tâche 93

MODIFICATION ET RESTAURATION DU NIVEAU DE PROTECTION

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

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

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

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

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

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

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

PROGRAMMATION DE L'EXECUTION DE L'ANALYSE

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

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

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

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

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

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

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

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

COMPOSITION DE LA LISTE DES OBJETS A ANALYSER

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

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

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

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

   La fenêtre **Ma Protection** s'ouvre.

2. Dans la partie gauche de la fenêtre, sélectionnez la section **Analyse**.

3. Dans la partie droite de la fenêtre, cliquez sur le lien **Ajouter** afin d'ouvrir la liste des objets à analyser.

4. Dans la fenêtre **Sélection de l'objet à analyser** qui s'ouvre, sélectionnez l'objet et cliquez sur le bouton **Ajouter**. Une fois que vous aurez ajouté tous les objets requis, cliquez sur le bouton **OK**. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

- *Pour former la liste des objets pour la tâche d'analyse complète, d'analyse rapide ou de recherche de vulnérabilités, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Recherche de vulnérabilités**).

4. Pour la tâche sélectionnée, dans le groupe **Objets à analyser**, cliquez sur le bouton **Configuration**.

5. Dans la fenêtre ouverte **Objets à analyser**, à l'aide des liens **Ajouter**, **Modifier**, **Supprimer** formez la liste. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

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

SELECTION DE LA METHODE D'ANALYSE

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

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

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

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

4. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.

5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Méthodes d'analyse**, définissez les paramètres requis.

SELECTION DE LA TECHNOLOGIE D'ANALYSE

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

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).
4. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
5. Dans la fenêtre qui s'ouvre, sélectionnez la valeur des paramètres souhaitée dans le groupe **Technologies d'analyse** de l'onglet **Avancé**.

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

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

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).
4. Pour la tâche sélectionnée, dans le groupe **Action**, désignez l'action requise.

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

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

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

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

MODIFICATION DU TYPE D'OBJETS A ANALYSER

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

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

- La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple txt) et son activation ultérieure est relativement faible. Mais il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, exe, dll, doc). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est assez élevé.

- Un individu malintentionné peut envoyer un virus sur votre ordinateur dans un fichier exécutable renommé en fichier txt. Si vous avez sélectionné l'analyse des fichiers selon l'extension, ce fichier sera ignoré lors de l'analyse. Si vous avez choisi l'analyse des fichiers selon le format, alors l'Antivirus Fichiers analysera l'en-tête du fichier, quelle que soit l'extension, et identifiera le fichier comme étant au format exe. Le fichier sera alors soumis à une analyse antivirus minutieuse.

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

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

ANALYSE DES FICHIERS COMPOSES

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

Pour chaque type de fichier composé, vous pouvez décider d'analyser tous les fichiers ou uniquement les nouveaux. Pour réaliser la sélection, cliquez sur le lien situé à côté du nom de l'objet. Il change de valeur lorsque vous appuyez sur le bouton gauche de la souris. Si le mode d'analyse uniquement des nouveaux fichiers ou des fichiers modifiés (cf. page 92) est sélectionné, les liens pour la sélection de l'analyse de tous les fichiers ou des nouveaux fichiers uniquement seront inaccessibles.

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

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

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

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).

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

5. Dans la fenêtre qui s'ouvre, cliquez sur **Avancé** dans le groupe **Analyse des fichiers composés** de l'onglet **Zone d'action**.

6. Dans la fenêtre **Fichiers composés** qui s'ouvre, cochez la case **Ne pas décompacter les fichiers composés de grande taille** et définissez la taille maximale des fichiers à analyser.

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

OPTIMISATION DE L'ANALYSE

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

Il est également possible de limiter la durée de l'analyse d'un objet. A l'issue du temps défini, l'objet sera exclu de l'analyse en cours (sauf les archives et les fichiers incluant quelques objets).

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

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

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

5. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Optimisation de l'analyse**, cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

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

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

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

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

ANALYSE DES DISQUES AMOVIBLES A LA CONNEXION

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

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

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dans la rubrique **Analyse de l'ordinateur**, choisissez la sous-rubrique **Paramètres généraux**.

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

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

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

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

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dans la rubrique **Analyse de l'ordinateur**, choisissez la sous-rubrique **Paramètres généraux**.

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

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

RECHERCHE DE VULNERABILITES

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

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

Une fois que la tâche de recherche des vulnérabilités (cf. page 67) a été lancée, vous pouvez suivre sa progression dans le champ **Fin** de la fenêtre **Recherche de Vulnérabilités**. Les vulnérabilités identifiées dans le système et dans les applications à la suite de l'analyse figurent dans cette même fenêtre sous les onglets **Vulnérabilités du système** et **Applications vulnérables**.

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

Tout comme pour les tâches de recherche de virus, il est possible de programmer l'exécution de recherche de vulnérabilités, de composer la liste des objets à analyser (cf. page 88), de sélectionner le compte utilisateur (cf. rubrique "Lancement de l'analyse sous les privilèges d'un autre utilisateur" à la page 90) et de créer un raccourci pour l'exécution rapide de la tâche. Par défaut, les applications installées sont choisies en guise d'objets à analyser.

MISE A JOUR

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

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

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

- Bases de Kaspersky PURE.

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

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

- Modules logiciels.

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

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

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

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

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

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

Avant d'actualiser les bases, Kaspersky Internet Security crée une copie de sauvegarde au cas où vous souhaiteriez utiliser à nouveau les bases de la version antérieure (cf. rubrique "Annulation de la dernière mise à jour" à la page 97).

Les informations relatives à l'état actuel des bases de Kaspersky PURE figurent dans la rubrique **Mise à jour** de la fenêtre **Ma Protection de l'ordinateur**.

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

DANS CETTE SECTION

Sélection de la source de mises à jour 95

Programmation de l'exécution de la mise à jour 96

Annulation de la dernière mise à jour 97

Analyse de la quarantaine après la mise à jour 98

Utilisation du serveur proxy 98

Lancement de la mise à jour avec les privilèges d'un autre utilisateur 99

SELECTION DE LA SOURCE DE MISES A JOUR

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

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

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

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

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

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

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** la sous-rubrique **Paramètres de la mise à jour**.
4. Dans la partie droite de la fenêtre, dans le groupe **Source des mises à jour**, cliquez sur **Configuration**.
5. Sous l'onglet **Source** de la fenêtre qui s'ouvre, cliquez sur le lien **Ajouter** pour ouvrir la fenêtre **Sélection de la source des mises à jour**.
6. Dans le champ **Source**, sélectionnez le dossier qui contient les mises à jour ou saisissez l'adresse du serveur d'où les mises à jour seront téléchargées.

DANS CETTE SECTION

Sélection de la région du serveur de mises à jour 95

Mise à jour depuis un dossier partagé 96

SELECTION DE LA REGION DU SERVEUR DE MISES A JOUR

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

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

Pour choisir la région du serveur, procédez comme suit :

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

MISE A JOUR DEPUIS UN DOSSIER PARTAGE

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

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** la sous-rubrique **Paramètres de la mise à jour**.
4. Dans le groupe **Avancé** de la partie droite de la fenêtre, cochez la case **Copier la mise à jour des bases dans le dossier** et dans le champ du dessous, saisissez le chemin d'accès au dossier partagé qui héberge les mises à jour récupérées. Vous pouvez également choisir le dossier en cliquant sur le bouton **Parcourir**.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** la sous-rubrique **Paramètres de la mise à jour**.
4. Dans la partie droite de la fenêtre, dans le groupe **Source des mises à jour**, cliquez sur **Configuration**.
5. Sous l'onglet **Source** de la fenêtre qui s'ouvre, cliquez sur le lien **Ajouter** pour ouvrir la fenêtre **Sélection de la source des mises à jour**.
6. Sélectionnez le dossier ou saisissez le chemin d'accès complet dans le champ **Source**.
7. Sous l'onglet **Source**, désélectionnez la case **Serveurs de mise à jour de Kaspersky Lab**.

PROGRAMMATION DE L'EXECUTION DE LA MISE A JOUR

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

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

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

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** la sous-rubrique **Paramètres de la mise à jour**.
4. Dans la partie droite de la fenêtre, dans le groupe **Mode d'exécution**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution** dans le groupe **Programmation**, choisissez l'option **Selon la programmation**, puis configurez le mode d'exécution de la mise à jour.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** la sous-rubrique **Paramètres de la mise à jour**.
4. Dans la partie droite de la fenêtre, dans le groupe **Mode d'exécution**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Programmation**, choisissez l'option **Selon la programmation**, puis cochez la case **Lancer les tâches non exécutées**.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** la sous-rubrique **Paramètres de la mise à jour**.
4. Dans la partie droite de la fenêtre, dans le groupe **Mode d'exécution**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution** dans le groupe **Programmation**, choisissez l'option **Selon la programmation**, puis indiquez la durée du report dans le champ **Intervalle entre le lancement et le démarrage de l'application**.

ANNULATION DE LA DERNIERE MISE A JOUR

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

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

Si les bases sont endommagées, Kaspersky PURE recommande de lancer la tâche de mise à jour pour télécharger l'ensemble actuel des bases pour la protection actuelle.

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

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

   La fenêtre **Ma Protection** s'ouvre.

2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Restaurer les mises à jour précédentes**.

ANALYSE DE LA QUARANTAINE APRES LA MISE A JOUR

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

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

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

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** la sous-rubrique **Paramètres de la mise à jour**.

4. Dans le groupe **Avancé** de la partie droite de la fenêtre, cochez la case **Analyser les fichiers en quarantaine après mise à jour**.

UTILISATION DU SERVEUR PROXY

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

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

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** la sous-rubrique **Paramètres de la mise à jour**.

4. Dans la partie droite de la fenêtre, dans le groupe **Source des mises à jour**, cliquez sur **Configuration**.

5. Dans la fenêtre qui s'ouvre, sous l'onglet **Source**, cliquez sur le lien **Serveur proxy**.

6. Dans la fenêtre **Paramètres du serveur proxy** qui s'ouvre, configurez les paramètres du serveur proxy.

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

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

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

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

ANTIVIRUS FICHIERS

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

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

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Fichier. Dans la majorité des cas, il suffit de changer le niveau de protection.

Quand l'analyse du système de fichiers doit être temporairement désactivée, vous pouvez configurer la suspension automatique de l'Antivirus Fichiers, voire désactivé le composant le cas échéant.

Vous pouvez composer une zone de protection et sélectionner le mode d'analyse des objets.

Le mode de recherche des menaces à l'aide des signatures des bases de l'application est toujours activé par défaut. De plus, il est possible d'utiliser également l'analyse heuristique (cf. page 103) et diverses technologies d'analyse (cf. page 104).

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

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

Ensuite, l'application affiche une notification (cf. page 246) sur la menace détectée et exécute l'action définie. Vous pouvez modifier l'action exécutée après la découverte d'une menace.

Si vous travaillez en mode automatique (cf. rubrique "Utilisation du mode de protection interactif" à la page 60), Kaspersky PURE appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants, il s'agit de l'action **Réparer. Supprimer, si la réparation est impossible**, pour les objets suspects : **Mettre en quarantaine**. Si vous utilisez le mode interactif (cf. rubrique "Utilisation du mode de protection interactif" à la page 60), l'application affiche un message après la découverte d'un objet dangereux et vous permet de choisir l'action à exécuter parmi la liste des actions proposées.

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

DANS CETTE SECTION

Activation et désactivation de l'Antivirus Fichiers 100

Arrêt automatique de l'Antivirus Fichiers 101

Constitution de la zone de protection 101

Modification et restauration du niveau de protection 102

Modification du mode d'analyse 103

Utilisation de l'analyse heuristique 103

Technologie d'analyse 104

Modification de l'action à réaliser sur les objets découverts 104

Analyse des fichiers composés 104

Optimisation de l'analyse 105

ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS FICHIERS

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

Pour activer ou désactiver l'Antivirus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, décochez la case **Activer l'Antivirus Fichier** s'il faut désactiver le composant. Cochez cette case s'il faut activer le composant.

ARRET AUTOMATIQUE DE L'ANTIVIRUS FICHIERS

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

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

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Suspension de la tâche**, cochez la case **Selon la programmation**, puis cliquez sur **Programmation**.
6. Dans la fenêtre **Suspension de la tâche**, indiquez la durée (au format hh:mm) pendant laquelle la protection sera suspendue (champs **Pause à partir de** et **Reprendre à**).

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Suspension de la tâche**, cochez la case **Au lancement des applications** puis cliquez sur **Liste**.
6. Dans la fenêtre **Applications**, composez la liste des applications pendant l'utilisation desquelles le composant sera suspendu.

CONSTITUTION DE LA ZONE DE PROTECTION

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

Vous pouvez élargir ou restreindre la zone de protection en ajoutant ou en supprimant des objets ou en modifiant le type de fichiers à analyser. Par exemple, vous pouvez décider d'analyser uniquement les fichiers exe exécutés depuis des disques de réseau.

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

- La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple txt) et son activation ultérieure est relativement faible. Mais il existe également des formats de fichier qui contiennent ou

qui pourraient contenir un code exécutable (par exemple, exe, dll, doc). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est assez élevé.

- Un individu malintentionné peut envoyer un virus sur votre ordinateur dans un fichier exécutable renommé en fichier txt. Si vous avez sélectionné l'analyse des fichiers selon l'extension, ce fichier sera ignoré lors de l'analyse. Si vous avez choisi l'analyse des fichiers selon le format, alors l'Antivirus Fichiers analysera l'en-tête du fichier, quelle que soit l'extension, et identifiera le fichier comme étant au format exe. Le fichier sera alors soumis à une analyse antivirus minutieuse.

Afin de modifier la liste des objets à analyser, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, dans le groupe **Zone de protection** de l'onglet **Général**, ouvrez la fenêtre de sélection des objets en cliquant sur le lien **Ajouter**.
6. Dans la fenêtre **Sélection de l'objet à analyser**, sélectionnez l'objet et cliquez sur le bouton **Ajouter**.
7. Après avoir ajouté tous les fichiers requis, cliquez sur **OK** dans la fenêtre **Sélection de l'objet à analyser**.
8. Pour exclure un objet de la liste, désélectionnez la case située en regard de celui-ci.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le bloc **Type de fichiers**, sélectionnez le paramètre requis.

MODIFICATION ET RESTAURATION DU NIVEAU DE PROTECTION

En fonction des besoins actuels, vous pourrez choisir un des niveaux de protection prédéfinis pour les fichiers ou la mémoire ou configurer vous-même les paramètres de fonctionnement de l'Antivirus Fichiers.

Sachez que si vous configurez les paramètres de fonctionnement du composant, vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des valeurs optimales recommandées par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Avant d'activer le niveau de protection bas pour les fichiers, il est conseillé de lancer une analyse complète de l'ordinateur (cf. rubrique "Procédure d'exécution d'une analyse complète de l'ordinateur" à la page 67) au niveau de protection élevé.

Pour modifier le niveau de protection défini des fichiers et de la mémoire, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.

4. Dans le groupe **Niveau de protection** de la partie droite de la fenêtre, sélectionnez le niveau de protection requis ou cliquez sur le bouton **Configuration** afin de définir manuellement les paramètres d'analyse.

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

Pour restaurer les paramètres de protection par défaut, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Par défaut**.

MODIFICATION DU MODE D'ANALYSE

Le mode d'analyse désigne la condition de déclenchement de l'Antivirus Fichiers. Kaspersky PURE utilise par défaut le mode intelligent dans lequel la décision d'analyser un objet est prise sur la base des opérations exécutées avec celui-ci. Par exemple, dans le cas d'un fichier Microsoft Office, Kaspersky PURE analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires sur le fichier sont exclues de l'analyse.

Vous pouvez modifier le mode d'analyse des objets. La sélection du mode dépend du type de fichiers que vous manipulez le plus souvent.

Afin de modifier le mode d'analyse des objets, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Mode d'analyse**, sélectionnez le mode requis.

UTILISATION DE L'ANALYSE HEURISTIQUE

L'Antivirus Fichiers utilise toujours l'*analyse sur la base des signatures* au cours de laquelle Kaspersky PURE compare l'objet trouvé aux signatures des bases.

Pour augmenter l'efficacité de la protection, vous pouvez utiliser *l'analyse heuristique* (analyse de l'activité de l'objet dans le système). Cette analyse permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases.

Pour activer ou désactiver l'utilisation de l'analyse heuristique, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.

5. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance** dans le groupe **Méthode d'analyse**, cochez la case **Analyse heuristique** et définissez le niveau de détail de l'analyse. Décochez la case **Analyse heuristique** s'il n'est pas nécessaire d'utiliser ce mode d'analyse.

TECHNOLOGIE D'ANALYSE

En plus de l'analyse heuristique, vous pouvez faire intervenir des technologies spéciales qui permettent d'optimiser la vitesse de la recherche de virus en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Technologies d'analyse**, définissez les paramètres requis.

MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS DECOUVERTS

Quand l'application découvre des objets infectés ou potentiellement infectés, elle exécute une action en fonction du mode de fonctionnement sélectionné : automatique ou interactif (cf. rubrique "Antivirus Fichiers" à la page 99). Vous pouvez modifier l'action à exécuter.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Action**, sélectionnez l'option requise.

ANALYSE DES FICHIERS COMPOSES

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

Pour chaque type de fichier composé, vous pouvez décider d'analyser tous les fichiers ou uniquement les nouveaux.

Kaspersky PURE analyse par défaut uniquement les objets OLE joints. Les paquets d'installation et les fichiers qui contiennent des objets OLE sont exécutés à l'ouverture, ce qui les rend plus dangereux que des archives.

Lors de l'analyse de fichiers composés de grande taille, le décompactage préalable peut prendre un certain temps. Il est possible de réduire la durée en activant le décompactage en arrière plan des fichiers composés dont la taille dépasse la limite définie. Si un objet malveillant est découvert pendant l'utilisation de ces fichiers, Kaspersky PURE vous le signale.

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

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

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, dans le groupe **Analyse des fichiers composés** de l'onglet **Performance**, sélectionnez les types de fichiers composés à analyser.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, cliquez sur **Avancé** dans le groupe **Analyse des fichiers composés** de l'onglet **Performance**.
6. Dans la fenêtre **Fichiers composés**, cochez la case **Ne pas décompacter les fichiers composés de grande taille** et définissez la taille maximale des fichiers à analyser.

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

Pour décompacter les fichiers composés de grande taille en arrière plan, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, cliquez sur **Avancé** dans le groupe **Analyse des fichiers composés** de l'onglet **Performance**.
6. Dans la fenêtre **Fichiers composés**, cochez la case **Décompacter les fichiers composés en arrière-plan** et définissez la taille minimale du fichier dans le champ en dessous.

OPTIMISATION DE L'ANALYSE

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

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Fichiers**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.

5. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance**, dans le groupe **Optimisation de l'analyse**, cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

ANTIVIRUS COURRIER

L'Antivirus Courrier analyse le courrier entrant et sortant à la recherche d'objets dangereux. Il est lancé au démarrage du système d'exploitation, se trouve en permanence dans la mémoire vive de l'ordinateur et analyse tous les messages envoyés et reçus via les protocoles POP3, SMTP, IMAP, MAPI1 et NNTP ainsi que les messages envoyés via des connexions sécurisées (SSL) via les protocoles POP3 et IMAP (cf. section "Analyse des connexions sécurisées" à la page 157).

L'icône de Kaspersky Internet Security dans la zone de notification de la barre des tâches indique le fonctionnement du composant. Cette icône prend cette apparence chaque fois qu'un message est analysé.

Chaque message, reçu ou envoyé par l'utilisateur, est intercepté et décomposé entre ses différentes parties : en-tête du message, corps, pièce jointe. Le corps et la pièce jointe du message (y compris les objets OLE) sont soumis à la recherche de menaces.

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Courrier. Dans la majorité des cas, il suffit de sélectionner un autre niveau de protection (cf. rubrique "Modification et restauration du niveau de protection" à la page 108).

Vous pouvez désigner les types de message à analyser, ainsi que les modes d'analyse à utiliser. Le mode de recherche des menaces à l'aide des signatures des bases de l'application est toujours activé par défaut. Il est également possible d'utiliser l'analyse heuristique. De plus, vous pouvez activer le filtrage des pièces jointes (cf. page 109) qui permet de renommer automatiquement ou de supprimer les fichiers du type défini.

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

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

Ensuite, l'application affiche une notification (cf. page 246) sur la menace détectée et exécute l'action définie. Vous pouvez modifier l'action exécutée après la découverte d'une menace (cf. rubrique "Modification de l'action à réaliser sur les objets découverts" à la page 109).

Si vous travaillez en mode automatique (cf. rubrique "Utilisation du mode de protection interactif" à la page 60), Kaspersky PURE appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants, il s'agit de l'action **Réparer. Supprimer, si la réparation est impossible**, pour les objets suspects : **Mettre en quarantaine**. Si vous utilisez le mode interactif (cf. rubrique "Utilisation du mode de protection interactif" à la page 60), l'application affiche un message après la découverte d'un objet dangereux et vous permet de choisir l'action à exécuter parmi la liste des actions proposées.

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

Si la réparation réussit, l'utilisateur peut accéder au message. Dans le cas contraire, l'objet infecté est supprimé du message. Suite au traitement antivirus, un texte spécial est inclus dans l'objet du message. Ce texte indique que le message a été traité par Kaspersky PURE.

Le cas échéant, vous pouvez désactiver l'Antivirus Courrier (cf. rubrique "Activation et désactivation de l'Antivirus Courrier" à la page 107).

Un plug-in spécial (cf. section "Analyse du courrier dans Microsoft Office Outlook" à la page 110) qui permet de réaliser une configuration plus fine de l'analyse du courrier a été ajouté à Microsoft Office Outlook.

Si vous utilisez The Bat!, Kaspersky PURE peut être utilisé conjointement à d'autres logiciels antivirus. Dans ce cas, les règles de traitement du courrier (cf. section "Analyse du courrier dans The Bat!" à la page 111) sont définies directement dans The Bat! et prévalent sur les paramètres de protection du courrier de l'application.

S'agissant des autres clients de messagerie (dont Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail), l'Antivirus Courrier analyse le courrier entrant et sortant via les protocoles SMTP, POP3, IMAP et NNTP.

N'oubliez pas qu'en cas d'utilisation de client de messagerie Thunderbird, les messages transmis via le protocole IMAP ne sont pas soumis à l'analyse antivirus en cas d'utilisation de filtres triant les messages du dossier **Boîte aux lettres**.

DANS CETTE SECTION

Activation et désactivation de l'Antivirus Courrier 107

Constitution de la zone de protection 107

Modification et restauration du niveau de protection 108

Utilisation de l'analyse heuristique 109

Modification de l'action à réaliser sur les objets découverts 109

Filtrage des pièces jointes 109

Analyse des fichiers composés 110

Analyse du courrier dans Microsoft Office Outlook 110

Analyse du courrier dans The Bat! 111

ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS COURRIER

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

Pour activer ou désactiver l'Antivirus Courrier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Courrier**.
4. Dans la partie droite de la fenêtre, décochez la case **Activer l'Antivirus Courrier** s'il faut désactiver le composant. Cochez cette case s'il faut activer le composant.

CONSTITUTION DE LA ZONE DE PROTECTION

La zone de protection désigne les types de message qu'il faut analyser. Kaspersky PURE analyse par défaut aussi bien les messages entrant que les messages sortant.

Si vous avez choisi l'analyse uniquement des messages entrants, il est conseillé au tout début de l'utilisation de Kaspersky PURE d'analyser le courrier sortant car le risque existe que votre ordinateur abrite des vers de messagerie qui se propagent via le courrier électronique. Vous éviterez ainsi les inconvénients liés à la diffusion non contrôlée de messages infectés depuis votre ordinateur.

La zone de protection reprend également les paramètres d'intégration de l'Antivirus Courrier dans le système ainsi que les protocoles analysés. Par défaut, l'Antivirus Courrier s'intègre aux clients de messagerie Microsoft Office Outlook et The Bat!

Pour désactiver la protection du courrier sortant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Courrier**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, dans le groupe **Zone de protection** de l'onglet **Général**, sélectionnez l'option **Analyser uniquement le courrier entrant**.

Pour sélectionner les paramètres d'intégration de l'Antivirus Courrier au système ainsi que les protocoles à analyser, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Courrier**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. De groupe **Intégration au système** de l'onglet **Avancé** de la fenêtre qui s'ouvre, sélectionnez les paramètres requis.

MODIFICATION ET RESTAURATION DU NIVEAU DE PROTECTION

En fonction des besoins actuels, vous pourrez choisir un des niveaux de protection prédéfinis pour la protection du courrier ou configurer vous-même les paramètres de fonctionnement de l'Antivirus Courrier.

Sachez que si vous configurez les paramètres de fonctionnement du composant, vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des valeurs optimales recommandées par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Courrier**.
4. Dans le groupe **Niveau de protection** de la partie droite de la fenêtre, sélectionnez le niveau de protection requis ou cliquez sur le bouton **Configuration** afin de définir manuellement les paramètres d'analyse.

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

Pour restaurer les paramètres de protection du courrier par défaut, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Courrier**.

4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Par défaut**.

UTILISATION DE L'ANALYSE HEURISTIQUE

L'Antivirus Courrier utilise toujours l'*analyse sur la base des signatures* au cours de laquelle Kaspersky PURE compare l'objet trouvé aux signatures des bases.

Pour augmenter l'efficacité de la protection, vous pouvez utiliser *l'analyse heuristique* (analyse de l'activité de l'objet dans le système). Cette analyse permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases.

Pour activer ou désactiver l'utilisation de l'analyse heuristique, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Courrier**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Méthode d'analyse** cochez la case **Analyse heuristique** et définissez le niveau de détail de l'analyse. Décochez la case **Analyse heuristique** s'il n'est pas nécessaire d'utiliser ce mode d'analyse.

MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS DECOUVERTS

Quand l'application découvre des objets infectés ou potentiellement infectés, elle exécute une action en fonction du mode de fonctionnement sélectionné : automatique ou interactif (cf. rubrique "Antivirus Courrier" à la page 101). Vous pouvez modifier l'action à exécuter.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Courrier**.
4. Dans la partie droite de la fenêtre, dans le groupe **Action**, sélectionnez l'option requise.

FILTRAGE DES PIECES JOINTES

Bien souvent, les programmes malveillants sont diffusés par courrier sous la forme d'objets joints aux messages. Pour protéger l'ordinateur, par exemple, contre l'exécution automatique du fichier en pièce jointe, vous pouvez activer le filtrage des pièces jointes qui permet de renommer automatiquement ou de supprimer les fichiers du type défini.

Pour activer le filtrage des pièces jointes, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Courrier**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.

5. Dans la fenêtre qui s'ouvre, sous l'onglet **Filtre des pièces jointes**, sélectionnez le mode de filtrage des pièces jointes. Lorsque les deux derniers modes sont sélectionnés, la liste des types d'objet (extension) devient active. Elle vous permet de sélectionner les types requis ou d'ajouter un masque d'un nouveau type.

   Pour ajouter un masque d'un nouveau type à la liste, cliquez sur le lien **Ajouter** et ouvrez la fenêtre **Masque de nom de fichiers**, puis saisissez les données requises.

ANALYSE DES FICHIERS COMPOSES

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

Vous pouvez activer ou désactiver l'analyse des archives jointes et limiter la taille maximale des archives à analyser.

Si votre ordinateur n'est protégé par aucun moyen du réseau local (l'accès à Internet s'opère sans serveur proxy ou pare-feu), il est conseillé de ne pas désactiver l'analyse des archives en pièce jointe.

Pour configurer les paramètres d'analyse des fichiers composés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Antivirus Courrier**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, définissez les paramètres requis.

ANALYSE DU COURRIER DANS MICROSOFT OFFICE OUTLOOK

Si vous utilisez Microsoft Office Outlook, vous pouvez configurer des paramètres complémentaires pour la recherche de virus dans votre courrier.

Lors de l'installation de Kaspersky PURE, un plug-in spécial est intégré à Microsoft Office Outlook. Il permet de passer rapidement à la configuration des paramètres de l'Antivirus Courrier et de définir à quel moment la recherche d'éventuels objets dangereux sera lancée dans le message.

Le plug-in se présente sous la forme de l'onglet **Protection du courrier** situé dans le menu **Service** → **Paramètres**.

Pour choisir le moment auquel l'analyse du courrier aura lieu, procédez comme suit :

1. Ouvrez la fenêtre principale de Microsoft Office Outlook.
2. Dans le menu de l'application, choisissez l'option **Service** → **Paramètres**.
3. Sous l'onglet **Protection du courrier**, sélectionnez les paramètres requis.

ANALYSE DU COURRIER DANS THE BAT!

Les actions à réaliser sur les objets infectés des messages électroniques dans The Bat! sont définies par le programme en lui-même.

Les paramètres de l'Antivirus Courrier qui définissent l'analyse ou non du courrier entrant et sortant ainsi que les actions à réaliser sur les objets dangereux de messages et les exclusions sont ignorées. Le seul élément pris en considération par The Bat!, c'est l'analyse des archives jointes.

Les paramètres de la protection du courrier sont diffusés à tous les composants antivirus installés sur l'ordinateur compatibles avec The Bat!.

Il ne faut pas oublier que lors de la réception de messages, ceux-ci sont d'abord analysés par l'Antivirus Courrier, puis ensuite uniquement après par le plug-in du client de messagerie The Bat!. Kaspersky PURE signalera sans défaut la découverte d'un objet malveillant. Si dans la fenêtre de notification de l'Antivirus Courrier vous choisissez l'option **Réparer** (**Supprimer**), les actions liées à la suppression de la menace seront exécutées par l'Antivirus Courrier. Si vous choisissez **Ignorer**, alors l'objet sera neutralisé par le plug-in de The Bat!. Lors de l'envoi de courrier, les messages sont d'abord analysés par le plug-in puis par l'Antivirus Courrier.

Vous devez définir les critères suivants :

- Le flux de messagerie qui sera soumis à l'analyse (courrier entrant, sortant) ;
- Le moment où il faudra analyser les objets du message (à l'ouverture du message, avant l'enregistrement sur le disque) ;
- Les actions exécutées par le client de messagerie en cas de découverte d'objets dangereux dans les messages électroniques. Vous pouvez par exemple choisir :
  - **Tenter de réparer les parties infectées** : quand cette option est choisie, une tentative de réparation de l'objet sera lancée. Si elle échoue, l'objet restera dans le message.
  - **Supprimer les parties infectées** : quand cette option est choisi, l'objet dangereux du message sera supprimé, qu'il soit infecté ou potentiellement infecté.

Par défaut, tous les objets infectés des messages sont placés en quarantaine par The Bat! sans réparation.

Les messages électroniques qui contiennent des objets dangereux ne sont pas différenciés dans The Bat! par un titre spécial.

Pour configurer les paramètres de la protection du courrier dans The Bat!, procédez comme suit :

1. Ouvrez la fenêtre principale de The Bat!.
2. Dans le menu **Propriétés** du client de messagerie, sélectionnez l'option **Configuration**.
3. Dans l'arborescence des paramètres, choisissez l'objet **Protection contre les virus**.

ANTIVIRUS INTERNET

Chaque fois que vous utilisez Internet, vous exposez votre ordinateur et les données qu'il contient à un risque d'infection par des programmes dangereux. Ils peuvent s'infiltrer dans votre ordinateur tandis que vous téléchargez des programmes gratuits ou que vous consultez des informations sur des sites web apparemment inoffensifs, mais soumis à des attaques de pirates avant votre visite. De plus, les vers de réseau peuvent s'introduire sur votre ordinateur avant l'ouverture des pages Web ou le téléchargement d'un fichier, à savoir directement dès l'ouverture de la connexion Internet.

Le composant *Antivirus Internet* a été développé pour protéger votre ordinateur durant l'utilisation d'Internet. Il protège les informations reçues via les protocoles HTTP, HTTPS et FTP et empêche l'exécution des scripts dangereux.

La protection Internet prévoit le contrôle du flux de données qui transite uniquement via les ports indiqués dans la liste des ports contrôlés. La liste des ports le plus souvent utilisés pour le transfert de données est livrée avec Kaspersky PURE. Si vous utilisez des ports qui ne figurent pas dans cette liste, ajoutez-les à la liste des ports contrôlés (cf. rubrique "Composition de la liste des ports contrôlés" à la page 159) afin de garantir la protection du flux de données transitant par ceux-ci.

L'analyse du flux de données se déroule selon un ensemble défini de paramètres désigné sous le concept de niveau de protection (cf. rubrique "Modification et restauration du niveau de protection" à la page 113). Quand l'Antivirus Internet découvre une menace, il exécute l'action définie.

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Internet. Dans la majorité des cas, il suffit de sélectionner le niveau de protection qui convient.

Algorithme de fonctionnement du composant

L'Antivirus Internet protège les informations qui arrivent sur l'ordinateur et qui sont envoyées depuis celui-ci via les protocoles HTTP, HTTPS et FTP et empêche l'exécution de scripts dangereux sur l'ordinateur. Par défaut, l'analyse des connexions cryptées (via le protocole HTTPS) est désactivée. Vous pouvez l'activer et la configurer (cf. rubrique "Analyse des connexions cryptées" à la page 157).

La protection des données s'opère selon l'algorithme suivant :

1. Chaque page ou fichier qui reçoit une requête de l'utilisateur ou d'un programme quelconque via le protocole HTTP, HTTPS et FTP est intercepté et analysé par l'Antivirus Internet pour découvrir la présence éventuelle de code malveillant. L'identification des objets malveillants est réalisée à l'aide des bases utilisées par Kaspersky PURE et d'un algorithme heuristique. Les bases contiennent la définition de tous les programmes malveillants connus à ce jour et les moyens de les neutraliser. L'algorithme heuristique permet d'identifier les nouveaux virus dont les définitions ne sont pas encore reprises dans les bases.

2. Les comportements suivants sont possibles en fonction des résultats de l'analyse :

   - Si la page Web ou l'objet que souhaite ouvrir l'utilisateur contient un code malveillant, l'accès est bloqué. Dans ce cas, un message apparaît à l'écran pour avertir l'utilisateur que l'objet ou la page demandé est infecté.

   - Si aucun code malveillant n'a été découvert dans le fichier ou la page Web, l'utilisateur pourra y accéder immédiatement.

L'analyse des scripts est réalisée selon l'algorithme suivant :

1. Chaque script lancé est intercepté par l'Antivirus Internet et soumis à la recherche d'un code malveillant éventuel.

2. Si le script contient un code malveillant, l'Antivirus Internet le bloque et avertit l'utilisateur via un message spécial.

3. Si le script ne contient aucun code malveillant, le script est exécuté.

L'Antivirus Internet intercepte uniquement les scripts basés sur la technologie Microsoft Windows Script Host.

DANS CETTE SECTION

Activation et désactivation de l'Antivirus Internet 113

Modification et restauration du niveau de protection 113

Modification de l'action à réaliser sur les objets découverts 114

Blocage des scripts dangereux 114

Analyse des liens par rapport aux bases d'URL de phishing ou suspectes 114

Utilisation de l'analyse heuristique 115

Optimisation de l'analyse 115

Module d'analyse des liens 116

Composition d'une liste d'adresses de confiance 117

ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS INTERNET

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

Pour activer ou désactiver l'Antivirus Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
4. Dans la partie droite de la fenêtre, décochez la case **Activer l'Antivirus Internet** s'il faut désactiver le composant. Cochez cette case s'il faut activer le composant.

MODIFICATION ET RESTAURATION DU NIVEAU DE PROTECTION

En fonction des besoins actuels, vous pourrez choisir un des niveaux de protection prédéfinis ou configurer vous-même les paramètres de fonctionnement de l'Antivirus Internet.

Sachez que si vous configurez les paramètres de fonctionnement du composant, vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des valeurs optimales recommandées par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Afin de modifier le niveau de sécurité défini du trafic Internet, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
4. Dans le groupe **Niveau de protection** de la partie droite de la fenêtre, sélectionnez le niveau de protection requis ou cliquez sur le bouton **Configuration** afin de définir manuellement les paramètres d'analyse.

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

Pour restaurer les paramètres de protection par défaut du trafic Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Par défaut**.

MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS DECOUVERTS

Quand l'application découvre des objets infectés ou potentiellement infectés, elle exécute une action en fonction du mode de fonctionnement sélectionné : automatique ou interactif.

Si vous travaillez en mode automatique (cf. rubrique "Utilisation du mode de protection interactif" à la page 60), Kaspersky PURE appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants, il s'agit de l'action **Réparer. Supprimer, si la réparation est impossible**, pour les objets suspects : **Mettre en quarantaine**. Si vous utilisez le mode interactif (cf. rubrique "Utilisation du mode de protection interactif" à la page 60), l'application affiche un message après la découverte d'un objet dangereux et vous permet de choisir l'action à exécuter parmi la liste des actions proposées.

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

1. Ouvrez la fenêtre principale de l'application
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
4. Dans la partie droite de la fenêtre, dans le groupe **Action**, sélectionnez l'option requise.

BLOCAGE DES SCRIPTS DANGEREUX

L'Antivirus Internet peut analyser tous les scripts traités par Microsoft Internet Explorer ainsi que n'importe quel script WSH (JavaScript, Visual Basic Script, etc.) lancé pendant l'utilisateur travaille sur l'ordinateur. Si le script constitue une menace pour l'ordinateur, son exécution sera bloquée.

Pour que l'Antivirus Internet analyse et bloque les scripts, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans la rubrique **Avancé**, assurez-vous que la case **Bloquer les scripts dangereux dans Microsoft Internet Explorer** est cochée. Si la case n'est pas cochée, cochez-la.

ANALYSE DES LIENS PAR RAPPORT AUX BASES D'URL DE PHISHING OU SUSPECTES

L'Antivirus Internet peut rechercher la présence éventuelle de virus dans le trafic Web et déterminer si les liens appartiennent à la liste des URL suspectes ou des URL de phishing.

L'analyse des liens pour voir s'ils appartiennent à la liste des adresses de phishing permet d'éviter les attaques de phishing qui, en règle générale, se présentent sous la forme de messages électroniques prétendument envoyés par une

institution financière et qui contiennent des liens vers le site de ces institutions. Le texte du message invite le destinataire à cliquer sur le lien et à saisir des données confidentielles (numéro de carte de crédit, code d'accès aux services de banque en ligne) sur la page qui s'affiche. L'exemple type est le message envoyé par la banque dont vous êtes client et qui contient un lien vers un site officiel. En cliquant sur le lien, vous ouvrez en réalité une copie conforme du site Internet de la banque et il arrive même que l'adresse du site s'affiche, toutefois vous vous trouvez en fait sur un site fictif. Toutes vos actions sur ce site sont surveillées et pourraient servir au vol de votre argent.

La liste des adresses de phishing est reprise dans la distribution de Kaspersky PURE. Dans la mesure où le lien vers un site de phishing peut figurer non seulement dans un courrier, mais également dans un message ICQ, l'Antivirus Internet contrôle les tentatives d'accès à un site de phishing au niveau de l'analyse du trafic Web et bloque l'accès à ces sites Web.

Pour que l'Antivirus Internet analyse les liens en fonction des bases d'URL suspectes ou de phishing, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans le groupe **Méthodes d'analyse** de la fenêtre **Antivirus Internet** qui s'ouvre, assurez-vous que la case **Analyser les liens selon la base des URL suspectes** et/ou la case **Analyser les liens selon la base des URL de phishing** sont cochées Si les cases ne sont pas cochées, cochez-les.

UTILISATION DE L'ANALYSE HEURISTIQUE

L'Antivirus Courrier utilise toujours l'*analyse sur la base des signatures* au cours de laquelle Kaspersky PURE compare l'objet trouvé aux signatures des bases.

Pour augmenter l'efficacité de la protection, vous pouvez utiliser *l'analyse heuristique* (analyse de l'activité de l'objet dans le système). Cette analyse permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases.

Pour activer ou désactiver l'utilisation de l'analyse heuristique, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre **Antivirus Internet**, qui s'ouvre dans le groupe **Méthode d'analyse**, cochez la case **Analyse heuristique** et définissez le niveau de détail de l'analyse. Décochez la case **Analyse heuristique** s'il n'est pas nécessaire d'utiliser ce mode d'analyse.

OPTIMISATION DE L'ANALYSE

Afin d'augmenter l'efficacité de la détection des codes malveillants, l'Antivirus Internet utilise la technologie de mise en cache de fragments des objets envoyés via Internet. Toutefois, la mise en cache augmente la durée de traitement de l'objet et peut entraîner des problèmes lors de la copie et du traitement d'objets volumineux. Pour optimiser la manipulation des objets téléchargés depuis Internet, vous pouvez limiter la durée de mise en cache des fragments d'objets.

Pour limiter la durée de mise en cache, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.

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

5. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Optimisation de l'analyse**, cochez la case **Limiter la durée de mise en cache du trafic** et définissez le temps (en secondes) dans le champ de droite.

MODULE D'ANALYSE DES LIENS

Kaspersky PURE propose un module d'analyse des liens qui est administré par l'Antivirus Internet. Le module est intégré aux navigateurs Microsoft Internet Explorer et Mozilla Firefox sous la forme d'un plug-in.

Le module analyse tous les liens sur une page afin de voir s'il s'agit de liens suspects ou de phishing. Vous pouvez composer la liste des URL des sites dont le contenu ne doit pas être soumis à la recherche de liens suspects ou de phishing, ainsi que la liste des URL de sites dont le contenu doit absolument être analysé. Vous pouvez également désactiver l'analyse des liens.

- *Pour activer le module d'analyse des liens, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.

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

5. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Avancé**, cochez la case **Signaler les liens suspects ou d'hameçonnage dans Microsoft Internet Explorer et Mozilla Firefox**.

- *Pour composer la liste des URL dont le contenu ne doit pas être soumis à la recherche de liens suspects ou de phishing, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.

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

5. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Avancé**, cliquez sur le bouton **Configuration**.

6. Dans la fenêtre **Module d'analyse des liens** qui s'ouvre, sélectionnez l'option **Pour toutes les URL** puis cliquez sur le bouton **Exclusions**.

7. Dans la fenêtre **Liste des URL de confiance** qui s'ouvre, composez la liste des URL dont le contenu ne doit pas être soumis à la recherche de liens suspects ou d'hameçonnage.

- *Pour composer la liste des URL dont le contenu doit être soumis à la recherche de liens suspects ou de phishing, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.

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

5. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Avancé**, cliquez sur le bouton **Configuration**.

6. Dans la fenêtre **Module d'analyse des liens** qui s'ouvre, sélectionnez l'option **Pour les pages Internet indiquées** puis cliquez sur le bouton **Sélection**.

7. Dans la fenêtre **Liste des URL analysées** qui s'ouvre, composez la liste des URL dont le contenu doit être soumis à la recherche de liens suspects ou d'hameçonnage.

COMPOSITION D'UNE LISTE D'ADRESSES DE CONFIANCE

Vous pouvez composer une liste d'URL dont le contenu ne présente absolument aucun danger. Antivirus Internet n'analysera pas les informations en provenance de ces adresses. Cette fonctionnalité peut être utilisée, par exemple, si l'Antivirus Internet empêche le téléchargement d'un fichier depuis un site web que vous connaissez.

Pour composer une liste d'URL de confiance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.

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

5. Dans le groupe **Optimisation** de l'analyse de la fenêtre **Antivirus Internet** qui s'ouvre, cochez la case **Ne pas analyser le trafic HTTP** en provenance des URL de confiance puis cliquez sur le bouton **Sélection**.

6. Dans la fenêtre **Liste des URL de confiance** qui s'ouvre, composez la liste des adresses dont le contenu est fiable selon vous.

S'il faut à l'avenir exclure temporairement une adresse de la liste des sites de confiance, il n'est pas nécessaire de la supprimer de la liste. Il suffit simplement de décocher la case située à gauche.

ANTIVIRUS IM

L'Antivirus IM est prévu pour analyser le trafic transmis par les *clients de messageries instantanées*.

Les messages transmis via les clients de messagerie instantanée peuvent contenir des liens vers des sites web suspects ou vers des sites web utilisés par les individus malintentionnés dans le cadre d'attaques de phishing. Les programmes malveillants utilisent les clients de messagerie instantanée pour diffuser des messages non sollicités ainsi que des liens vers des applications (voire les applications elles-mêmes) qui volent les numéros et les mots de passe des utilisateurs.

Kaspersky PURE garantit une utilisation sans danger des systèmes de messagerie instantanée tels que ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent et IRC.

Certains clients de messagerie instantanée, par exemple, Yahoo! Messenger et Google Talk utilisent une connexion sécurisée. Pour analyser le trafic de ces applications, il faut activer l'analyse des connexions cryptées (cf. page 157).

Les messages sont interceptés par l'Antivirus IM et soumis à la recherche d'objets dangereux ou de liens. Vous pouvez sélectionner les types de messages (cf. page 118) qu'il faut analyser et sélectionner les différentes méthodes d'analyse.

Quand il découvre une menace dans un message, l'Antivirus IM remplace le message par un avertissement pour l'utilisateur.

Les fichiers transmis par la messagerie instantanée sont analysés par l'Antivirus Fichiers (cf. page 99) pendant la tentative d'enregistrement.

DANS CETTE SECTION

Activation et désactivation de l'Antivirus IM 118

Constitution de la zone de protection 118

Sélection de la méthode d'analyse 118

ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS IM

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

Pour activer ou désactiver l'Antivirus IM, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.
4. Dans la partie droite de la fenêtre, décochez la case **Activer l'Antivirus IM** s'il faut désactiver le composant. Cochez cette case s'il faut activer le composant.

CONSTITUTION DE LA ZONE DE PROTECTION

La zone de protection désigne les types de message qu'il faut analyser. Kaspersky PURE analyse par défaut aussi bien les messages entrant que les messages sortant. Si vous êtes convaincu que les messages que vous envoyez ne peuvent contenir aucun objet dangereux, vous pouvez vous passer de l'analyse du trafic sortant.

Pour désactiver l'analyse des messages sortant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.
4. Choisissez l'option **Analyser uniquement le courrier entrant** dans le groupe **Zone de protection** de la partie droite de la fenêtre.

SELECTION DE LA METHODE D'ANALYSE

La méthode d'analyse désigne l'analyse des liens, inclus dans les messages envoyés par messagerie instantanée, pour savoir s'ils appartiennent à la liste des adresses suspectes et (ou) à la liste des adresses de phishing.

Pour augmenter l'efficacité de la protection, vous pouvez utiliser *l'analyse heuristique* (analyse de l'activité de l'objet dans le système). Cette analyse permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases. Lors de l'analyse heuristique, n'importe quel script contenu dans les messages de client de messagerie instantanée est exécuté dans l'environnement protégé. Si l'activité du script est caractéristique des objets malveillants, alors l'objet peut être considéré, avec une probabilité élevée, comme un objet malveillant ou suspect. L'analyse heuristique est activée par défaut.

Pour analyser les liens des messages selon la base des adresses suspectes, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.

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

Pour analyser les liens des messages selon la base des adresses de phishing, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.

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

Pour activer l'utilisation de l'analyse heuristique, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.

4. Cochez la case **Analyse heuristique** dans le groupe **Méthodes d'analyse** de la partie droite de la fenêtre.

ANTI-SPAM

Kaspersky PURE reprend le composant *Anti-Spam* qui permet d'identifier les messages non sollicités (spam) et de les traiter conformément aux règles de votre client de messagerie. Ce composant permet de gagner du temps lors de l'utilisation du courrier électronique.

L'Anti-Spam se présente sous la forme d'un plug-in dans les clients de messagerie suivants :

- Microsoft Office Outlook (cf. page 134) ;
- Microsoft Outlook Express (Windows Mail) (cf. page 134) ;
- The Bat! (cf. page 135) ;
- Thunderbird (cf. page 136).

La composition de listes d'expéditeurs autorisés et interdits permet d'indiquer à l'Anti-Spam les messages qu'il faudra considérer comme du courrier normal ou comme du courrier indésirable. Les messages qui ne vous sont pas adressés pourront être également considérés comme indésirables (cf. page 128). De plus, l'Anti-Spam peut rechercher la présence éventuelle dans le message d'expressions autorisées ou interdites, ainsi que d'expressions figurant dans la liste des expressions vulgaires.

Afin qu'Anti-Spam puisse établir efficacement une distinction entre courrier indésirable et courrier normal, il faut l'entraîner (cf. section "Entraînement d'Anti-Spam" à la page 122).

Algorithme de fonctionnement du composant

L'Anti-Spam utilise l'algorithme d'apprentissage automatique qui permet au composant d'établir une distinction plus précise entre courrier indésirable et courrier normal au fil du temps. Le contenu du message constitue la source de données pour l'algorithme.

Le fonctionnement du composant Anti-Spam est scindé en deux étapes :

1. Application de critères de filtrage stricts aux messages. Ceux-ci permettent de déterminer rapidement si un message appartient ou non au courrier indésirable. L'Anti-Spam attribue l'état *courrier indésirable* ou *courrier normal* au message, l'analyse est suspendue et le message est transmis au client de messagerie pour traitement (cf. étapes 1 à 5 de l'algorithme ci-après).

2. Etude des messages qui ont répondu aux critères stricts de sélection des étapes précédentes. Ces messages ne peuvent pas être automatiquement considérés comme du courrier indésirable. Pour cette raison, l'Anti-Spam doit calculer la *probabilité* de leur appartenance au courrier indésirable.

L'algorithme de fonctionnement de l'Anti-Spam contient les étapes suivantes :

1. L'adresse de l'expéditeur du message est contrôlée afin de voir si elle figure dans les listes des expéditeurs autorisés ou interdits.

   - Si l'adresse de l'expéditeur se trouve dans la liste des adresses autorisées, le message reçoit l'état *courrier normal*.

   - Si l'adresse de l'expéditeur figure dans la liste des adresses interdites, le message reçoit l'état *courrier indésirable*.

2. Si le message a été envoyé via Microsoft Exchange Explorer et que l'analyse de tels messages est désactivée, le message reçoit l'état *courrier normal*.

3. Le composant vérifie si le message contient des expressions tirées de la liste des expressions autorisées. Si le message contient ne serait-ce qu'une expression de la liste, le message reçoit l'état *courrier normal*. Cette étape est ignorée par défaut.

4. L'analyse du message cherche à déterminer la présence de texte issu de la liste des expressions interdites et de la liste des expressions vulgaires. Le coefficient pondéré est calculé en fonction du nombre de mots de ces listes présents dans le message. Si la somme du coefficient pondéré est supérieure à 100, le message est considéré comme appartenant au *courrier indésirable*. Cette étape est ignorée par défaut.

5. Si le texte contient une adresse reprise dans la base des URL de phishing ou suspectes, le message reçoit l'état *courrier indésirable*.

6. Le message est analysé selon les règles heuristiques. Si l'analyse met en évidence des éléments caractéristiques du courrier indésirable, la probabilité que le message appartienne au courrier indésirable augmente.

7. Le message est analysé à l'aide de la technologie GSG. L'Anti-Spam analyse les images incluses dans le message. Si celles-ci contiennent des éléments caractéristiques du courrier indésirable, la probabilité que le message appartienne au courrier indésirable augmente.

8. Les documents au format rtf joints au message sont analysés. L'Anti-Spam recherche les éléments caractéristiques du courrier indésirable dans les documents joints. A la fin de l'analyse, l'Anti-Spam calcule l'augmentation de la probabilité qu'un message appartienne au courrier indésirable. La technologie est désactivée par défaut.

9. Le composant procède à la recherche de signes complémentaires caractéristiques du courrier indésirable. Chaque fois qu'un de ces signes est identifié, la probabilité que le message appartienne au courrier indésirable augmente.

10. Si l'Anti-Spam a été entraîné, le message est analysé à l'aide de la technologie iBayes. L'algorithme d'auto-apprentissage iBayes calcule la probabilité qu'un message appartienne au courrier indésirable sur la base de la fréquence d'utilisation d'expressions propres au courrier indésirable dans le message.

Suite à l'analyse du message, l'application détermine la probabilité que le message est un message non sollicité via la valeur de l'*indice de courrier indésirable*. Le message reçoit l'état *courrier indésirable* ou courrier *indésirable potentiel* en fonction des seuils d'indice de courrier indésirable (cf. rubrique "Régulation des seuils d'indice de courrier indésirable" à la page 130). De plus, par défaut, le **texte [!! SPAM]** ou **[?? Probable Spam]** est ajouté par défaut à l'objet du courrier indésirable ou indésirable potentiel (cf. rubrique "**Ajout d'une remarque à l'objet du message**" à la page 132). Ensuite,

le message est traité selon les règles pour les clients de messagerie que vous avez définies (cf. rubrique "Configuration du traitement du courrier indésirable par les clients de messagerie" à la page 134).

DANS CETTE SECTION

Activation et désactivation de l'Anti-Spam 121

Modification et restauration du niveau de protection 121

Entraînement d'Anti-Spam 122

Analyse des liens dans les messages 125

Identification du courrier indésirable sur la base des expressions et des adresses. Composition des listes 125

Régulation des seuils d'indice de courrier indésirable 130

Utilisation d'indices complémentaires pour le filtrage du courrier indésirable 131

Sélection de l'algorithme d'identification du courrier indésirable 131

Ajout d'une remarque à l'objet du message 132

Filtrage des messages sur le serveur Gestionnaire de messages 132

Exclusion des messages Microsoft Exchange Server de l'analyse 133

Configuration du traitement du courrier indésirable par les clients de messagerie 134

ACTIVATION ET DESACTIVATION DE L'ANTI-SPAM

Par défaut, l'Anti-Spam est activé et fonctionne en mode optimal. Vous pouvez désactiver l'Anti-Spam le cas échéant.

Pour activer ou désactiver l'Anti-Spam, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, décochez la case **Activer l'Anti-Spam** s'il faut désactiver le composant. Cochez cette case s'il faut activer le composant.

MODIFICATION ET RESTAURATION DU NIVEAU DE PROTECTION

En fonction des besoins actuels, vous pourrez choisir un des niveaux de protection prédéfinis pour la protection du courrier ou configurer vous-même les paramètres de fonctionnement de l'Anti-Spam.

Sachez que si vous configurez les paramètres de fonctionnement du composant, vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des valeurs optimales recommandées par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Pour modifier le niveau de protection prédéfini d'Anti-Spam, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

4. Dans le groupe **Niveau de protection** de la partie droite de la fenêtre, sélectionnez le niveau de protection requis ou cliquez sur le bouton **Configuration** afin de définir manuellement les paramètres d'analyse.

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

Pour restaurer les paramètres de fonctionnement par défaut de l'Anti-Spam, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Par défaut**.

ENTRAINEMENT D'ANTI-SPAM

Un des outils d'identification du courrier indésirable est l'algorithme d'auto-apprentissage iBayes. À l'issue de l'exécution de cet algorithme, l'application décide d'attribuer un certain statut au message sur la base des expressions qu'il renferme. Avant de pouvoir utiliser l'algorithme iBayes, il faut lui présenter des échantillons de phrases de messages utiles et de messages non sollicités, c'est-à-dire l'*entraîner*.

Il existe plusieurs approches pour entraîner l'Anti-Spam :

- Utilisation de l'Assistant d'apprentissage (apprentissage groupé). L'entraînement à l'aide de l'Assistant d'apprentissage est préférable au tout début de l'utilisation de l'Anti-Spam.
- Entraînement de l'Anti-Spam sur les messages sortants.
- Entraînement directement pendant l'utilisation du courrier électronique à l'aide du client de messagerie dont la fenêtre reprend des boutons et des options de menu spéciaux pour l'apprentissage.
- Entraînement lors de l'utilisation des rapports de l'Anti-Spam.

DANS CETTE SECTION

Utilisation de l'Assistant d'apprentissage 122

Apprentissage sur le courrier sortant 123

Utilisation des éléments de l'interface du client de messagerie 123

Ajout d'adresses à la liste des expéditeurs autorisés 124

Entraînement à l'aide des rapports 124

UTILISATION DE L'ASSISTANT D'APPRENTISSAGE

L'Assistant d'apprentissage permet d'entraîner l'Anti-Spam par lot. Pour ce faire, il faut désigner les répertoires des comptes utilisateur des clients de messagerie Microsoft Office Outlook et Microsoft Outlook Express (Windows Mail) qui contiennent le courrier indésirable et le courrier normal.

Pour assurer une identification efficace du courrier indésirable, il est indispensable de réaliser l'entraînement sur un minimum de 50 exemplaires de courrier normal et de 50 exemplaires de courrier indésirable. L'algorithme iBayes ne fonctionnera pas si ces actions ne sont pas exécutées.

Afin de gagner du temps, l'Assistant réalisera l'entraînement uniquement sur 50 messages de chaque dossier sélectionné.

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

Pour lancer l'assistant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Entraînement d'Anti-Spam**, cliquez sur le bouton **Entraîner**.

Lors de l'apprentissage sur la base du courrier normal, les adresses des expéditeurs sont ajoutées automatiquement à la liste des expéditeurs autorisés. Vous pouvez désactiver cette fonction (cf. rubrique "Ajout d'adresses à la liste des expéditeurs autorisés" à la page 124).

VOIR EGALEMENT

Que faire avec un grand nombre de messages non sollicités 80

APPRENTISSAGE SUR LE COURRIER SORTANT

Vous pouvez entraîner l'Anti-Spam sur la base de 50 exemples de messages sortants. Une fois que l'apprentissage aura été activé, l'Anti-Spam analysera chaque message que vous envoyez et les utilisera en tant que modèle de courrier normal. L'apprentissage sera terminé après l'envoi de 50 messages.

Pour activer l'apprentissage de l'Anti-Spam sur la base du courrier sortant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, groupe **Courrier sortant**, cochez la case **Apprentissage sur le courrier sortant**.

Lors de l'apprentissage sur le courrier sortant, les adresses des destinataires de ces messages sont ajoutées automatiquement à la liste des expéditeurs autorisés. Vous pouvez désactiver cette fonction (cf. rubrique "Ajout d'adresses à la liste des expéditeurs autorisés" à la page 124).

UTILISATION DES ELEMENTS DE L'INTERFACE DU CLIENT DE MESSAGERIE

L'entraînement d'Anti-Spam pendant l'utilisation du courrier électronique suppose l'utilisation des éléments spéciaux de l'interface de votre client de messagerie.

Les boutons pour l'entraînement d'Anti-Spam apparaissent dans l'interface des clients de messagerie Microsoft Office Outlook et Microsoft Outlook Express (Windows Mail) uniquement après l'installation de Kaspersky PURE.

Pour entraîner l'Anti-Spam à l'aide du client de messagerie, procédez comme suit :

1. Lancez le client de messagerie.

2. Sélectionnez le message à l'aide duquel vous souhaitez entraîner l'Anti-Spam.

3. Exécutez une des actions suivantes en fonction du client de messagerie que vous utilisez :

   - Cliquez sur le bouton **Courrier indésirable** ou **Courrier normal** dans la barre d'outils de Microsoft Office Outlook ;

   - Cliquez sur le bouton **Courrier indésirable** ou **Courrier normal** dans la barre d'outils de Microsoft Outlook Express (Windows Mail) ;

   - Utilisez les éléments **Marquer comme courrier indésirable** ou **Marquer comme courrier normal** dans le menu **Spécial** du client de messagerie The Bat! ;

   - utilisez le bouton **Courrier indésirable/Courrier normal** dans la barre d'outils du client de messagerie Mozilla Thunderbird.

Une fois que vous aurez choisi une des actions ci-dessus, l'Anti-Spam poursuivra son entraînement sur la base du message sélectionné. Si vous sélectionnez plusieurs messages, l'entraînement portera sur tous les messages sélectionnés.

Si le message est considéré comme normal, l'adresse de l'expéditeur est ajoutée à la liste des expéditeurs autorisés.

AJOUT D'ADRESSES A LA LISTE DES EXPEDITEURS AUTORISES

Lors de l'apprentissage de l'Anti-Spam sur la base du courrier normal à l'aide de l'Assistant d'apprentissage, ainsi que lors de l'apprentissage directement dans la fenêtre du client de messagerie, les adresses des expéditeurs des messages normaux sont ajoutées automatiquement à la liste des expéditeurs autorisés (cf. section "Expéditeurs interdits et autorisés" à la page 128). Cette liste est également enrichie des adresses des destinataires des messages sortants lors de l'apprentissage sur la base du courrier sortant.

Vous pouvez désactiver cette fonction afin que la liste des expéditeurs autorisés ne soit pas enrichie automatiquement suite à l'apprentissage.

Pour désactiver l'ajout d'adresses à la liste des expéditeurs autorisés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

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

5. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Considérer les messages suivants comme du courrier normal**, cochez la case **D'expéditeurs autorisés** et cliquez sur le bouton **Sélection**.

   La fenêtre **Expéditeurs autorisés** s'ouvre.

6. Décochez la case **Ajouter les adresses des expéditeurs autorisés pendant l'apprentissage d'Anti-Spam dans le client de messagerie**.

ENTRAINEMENT A L'AIDE DES RAPPORTS

Il est possible d'entraîner l'Anti-Spam sur la base de ses rapports qui reprennent les informations relatives aux messages classés dans la catégorie de courrier indésirable potentiel. L'apprentissage consiste à associer au message le commentaire **courrier indésirable** ou **courrier normal** et à les ajouter à la liste des expéditeurs autorisés ou interdits.

Pour entraîner l'Anti-Spam sur la base du rapport, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Le lien **Rapport** permet d'accéder à la fenêtre des rapports de Kaspersky PURE.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.

   La fenêtre **Rapport détaillé** s'ouvre.

4. Sélectionnez le composant **Anti-Spam** dans la liste déroulante de la partie supérieure gauche de la fenêtre.

5. Dans la partie droite de la fenêtre, à l'aide des entrées de la colonne **Objet**, définissez les messages qui vont servir à l'apprentissage de l'Anti-Spam. Pour chacun de ces messages, ouvrez le menu contextuel (d'un clic droit de la souris) et sélectionnez un des points du menu pour définir l'action à exécuter sur le message :

   - Marquer comme courrier indésirable ;
   - Marquer comme courrier normal ;
   - Ajouter à la liste des expéditeurs autorisés ;
   - Ajouter à la liste des expéditeurs interdits ;

ANALYSE DES LIENS DANS LES MESSAGES

L'Anti-Spam permet d'analyser les liens contenus dans les messages électroniques afin de voir s'ils appartiennent à la liste des URL suspectes et des URL de phishing. Ces listes sont livrées avec Kaspersky PURE. Si le message contient un lien d'hameçonnage ou suspect et si le corps du message contient des éléments d'hameçonnage, ce message est considéré comme indésirable.

Pour activer l'analyse des liens selon les bases des URL suspectes et de phishing procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, dans le groupe **Considérer les messages suivants comme du courrier indésirable** cochez la case **Contenant des liens de la base des URL suspectes** et **Présentant des éléments d'hameçonnage**.

IDENTIFICATION DU COURRIER INDESIRABLE SUR LA BASE DES EXPRESSIONS ET DES ADRESSES. COMPOSITION DES LISTES

Vous pouvez composer des listes d'expressions interdites, autorisées ou vulgaires ainsi que des listes d'adresses d'expéditeurs autorisés ou interdits et une liste avec vos propres adresses. En cas d'utilisation de ces listes, l'Anti-Spam analyse le contenu du message afin d'identifier la présence d'expression figurant dans les listes et il vérifie également les adresses de l'expéditeur et des destinataires pour voir si elles correspondent aux entrées des listes. S'il découvre une expression ou une adresse, l'Anti-Spam classe le message dans la catégorie courrier normal ou courrier indésirable en fonction de la liste dans laquelle figure l'expression ou l'adresse.

Les messages suivants sont classés dans la catégorie courrier indésirable :

- Les messages contenant des expressions interdites ou vulgaires dont le coefficient pondéré total dépasse100 ;
- Les messages envoyés depuis une adresse interdite ou qui ne vous sont pas adressés.

Les messages suivants sont classés dans la catégorie courrier normal :

- Les messages contenant des expressions autorisées ;

- Les messages en provenance d'adresses autorisées.

Masques d'expressions clés et d'adresses d'expéditeurs

Vous pouvez utiliser des *masques d'expression* dans les listes d'expressions autorisées, interdites ou vulgaires. Vous pouvez utiliser des *masques d'adresse* dans les listes d'adresses d'expéditeur autorisé et interdit ainsi que dans la liste des adresses de confiance.

Un masque est un modèle de ligne auquel l'expression ou l'adresse est comparée. Certains caractères sont employés dans le masque pour remplacer d'autres caractères : ***** remplace n'importe quelle séquence de caractères, tandis que **?** remplace un caractère. Si de tels caractères sont utilisés dans le masque, celui-ci pourra correspondre à plusieurs expressions ou à plusieurs adresses (cf. exemples ci-dessous).

Si le caractère ***** ou **?** fait partie de l'expression (par exemple, *Quelle heure est-il?*), il faudra le faire précéder du caractère **** afin que l'Anti-Spam l'interprète correctement. Ainsi, au lieu du caractère *****, il faudra utiliser la combinaison *****, et au lieu de **?**, la combinaison **\?** (par exemple, *Quelle heure est-il\?*).

Exemple de masques d'expression :

- *Visitez notre ** : ce masque correspond au message commençant par *Visitez notre* suivi de n'importe quel autre texte.

Exemples de masques d'adresses :

- *admin@test.com* : ce masque correspond uniquement à l'adresse *admin@test.com*.
- *admin@** : ce masque correspond à l'adresse d'un expéditeur portant le nom *admin*, par exemple : *admin@test.com*, *admin@exemple.org.*
- **@test** : ce masque correspond à l'adresse de n'importe quel expéditeur d'un domaine de messagerie commençant par *test*, par exemple : *admin@test.com*, *info@test.org.*
- *info.*@test.???* : ce masque correspond à l'adresse de n'importe quel expéditeur dont le nom commence par *info.* et dont le domaine de messagerie commence par *test.* et se termine par trois caractères quelconques, par exemple : *info.product@test.com*, *info.company@test.org*, mais pas *info.product@test.com/fr*.

DANS CETTE SECTION

Expressions interdites et autorisées 126

Expressions vulgaires 127

Expéditeurs interdits et autorisés 128

Vos adresses 128

Exportation et importation des listes d'expressions et d'adresses 129

EXPRESSIONS INTERDITES ET AUTORISEES

La liste des *expressions interdites* peut reprendre des expressions qui, d'après vos observations, sont caractéristiques des messages non sollicités et vous pouvez associer un coefficient pondéré à chaque expression. Le *coefficient pondéré* permet d'indiquer à quel point une expression est propre au courrier indésirable : plus le coefficient est élevé, plus il est probable que le message contenant cette expression est indésirable. La valeur du coefficient pondéré de l'expression peut être comprise entre 0 et 100. Si la somme des coefficients pondérés de toutes les expressions découvertes dans le message est supérieure à 100, le message est traité comme un message non sollicité.

Les expressions clés caractéristiques du courrier normal peuvent être saisies dans la liste des *expressions autorisées*. Quand il identifie une de ces expressions dans un message, l'Anti-Spam considère ce dernier comme normal.

La liste des expressions autorisées ou interdites accepte aussi bien des expressions complètes que des masques (cf. rubrique "Identification du courrier indésirable sur la base des expressions et des adresses. Composition des listes" à la page 125).

Pour composer la liste des expressions autorisées ou interdites, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Sous l'onglet **Général** de la fenêtre qui s'ouvre, procédez comme suit :
   - S'il faut créer une liste d'expressions interdites, dans le groupe **Considérer les messages suivants comme du courrier indésirable**, cochez la case **Contenant des expressions interdites**, puis cliquez sur le bouton **Sélection**, situé à droite.

     La fenêtre **Liste des expressions interdites** s'ouvre.
   - S'il faut créer une liste d'expressions autorisées, dans le groupe **Considérer les messages suivants comme du courrier normal**, cochez la case **Contenant des expressions autorisées**, puis cliquez sur le bouton **Sélection**, situé à droite.

     La fenêtre **Liste des expressions autorisées** s'ouvre.
6. Cliquez sur le lien **Ajouter** pour ouvrir la fenêtre **Expression interdite** (ou la fenêtre **Expression autorisée**).
7. Saisissez l'expression entière ou un masque d'expression et pour l'expression interdite, définissez le coefficient pondéré, puis cliquez sur le bouton **OK**.

Si, à l'avenir, vous ne souhaitez plus utiliser un masque, il n'est pas nécessaire de le supprimer. Il suffit de désélectionner la case en regard du masque en question.

EXPRESSIONS VULGAIRES

Les experts de Kaspersky Lab ont composé la liste d'expressions vulgaires utilisée par Kaspersky PURE. La liste contient les expressions vulgaires dont la présence dans un message permet d'affirmer avec une certitude très élevée qu'il s'agit d'un message non sollicité. Vous pouvez enrichir la liste et y ajouter des expressions complètes ou des masques d'expression (cf. rubrique "Identification du courrier indésirable sur la base des expressions et des adresses. Composition des listes" à la page 125).

Pour modifier la liste des expressions vulgaires, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Considérer les messages suivants comme du courrier indésirable**, cochez la case **Contenant des expressions interdites** et cliquez sur le bouton **Sélection**.

   La fenêtre **Liste des expressions interdites** s'ouvre.
6. Cochez la case **Considérer les expressions vulgaires comme interdites**, puis cliquez sur le lien **expressions vulgaires** pour ouvrir la fenêtre **Accord**.

7. Lisez le texte du contrat et si vous en acceptez les dispositions présentées dans la fenêtre, cochez la case dans la partie inférieure de la fenêtre, puis cliquez sur **OK**.

   La fenêtre **Liste de langage vulgaire** s'ouvre.

8. Cliquez sur le lien **Ajouter** pour ouvrir la fenêtre **Expression interdite**.

9. Saisissez l'expression complète ou son masque et définissez le coefficient pondéré de l'expression, puis cliquez sur **OK**.

Si, à l'avenir, vous ne souhaitez plus utiliser un masque quelconque, il n'est pas nécessaire de le supprimer. Il suffit de désélectionner la case en regard du masque en question dans la fenêtre **Liste de langage vulgaire**.

EXPEDITEURS INTERDITS ET AUTORISES

La liste des *expéditeurs interdits* reprend les adresses des expéditeurs dont les messages seront considérés comme indésirables par l'Anti-Spam. Les adresses des expéditeurs qui ne devraient pas envoyer de courrier indésirable sont reprises dans la liste des *expéditeurs autorisés*. Cette liste est créée automatiquement pendant l'entraînement du composant Anti-Spam (cf. rubrique "Ajout d'adresses à la liste des expéditeurs autorisés" à la page 124). De plus, vous pouvez enrichir vous-même cette liste.

Vous pouvez ajouter à la liste des expéditeurs autorisés ou interdits des adresses complètes ou des masques d'adresses (cf. rubrique "Identification du courrier indésirable sur la base des expressions et des adresses. Composition des listes" à la page 125).

Pour composer la liste des expéditeurs autorisés ou interdits, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

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

5. Sous l'onglet **Général** de la fenêtre qui s'ouvre, procédez comme suit :

   - S'il faut créer une liste d'expéditeurs interdits, dans le groupe **Considérer les messages suivants comme du courrier indésirable**, cochez la case **D'expéditeurs interdits**, puis cliquez sur le bouton **Sélection**, situé à droite.

     La fenêtre **Liste des expéditeurs interdits** s'ouvre.

   - S'il faut créer une liste d'expéditeurs autorisés, dans le groupe **Considérer les messages suivants comme du courrier normal**, cochez la case **D'expéditeurs autorisés**, puis cliquez sur le bouton **Sélection**, situé à droite.

     La fenêtre **Liste des expéditeurs autorisés** s'ouvre.

6. Cliquez sur le lien **Ajouter** pour ouvrir la fenêtre **Masque d'adresse de courrier électronique**.

7. Saisissez le masque de l'adresse, puis cliquez sur **OK**.

Si, à l'avenir, vous ne souhaitez plus utiliser un masque, il n'est pas nécessaire de le supprimer. Il suffit de désélectionner la case en regard du masque en question.

VOS ADRESSES

Vous pouvez composer une liste reprenant vos adresses électroniques afin que l'Anti-Spam considère comme du courrier indésirable les messages qui ne vous sont pas adressés.

Pour composer la liste de vos adresses, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

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

5. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, cochez la case **Dont je ne suis pas le destinataire** et cliquez sur le bouton **Mes adresses**.

   La fenêtre **Mes adresses** s'ouvre.

6. Cliquez sur le lien **Ajouter** pour ouvrir la fenêtre **Masque d'adresse de courrier électronique**.

7. Saisissez le masque de l'adresse, puis cliquez sur **OK**.

Si, à l'avenir, vous ne souhaitez plus utiliser un masque quelconque, il n'est pas nécessaire de le supprimer. Il suffit de désélectionner la case en regard du masque en question dans la fenêtre **Mes adresses**.

EXPORTATION ET IMPORTATION DES LISTES D'EXPRESSIONS ET D'ADRESSES

Une fois que vous avez créé une liste d'adresses et d'expressions, vous pouvez l'utiliser à plusieurs reprises : par exemple, transférer les adresses dans une liste identique sur un autre ordinateur doté de Kaspersky PURE.

Voici la marche est à suivre :

1. Procédez à une *exportation*, c.-à-d. copiez les entrées de la liste dans un fichier.

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

3. Procédez à une *importation*, c.-à-d. ajoutez les entrées du fichier à une liste identique sur un autre ordinateur.

Lors de l'exportation de la liste, vous serez invité à copier uniquement l'élément sélectionné de la liste ou toute la liste. Lors de l'importation, vous pouvez ajouter de nouveaux éléments à la liste ou écraser la liste existante par la liste importée.

➧ *Pour exporter les entrées de la liste, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

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

5. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, cochez la case dans la ligne contenant le nom de la liste de laquelle il faut exporter les entrées, puis cliquez sur le bouton qui lui correspond à droite.

6. Dans la fenêtre qui s'ouvre avec la liste, cochez les cases en regarde des entrées qu'il faut inclure dans le fichier.

7. Cliquez sur le lien **Exporter**.

   Une fenêtre s'ouvre et vous avez la possibilité d'exporter uniquement les éléments sélectionnés. Exécutez dans cette fenêtre une des opérations suivantes :

   - Cliquez sur le bouton **Oui** s'il faut uniquement inclure les entrées sélectionnées ;

   - Cliquez sur le bouton **Non** s'il faut inclure la liste complète.

8. Dans la fenêtre qui s'ouvre, désignez le type et le nom du fichier à enregistrer et confirmez l'enregistrement.

Pour importer les entrées d'un fichier dans la liste, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, cochez la case dans la ligne contenant le nom de la liste dans laquelle il faut importer les entrées, puis cliquez sur le bouton à droite.
6. Dans la fenêtre contenant la liste, cliquez sur le lien **Importer**. Si vous importez la liste des expéditeurs autorisés, alors un menu dans lequel il faudra choisir l'option **Importer depuis un fichier** apparaît. Pour les autres listes, il n'est pas nécessaire de choisir une option du menu.

   Si la liste n'est pas vide, une fenêtre s'ouvre et vous avez la possibilité d'ajouter les éléments importés. Exécutez dans cette fenêtre une des opérations suivantes :

   - Cliquez sur le bouton **Oui** s'il faut ajouter des entrées du fichier à la liste ;
   - Cliquez sur le bouton **Non** s'il faut remplacer les entrées actuelles de la liste par celles du fichier.
7. Dans la fenêtre qui s'ouvre, sélectionnez le fichier contenant la liste des entrées qu'il faut importer.

Importation de la liste des expéditeurs autorisés depuis le carnet d'adresses

Il est possible d'importer les adresses du carnet d'adresses de Microsoft Office Outlook/Microsoft Outlook Express (Windows Mail) dans la liste des expéditeurs autorisés.

Pour importer la liste des expéditeurs autorisés depuis le carnet d'adresses, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Considérer les messages suivants comme du courrier normal**, cochez la case **D'expéditeurs autorisés** et cliquez sur le bouton **Sélection**.

   La fenêtre **Liste des expéditeurs autorisés** s'ouvre.
6. Cliquez sur le lien **Importer** afin d'ouvrir la fenêtre de sélection de la source, puis choisissez l'option **Importer depuis le carnet d'adresses**.
7. Dans la fenêtre qui s'ouvre, sélectionnez le carnet d'adresses requis.

REGULATION DES SEUILS D'INDICE DE COURRIER INDESIRABLE

L'identification du courrier indésirable repose sur l'utilisation de technologies modernes de filtrage qui permettent à l'Anti-Spam de séparer (cf. rubrique "Entraînement d'Anti-Spam" à la page 122) le courrier (potentiellement) indésirable du courrier normal. Chaque élément de courrier normal ou de courrier indésirable se voit attribuer un coefficient.

Quand un message arrive dans votre boîte aux lettres, l'Anti-Spam exploite la technologie iBayes pour voir si le message contient des éléments de courrier indésirable ou de courrier normal. Les coefficients de chaque élément de courrier indésirable (courrier normal) sont ajoutés pour obtenir l'*indice de courrier indésirable*. Plus l'indice de courrier indésirable n'est élevé, plus la probabilité que le message soit un message non sollicité est grande. Par défaut, un message est

considéré comme normal si l'indice de courrier indésirable est inférieur à 60. Si l'indice de courrier indésirable est supérieur à 60, alors le message est classé dans la catégorie du courrier indésirable potentiel. Et si la valeur est supérieure à 90, le message est considéré comme du courrier indésirable. Vous pouvez modifier le seuil de l'indice de courrier indésirable.

Pour modifier le seuil de l'indice de courrier indésirable, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Indice de courrier indésirable**, modifiez la valeur de l'indice à l'aide du curseur ou du champ de saisie.

UTILISATION D'INDICES COMPLEMENTAIRES POUR LE FILTRAGE DU COURRIER INDESIRABLE

Les résultats du calcul de l'indice de courrier indésirable peuvent être influencés par des éléments complémentaires du message tels que l'absence d'adresse du destinataire dans le champ "À" ou un objet un peu trop long (plus de 250 caractères). Quand ces signes sont présents, la probabilité que le message soit non sollicité augmente. Et par conséquent, la valeur de l'indice de courrier indésirable augmente. Vous pouvez choisir les éléments complémentaires à prendre en compte durant l'analyse des messages.

Pour utiliser des éléments complémentaires qui augmenteront la valeur de l'indice de courrier indésirable, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, cliquez sur le bouton **Avancé**.
6. Dans la fenêtre **Avancé** qui s'ouvre, cochez la case en regard des éléments dont il faudra tenir compte pendant l'analyse des messages et qui augmenteront l'indice de courrier indésirable.

SELECTION DE L'ALGORITHME D'IDENTIFICATION DU COURRIER INDESIRABLE

La recherche des messages non sollicités dans le courrier s'opère à l'aide d'algorithmes d'identification :

- **Analyse heuristique**. Anti-Spam analyse les messages à l'aide des règles heuristiques. L'analyse heuristique est toujours utilisée.
- **Identification des images (GSG)**. Anti-Spam applique la technologie GSG pour identifier le courrier indésirable sous la forme d'images.
- **Analyse des documents rtf joints**. Anti-Spam analyse les documents joints au message afin de voir s'ils présentent des éléments caractéristiques du courrier indésirable.
- **Algorithme d'auto-apprentissage par l'analyse de texte (iBayes)**. L'algorithme d'iBayes repose sur l'analyse de la fréquence d'utilisation de mots caractéristiques du spam dans le texte du message. À l'issue de l'analyse,

le message est considéré comme indésirable ou normal. Avant de commencer à utiliser l'algorithme iBayes, vous devez absolument entraîner l'Anti-Spam (cf. rubrique "Entraînement d'Anti-Spam" à la page 122).

Afin d'utiliser /de ne pas utiliser un algorithme quelconque d'identification du courrier indésirable lors de l'analyse du courrier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, groupe **Algorithmes d'identification**, cochez/décochez les cases correspondantes.

AJOUT D'UNE REMARQUE A L'OBJET DU MESSAGE

L'Anti-Spam peut ajouter les indications suivantes au champ **Objet** des messages qui ont été classés dans la catégorie courrier indésirable ou courrier indésirable potentiel :

- **[!! SPAM]** : pour les messages considérés comme indésirables.
- **[?? Probable Spam]** : pour les messages considérés comme courrier indésirable potentiel.

La présence de cette remarque dans l'objet du message peut vous aider à différencier visuellement le courrier indésirable et potentiellement indésirable lors du survol de la liste des messages.

Pour que l'Anti-Spam ajoute /n'ajoute pas de remarque à l'objet des messages, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans le groupe **Actions** de l'onglet **Avancé** de la fenêtre qui s'ouvre, cochez les cases en regard des intitulés à ajouter à l'objet des messages. Une fois la case cochée, vous pouvez modifier le texte de la remarque. Pour ne pas ajouter de remarque, désélectionnez la case correspondante.

FILTRAGE DES MESSAGES SUR LE SERVEUR. GESTIONNAIRE DE MESSAGES

Vous pouvez consulter la liste des messages électroniques sur le serveur sans les télécharger sur votre ordinateur. Ceci permet de refuser la remise de certains messages, ce qui non seulement fait gagner du temps et réduit le trafic dans le cadre de l'utilisation du courrier électronique, mais contribue également à réduire la probabilité de télécharger du courrier indésirable ou des virus sur l'ordinateur.

Le *Gestionnaire de messages* permet de manipuler les messages sur le serveur.

La fenêtre du Gestionnaire de messages s'ouvre chaque fois avant la réception d'un message, pour autant qu'il soit activé.

Sachez cependant que le Gestionnaire de messages s'ouvre uniquement lors de la réception de messages via le protocole POP3. Le Gestionnaire de messages ne s'ouvre pas si le serveur POP3 ne prend pas en charge la consultation des en-têtes des messages électroniques ou si tous les messages présents sur le serveur ont été envoyés par des expéditeurs de la liste des expéditeurs autorisés (cf. page 128).

La liste de messages sur le serveur s'affiche dans la partie centrale de la fenêtre du Gestionnaire de messages. Sélectionnez un message dans la liste pour voir son en-tête en détail.

La consultation des en-têtes peut être utile dans les situations suivantes : les diffuseurs de courrier indésirable installent sur l'ordinateur de votre collègue un programme malveillant qui envoie des messages non sollicités au nom du collègue aux adresses de son répertoire. La probabilité que votre adresse figure dans ce répertoire est élevée et par conséquent, le programme malveillant peut envoyer une multitude de messages non sollicités à votre adresse.

Dans la situation décrite, l'adresse de l'expéditeur ne permet pas de dire si le message a été envoyé directement par votre collègue ou par un diffuseur de messages non sollicités à l'aide d'un programme malveillant. L'en-tête du message offre des informations plus détaillées sur l'heure de l'envoi et l'origine du message, sa taille et le parcours suivi entre l'expéditeur et votre serveur de messagerie. Ces données vous permettront de décider si ce message peut être téléchargé du serveur ou s'il est préférable de le supprimer.

Pour utiliser le Gestionnaire de messages, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. De le groupe **Courrier entrant** de l'onglet **Avancé** de la fenêtre qui s'ouvre, cochez la case **Ouvrir le Gestionnaire de messages lors de la réception de courrier via le protocole POP3**.

Pour supprimer des messages du serveur à l'aide du Gestionnaire de messages, procédez comme suit :

1. Dans la fenêtre du Gestionnaire de messages qui s'ouvre avant la remise du message, cochez la case en regard du message dans la colonne **Supprimer**.
2. Dans la partie supérieure de la fenêtre, cliquez sur le bouton **Supprimer la sélection**.

Les messages seront supprimés du serveur. Dans ce cas, vous recevrez un message avec l'intitulé **[!! SPAM]** qui sera traité selon les règles de votre client de messagerie (cf. rubrique "Configuration du traitement du courrier indésirable par les clients de messagerie" à la page 134).

EXCLUSION DES MESSAGES MICROSOFT EXCHANGE SERVER DE L'ANALYSE

Vous pouvez exclure de la recherche du courrier indésirable les messages envoyés dans le cadre du réseau interne (par exemple, le courrier d'entreprise). N'oubliez pas que les messages seront considérés comme des messages internes si Microsoft Office Outlook est utilisé sur tous les postes du réseau et que les boîtes aux lettres des utilisateurs se trouvent sur un même serveur Exchange ou que ces serveurs sont unis par des connecteurs X400.

Par défaut, l'Anti-Spam n'analyse pas les messages de Microsoft Exchange Server.

Pour que l'Anti-Spam analyse les messages de Microsoft Exchange Server, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Anti-Spam**.
4. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Exclusions**, désélectionnez la case **Ne pas analyser les messages Microsoft Exchange Server**.

CONFIGURATION DU TRAITEMENT DU COURRIER INDESIRABLE PAR LES CLIENTS DE MESSAGERIE

Si l'analyse indique que le message est un exemplaire de courrier indésirable ou de courrier indésirable potentiel, la suite des opérations réalisées par l'Anti-Spam dépendra de l'état du message et de l'action sélectionnée. Par défaut, les messages électroniques classés comme courrier indésirable ou courrier indésirable potentiel sont modifiés : le texte **[!! SPAM]** ou **[?? Probable Spam]** est ajouté respectivement au champ **Objet du message** (cf. rubrique "Ajout d'une remarque à l'objet du message" à la page 132).

Vous pouvez sélectionner des actions complémentaires à exécuter sur le courrier indésirable et le courrier indésirable potentiel. Des plug-ins spéciaux sont prévus dans les clients de messagerie Microsoft Office Outlook et Microsoft Outlook Express (Windows Mail). Pour les clients de messagerie The Bat! et Thunderbird, vous pouvez configurer des règles de filtrage.

DANS CETTE SECTION

Microsoft Office Outlook 134

Microsoft Outlook Express (Windows Mail) 134

Création de règles de traitement des messages pour le courrier indésirable 134

The Bat! 135

Thunderbird 136

MICROSOFT OFFICE OUTLOOK

Par défaut, le courrier qui est considéré comme courrier indésirable ou courrier indésirable potentiel par l'Anti-Spam est marqué à l'aide du texte **[!! SPAM]** ou **[?? Probable Spam]** dans l'**Objet**. Si un traitement complémentaire des messages après l'analyse par l'Anti-Spam s'impose, vous pouvez configurer Microsoft Office Outlook. La fenêtre de configuration du traitement du courrier indésirable s'ouvre automatiquement au premier lancement du client de messagerie après le chargement de Kaspersky PURE. De plus, les paramètres de traitement du courrier indésirable et du courrier indésirable potentiel dans Microsoft Office Outlook sont repris sur l'onglet spécial **Anti-Spam** du menu **Service** → **Paramètres**.

MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL)

Par défaut, le courrier qui est considéré comme courrier indésirable ou courrier indésirable potentiel par l'Anti-Spam est marqué à l'aide du texte **[!! SPAM]** ou **[?? Probable Spam]** dans l'**Objet**. Si un traitement complémentaire des messages après l'analyse par l'Anti-Spam s'impose, vous pouvez configurer Microsoft Outlook Express (Windows Mail).

La fenêtre de configuration du traitement du courrier indésirable s'ouvre au premier lancement du client de messagerie après l'installation de l'application. Vous pouvez l'ouvrir également en cliquant sur le bouton **Configuration** situé dans la barre d'outils du client de messagerie à côté des boutons **Courrier indésirable** et **Courrier normal**.

CREATION DE REGLES DE TRAITEMENT DES MESSAGES POUR LE COURRIER INDESIRABLE

Les instructions ci-dessous décrivent la création d'une règle de traitement des messages pour le courrier indésirable en utilisant l'Anti-Spam dans le client de messagerie Microsoft Office Outlook. Vous pouvez vous inspirer de ces instructions pour créer vos propres règles.

Pour créer une règle de traitement d'un message à la recherche de courrier indésirable, procédez comme suit :

1. Lancez Microsoft Office Outlook et utilisez la commande **Service** → **Règles et notifications** du menu principal de l'application. La méthode à employer pour ouvrir l'Assistant dépend de la version de Microsoft Office Outlook que vous utilisez. Dans notre cas, nous envisageons la création d'une règle dans Microsoft Office Outlook 2003.

2. Dans la fenêtre **Règles et notification**, passez à l'onglet **Règles pour le courrier électronique** et cliquez sur **Nouvelle**. Cette action entraîne le lancement de l'Assistant de création d'une règle. Il contient une succession de fenêtres (étapes) :

   a. Vous devez choisir entre la création d'une règle à partir de zéro ou selon un modèle. Sélectionnez l'option **Créer une règle** et en guise de condition de l'analyse, sélectionnez **Analyse des messages après la réception**. Cliquez sur **Suivant**.

   b. Dans la fenêtre de sélection des conditions de tri des messages, cliquez sur **Suivant** sans cocher aucune case. Confirmez l'application de cette règle à tous les messages reçus dans la fenêtre de confirmation.

   c. Dans la fenêtre de sélection des actions sur les messages, cochez la case **exécuter une action complémentaire** dans la liste des actions. Dans la partie inférieure de la fenêtre, cliquez sur le lien **action complémentaire**. Dans la fenêtre qui s'ouvre, sélectionnez **Kaspersky Anti-Spam** dans la liste déroulante, puis cliquez sur **OK**.

   d. Dans la fenêtre des exclusions de la règle, cliquez sur **Suivant** sans cocher aucune case.

   e. Dans la fenêtre finale de création de la règle, vous pouvez changer son nom (le nom par défaut est Kaspersky Anti-Spam). Assurez-vous que la case **Activer la règle** est cochée, puis cliquez sur **Terminer**.

3. Par défaut, la nouvelle règle sera ajoutée en tête de la liste des règles de la fenêtre **Règles et notifications**. Déplacez cette règle à la fin de la liste si vous voulez qu'elle soit appliquée en dernier lieu au message.

Tous les messages qui arrivent dans la boîte aux lettres sont traités sur la base des règles. L'ordre d'application des règles dépend de la priorité attribuée à chaque règle. Les règles sont appliquées dans l'ordre de la liste. Chaque règle a une priorité inférieure à la règle précédente. Vous pouvez élever ou réduire la priorité d'application d'une règle en la déplaçant vers le haut ou vers le bas dans la liste. Si vous ne souhaitez pas que le message, après l'exécution d'une règle quelconque, soit traité par une règle de l'Anti-Spam, il faudra cocher la case **arrêter le traitement ultérieur des règles** dans les paramètres de cette règle (cf. Etape 3 de la fenêtre de création des règles).

THE BAT!

Les actions à exécuter sur le courrier indésirable et le courrier indésirable potentiel dans The Bat! sont définies à l'aide des outils du client.

Pour passer à la configuration des règles de traitement du courrier indésirable dans The Bat!, procédez comme suit :

1. Dans le menu **Propriétés** du client de messagerie, sélectionnez l'option **Configuration**.

2. Sélectionnez l'objet **Protection contre le courrier indésirable** dans l'arborescence des paramètres.

Les paramètres de protection contre le courrier indésirable sont appliqués à tous les modules de l'Anti-Spam installés sur l'ordinateur compatibles avec The Bat!

Vous devez définir le niveau d'évaluation et indiquer comment agir sur les messages correspondant au niveau défini (pour l'Anti-Spam, la probabilité que le message est un exemple de courrier indésirable) :

- Supprimer les messages dont le niveau d'évaluation est supérieur au niveau indiqué ;
- Déplacer les messages du niveau défini dans un dossier spécial pour les messages non sollicités ;
- Déplacer les messages non sollicités marqués d'un en-tête spéciale dans le dossier du courrier indésirable ;
- Laisser les messages non sollicités dans le dossier **Entrant**.

Suite au traitement des messages électroniques, Kaspersky PURE attribue le statut courrier indésirable ou courrier indésirable potentiel en fonction d'un indice dont vous pouvez modifier la valeur. Dans The Bat!, on retrouve un algorithme spécial d'évaluation des messages qui repose également sur un indice de courrier indésirable. Afin d'éviter les écarts entre l'indice de courrier indésirable dans Kaspersky PURE et dans The Bat!, tous les messages analysés par l'Anti-Spam reçoivent une évaluation correspondant à l'état du message : courrier normal - 0%, courrier indésirable

potentiel - 50%, courrier indésirable - 100%. Ainsi, l'évaluation du message dans The Bat! correspond non pas à l'indice de courrier indésirable attribué par l'Anti-Spam mais bien à l'indice de l'état correspondant.

Pour de plus amples informations sur l'évaluation du courrier indésirable et sur les règles de traitement, consultez la documentation relative au client de messagerie The Bat!

THUNDERBIRD

Par défaut, le courrier qui est considéré comme courrier indésirable ou courrier indésirable potentiel par l'Anti-Spam est marqué à l'aide du texte **[!! SPAM]** ou **[?? Probable Spam]** dans l'**Objet**. Si un traitement complémentaire des messages après l'analyse par l'Anti-Spam s'impose, vous pouvez configurer Thunderbird dans la fenêtre de configuration accessible via **Outils** → **Filtres de messages** (pour obtenir les instructions d'utilisation détaillées du client de messagerie, consultez l'aide de Mozilla Thunderbird).

Le plug-in de l'Anti-Spam pour Thunderbird permet d'étudier les messages reçus et envoyés à l'aide de ce client de messagerie et de vérifier si le courrier contient des messages non sollicités. Le module est intégré à Thunderbird et transmet les messages à l'Anti-Spam afin qu'ils puissent être analysés à l'aide de la commande du menu **Outils** → **Traquer les indésirables dans ce dossier**. Ainsi, la recherche des messages non sollicités revient à Kaspersky PURE et non pas à Thunderbird. Les fonctions de Thunderbird ne sont en rien modifiées.

L'état du plug-in de l'Anti-Spam apparaît sous la forme d'une icône dans la barre d'état de Thunderbird. Une icône grise indique qu'un problème s'est présenté dans le fonctionnement du plug-in ou que l'Anti-Spam est désactivé. Vous pouvez ouvrir la fenêtre de configuration des paramètres de Kaspersky PURE d'un double-clique sur l'icône de l'application. Pour passer à la configuration des paramètres de l'**Anti-Spam**, cliquez sur le bouton **Configuration** dans le groupe Anti-Spam.

ANTI-BANNIERE

L'Anti-bannière a été développé pour bloquer l'affichage des bannières sur les sites que vous visitez et dans l'interface de quelques applications. Le message publicitaire des bannières peut vous distraire tandis que le chargement des bannières augmente le volume du trafic téléchargé.

Avant de pouvoir s'afficher sur la page Web ou dans la fenêtre de l'application, la bannière doit être téléchargée depuis Internet. L'Anti-bannière vérifie l'adresse d'où le téléchargement a lieu. Si l'adresse correspond à un masque quelconque de la liste livrée avec Kaspersky PURE ou de la liste des adresses de bannières interdites que vous avez créée, l'Anti-bannière bloque le bandeau publicitaire. Le blocage des bannières dont les masques d'adresse ne figurent pas dans les listes citées est décidé par l'analyseur heuristique.

De plus, vous pouvez créer la liste des adresses autorisées sur la base de laquelle les bannières seront affichées.

DANS CETTE SECTION

Activation et désactivation de l'Anti-bannière 136

Sélection des méthodes d'analyse 137

Composition des listes d'adresses de bannières autorisées ou interdites 137

Exportation et importation des listes d'adresses 137

ACTIVATION ET DESACTIVATION DE L'ANTI-BANNIERE

Par défaut, l'Anti-bannière est activé et fonctionne en mode optimal. Vous pouvez désactiver l'Anti-bannière le cas échéant.

Pour activer ou désactiver l'Anti-bannière, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

4. Dans la partie droite de la fenêtre, décochez la case **Activer l'Anti-bannière** s'il faut désactiver le composant. Cochez cette case s'il faut activer le composant.

SELECTION DES METHODES D'ANALYSE

Vous pouvez désigner la méthode que devra utiliser l'Anti-bannière pour analyser les adresses d'où les bannières pourront être chargées. En plus de ces méthodes, l'Anti-bannière analyse l'adresse afin de voir si elle correspond aux masques de la liste des adresses autorisées ou interdites, quand de telles listes sont utilisées.

Pour sélectionner les méthodes d'analyse des adresses par l'Anti-bannière, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

4. Dans la partie droite de la fenêtre, dans le groupe **Méthodes d'analyse**, cochez la case en regard des noms de méthode à utiliser.

COMPOSITION DES LISTES D'ADRESSES DE BANNIERES AUTORISEES OU INTERDITES

Les listes d'adresses de bannières autorisées ou interdites permettent d'indiquer les adresses au départ desquelles l'affichage des bannières doit être autorisé ou interdit. Composez une liste de masques d'adresses interdites et l'Anti-bannière bloquera le chargement et l'affichage des bannières depuis les adresses correspondant à ces masques. Composez une liste de masques d'adresses autorisées et l'Anti-bannière chargera et affichera les bannières depuis les adresses correspondant à ces masques.

Pour ajouter un masque à la liste des adresses autorisées ou interdites, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

4. Dans le groupe **Avancé** de la partie droite de la fenêtre, cochez la case **Utiliser la liste "noire" des adresses** (ou **Utiliser la liste "blanche" des adresses**), puis cliquez sur le bouton **Configuration** situé à droite de la case.

   La fenêtre **Liste "noire"** (ou **Liste "blanche"**) s'ouvre.

5. Cliquez sur le lien **Ajouter** pour ouvrir la fenêtre **Masque d'adresse (URL)**.

6. Saisissez le masque de l'adresse interdite (autorisée) de la bannière et cliquez sur le bouton **OK**.

Si, à l'avenir, vous ne souhaitez plus utiliser un masque, il n'est pas nécessaire de le supprimer. Il suffit de désélectionner la case en regard du masque en question.

EXPORTATION ET IMPORTATION DES LISTES D'ADRESSES

Une fois que vous aurez créé une liste d'adresses de bannière autorisées ou interdites, vous pourrez la réutiliser, par exemple en transférant les adresses de bannière dans une liste identique sur un autre ordinateur équipé de Kaspersky PURE.

Voici la marche est à suivre :

1. Procédez à une *exportation*, c.-à-d. copiez les entrées de la liste dans un fichier.

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

3. Procédez à une *importation*, c.-à-d. ajoutez les entrées du fichier à une liste identique sur un autre ordinateur.

Lors de l'exportation de la liste, vous serez invité à copier uniquement l'élément sélectionné de la liste ou toute la liste. Lors de l'importation, vous pouvez ajouter de nouveaux éléments à la liste ou écraser la liste existante par la liste importée.

Pour exporter les adresses de bannière depuis la liste des adresses autorisées ou interdites, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

4. Dans la partie droite de la fenêtre, dans le groupe **Avancé**, cliquez sur le bouton **Configuration** situé sur la ligne du nom de la liste au départ de laquelle il faut copier l'adresse.

5. Dans la fenêtre **Liste noire** (ou **Liste blanche**) qui s'ouvre, cochez la case en regarde des adresses à inclure dans le fichier.

6. Cliquez sur le bouton **Exporter**.

   Une fenêtre s'ouvre et vous avez la possibilité d'exporter uniquement les éléments sélectionnés. Exécutez dans cette fenêtre une des opérations suivantes :

   - Cliquez sur le bouton **Oui** s'il faut uniquement inclure les adresses sélectionnées ;

   - Cliquez sur le bouton **Non** s'il faut inclure la liste complète.

7. Dans la fenêtre qui s'ouvre, saisissez un nom pour le fichier à enregistrer et confirmez l'enregistrement.

Pour importer les adresses de bannière d'un fichier dans la liste des adresses autorisées ou interdites, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

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

4. Dans la partie droite de la fenêtre, dans le groupe **Avancé**, cliquez sur le bouton **Configuration** situé sur la ligne du nom de la liste à laquelle il faut ajouter l'adresse.

5. Dans la fenêtre **Liste noire** (ou **Liste blanche**) qui s'ouvre; cliquez sur le bouton **Importer**.

   Si la liste n'est pas vide, une fenêtre s'ouvre et vous avez la possibilité d'ajouter les éléments importés. Exécutez dans cette fenêtre une des opérations suivantes :

   - Cliquez sur le bouton **Oui** s'il faut ajouter des entrées du fichier à la liste ;

   - Cliquez sur le bouton **Non** s'il faut remplacer les entrées actuelles de la liste par celles du fichier.

6. Dans la fenêtre qui s'ouvre, sélectionnez le fichier contenant la liste des entrées qu'il faut importer.

CONTROLE DES APPLICATIONS

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

Le composant surveille les actions en exécution dans le système par les applications installées sur les ordinateurs, et il les règle sur la base des règles du Contrôle des Applications. Ces règles réglementent l'activité potentiellement dangereuse, y compris l'accès des applications aux ressources demandées (fichiers et dossiers, clés du registre, adresses de réseau, etc.).

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

Au premier lancement de l'application sur l'ordinateur, le composant Contrôle des Applications analyse la protection de l'application et la place dans un des groupes de confiance. Le groupe de confiance définit les règles que Kaspersky PURE appliquera pour contrôler l'activité de cette application. Les règles du Contrôle des Applications représentent l'ensemble des privilèges d'accès aux ressources de l'ordinateur et des restrictions pour différentes actions des applications sur l'ordinateur.

Vous pouvez configurer les conditions de répartition des applications selon les groupes (cf. page 140), déplacer l'application dans un autre groupe (cf. page 141), et modifier les règles de Kaspersky PURE (cf. page 142).

Pour contribuer au fonctionnement plus efficace du Contrôle des Applications, il est conseillé de participer au Kaspersky Security Network (cf. rubrique "Participation au Kaspersky Security Network" à la page 248). Les données obtenues à l'aide de Kaspersky Security Network permettent de référer plus précisément les applications à un groupe de confiance ou à un autre, et aussi appliquer les règles optimales du contrôle des applications.

Au deuxième lancement de l'application, le Contrôle des Applications vérifie son intégrité. Si l'application n'a pas été modifiée, le composant applique les règles existantes. En cas de modification de l'application, le Contrôle des Applications l'analysera à nouveau, comme à l'occasion de la première exécution.

Afin de contrôler l'accès des applications à différentes ressources de l'ordinateur, vous pouvez utiliser la liste prédéfinie de ressources protégées ou compléter la liste aves les ressources d'utilisateurs (cf. page 145).

DANS CETTE SECTION

Activation et désactivation du Contrôle des Applications 139

Répartition des applications selon les groupes 140

Consultation de l'activité des applications 141

Modification du groupe de confiance 141

Règles du Contrôle des Applications 142

Protection des ressources du système d'exploitation et des données personnelles 145

ACTIVATION ET DESACTIVATION DU CONTROLE DES APPLICATIONS

Le Contrôle des Applications est activé par défaut et fonctionne selon le mode défini par les experts de Kaspersky Lab, mais vous pouvez le désactiver si nécessaire.

Pour activer ou désactiver le Contrôle des Applications, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, choisissez-le composant **Contrôle des Applications** dans la rubrique **Protection**.

4. Dans la partie droite de la fenêtre, décochez la case **Activer le Contrôle des Applications** s'il faut désactiver le composant. Cochez cette case s'il faut activer le composant.

REPARTITION DES APPLICATIONS SELON LES GROUPES

Au premier lancement de l'application sur l'ordinateur, le composant Contrôle des Applications analyse la protection de l'application et la place dans un des groupes de confiance.

A la première étape de l'analyse de l'application, Kaspersky PURE cherche l'enregistrement sur l'application dans la base interne des applications connues, et puis envoie une demande à la base Kaspersky Security Network (dans le cas de la connexion à Internet). Si l'enregistrement a été trouvé dans la base, alors l'application se place dans le groupe enregistré dans la base.

Les applications qui ne présentent aucun danger pour le système se placent dans le groupe **De confiance**. Par défaut, ce groupe réunit les applications possédant une signature numérique, ainsi que les applications dont l'objet parent possède une signature numérique.

Vous pouvez désactiver l'ajout automatique des applications de la base de Kaspersky Security Network ou possédant une signature numérique au groupe **De confiance.**

Le comportement des applications que le Contrôle des Applications place dans le groupe **De confiance** sera tout de même contrôlé par le composant Défense Proactive.

Pour répartir les applications inconnues dans les groupes (absents dans la base Kaspersky Security Network et sans la signature numérique), Kaspersky PURE utilise par défaut l'analyse heuristique. Pendant cette analyse, le classement de danger de l'application se définit. A la base de ce classement l'application se place dans un groupe ou dans l'autre. A la place de l'analyse heuristique, vous pouvez indiquer le groupe dans lequel Kaspersky PURE va automatiquement placer toutes les applications inconnues.

Par défaut, le Contrôle des Applications analyse l'application pendant 30 secondes. Si à l'issue de ce temps, la définition du classement de danger n'a pas été terminée, l'application se place dans le groupe **Restrictions faibles**, et la définition du classement du danger continue en arrière plan. Puis l'application se place dans le groupe définitif. Vous pouvez modifier la durée consacrée à l'analyse des applications exécutées. Si vous êtes convaincu que toutes les applications exécutées sur votre ordinateur ne menacent pas la sécurité, vous pouvez réduire la durée de l'analyse. Si, au contraire, vous installez une application dont vous ne pouvez garantir la fiabilité en matière de sécurité, il est conseillé d'augmenter la durée de l'analyse.

Si le classement de danger et élevé, Kaspersky PURE va vous informer de ce fait et va proposer de sélectionner le groupe à placer cette application. La notification contient les statistiques d'utilisation de cette application par les participants de Kaspersky Security Network. Sur la base de ces statistiques et en connaissant l'historique de l'apparition de l'application sur l'ordinateur, vous pouvez prendre une décision plus objective sur le groupe à placer cette application.

- *Pour désactiver l'ajout automatique au groupe **De confiance** des applications contenues dans la base de Kaspersky Security Network ou qui possèdent une signature numérique, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.

  2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

  3. Dans la partie gauche de la fenêtre, choisissez-le composant **Contrôle des Applications** dans la rubrique **Protection**.

  4. Dans la partie droite de la fenêtre, dans le groupe **Applications de confiance**, décochez les cases **Avec une signature numérique** et **Présentes dans la base de Kaspersky Security Network**.

- *Pour utiliser l'analyse heuristique pour répartir les applications inconnues dans les groupes, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, choisissez-le composant **Contrôle des Applications** dans la rubrique **Protection**.

4. Dans la partie droite de la fenêtre, dans le groupe **Applications de confiance**, sélectionnez l'option **Utiliser l'analyse heuristique pour définir le groupe**.

Pour modifier la durée accordée à la définition du groupe de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, choisissez-le composant **Contrôle des Applications** dans la rubrique **Protection**.

4. Dans la partie droite de la fenêtre, dans le groupe **Avancé**, mettez au point **Durée maximale pour déterminer le groupe de l'application**.

Pour placez toutes les applications inconnues dans le groupe indiqué, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, choisissez-le composant **Contrôle des Applications** dans la rubrique **Protection**.

4. Dans la parties droite de la fenêtre, dans le groupe **Applications de confiance**, sélectionnez l'option **Placer automatiquement dans le groupe** et sélectionnez le groupe nécessaire dans la liste déroulante.

CONSULTATION DE L'ACTIVITE DES APPLICATIONS

Vous pouvez consulter les informations sur toutes les applications utilisées sur votre ordinateur, et sur tous les processus en cours d'exécution.

Pour consulter l'activité des applications, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.

3. Cliquez sur le lien **Surveillance des Applications** situé dans la partie droite de la fenêtre.

4. Dans la fenêtre **Surveillance des Applications** sélectionnez la catégorie requise dans la liste **Catégorie**.

MODIFICATION DU GROUPE DE CONFIANCE

Au premier lancement de l'application, Kaspersky PURE la place automatiquement dans un groupe ou dans l'autre (cf. section "Répartition des applications selon les groupes" à la page 140). Le cas échéant, vous pouvez manuellement déplacer l'application dans un autre groupe.

Les experts de Kaspersky Lab déconseillent de déplacer les applications du groupe défini automatiquement dans un autre groupe. Au lieu de cela, modifiez si nécessaire les règles pour l'application en question (cf. rubrique "Modification des règles de l'application" à la page 143).

Pour déplacer l'application dans un autre groupe, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.

3. Cliquez sur le lien **Surveillance des Applications** situé dans la partie droite de la fenêtre.

4. Dans la fenêtre **Surveillance des Applications** sélectionnez la catégorie requise dans la liste **Catégorie**.

5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'application nécessaire, puis sélectionnez l'option **Déplacer dans un groupe → <nom du groupe>**.

Pour replacer l'application dans le groupe par défaut, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.

3. Cliquez sur le lien **Surveillance des Applications** situé dans la partie droite de la fenêtre.

4. Dans la fenêtre **Surveillance des Applications** sélectionnez la catégorie requise dans la liste **Catégorie**.

5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel pour l'application nécessaire, puis sélectionnez l'option **Déplacer dans un groupe → Rétablir le groupe par défaut**.

REGLES DU CONTROLE DES APPLICATIONS

Les règles du Contrôle des Applications représentent l'ensemble des privilèges d'accès aux ressources de l'ordinateur et des restrictions pour différentes actions des applications sur l'ordinateur.

Par défaut, les règles du groupe de confiance dans lequel Kaspersky PURE a placé l'application à son premier lancement sont appliquées pour contrôler l'application. Les règles des groupes ont été élaborées par les experts de Kaspersky Lab pour le contrôle optimal de l'activité des applications. Le cas échéant, vous pouvez modifier ces règles, et les aussi configurer au niveau d'une application en particulier. Les règles de l'application ont une priorité plus élevée que les règles du groupe.

DANS CETTE SECTION

Modification des règles du groupe 142

Modification des règles de l'application 143

Création d'une règle de réseau de l'application 143

Configuration des exclusions 144

Restriction héritée du processus parent 144

Suppression de règles pour les applications 145

MODIFICATION DES REGLES DU GROUPE

Les ensembles optimaux des privilèges d'accès aux ressources de l'ordinateur sont définis par défaut pour différents groupes de confiance. Vous pouvez modifier les règles proposées du groupe.

Pour modifier les règles du groupe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez-le composant **Contrôle des Applications** dans la rubrique **Protection**.
4. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration des règles**.
5. Sélectionnez le groupe requis dans la fenêtre **Règles de groupes d'application** qui s'ouvre.
6. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles**, modifiez les règles d'accès pour les catégories de ressource requises.

MODIFICATION DES REGLES DE L'APPLICATION

A la première exécution de l'application, le Contrôle des Applications définit sont état et la place dans le groupe correspondant. Ensuite, le composant enregistre les actions exécutées par l'application dans le système et régit son activité sur la base du groupe auquel elle appartient. Lorsque l'application contacte la ressource, le composant vérifie si l'application possède les privilèges d'accès requis et exécute l'action définie par la règle. Vous pouvez modifier la règle rédigée pour l'application afin de définir son état et de la place dans le groupe correspondant.

Pour modifier une règle pour l'application, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.
3. Cliquez sur le lien **Surveillance des Applications** situé dans la partie droite de la fenêtre.
4. Dans la fenêtre **Surveillance des Applications** sélectionnez la catégorie requise dans la liste **Catégorie**.
5. Choisissez l'application, puis dans la colonne **Groupe**, cliquez avec le bouton gauche de la souris sur le lien représentant le groupe de l'application.
6. Dans le menu déroulant, choisissez l'option **Paramètres de l'utilisateur**.
7. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles**, modifiez les règles d'accès pour les catégories de ressource requises.

CREATION D'UNE REGLE DE RESEAU DE L'APPLICATION

Si vous devez traiter l'accès de l'application à un service de réseau en particulier, vous pouvez créer une règle de réseau.

Pour créer une règle qui régit l'activité de réseau de l'application, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.
3. Cliquez sur le lien **Surveillance des Applications** situé dans la partie droite de la fenêtre.
4. Dans la fenêtre **Surveillance des Applications** sélectionnez la catégorie requise dans la liste **Catégorie**
5. Choisissez l'application, puis dans la colonne **Groupe**, cliquez avec le bouton gauche de la souris sur le lien représentant le groupe de l'application.

6. Dans le menu déroulant, choisissez l'option **Paramètres de l'utilisateur**.

7. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles**, sélectionnez dans la liste déroulante la catégorie **Règles de réseau** puis cliquez sur le lien **Ajouter**.

8. Dans la fenêtre **Règle de réseau** qui s'ouvre, définissez les paramètres de la règle de réseau.

9. 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**.

   Une fois que vous aurez créé une règle, vous pourrez modifier ses paramètres ou la supprimer à l'aide des liens de la partie inférieure de l'onglet. Pour désactiver une règle, décochez la case en regard de son nom.

CONFIGURATION DES EXCLUSIONS

Lors de la création de règles pour l'application, Kaspersky PURE contrôle par défaut toute action des applications, l'accès aux fichiers et aux répertoires, l'accès au milieu d'exécution et l'accès au réseau. Vous pouvez exclure certaines actions de l'analyse.

Pour exclure des actions d'une application de l'analyse, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.

3. Cliquez sur le lien **Surveillance des Applications** situé dans la partie droite de la fenêtre.

4. Dans la fenêtre **Surveillance des Applications** sélectionnez la catégorie requise dans la liste **Catégorie**

5. Choisissez l'application, puis dans la colonne **Groupe**, cliquez avec le bouton gauche de la souris sur le lien représentant le groupe de l'application.

6. Dans le menu déroulant, choisissez l'option **Paramètres de l'utilisateur**.

7. Dans la fenêtre qui s'ouvre, sous l'onglet **Exclusions**, cochez les cases correspondantes aux actions à exclure. En cas d'exclusion de l'analyse du trafic de réseau de l'application, configurez les paramètres avancés d'exclusion.

   Toutes les exclusions créées dans les règles pour les applications sont accessibles dans la fenêtre de configuration des paramètres de l'application, dans le groupe **Menaces et exclusions**.

RESTRICTION HERITEE DU PROCESSUS PARENT

L'utilisateur ou une autre application en cours d'exécution peut être à l'origine du lancement d'une application. Si l'application a été lancée par une autre, alors la séquence de lancement est composée des applications mère et fille.

Lorsque l'application tente d'accéder à la ressource contrôlée, le Contrôle des Applications analyse les privilèges de tous les processus parent de cette application afin de voir s'ils peuvent accéder à la ressource. Dans ce cas, c'est la règle de la priorité minimale qui est appliquée : lorsque les privilèges d'accès de l'application et du processus parent sont comparés, les privilèges d'accès avec la priorité minimale seront appliqués à l'activité de l'application.

Priorité des privilèges d'accès :

1. Autoriser. Ces privilèges d'accès ont une priorité élevée.

2. Confirmer l'action.

3. Bloquer. Ces privilèges d'accès ont une priorité faible.

Ce mécanisme empêche l'utilisation d'applications de confiance par des applications douteuses ou dont les privilèges sont réduits pour exécuter des actions avec des privilèges.

Si l'activité de l'application est bloquée à cause du manque des droits chez un des processus parental, vous pouvez changer ces règles (cf. section "Modification des règles pour l'application sélectionnée" à la page 143) ou désactiver l'héritage des restrictions du processus parent.

Modifiez les privilèges du processus parent et désactivez l'héritage des restrictions uniquement si vous êtes absolument certain que l'activité du processus ne menace pas la sécurité du système !

Pour désactiver l'héritage des restrictions du processus parent, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.

3. Cliquez sur le lien **Surveillance des Applications** situé dans la partie droite de la fenêtre.

4. Dans la fenêtre **Surveillance des Applications** sélectionnez la catégorie requise dans la liste **Catégorie**

5. Choisissez l'application, puis dans la colonne **Groupe**, cliquez avec le bouton gauche de la souris sur le lien représentant le groupe de l'application.

6. Dans le menu déroulant, choisissez l'option **Paramètres de l'utilisateur**.

7. Dans la fenêtre qui s'ouvre, accédez à l'onglet **Règles** et décochez la case **Restriction héritée du processus parent (application)**.

SUPPRESSION DE REGLES POUR LES APPLICATIONS

Les règles des applications qui n'ont pas été utilisées depuis 60 jours sont supprimées automatiquement par défaut. Vous pouvez modifier la durée de conservation des règles des applications non utilisées et désactiver la suppression automatique.

Pour définir la durée de conservation des règles des applications, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Ma Protection**.

3. Pour le composant sélectionné dans le groupe **Avancé**, cochez la case **Supprimer les règles des applications qui n'ont plus été lancées depuis** et dans le champ à droite, définissez le nombre de jours requis.

Pour désactiver la suppression automatique des règles pour les applications non utilisées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Ma Protection**.

3. Après avoir choisi le composant, dans le groupe **Avancé**, décochez la case **Supprimer les règles d'applications qui n'ont plus été lancées depuis**.

PROTECTION DES RESSOURCES DU SYSTEME D'EXPLOITATION ET DES DONNEES PERSONNELLES

Le Contrôle des Applications gère les privilèges des applications au niveau des actions à exécuter sur différentes catégories de ressources du système d'exploitation et des données personnelles.

Les experts de Kaspersky Lab ont sélectionné des catégories de ressources à protéger. Il est impossible de modifier cette liste. Cependant, vous pouvez compléter cette liste avec les catégories d'utilisateurs et/ou les ressources distinctes. Vous pouvez aussi refuser le contrôle des ressources sélectionnées.

- *Pour ajouter des données personnelles à protéger, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Ma Protection**.
3. Une fois le composant sélectionné, cliquez sur **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Données personnelles**, sélectionnez la catégorie de données personnelles requise dans la liste déroulante **Catégorie** et ouvrez la fenêtre d'ajout des ressources en cliquant sur le lien **Ajouter**.
5. Dans la fenêtre **Ressource de l'utilisateur** qui s'ouvre, cliquez sur **Parcourir** et saisissez les données requises en fonction de la ressource ajoutée.

Après avoir ajouté la ressource, vous pouvez la modifier ou la supprimer à l'aide des boutons du même nom dans la partie supérieure de l'onglet. Pour désactiver le contrôle d'une ressource ou d'une catégorie, décochez la case à côté de lui.

- *Pour créer une catégorie de données personnelles à protéger, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Ma Protection**.
3. Une fois le composant sélectionné, cliquez sur **Configuration**.
4. Sous l'onglet **Données personnelles** de la fenêtre qui s'ouvre, cliquez sur le lien **Ajouter une catégorie** pour ajouter des ressources.
5. Dans la fenêtre **Catégorie des ressources d'utilisateur** qui s'ouvre, saisissez le nom de la nouvelle catégorie de ressource.

- *Pour ajouter des paramètres et des ressources du système d'exploitation à protéger, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Ma Protection**.
3. Une fois le composant sélectionné, cliquez sur **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Système d'exploitation**, sélectionnez la catégorie d'objet du système d'exploitation requise dans la liste déroulante **Catégorie** et ouvrez la fenêtre d'ajout des ressources en cliquant sur le lien **Ajouter**.

Après avoir ajouté la ressource, vous pouvez la modifier ou la supprimer à l'aide des boutons du même nom dans la partie supérieure de l'onglet. Pour désactiver le contrôle d'une ressource ou d'une catégorie, décochez la case à côté de lui.

DEFENSE PROACTIVE

La Défens Proactive protège l'ordinateur contre les nouvelles menaces dont les informations ne figurent pas encore dans les bases de Kaspersky PURE.

Les technologies préventives sur lesquelles repose la Défense Proactive évitent les pertes de temps et permettent de neutraliser la nouvelle menace avant qu'elle n'ait pu nuire à votre ordinateur. À la différence des technologies réactives qui réalisent l'analyse selon les enregistrements des bases de Kaspersky PURE, les technologies préventives identifient les nouvelles menaces en suivant les séquences d'actions exécutées par une application quelconque. Si l'analyse de la séquence d'actions de l'application éveille des soupçons, Kaspersky PURE bloque l'activité de cette application.

Ainsi, si un programme se copie dans une ressource de réseau, dans le répertoire de démarrage et dans la base de registres, on peut affirmer sans crainte qu'il s'agit d'un ver. Parmi les séquences d'actions dangereuses, nous pouvons citer également les tentatives de modification du fichier HOSTS, la dissimulation de l'installation de pilotes, etc. Vous pouvez néanmoins refuser de contrôler une activité dangereuse (cf. page 148) ou l'autre.

À la différence du composant Contrôle des Applications, la Défense Proactive réagit précisément à la séquence d'actions de l'application. L'analyse de l'activité a lieu pour toutes les applications, y compris pour celles placées dans le groupe **De confiance** par le composant Contrôle des Applications (cf. page 139).

Vous pouvez créer un groupe d'applications (cf. page 148) de confiance pour la Défense Proactive. Les notifications sur l'activité de ces applications ne seront pas affichées.

Si l'ordinateur tourne sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 ou Microsoft Windows 7 x64, certains événements ne seront pas contrôlés. Ceci est lié aux particularités des systèmes d'exploitation cités. Ainsi, l'envoi des données par les applications de confiance et l'activité suspecte dans le système ne seront pas contrôlés en entier.

DANS CETTE SECTION

Activation et désactivation de la Défense Proactive 147

Composition d'un groupe d'applications de confiance 148

Utilisation de la liste des activités dangereuses 148

Modification d'une règle de contrôle de l'activité dangereuse 148

Retour à l'état antérieur aux actions du programme malveillant 149

ACTIVATION ET DESACTIVATION DE LA DEFENSE PROACTIVE

La Défense Proactive est activée par défaut et fonctionne selon le mode optimal. Le cas échéant, vous pouvez désactiver la Défense Proactive.

Pour activer ou désactiver la Défense Proactive, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Défense Proactive**.
4. Dans la partie droite de la fenêtre, décochez la case **Activer la Défense Proactive** s'il faut désactiver le composant. Cochez cette case s'il faut activer le composant.

COMPOSITION D'UN GROUPE D'APPLICATIONS DE CONFIANCE

Les applications auxquelles Contrôle des Applications a attribué l'état **De confiance** ne présentent aucun danger pour le système. Toutefois, l'activité de ces applications est contrôlée également par la Défense Proactive.

Vous pouvez composer des groupes d'applications de confiance dont l'activité sera ignorée par la Défense Proactive. Les applications dotées d'une signature numérique et les applications figurant dans la base de Kaspersky Security Network sont reprises par défaut dans la catégorie des applications de confiance.

Pour modifier les paramètres de composition d'un groupe d'applications de confiance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Défense Proactive**.
4. Dans le groupe **Applications de confiance** de la partie droite de la fenêtre cochez la case en regard des paramètres requis.

UTILISATION DE LA LISTE DES ACTIVITES DANGEREUSES

La liste des actions en rapport avec les activités dangereuses ne peut être modifiée. Vous pouvez néanmoins refuser de contrôler une activité dangereuse ou l'autre.

Pour refuser de contrôler une activité dangereuse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Défense Proactive**.
4. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
5. Dans la fenêtre **Défense Proactive** qui s'ouvre, décochez la case située en regard du nom de l'activité dont vous refusez le contrôle.

MODIFICATION D'UNE REGLE DE CONTROLE DE L'ACTIVITE DANGEREUSE

Il est impossible de modifier l'action des applications dont l'activité est jugée dangereuse. Vous pouvez exécuter les opérations suivantes :

- refuser de contrôler une activité quelconque (cf. page 148) ;
- Composer une liste d'exclusions reprenant les applications que vous n'estimez pas dangereuses ;
- Modifier la règle qui définit le fonctionnement de la Défense Proactive lors de la découverte d'activités dangereuses.

Afin de modifier une règle, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Défense Proactive**.

4. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

5. Dans la fenêtre **Défense Proactive** qui s'ouvre, dans la colonne **Evènement**, sélectionnez l'événement pour lequel la règle doit être modifiée.

6. Pour l'événement sélectionné, configurez les paramètres nécessaires de la règle à l'aide des liens dans le bloc de **Description de la règle**. Par exemple :

   a. Cliquez sur le lien indiquant l'action établie et dans la fenêtre **Sélectionner une action** ouverte, sélectionnez l'action nécessaire parmi les actions proposées.

   b. Cliquez sur le lien indiquant la période (n'est pas définie pour tous les types d'activité) et dans la fenêtre **Détection de processus cachés ouverte**, indiquez l'intervalle selon lequel la recherche des processus cachés s'exécutera.

   c. Cliquez sur le lien **Act./Désact.**, pour indiquer la nécessité de créer un rapport sur l'opération exécutée.

RETOUR A L'ETAT ANTERIEUR AUX ACTIONS DU PROGRAMME MALVEILLANT

La Défense Proactive permet d'annuler les effets de l'activité malveillante dans le système.

Quand Kaspersky PURE fonctionne en mode automatique, l'annulation des actions d'une application malveillante s'opère automatiquement quand Ma Défense Proactive découvre une activité malveillante. En mode interactif (cf. page 60), vous pouvez modifier l'action à exécuter en cas de découverte d'une activité malveillante.

Le retour à l'état antérieur aux actions du programme malveillant touche un ensemble de données clairement délimité. Cette procédure n'a aucun impact négatif sur le fonctionnement du système d'exploitation, ni sur l'intégrité des informations enregistrées sur l'ordinateur.

Pour configurer le retour à l'état antérieur aux actions du programme malveillant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Défense Proactive**.

4. Dans la partie droite de la fenêtre, dans le groupe **Avancé**, sélectionnez la réaction souhaitée face aux actions des programmes malveillants.

PROTECTION DU RESEAU

Les différents composants de la protection, les outils et les paramètres de Kaspersky PURE garantissent la protection et le contrôle de votre utilisation du réseau.

Les rubriques suivantes contiennent des informations détaillées sur les principes de fonctionnement et la configuration du Pare-feu, de la Prévention des intrusions, l'analyse des connexions cryptées, la surveillance de l'activité de réseau, les paramètres du serveur proxy et le contrôle des ports de réseau.

DANS CETTE SECTION

Pare-feu 151

Prévention des intrusions 154

Analyse des connexions cryptées 157

Surveillance du réseau 159

Configuration des paramètres du serveur proxy 159

Composition de la liste des ports contrôlés 159

PARE-FEU

Le Pare-feu vous protège pendant l'utilisation des réseaux locaux et d'Internet.

Le composant filtre toute activité de réseau conformément aux règles de réseau du contrôlé des applications. La Règle de réseau est une action que le Pare-feu exécute lorsqu'il détecte une tentative de connexion avec un état déterminé. L'état est attribué à chaque connexion de réseau et est défini par les paramètres suivants : sens et protocole du transfert de données, adresses et de ports utilisés pour la connexion.

Le Pare-feu analyse les paramètres du réseau auquel vous connectez l'ordinateur. Si l'application fonctionne en mode interactif, le Pare-feu vous informera de l'état du réseau contacté lors de la première connexion. Si le mode interactif est désactivé, le Pare-feu déterminera l'état en fonction du type de réseau, de la plage d'adresses et d'autres caractéristiques. Vous pouvez modifier l'état de la connexion de réseau manuellement.

DANS CETTE SECTION

Activation et désactivation du Pare-feu 151

Modification de l'état du réseau 151

Extension de la plage d'adresses du réseau 152

Utilisation des règles du Pare-feu 152

Configuration des notifications sur les modifications du réseau 153

Paramètres de fonctionnement avancés du Pare-feu 154

ACTIVATION ET DESACTIVATION DU PARE-FEU

Par défaut, le Pare-feu est activé et fonctionne en mode optimal. Le cas échéant, vous pouvez désactiver le Pare-feu.

Pour activer ou désactiver le Pare-feu, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Pare-feu**.
4. Dans la partie droite de la fenêtre, décochez la case **Activer le Pare-feu** s'il faut désactiver le composant. Cochez cette case s'il faut activer le composant.

MODIFICATION DE L'ETAT DU RESEAU

La sélection des règles appliquées au filtrage de l'activité de réseau de la connexion sélectionnée dépend de l'état de la connexion. Le cas échéant, vous pouvez modifier l'état du réseau.

Pour modifier l'état d'une connexion de réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Pare-feu**.
3. Une fois le composant sélectionné, cliquez sur **Configuration**.
4. Sous l'onglet **Réseau** de la fenêtre qui s'ouvre, sélectionnez la connexion de réseau active, puis cliquez sur le lien **Modifier**.

5. Dans la fenêtre qui s'ouvre, sous l'onglet **Propriétés**, sélectionnez l'état requis dans la liste déroulante.

EXTENSION DE LA PLAGE D'ADRESSES DE RESEAU

Une ou plusieurs plages d'adresses IP correspondent à chaque réseau. Si vous vous connectez à un réseau dont l'accès aux sous-réseaux s'opère via un routeur, vous pouvez ajouter manuellement les sous-réseaux accessibles via celui-ci.

Exemple : vous vous connectez au réseau d'un des bureaux de votre entreprise et vous souhaitez que les règles de filtrage du bureau où vous êtes connecté directement et celles des bureaux accessibles via le réseau soient identiques.

Demandez à l'administrateur du réseau qu'il vous communique les plages d'adresses de ces bureaux et ajoutez-les.

Pour élargir la plage d'adresses du réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Pare-feu**.
3. Une fois le composant sélectionné, cliquez sur **Configuration**.
4. Sous l'onglet **Réseau** de la fenêtre qui s'ouvre, sélectionnez la connexion de réseau active, puis cliquez sur le lien **Modifier**.
5. Sous l'onglet **Propriétés** de la fenêtre qui s'ouvre, cliquez sur le lien **Ajouter** du groupe **Sous-réseaux** complémentaires.
6. Dans la fenêtre **Adresse IP** qui s'ouvre, définissez l'adresse IP ou un masque d'adresses.

UTILISATION DES REGLES DU PARE-FEU

Le Pare-feu fonctionne sur la base de règles de deux types :

- *Règles pour les paquets.* Elles sont utilisées pour définir des restrictions pour les paquets quelles que soient les applications. Le plus souvent, ces règles limitent l'activité de réseau entrante sur des ports particuliers des protocoles TCP et UDP et filtrent les messages ICMP.
- *Règles des applications*. Elles sont utilisées pour définir des restrictions pour l'activité de réseau d'une application particulière. Ces règles permettent de configurer en détail le filtrage de l'activité lorsque, par exemple, un type déterminé des connexions de réseau est interdit pour certaines applications mais autorisé pour d'autres.

La priorité des règles pour les paquets est plus élevée que la priorité des règles des applications. Si des règles pour les paquets et des règles des applications sont définies pour la même activité de réseau, celle-ci sera traitée selon les règles pour les paquets. Outre cela, vous pouvez définir une priorité d'exécution pour chaque règle.

CREATION D'UNE REGLE POUR UN PAQUET

Les règles pour les paquets sont un ensemble de conditions et d'actions à réaliser sur les paquets lorsque les conditions définies sont vérifiées.

Au moment de créer des règles pour les paquets, n'oubliez pas qu'elles ont priorité sur les règles pour les applications.

Pour créer une règle pour un paquet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Pare-feu**.
3. Une fois le composant sélectionné, cliquez sur **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de filtrage**, sélectionnez le groupe **Règles pour les paquets** puis cliquez sur le lien **Ajouter**.

5. Dans la fenêtre **Règle de réseau** qui s'ouvre, définissez les paramètres requis, puis cliquez sur le bouton **OK**.

6. Pour définir la priorité de la nouvelle règle, déplacez-la vers le haut ou vers le bas de la liste à l'aide des boutons **Haut** et **Bas**.

   Une fois que vous aurez créé une règle, vous pourrez modifier ses paramètres ou la supprimer à l'aide des liens de la partie inférieure de l'onglet. Pour désactiver une règle, décochez la case en regard de son nom.

MODIFICATION DES REGLES DU GROUPE

De manière analogique au composant Contrôle des Applications (cf. page 139), pour le filtrage de l'activité de réseau de l'application, le Pare-feu applique par défaut les règles du groupe où cette application a été placée.

Les règles de réseau du groupe de confiance définissent les privilèges d'accès aux différents réseaux que les applications placées dans ce groupe posséderont. Vous pouvez modifier les règles de réseau proposées du groupe.

Pour modifier une règle de réseau du groupe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

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

3. Après avoir choisi le composant, cliquez sur le bouton **Configuration des règles**.

4. Dans la fenêtre qui s'ouvre, sélectionnez le groupe, ouvrez le menu contextuel pour le réseau d'un clic droit de la souris et choisissez la valeur souhaitée : **Tout autoriser**, **Interdire** ou **Confirmer l'action**.

MODIFICATION DES REGLES DE L'APPLICATION

Vous pouvez créer les règles de réseau pour des applications distinctes. Les règles de réseau de l'application ont une priorité plus élevée que les règles de réseau du groupe.

Le cas échéant, vous pouvez créer des règles de réseau (cf. page 143) pour les applications à l'aide du composant Contrôle des Applications.

Pour créer une règle pour l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

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

3. Une fois le composant sélectionné, cliquez sur **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de filtrage**, sélectionnez le groupe de règles pour l'application puis cliquez sur le lien **Ajouter**.

5. Dans la fenêtre **Règle de réseau** qui s'ouvre, définissez les paramètres de la règle de réseau.

6. Pour définir la priorité de la nouvelle règle, déplacez-la vers le haut ou vers le bas de la liste à l'aide des boutons **Haut** et **Bas**.

   Une fois que vous aurez créé une règle, vous pourrez modifier ses paramètres ou la supprimer à l'aide des liens de la partie inférieure de l'onglet. Pour désactiver une règle, décochez la case en regard de son nom.

CONFIGURATION DES NOTIFICATIONS SUR LES MODIFICATIONS DU RESEAU

Les paramètres des connexions de réseau peuvent changer pendent l'utilisation. Vous pouvez recevoir des notifications sur les modifications des paramètres.

Pour configurer les notifications sur les modifications des paramètres de connexion de réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Pare-feu**.
3. Une fois le composant sélectionné, cliquez sur **Configuration**.
4. Sous l'onglet **Réseau** de la fenêtre qui s'ouvre, sélectionnez la connexion de réseau active, puis cliquez sur le lien **Modifier**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, cochez les cases en regard des événements au sujet desquels vous souhaitez être averti.

PARAMETRES DE FONCTIONNEMENT AVANCES DU PARE-FEU

Vous pouvez définir des paramètres complémentaires pour le Pare-feu tels que l'autorisation du mode actif pour FTP, le blocage des connexions s'il est impossible de demander une confirmation de l'action (l'interface de l'application n'est pas chargée) ou le fonctionnement jusqu'à l'arrêt complet du système.

Tous les paramètres sont activés par défaut.

Afin de définir les paramètres de fonctionnement avancés du Pare-feu, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez-le composant **Pare-feu**.
3. Une fois le composant sélectionné, cliquez sur **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de filtrage**, cliquez sur le bouton **Avancé**.
5. Dans la fenêtre **Avancé** qui s'ouvre, cochez/décochez les cases en regard des paramètres requis.

PREVENTION DES INTRUSIONS

La Prévention des intrusions recherche dans le trafic entrant toute trace d'activité caractéristique des attaques de réseau. Dès qu'il décèle une tentative d'attaque contre votre ordinateur, Kaspersky PURE bloque toute activité de réseau de l'ordinateur qui vous attaque.

Par défaut, le blocage dure une heure. Vous pouvez modifier les paramètres de blocage (cf. page 156). Un message vous avertit qu'une tentative d'attaque de réseau a été menée et vous fournit des informations relatives à l'ordinateur à l'origine de l'attaque. Les descriptions des attaques de réseau connues à l'heure actuelle (cf. section "Types d'attaques de réseau identifiées" à la page 155) et les moyens de lutter contre celles-ci figurent dans les bases de Kaspersky PURE. L'enrichissement de la liste avec les attaques découvertes par la Protection contre les attaques de réseau a lieu lors de la mise à jour (cf. section "Mise à jour" à la page 93) des bases.

DANS CETTE SECTION

Types d'attaques de réseau identifiées 155

Activation et désactivation de la Prévention des intrusions 156

Modification des paramètres de blocage 156

TYPES D'ATTAQUES DE RESEAU IDENTIFIEES

Il existe à l'heure actuelle de nombreux types d'attaques de réseau différentes. Ces attaques exploitent des vulnérabilités du système d'exploitation ou d'autres programmes système ou applicatif.

Afin de garantir la protection de l'ordinateur en permanence, il est bon de connaître les menaces qui planent sur lui. Les attaques de réseau connues peuvent être scindées en trois grands groupes :

- *Balayage des ports* : ce type de menace n'est pas une attaque en tant que telle mais elle devance d'habitude l'attaque car il s'agit d'une des principales manières d'obtenir des informations sur le poste distant. Cette méthode consiste à balayer les ports UDP-/TCP- utilisés par les services de réseau sur l'ordinateur convoité afin de définir leur état (ouvert ou fermé).

  Le balayage des ports permet de comprendre les types d'attaque qui pourraient réussir. De plus, les informations obtenues suite au balayage donnent à l'individu malintentionné une idée du système d'exploitation utilisé sur l'ordinateur distant. Ceci limite encore plus le cercle des attaques potentielles et, par conséquent, le temps consacré à leur organisation et cela permet également d'utiliser des vulnérabilités propres à ce système d'exploitation.

- *Les attaques par déni de service* sont des attaques qui rendent le système pris pour cible instable ou totalement inopérationnel. Parmi les conséquences de ce genre d'attaque, citons l'impossibilité d'utiliser les ressources informatiques ciblées par l'attaque (par exemple, impossible d'accéder à Internet).

  Il existe deux types principaux d'attaques DoS :

  - Envoi vers la victime de paquets spécialement formés et que l'ordinateur n'attend pas. Cela entraîne une surcharge ou un arrêt du système ;

  - Envoi vers la victime d'un nombre élevé de paquets par unité de temps ; l'ordinateur est incapable de les traiter, ce qui épuise les ressources du système.

  Voici des exemples frappants de ce groupe d'attaques :

  - *L'attaque Ping of death* : envoi d'un paquet ICMP dont la taille dépasse la valeur admise de 64 Ko. Cette attaque peut entraîner une panne dans certains systèmes d'exploitation.

  - *L'attaque Land* consiste à envoyer vers le port ouvert de votre ordinateur une requête de connexion avec lui-même. Suite à cette attaque, l'ordinateur entre dans une boucle, ce qui augmente sensiblement la charge du processeur et qui entraîne une panne éventuelle du système d'exploitation.

  - *L'attaque ICMP Flood* consiste à envoyer vers l'ordinateur de l'utilisateur un grand nombre de paquets ICMP. Cette attaque fait que l'ordinateur est obligé de répondre à chaque nouveau paquet, ce qui entraîne une surcharge considérable du processeur.

  - *L'attaque SYN Flood* consiste à envoyer vers votre ordinateur un nombre élevé de requêtes pour l'ouverture d'une connexion. Le système réserve des ressources définies pour chacune de ces connexions. Finalement, l'ordinateur gaspille toutes ses ressources et cesse de réagir aux autres tentatives de connexion.

- *Attaques d'intrusion* qui visent à s'emparer du système. Il s'agit du type d'attaque le plus dangereux car en cas de réussite, le système passe entièrement aux mains de l'individu malintentionné.

  Ce type d'attaque est utilisé lorsque l'individu malintentionné doit absolument obtenir des informations confidentielles sur l'ordinateur distant (par exemple, numéro de carte de crédit, mots de passe) ou simplement pour s'introduire dans le système en vue d'utiliser ultérieurement les ressources au profit de l'individu malintentionné (utilisation du système dans un réseau de zombies ou comme base pour de nouvelles attaques).

  Ce groupe reprend le plus grand nombre d'attaques. Elles peuvent être réparties en trois sous-groupes en fonction du système d'exploitation utilisés par les victimes : attaques sous Microsoft Windows, attaques sous Unix et un groupe commun pour les services de réseau utilisés dans les deux systèmes d'exploitation.

  Les attaques utilisant les services de réseau du système d'exploitation les plus répandues sont :

- *Attaque par débordement de tampon*. Le débordement de tampon survient en cas d'absence de contrôle (ou de contrôle insuffisant) lors de l'utilisation de massifs de données. Il s'agit de l'une des vulnérabilités les plus anciennes et les plus faciles à exploiter.

- *Attaques qui reposent sur des erreurs dans les chaînes de format*. Les erreurs dans les chaînes de format surviennent en raison d'un contrôle insuffisant des valeurs des paramètres entrant des fonctions d'entrée-sortie de format de type *printf()*, *fprintf()*, *scanf()* ou autres de la bibliothèque standard du langage C. Lorsqu'une telle vulnérabilité est présente dans un logiciel, l'individu malintentionné, qui peut envoyer des requêtes formulées spécialement, peut prendre le contrôle complet du système.

  Le système de détection des intrusions analyse automatiquement l'utilisation de telles vulnérabilité et les bloque dans les services de réseau les plus répandus (FTP, POP3, IMAP), s'ils fonctionnent sur l'ordinateur de l'utilisateur.

- *Les attaques ciblant les ordinateurs fonctionnant sous Microsoft Windows,* reposent sur l'exploitation de vulnérabilités d'un logiciel installé (par exemple, des applications telles que Microsoft SQL Server, Microsoft Internet Explorer, Messenger ainsi que les composants systèmes accessibles via le réseau tels que DCom, SMB, Wins, LSASS, IIS5).

De plus, dans certains cas, les attaques d'intrusion exploitent divers types de scripts malveillants, y compris des scripts traités par Microsoft Internet Explorer et diverses versions du ver Helkern. L'attaque Helkern consiste à envoyer vers l'ordinateur distant des paquets UDP d'un certain type capable d'exécuter du code malveillant.

ACTIVATION ET DESACTIVATION DE LA PREVENTION DES INTRUSIONS

Par défaut, la Prévention des intrusions est activée et fonction en mode optimal. Le cas échéant, vous pouvez désactiver la Prévention des intrusions.

Pour activer ou désactiver la Prévention des intrusions, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Prévention des intrusions**.
4. Dans la partie droite de la fenêtre, décochez la case **Activer la Prévention des intrusions** s'il faut désactiver le composant. Cochez cette case s'il faut activer le composant.

MODIFICATION DES PARAMETRES DE BLOCAGE

Par défaut la Prévention des intrusions bloque l'activité de l'ordinateur attaquant durant une heure. Vous pouvez annuler le blocage de l'ordinateur sélectionné ou modifier la durée du blocage.

Pour modifier la durée du blocage de l'ordinateur attaquant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Prévention des intrusions**.
4. Dans la partie droite de la fenêtre, cochez la case **Ajouter l'ordinateur à l'origine de l'attaque à la liste des ordinateurs bloqués pendant** et définissez la durée du blocage.

Pour annuler le blocage de l'ordinateur attaquant, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Dans la partie gauche de la fenêtre, sélectionnez **Protection**.

3. Cliquez sur le lien **Surveillance du réseau** dans la section **Utilisation d'Internet** de la partie droite de la fenêtre pour ouvrir la fenêtre **Surveillance du réseau**.

4. Sous l'onglet **Ordinateurs bloqués**, sélectionnez l'ordinateur bloqué et débloquez-le à l'aide du lien **Débloquer**.

ANALYSE DES CONNEXIONS CRYPTEES

Les connexions à l'aide des protocoles SSL/TLS protègent le canal d'échange des données sur Internet. Les protocoles SSL/TLS permettent d'identifier les parties qui échangent les données sur la base de certificats électroniques, de crypter les données transmises et de garantir leur intégrité tout au long de la transmission.

Ces particularités du protocole sont exploitées par les individus malintentionnés afin de diffuser leurs logiciels malveillants car la majorité des logiciels antivirus n'analyse pas le trafic SSL/TLS.

Kaspersky PURE analyse les connexions cryptées à l'aide d'un certificat de Kaspersky Lab.

Si un certificat non valide est découvert au moment d'établir la connexion avec le serveur (par exemple, il a été remplacé par un individu malintentionné), un message s'affichera et invitera l'utilisateur à accepter ou non le certificat.

Si vous êtes certain que la connexion au site ne constituera jamais une menace, même si le certificat n'est pas correct, vous pouvez l'ajouter à la liste des adresses de confiance. Kaspersky PURE n'analysera plus à l'avenir la connexion sécurisée avec ce site.

Pour activer l'analyse des connexions sécurisées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dans la rubrique **Protection**, choisissez la sous-rubrique **Réseau**.

4. Dans la partie droite de la fenêtre, cochez la case **Analyse des connexions sécurisées** et cliquez sur le bouton **Installer le certificat**.

5. Dans la fenêtre qui s'affiche, cliquez sur **Installer le certificat**. Lancez l'Assistant et suivez les indications pour l'installation du certificat.

L'installation automatique du certificat a lieu uniquement lors de l'utilisation de Microsoft Internet Explorer. Pour l'analyse des connexions sécurisées dans Mozilla Firefox et Opera, installez le certificat de Kaspersky Lab manuellement.

ANALYSE DES CONNEXIONS CRYPTEES DANS MOZILLA FIREFOX

Le navigateur Mozilla Firefox n'utilise pas le référentiel des certificats de Microsoft Windows. Pour analyser les connexions cryptées à l'aide de Firefox, il faut installer manuellement le certificat de Kaspersky Lab.

Pour installer le certificat de Kaspersky Lab, procédez comme suit :

1. Dans le menu du navigateur, sélectionnez l'option **Outils** → **Configuration**.

2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.

3. Dans le groupe **Certificats**, sélectionnez l'onglet **Sécurité** et cliquez sur **Voir le certificat**.

4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certification**, puis cliquez sur le bouton **Restaurer**.

5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. Dans la fenêtre qui s'ouvre, cochez les cases afin de choisir les actions dont l'analyse sera soumise à l'application du certificat installé. Pour consulter les informations relatives au certificat, cliquez sur le bouton **Voir**.

Pour installer le certificat de Kaspersky Lab pour Mozilla Firefox version 3.x, procédez comme suit :

1. Dans le menu du navigateur, sélectionnez l'option **Outils** → **Configuration**.
2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
3. Sous l'onglet **Cryptage**, cliquez sur **Voir le certificat**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certification** puis cliquez sur le bouton **Importer**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab : *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Dans la fenêtre qui s'ouvre, cochez les cases afin de choisir les actions dont l'analyse sera soumise à l'application du certificat installé. Pour consulter les informations relatives au certificat, cliquez sur **Voir**.

Si votre ordinateur tourne sous Microsoft Windows Vista, alors le chemin d'accès au certificat de Kaspersky Lab sera le suivant : *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

ANALYSE DES CONNEXIONS CRYPTEES DANS OPERA

Le navigateur Opera n'utilise pas le référentiel de certificats de Microsoft Windows. Pour analyser les connexions cryptées à l'aide d'Opera, il faut installer manuellement le certificat de Kaspersky Lab.

Pour installer le certificat de Kaspersky Lab, procédez comme suit :

1. Dans le menu du navigateur, sélectionnez l'option **Outils** → **Configuration**.
2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
3. Sélectionnez l'onglet **Sécurité** dans la partie gauche de la fenêtre et cliquez sur le bouton **Administration des certificats**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Editeurs**, puis cliquez sur le bouton **Importer**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab : *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Dans la fenêtre qui s'affiche, cliquez sur **Installer**. Le certificat de Kaspersky Lab sera installé. Pour consulter les informations relatives au certificat et pour sélectionner les actions qui utiliseront le certificat, sélectionnez le certificat dans la liste et cliquez sur le bouton **Voir**.

Pour installer le certificat de Kaspersky Lab pour Opera version 9.x, procédez comme suit :

1. Dans le menu du navigateur, sélectionnez l'option **Outils** → **Configuration**.
2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
3. Sélectionnez l'onglet **Sécurité** dans la partie gauche de la fenêtre et cliquez sur le bouton **Administration des certificats**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certification** puis cliquez sur le bouton **Importer**.

5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. Dans la fenêtre qui s'affiche, cliquez sur **Installer**. Le certificat de Kaspersky Lab sera installé.

Si votre ordinateur tourne sous Microsoft Windows Vista, alors le chemin d'accès au certificat de Kaspersky Lab sera le suivant : *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

SURVEILLANCE DU RESEAU

La Surveillance du réseau est un outil conçu pour consulter les informations relatives à l'activité de réseau en temps réel.

Pour lancer la Surveillance du réseau, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Dans la partie gauche de la fenêtre, sélectionnez **Protection**.

3. Le lien **Surveillance du réseau** ouvre la fenêtre **Surveillance du réseau** qui reprend les informations en rapport avec l'activité de réseau.

CONFIGURATION DES PARAMETRES DU SERVEUR PROXY

Si la connexion à Internet s'opère via un serveur proxy, il faudra alors peut-être configurer les paramètres de connexion à ce dernier. Kaspersky PURE applique ces paramètres à quelques composants de la protection ainsi qu'à la mise à jour des bases et des modules de l'application.

Si votre réseau est doté d'un serveur proxy qui utilise un port inhabituel, il faudra l'ajouter à la liste des ports contrôlés (cf. section "Constitution de la liste des ports contrôlés" à la page 159).

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

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dans la section **Paramètres généraux**; sélectionnez la sous-section **Serveur proxy**.

4. Cochez la case **Utiliser le serveur proxy** et modifiez les paramètres de connexion au serveur proxy.

COMPOSITION DE LA LISTE DES PORTS CONTROLES

Les composants de la protection tels que l'Antivirus Courrier, l'Anti-Spam (cf. page 119), l'Antivirus Internet (cf. page 111) et l'Antivirus IM contrôlent les flux de données transmis par des protocoles définis et qui transitent par certains TCP-ports ouverts de l'ordinateur. Ainsi par exemple, Antivirus Courrier analyse les informations transmises via le protocole SMTP et Antivirus Internet, les informations transmises via les protocoles HTTP, HTTPS et FTP.

Vous pouvez activer le contrôle de tous les ports de réseau ou des ports sélectionnés uniquement. Dans le cadre du contrôle des ports sélectionnés, vous pouvez composer une liste d'applications pour lesquelles il faudra contrôler tous les ports. Il est conseillé d'inclure dans cette liste les applications qui reçoivent ou transmettent des données via FTP.

Pour ajouter un port à la liste des ports contrôlés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la rubrique **Protection**, choisissez la sous-rubrique **Réseau**.
4. Dans la partie droite de la fenêtre, cliquez sur le bouton **Sélectionner**.

   La fenêtre **Ports de réseau** s'ouvre.
5. Le lien **Ajouter**, situé sous la liste des ports dans la partie supérieure de la fenêtre, ouvre la fenêtre **Port de réseau** dans laquelle vous pouvez saisir le numéro du port et une description.

Pour exclure un port à la liste des ports contrôlés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la rubrique **Protection**, choisissez la sous-rubrique **Réseau**.
4. Dans la partie droite de la fenêtre, cliquez sur le bouton **Sélectionner**.

   La fenêtre **Ports de réseau** s'ouvre.
5. Dans la liste des ports de la partie supérieure de la fenêtre, décochez la case en regard de la description du port qu'il faut exclure.

Pour composer la liste des applications dont l'ensemble des ports devra être analysé, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la rubrique **Protection**, choisissez la sous-rubrique **Réseau**.
4. Dans la partie droite de la fenêtre, cliquez sur le bouton **Sélectionner**.

   La fenêtre **Ports de réseau** s'ouvre.
5. Cochez la case **Contrôler tous les ports pour les applications indiquées** et dans la liste des applications en dessous, cochez les cases en regard des noms des applications pour lesquelles il faut contrôler tous les ports.
6. Si l'application ne figure pas dans la liste, ajoutez-la d'une des manières suivantes :

   a. Pour sélectionner le mode d'ajout d'une application à la liste, ouvrez le menu via le lien **Ajouter** situé sous la liste des applications et sélectionnez une des options suivantes :

   - Choisissez l'option **Parcourir** pour désigner l'emplacement du fichier exécutable de l'application. La fenêtre **Application** s'ouvre après la sélection du fichier exécutable.
   - Sélectionnez l'option **Applications** afin de sélectionner une des applications en exécution pour l'instant. La fenêtre **Application** s'ouvre après la sélection de l'application.
7. Dans la fenêtre **Application** qui s'ouvre, saisissez une description de l'application sélectionnée.

ZONE DE CONFIANCE

La *zone de confiance* est une liste d'objets composée par l'utilisateur. Ces objets seront ignorés par l'application. En d'autres termes, il s'agit d'un ensemble d'exclusions de la protection de Kaspersky PURE.

La zone de confiance est composée sur la base de la liste des applications de confiance (cf. section "Composition de la liste des applications de confiance" à la page 162) et des règles d'exclusion (cf. section "Création de règles d'exclusion" à la page 162) en fonction des particularités des objets avec lesquels vous travaillez et des applications installées sur l'ordinateur. Il faudra peut-être inclure des objets dans la zone de confiance si Kaspersky PURE bloque l'accès à un objet ou à une application quelconque alors que vous êtes certain que cet objet ou cette application ne pose absolument aucun danger.

Par exemple, si vous estimez que les objets utilisés par l'application standard Bloc-Notes de Microsoft Windows ne posent aucun danger et ne doivent pas être analysés (vous faites confiance à cette application), ajoutez l'application Bloc-Notes à la liste des applications de confiance afin d'exclure de l'analyse les objets qui utilisent ce processus.

De plus, certaines actions jugées dangereuses peuvent être sans danger dans le cadre du fonctionnement de toute une série de programmes. Ainsi, l'interception des frappes au clavier est une action standard pour les programmes de permutation automatique de la disposition du clavier (par exemple, Punto Switcher). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

Quand une application est ajoutée à la liste des applications de confiance, l'activité de fichier et de réseau de celle-ci ne sera pas contrôlée (même les activités suspectes), ni les requêtes adressées à la base de registres système. Le fichier exécutable et le processus de l'application de confiance seront toujours soumis à la recherche de virus. Pour exclure entièrement l'application de l'analyse, il faut recourir aux règles d'exclusion.

Le recours aux exclusions d'applications de confiance de l'analyse permet de résoudre les éventuels problèmes de compatibilité entre Kaspersky PURE et d'autres applications (par exemple, le problème de la double analyse du trafic de réseau d'un ordinateur tiers par Kaspersky PURE et une autre application antivirus) et d'augmenter les performances de l'ordinateur, ce qui est particulièrement important en cas d'utilisation d'applications de serveur.

À leur tour, les règles d'exclusion de la zone de confiance permettent d'utiliser des applications légitimes qui pourraient être employées par des individus malintentionnés pour nuire à l'ordinateur et aux données de l'utilisateur. Ces applications en elles-mêmes n'ont pas de fonctions malveillantes, mais elles pourraient être utilisées en guise d'auxiliaire pour un programme malveillant. Cette catégorie reprend les applications d'administration à distance, les clients IRC, les serveurs FTP, divers utilitaires de suspension ou d'arrêt de processus, les enregistreurs de frappe, les applications d'identification de mots de passe, les numéroteurs automatiques vers des sites web payants, etc. Kaspersky PURE peut bloquer de telles applications. Pour éviter le blocage, il est possible de créer des règles d'exclusion de l'analyse pour les applications utilisées.

La *règle d'exclusion* est un ensemble de conditions qui, si elles sont vérifiées, entraîne l'exclusion de l'objet de l'analyse réalisée par Kaspersky PURE. Dans tous les autres cas, l'analyse de l'objet en question sera réalisée par tous les composants de la protection conformément aux paramètres de protection définis pour ceux-ci.

Les règles d'exclusion de la zone de confiance peuvent être utilisées par plusieurs composants de la protection (par exemple, l'Antivirus Fichiers (cf. rubrique "Antivirus Fichiers" à la page 99), Antivirus Courrier (cf. rubrique "Antivirus Courrier" à la page 106), Antivirus Internet (cf. rubrique "Antivirus Internet" à la page 111)), ou lors de l'exécution de tâches d'analyse..

DANS CETTE SECTION

Composition de la liste des applications de confiance 162

Création de règles d'exclusion 162

COMPOSITION DE LA LISTE DES APPLICATIONS DE CONFIANCE

Par défaut Kaspersky PURE analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les applications et du trafic de réseau qu'elles génèrent. Quand une application est ajoutée à la liste des applications de confiance, Kaspersky PURE l'exclut de l'analyse.

Pour ajouter une application à la liste des applications de confiance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez la sous-section **Menaces et exclusions**.
4. Dans la partie droite de la fenêtre, dans le groupe **Exclusions**, cliquez sur **Configuration**.
5. Cliquez sur le lien **Ajouter** de l'onglet **De confiance** de la fenêtre qui s'ouvre pour ouvrir le menu de sélection de l'application, puis choisissez une des options:
   - Choisissez l'option **Parcourir** pour désigner l'emplacement du fichier exécutable de l'application. La fenêtre **Exclusions pour les applications** s'ouvre après la sélection du fichier exécutable.
   - Sélectionnez l'option **Applications** afin de sélectionner une des applications en exécution pour l'instant. La fenêtre **Exclusions pour les applications** s'ouvre après la sélection de l'application.
6. Dans la fenêtre **Exclusions pour l'application** qui s'ouvre, cochez les cases en regard des types d'activité de l'application qu'il ne faut pas analyser.

Vous pouvez modifier les paramètres d'analyse de l'application ou la supprimer de la liste à l'aide des liens du même nom dans la partie inférieure de la liste. Pour exclure une application de la liste sans la supprimer, décochez la case en regard de l'application.

CREATION DE REGLES D'EXCLUSION

Si vous utilisez des applications que Kaspersky PURE considère légitimes mais qui pourraient être utilisées par des individus malintentionnés pour nuire à l'ordinateur ou aux données de l'utilisateur, il est conseillé de configurer des règles d'exclusion pour celles-ci.

Pour créer une règle d'exclusion, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez la sous-section **Menaces et exclusions**.
4. Dans la partie droite de la fenêtre, dans le groupe **Exclusions**, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles d'exclusion**, cliquez sur le lien **Ajouter**.
6. Dans la fenêtre **Règle d'exclusion** qui s'ouvre, définissez les paramètres de la règle d'exclusion.

EXECUTION DES APPLICATIONS EN ENVIRONNEMENT PROTEGE

La virtualisation est un environnement sûr et isolé du système d'exploitation principal qui permet d'exécuter des applications dont vous n'êtes pas sûr.

Dans l'Environnement protégé, les objets réels du système d'exploitation ne sont pas soumis aux modifications. C'est pourquoi, même si vous lancez l'application infectée dans l'Environnement protégé, toutes les actions de cette application seront limitées par l'environnement virtuel et n'influenceront pas le système d'exploitation.

L'exécution du navigateur en environnement protégé garantit la sécurité pendant la consultation de sites Web. Elle permet d'éviter l'intrusion de programmes malveillants et protège les données de l'utilisateur contre la modification et la suppression non autorisées. Elle offre également la possibilité de supprimer tous les objets accumulés pendant l'utilisation d'Internet : fichiers temporaires, cookies, historiques des sites visités, etc. Microsoft Internet Explorer figure dans la liste des applications lancées dans l'environnement protégé par défaut.

Le lancement d'une application (cf. rubrique "Lancement d'une application en Environnement protégé" à la page 163)dans l'environnement protégé est réalisé conformément au mode sélectionné. Afin de pouvoir lancer rapidement une application dans l'environnement protégé, il est possible de créer des raccourcis.

Pour que pendant le fonctionnement dans l'environnement normal les fichiers enregistrés ou modifiés dans l'environnement protégé soient accessibles, il faut utiliser le Dossier partagé de la Sandbox, spécialement créé et accessible aussi bien dans l'environnement protégé que dans l'environnement normal. Les fichiers placés dans ce dossier ne seront pas supprimés lors de la purge de l'environnement protégé.

L'environnement protégé d'exécution des applications n'est pas disponible sur les ordinateurs sous Microsoft Windows XP x64.

Sous Microsoft Windows Vista x64 et Microsoft Windows 7 x64 les fonctions de certaines applications dans l'Environnement protégé sont limitées. Quand une application de ce genre est lancée, un message apparaîtra à l'écran, si les notifications (cf. page 246) pour l'événement **La fonction de l'application en environnement protégé est limitée** ont été définies.

DANS CETTE SECTION

Lancement d'une application en Environnement protégé 163

Composition de la liste des applications à exécuter dans l'environnement protégé 164

Création d'un raccourci pour le lancement d'une application 165

Purge des données de l'environnement protégé 165

Utilisation du dossier virtuel 166

LANCEMENT D'UNE APPLICATION EN ENVIRONNEMENT PROTEGE

Si le mode **Toujours exécuter en environnement protégé** n'est pas défini pour l'application, il est possible de la lancer en environnement protégé de la manière suivante :

- depuis le menu contextuel de Microsoft Windows ;
- depuis la **fenêtre principale de Kaspersky PURE** (cf. page 45) ;
- via un raccourci créé (cf. la rubrique "Création d'un raccourci pour le lancement d'applications" à la page 165) au préalable.

Si le mode **Toujours exécuter en environnement protégé** est activé, alors l'application sera lancée en environnement protégé, quel que soit le mode de lancement choisi.

Les applications lancées dans l'environnement protégé sont marquées par un cadre vert autour de la fenêtre de l'application. Aussi, elles sont soulignées par la couleur verte dans la liste des applications contrôlées par le Contrôle des Applications (cf. la rubrique "Contrôle des Applications" à la page 139).

Il est conseillé d'installer les applications que vous avez l'intention d'utiliser en environnement protégés dans l'environnement normal Microsoft Windows.

- *Pour lancer l'application en environnement protégé depuis le menu contextuel Microsoft Windows, procédez comme suit :*

  1. Ouvrez le menu contextuel de l'objet sélectionné (raccourci ou fichier exécutable d'une application) en cliquant avec le bouton droit de la souris.
  2. Dans le menu déroulant, sélectionnez le point **Lancer en environnement protégé**.

- *Pour lancer l'application en environnement protégé depuis la fenêtre principale de Kaspersky PURE, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Ma Protection**.
  2. Dans la fenêtre qui s'ouvre, accédez à la rubrique **Contrôle des applications**.
  3. Dans le champ **Applications exécutées en environnement protégé** de la partie inférieure de l'application, ouvrez le menu contextuel de l'application requise, puis choisissez l'option **Exécuter**.

- *Pour lancer une application en environnement protégé à l'aide d'un raccourci, procédez comme suit :*

  1. Ouvrez le répertoire dans lequel vous avez créé le raccourci.
  2. Lancez l'application en double-cliquant sur le raccourci.

COMPOSITION DE LA LISTE DES APPLICATIONS A EXECUTER DANS L'ENVIRONNEMENT PROTEGE

La fenêtre **Protection de l'ordinateur** (cf. page 47) permet de composer la liste des applications à exécuter dans l'environnement protégé. La liste figure dans la section **Contrôle des Applications**.

Si vous ajoutez dans la liste l'application, qui permet de fonctionner en même temps avec plusieurs propres copies (par exemple, Windows Internet Explorer), alors après l'ajout dans la liste chaque sa nouvelle copie fonctionnera en environnement protégé. Lors de l'ajout dans la liste de l'application, qui permet d'utiliser uniquement une de ses copies, il faudra la redémarrer après l'ajout.

Lors de l'ajout d'une application à la liste des applications lancées en environnement protégé, il est possible de lui associer l'état **Toujours exécuter en environnement protégé**. Cela signifie que l'application sera toujours lancée en environnement protégé quel que soit le mode de lancement : via les méthodes standard de Microsoft Windows ou via les méthodes de Kaspersky PURE.

Il est déconseillé d'utiliser le mode **Toujours exécuter en environnement protégé** pour les applications système et les utilitaires car cela pourrait nuire au fonctionnement correct du système d'exploitation.

- *Pour ajouter une application à la liste des applications à exécuter dans l'environnement protégé, procédez comme suit :*

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

2. Dans la fenêtre qui s'ouvre, accédez à la rubrique **Contrôle des applications**.

3. Cliquez sur le lien **Ajouter** dans la partie inférieure de la fenêtre dans le champ **Applications exécutées en environnement protégé** pour ouvrir le menu.

4. Sélectionnez l'application requise dans le menu déroulant. Si vous sélectionnez **Parcourir**, vous ouvrirez une fenêtre dans laquelle vous devrez saisir le chemin d'accès au fichier exécutable. Si vous sélectionnez **Applications**, vous ouvrirez la liste des applications en cours d'exécution. L'icône de l'application sera ajoutée dans la liste.

   Pour supprimer une application de la liste des applications exécutées en environnement protégé, sélectionnez-la dans la liste puis cliquez sur le lien **Supprimer**.

Pour que l'application soit toujours lancée en environnement protégé, quel que soit le mode de lancement, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, accédez à la rubrique **Contrôle des applications**.

3. Dans le champ **Applications exécutées en environnement protégé** de la partie inférieure de l'application, ouvrez le menu contextuel de l'application requise, puis choisissez l'option **Toujours exécuter en environnement protégé**.

   La coche ✓ apparaîtra à côté de l'option du menu.

CREATION DE RACCOURCIS POUR LE LANCEMENT D'APPLICATIONS

Il est possible de créer des raccourcis dans Kaspersky PURE pour accélérer le lancement d'une application dans l'environnement protégé. Il est ainsi possible de lancer l'application voulue dans l'environnement protégé sans ouvrir la fenêtre principale de l'application, ni le menu contextuel de Microsoft Windows.

Pour créer un raccourci en vue de lancer une application dans l'environnement protégé, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, accédez à la rubrique **Contrôle des applications**.

3. Dans le champ **Applications exécutées en environnement protégé** de la partie inférieure de l'application, ouvrez le menu contextuel de l'application requise, puis choisissez l'option **Créer un raccourci**.

4. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès pour l'enregistrement du raccourci ainsi que le nom de celui-ci. Le raccourci est créé par défaut dans le dossier *Poste de travail* de l'utilisateur actuel et il porte le nom correspondant au processus de l'application.

PURGE DES DONNEES DE L'ENVIRONNEMENT PROTEGE

Lors du lancement d'une application dans l'environnement protégé, toutes les modifications qui sont le résultat du fonctionnement de l'application ont lieu uniquement dans l'environnement protégé. Par défaut, lors du lancement suivant de l'application, toutes les modifications introduites et les fichiers enregistrés seront à nouveau accessibles pendant la séance d'utilisation de l'environnement protégé.

Si les données enregistrées dans l'environnement protégé ne sont plus nécessaires ou s'il faut rendre les paramètres de l'environnement normal Windows à toutes les applications lancées, purgez l'environnement protégé.

Si vous ne souhaitez pas que les modifications introduites dans une application quelconque soit accessible au prochain lancement dans l'environnement protégé, vous pouvez activer le mode **Purger les données de l'environnement protégé à la fermeture**. Cela signifie que les modifications introduites pendant l'utilisation de l'application seront supprimées automatiquement au moment de quitter l'application.

Avant de purger les données enregistrées dans l'environnement protégé, il convient de s'assurer que toutes les informations qui pourraient vous être utiles plus tard sont enregistrées dans le dossier virtuel. Dans le cas contraire, les données seront supprimées et il sera impossible de les rétablir.

- *Pour purger les données de l'environnement protégé, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Protection de l'ordinateur**.
  2. Dans la fenêtre qui s'ouvre, accédez à la rubrique **Contrôle des applications**.
  3. Dans le champ **Applications exécutées en environnement protégé** de la partie inférieure de la fenêtre, cliquez sur le lien **Purger**.
  4. Confirmez la purge des données dans la fenêtre qui s'ouvre.

- *Pour que les données de l'environnement protégé soient purgées chaque fois que vous quittez l'application, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Ma Protection**.
  2. Dans la fenêtre qui s'ouvre, accédez à la rubrique **Contrôle des applications**.
  3. Dans le champ **Applications exécutées en environnement protégé** de la partie inférieure de l'application, ouvrez le menu contextuel de l'application requise, puis choisissez l'option **Purger les données de l'environnement protégé à la fermeture**.

     La coche apparaîtra à côté de l'option dans le menu et la coche apparaîtra sur l'icône de l'application dans la liste des applications lancées dans l'environnement protégé.

     Pour annuler la purge des données de l'environnement protégé au moment de quitter l'application, sélectionnez à nouveau cette option.

UTILISATION DU DOSSIER VIRTUEL

Lors de l'utilisation de l'environnement protégé, toutes les modifications qui résultent du fonctionnement de l'application touchent uniquement l'environnement protégé et n'ont aucun effet sur l'environnement normal. Ainsi, les fichiers enregistrés dans l'environnement protégé ne se retrouvent pas dans l'environnement normal.

Pour que les fichiers manipulés par l'utilisateur en environnement protégé soient accessibles en environnement normal, Kaspersky PURE propose un *dossier partagé dans l'environnement protégé*. Tous les fichiers enregistrés dans ce dossier pendant l'utilisation de l'environnement protégé seront accessibles dans l'environnement normal.

Le dossier partagé est un dossier sur le disque dur créé lors de l'installation de Kaspersky PURE.

Ce dossier est créé dans *%AllUsersProfile%\Application Data\Kaspersky Lab\SandboxShared* lors de l'installation de l'application et son emplacement ne peut être protégé.

Dans l'Assistant de Microsoft Windows, le dossier partagé est signalé par . Il est également possible d'accéder au dossier depuis la fenêtre principale de Kaspersky PURE.

- *Pour ouvrir le dossier partagé depuis la fenêtre principale de Kaspersky PURE, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Ma Protection**.
  2. Dans la fenêtre qui s'ouvre, accédez à la rubrique **Contrôle des applications**.
  3. Cliquez sur le lien **Dossier partagé**. Le dossier s'ouvre dans une fenêtre standard de l'Assistant Microsoft Windows.

QUARANTAINE ET DOSSIER DE SAUVEGARDE

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

L'objet potentiellement infecté peut-être identifié et mis en quarantaine pendant l'analyse ainsi que par l'Antivirus Fichiers, l'Antivirus Courrier ou la Défense Proactive.

Les objets sont placés en quarantaine dans les cas suivants :

- Le code de l'objet est semblable à celui d'une menace connue mais il a été partiellement modifié ou sa structure évoque celle d'un programme malveillant, mais ne figure pas dans la base. Dans ce cas, les objets sont placés en quarantaine suite à l'analyse heuristique pendant l'intervention de l'Antivirus Fichiers et de l'Antivirus Courrier, ainsi que pendant la recherche de virus. Le mécanisme d'analyse heuristique provoque rarement de faux positifs.

- La séquence d'actions réalisée par l'objet est suspecte. Dans ce cas, les objets sont placés en quarantaine suite à l'analyse de leur comportement par la Défense Proactive.

L'objet placé en quarantaine est déplacé et non pas copié : l'objet est supprimé du disque ou du message et il est enregistré dans le répertoire de quarantaine. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

Le dossier de sauvegarde est conçu pour l'enregistrement des copies de sauvegarde des objets infectés impossibles à réparer au moment de leur détection.

Lors de la prochaine mise à jour des bases de l'application, il se peut que Kaspersky PURE puisse identifier la menace et la neutraliser. C'est pour cette raison que le logiciel analyse les objets en quarantaine après chaque mise à jour (cf. page 98).

DANS CETTE SECTION

Conservation des objets de la quarantaine et de la sauvegarde. 167

Manipulation des objets en quarantaine 168

CONSERVATION DES OBJETS DE LA QUARANTAINE ET DE LA SAUVEGARDE.

La durée maximale de conservation par défaut des objets est de 30 jours. Les objets sont supprimés à l'issue de cette période. Vous pouvez annuler la restriction sur la durée de conservation ou la modifier.

En outre, vous pouvez indiquer la taille maximale de la quarantaine et de la sauvegarde. Une fois que la taille maximale est atteinte, le contenu de la quarantaine et de la sauvegarde est remplacé par de nouveaux objets. Par défaut, il n'y a pas de limite sur la taille maximale.

Pour configurer la durée maximale de conservation des objets, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dans la section **Paramètres généraux**, sélectionnez la sous-section **Rapports et stockages**.

4. Dans la partie droite de la fenêtre, cochez la case **Supprimer les objets après** et indiquez la durée maximale de la conservation des objets dans la quarantaine.

Pour configurer la taille maximale de la quarantaine ou de la sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Paramètres généraux**, sélectionnez la sous-section **Rapports et stockages**.
4. Dans la partie droite de la fenêtre, cochez la case **Taille maximale** et définissez la taille maximale de la quarantaine et du dossier de sauvegarde.

MANIPULATION DES OBJETS EN QUARANTAINE

La quarantaine de Kaspersky PURE permet de réaliser les opérations suivantes :

- Mettre en quarantaine les fichiers qui selon vous sont infectés par un virus ;
- Analyser et réparer tous les objets potentiellement infectés de la quarantaine à l'aide de la version actuelle des bases de Kaspersky PURE ;
- Restaurer les fichiers dans le dossier indiqué ou dans les dossiers où ils se trouvaient avant d'être placés en quarantaine (par défaut) ;
- Supprimer n'importe quel objet ou groupe d'objets de la quarantaine ;
- Envoyer les objets de la quarantaine à Kaspersky Lab pour étude.

Un objet peut être placé en quarantaine de deux manières :

- Via le lien **Placer en quarantaine** de la fenêtre **Etat de la protection** ;
- Via le menu contextuel de l'objet.

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

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Ma Protection**.
2. Cliquez sur le lien **Quarantaine** situé dans la partie supérieure de la fenêtre qui s'ouvre pour ouvrir la fenêtre **Etat de la protection**.
3. Sous l'onglet **Menaces détectées**, cliquez sur le lien **Mettre en quarantaine**.
4. Dans la fenêtre qui s'ouvre, choisissez l'objet qu'il faut placer en quarantaine.

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

1. Ouvrez la fenêtre de l'Assistant de Microsoft Windows et accédez au dossier contenant l'objet à mettre en quarantaine.
2. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'objet, puis choisissez l'option **Copier dans la quarantaine**.

Pour analyser un objet en quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Ma Protection**.
2. Cliquez sur le lien **Quarantaine** situé dans la partie supérieure de la fenêtre qui s'ouvre pour ouvrir la fenêtre **Etat de la protection**.
3. Sous l'onglet **Menaces détectées**, sélectionnez l'objet à analyser.

4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'option **Analyser**.

Pour réparer tous les objets en quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Protection de l'ordinateur**.
2. Cliquez sur le lien **Quarantaine** situé dans la partie supérieure de la fenêtre qui s'ouvre pour ouvrir la fenêtre **Etat de la protection**.
3. Sous l'onglet **Menaces détectées**, cliquez sur le lien **Réparer tous**.

Pour restaurer un fichier depuis la quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Protection de l'ordinateur**.
2. Cliquez sur le lien **Quarantaine** situé dans la partie supérieure de la fenêtre qui s'ouvre pour ouvrir la fenêtre **Etat de la protection**.
3. Sous l'onglet **Menaces détectées**, sélectionnez l'objet à restaurer.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'option **Restaurer**.

Pour supprimer un objet de la quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Ma Protection**.
2. Cliquez sur le lien **Quarantaine** situé dans la partie supérieure de la fenêtre qui s'ouvre pour ouvrir la fenêtre **Etat de la protection**.
3. Sous l'onglet **Menaces détectées**, sélectionnez l'objet à supprimer.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Supprimer de la liste**.

Pour envoyer l'objet en quarantaine à Kaspersky Lab pour étude, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Ma Protection**.
2. Cliquez sur le lien **Quarantaine** situé dans la partie supérieure de la fenêtre qui s'ouvre pour ouvrir la fenêtre **Etat de la protection**.
3. Sous l'onglet **Menaces détectées**, sélectionnez l'objet à envoyer pour examen.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'option **Envoyer**.

MES SAUVEGARDES

Pendant la copie de sauvegarde, les copies de fichiers sélectionnés sont placées dans l'espace de sauvegarde spécial.

l'espace de sauvegarde des copies de sauvegarde est un espace réservé sur le disque ou sur un autre support. Les référentiels sont utilisés dans le cadre des tâches de copie de sauvegarde pour enregistrer les données.

Lors de la création du référentiel (cf. la rubrique "Création de l'espace de sauvegarde" à la page 170), l'utilisateur choisit le support, détermine le nom du nouveau référentiel et définit les paramètres d'enregistrement des copies de sauvegarde. Il est possible également de définir un mot de passe d'accès au référentiel. Les informations de service relatives au référentiel sont ensuite enregistrées.

Pour exécuter la copie de sauvegarde des données, il faut créer une tâche de copie de sauvegarde (cf. la rubrique "Création d'une tâche de copie de sauvegarde" à la page 172). *La tâche de copie de sauvegarde* désigne la sélection de paramètres présentée à l'utilisateur qui définissent les données à copier, l'emplacement où les copies seront stockées et les conditions de copie. Tâches accessibles pour un nouveau lancement (manuel ou selon une programmation).

Les copies de sauvegarde créées dans le cadre d'une tâche sont conservées dans des *archives*. Les archives des copies de sauvegarde sont conservées dans l'espace de sauvegarde et elles portent le même nom que la tâche.

S'il faut restaurer des données au départ des copies de sauvegarde, la procédure de restauration (cf. la rubrique "Restauration des données" à la page 173) ou l'utilitaire Kaspersky Restore Utility est lancé. Les fichiers peuvent être restaurés dans leur emplacement d'origine ou dans n'importe quel autre répertoire.

Tous les événements liés à la copie de sauvegarde apparaissent dans le rapport (cf. la rubrique "Consultation du rapport sur les événements" à la page 176).

DANS CETTE SECTION

Création de l'espace de sauvegarde 170

Connexion d'un espace de sauvegarde créé antérieurement 171

Purge de l'espace de sauvegarde 171

Suppression de l'espace de sauvegarde 172

Création d'une tâche de copie de sauvegarde 172

Lancement de la sauvegarde 173

Restauration des données 173

Recherche des copies de sauvegarde 174

Consultation des données de la copie de sauvegarde 175

Consultation du rapport sur les événements 176

CREATION DE L'ESPACE DE SAUVEGARDE

La création de l'espace de sauvegarde est réalisée à l'aide d'un Assistant. L'Assistant de création de l'espace de sauvegarde est lancé d'une des deux manières suivantes :

- Depuis la fenêtre principale du module ;

- Depuis l'Assistant de création d'une tâche de copie de sauvegarde (cf. la rubrique "Création d'une tâche de copie de sauvegarde" à la page 172).

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Il est également possible de naviguer entre les étapes de l'Assistant à l'aide des liens situés dans la partie supérieure de la fenêtre.

Pour créer l'espace de sauvegarde de copies de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Espace de sauvegarde** et cliquez sur le bouton **Créer**.
3. Cette action lance l'Assistant de création de l'espace de sauvegarde de copies de sauvegarde. Voici, en détails, les étapes de l'Assistant :
   a. Sélectionnez le type de support qui sera utilisé pour le stockage dans la partie gauche de la fenêtre **Disque**.

      Pour la sécurité des données, il est conseillé de créer des stockages de données de sauvegarde sur des disques amovibles.

   b. Définissez un mot de passe pour protéger les données contre l'accès non autorisé dans la fenêtre **Protection** (le cas échéant).
   c. Limitez le nombre de version des fichiers qui seront présentes simultanément dans l'espace de sauvegarde ainsi que la durée de conservation des copies dans la fenêtre **Versions des fichiers** (le cas échéant).
   d. Saisissez le nom du nouveau référentiel et confirmez la création selon les paramètres définis dans la fenêtre **Résumé**.

CONNEXION D'UN ESPACE DE SAUVEGARDE CREE ANTERIEUREMENT

Si vous avez créé l'espace de sauvegarde à l'aide du module de copie de sauvegarde Kaspersky PURE, mais qu'il n'est pas accessible sur cet ordinateur (par exemple, après la réinstallation du système ou si l'espace de sauvegarde a été copié depuis un autre ordinateur), alors il faudra connecter l'espace de sauvegarde avant de pouvoir utiliser les données qu'il contient.

Pour connecter l'espace de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Espace de sauvegarde**, puis cliquez sur le bouton **Déverrouiller**.
3. Sélectionnez le type de l'espace de sauvegarde et désignez les paramètres de connexion requis dans la fenêtre **Sélection de l'espace de sauvegarde**.

   Si les paramètres ont été correctement définis, l'espace de sauvegarde apparaîtra dans la liste.

PURGE DE L'ESPACE DE SAUVEGARDE

En cas de manque d'espace dans l'espace de sauvegarde, il est possible de supprimer les anciennes versions ainsi que les copies de sauvegarde des fichiers qui ne se trouvent pas sur l'ordinateur.

Pour purger l'espace de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Espace de sauvegarde**.
3. Sélectionnez l'espace de sauvegarde qu'il faut purger, puis cliquez sur le bouton **Purger**.
4. Dans la fenêtre **Purge de l'espace de sauvegarde** qui s'ouvre, sélectionnez la version des fichiers qu'il faut supprimer de l'espace de sauvegarde.

SUPPRESSION DE L'ESPACE DE SAUVEGARDE

L'Assistant de suppression de l'espace de sauvegarde permet de supprimer l'espace de sauvegarde des copies de sauvegarde. Les actions à exécuter sur les données de l'espace de sauvegarde supprimés et sur les tâches qui utilisent l'espace de sauvegarde pour la copie de sauvegarde sont définies lors de la suppression.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Il est également possible de naviguer entre les étapes de l'Assistant à l'aide des boutons situés dans la partie supérieure de la fenêtre.

Pour supprimer l'espace de sauvegarde de copies de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Espace de sauvegarde**.
3. Sélectionnez l'espace de sauvegarde qu'il faut supprimer, puis cliquez sur le bouton **Supprimer**.
4. Cette action lance l'Assistant de suppression de l'espace de sauvegarde de copies de sauvegarde. Voici, en détails, les étapes de l'Assistant :
   a. Dans la fenêtre **Contenu**, sélectionnez l'action à exécuter sur les copies de sauvegarde qui se trouvent dans l'espace de sauvegarde à supprimer.
   b. Dans la fenêtre **Tâches**, sélectionnez l'action à réaliser sur les tâches qui utilisent l'espace de sauvegarde pour la copie de sauvegarde.
   c. Confirmez la suppression de l'espace de sauvegarde selon les paramètres définis dans la fenêtre **Résumé**.

CREATION D'UNE TACHE DE COPIE DE SAUVEGARDE

Les tâches de copie de sauvegarde permettent de créer des copies de sauvegarde des fichiers et proposent les paramètres suivants :

- La sélection de fichiers dont la copie de sauvegarde va être créée ;
- L'espace dans lequel les copies de sauvegarde seront créées ;
- Les conditions d'exécution de la copie de sauvegarde.

La création de la tâche est réalisée à l'aide d'un Assistant.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Il est également possible de naviguer entre les étapes de l'Assistant à l'aide des boutons situés dans la partie supérieure de la fenêtre.

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

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Mes Sauvegardes** puis cliquez sur le bouton **Créer**.
3. L'Assistant de création d'une tâche de copie de sauvegarde est lancé. Voici, en détails, les étapes de l'Assistant :
   a. Dans la fenêtre **Contenu**, sélectionnez les objets pour lesquels les copies de sauvegarde seront créées.
   b. Dans la fenêtre **Stockage**, sélectionnez l'espace de sauvegarde dans lequel les copies de sauvegarde seront créées.
   c. Dans la fenêtre **Planification**, définissez les conditions d'exécution de la tâche.
   d. Saisissez le nom de la nouvelle tâche et confirmez la création selon les paramètres définis dans la fenêtre **Résumé**.

LANCEMENT DE LA SAUVEGARDE

La tâche de copie de sauvegarde peut être lancée automatiquement (selon une planification définie) ou manuellement. Le mode de lancement actuel apparaît dans la liste des tâches (cf. ill. ci-après).

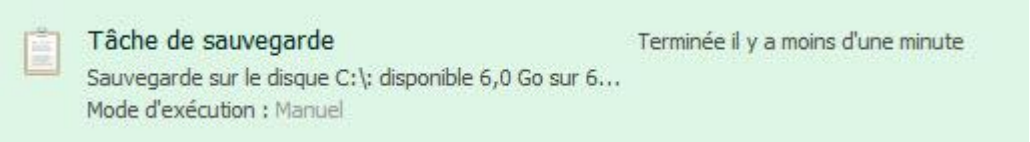


Illustration 14. Tâche de copie de sauvegarde

La planification pour l'exécution automatique de la tâche s'opère à l'aide d'une tâche qui pourra être modifiée ultérieurement.

Le cas échéant, vous pouvez lancer n'importe quelle tâche manuellement.

Pour lancer une tâche de copie de sauvegarde manuellement, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Mes Sauvegardes**.
3. Dans la partie droite de la fenêtre, choisissez la tâche à exécuter puis cliquez sur le bouton **Exécuter**.

   Le temps écoulé depuis le début de l'exécution de la tâche apparaît dans la ligne de la tâche sélectionnée. L'exécution d'une tâche peut être suspendue ou annulée à l'aide des boutons correspondant dans la partie supérieure de la fenêtre.

   Suite à l'exécution de la tâche, une archive contenant les copies de sauvegarde à cette date est créée dans l'espace de sauvegarde.

RESTAURATION DES DONNEES

Le cas échéant, les données peuvent être restaurées au départ de la copie de sauvegarde des fichiers. La procédure de restauration est accessible uniquement pour les référentiels connectés. Lors de la restauration, les données des copies de sauvegarde sont conservées dans le répertoire sélectionné.

Les fichiers peuvent être restaurés de plusieurs manières :

- restaurer la dernière version du fichier ;
- choisir une version à restaurer en fonction de la date.

Pour restaurer la dernière version du fichier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Restauration des données**.
3. Sélectionnez l'espace de sauvegarde qui abrite les copies de sauvegarde requises, puis cliquez sur le bouton **Restaurer**.
4. Dans la partie supérieure de la fenêtre **Restauration des données** depuis, dans la liste déroulante **Archive**, sélectionnez le nom de la tâche ayant débouché sur la création de l'archive avec les copies de sauvegarde requises.
5. Sélectionnez les fichiers à restaurer. Pour ce faire, cochez la case en regard des fichiers requis. Pour sélectionner toutes les archives, cliquez sur le bouton **Tout sélectionner** en bas de la liste. Cliquez sur le bouton **Restaurer** dans la partie supérieure de la fenêtre.
6. Dans la fenêtre **Restauration** qui s'ouvre, sélectionnez l'emplacement de sauvegarde des fichiers à restaurer ainsi que la condition de conservation en cas d'équivalence des noms. Cliquez sur le bouton **Restaurer**.

Pour choisir la version requise du fichier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Restauration des données**.
3. Sélectionnez l'espace de sauvegarde qui abrite les copies de sauvegarde requises, puis cliquez sur le bouton **Restaurer les données**.
4. Dans la partie supérieure de la fenêtre **Restauration des données** depuis, dans la liste déroulante **Archive**, sélectionnez le nom de la tâche ayant débouché sur la création de l'archive avec les copies de sauvegarde requises.
5. Sélectionnez le fichier dont il faut indiquer la version. Pour ce faire, cochez la case à côté du fichier requis. Cliquez sur le bouton **Version** dans la partie supérieure de la fenêtre.
6. Dans la fenêtre **Versions du fichier** qui s'ouvre, choisissez la version du fichier à restaurer puis cliquez sur le bouton **Restaurer**.
7. Dans la fenêtre **Restauration** qui s'ouvre, sélectionnez l'emplacement de sauvegarde des fichiers à restaurer ainsi que la condition de conservation en cas d'équivalence des noms. Cliquez sur le bouton **Restaurer**.

RECHERCHE DES COPIES DE SAUVEGARDE

Le filtre et la ligne de recherche permettent de rechercher des copies de sauvegarde dans l'espace de sauvegarde.

Le filtre des copies de réserve permet d'afficher uniquement les copies qui satisfont aux critères de recherche définis.

La ligne de recherche permet de trouver la copie de sauvegarde dans l'archive selon son nom.

Pour afficher les copies de sauvegarde des fichiers qui ne figuraient pas dans la liste des fichiers pour la copie de sauvegarde lors de la dernière exécution de la tâche (par exemple, ils avaient été supprimés de l'ordinateur), cochez la case **Afficher les fichiers supprimés**.

Pour filtrer les copies de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Restauration des données**.
3. Dans la partie droite de la fenêtre, sélectionnez l'espace de sauvegarde, puis cliquez sur le bouton **Restaurer**.
4. Dans la partie supérieure de la fenêtre **Restauration des données** depuis, sélectionnez les critères de recherche par filtre :
   - Dans la liste déroulante **Archive**, sélectionnez le nom de la tâche dont l'exécution a entraîné la création de l'archive avec les copies de sauvegarde requises.
   - Sélectionnez la date de création de l'archive avec les copies de sauvegarde requises dans la liste déroulante **Données**.
   - Dans la liste déroulante **Catégorie**, sélectionnez les types de fichier pour lesquels il faut trouver les copies de sauvegarde.

Seules les copies de sauvegarde qui répondent aux conditions définies seront affichées.

Pour trouver une copie de sauvegarde en fonction de son nom, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Restauration des données**.
3. Dans la partie droite de la fenêtre, sélectionnez l'espace de sauvegarde, puis cliquez sur le bouton **Restaurer**.
4. Dans la partie supérieure de la fenêtre **Restauration des données** depuis, dans le champ **Recherche**, saisissez le nom du fichier (entier ou partiel).

La liste reprend alors seulement les copies de sauvegarde des fichiers dont le nom débute par la séquence de caractères saisie.

CONSULTATION DES DONNEES DE LA COPIE DE SAUVEGARDE

Avant de restaurer les données, vous pouvez vérifier le contenu de la version sélectionnée de la copie de sauvegarde. Pour ce faire, vous pouvez ouvrir directement la dernière version ou choisir une version pour une date définie.

Pour ouvrir la dernière version du fichier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Restauration des données**.
3. Sélectionnez l'espace de sauvegarde qui abrite les copies de sauvegarde requises, puis cliquez sur le bouton **Restaurer**.
4. Dans la partie supérieure de la fenêtre **Restauration des données** depuis, dans la liste déroulante **Archive**, sélectionnez le nom de la tâche ayant débouché sur la création de l'archive avec les copies de sauvegarde requises.
5. Dan la partie droite de la fenêtre, sélectionnez le fichier requis dans la liste puis cliquez sur **Ouvrir**.

Pour ouvrir la version d'un fichier à une date déterminée, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Sauvegardes**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Restauration des données**.

3. Sélectionnez l'espace de sauvegarde qui abrite les copies de sauvegarde requises, puis cliquez sur le bouton **Restaurer**.

4. Dans la partie supérieure de la fenêtre **Restauration des données** depuis, dans la liste déroulante **Archive**, sélectionnez le nom de la tâche ayant débouché sur la création de l'archive avec les copies de sauvegarde requises.

5. Dan la partie droite de la fenêtre, sélectionnez le fichier requis dans la liste puis cliquez sur **Version**.

6. Dans la fenêtre **Versions du fichier** qui s'ouvre, sélectionnez la date requise et cliquez sur le bouton **Ouvrir**.

CONSULTATION DU RAPPORT SUR LES EVENEMENTS

Le moindre événement lié à la copie de sauvegarde et à la restauration des données est consigné dans le rapport.

Pour obtenir le rapport sur le fonctionnement du module de copie de sauvegarde, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.

3. Dans la fenêtre **Rapport** qui s'ouvre, configurez les paramètres d'affichage des informations sur les événements.

MON CONTROLE PARENTAL

Le *Contrôle Parental* permet de contrôler les actions de différents utilisateurs sur l'ordinateur et sur le réseau. La notion de contrôle inclut la possibilité de limiter l'accès aux ressources et aux applications et de consulter des rapports sur les actions des utilisateurs.

De nos jours, de plus en plus d'enfants et d'adolescents utilisent un ordinateur et Internet. Il faut parvenir à garantir la sécurité car l'utilisation d'Internet et les communications via ce réseau sont liées à toute une série de menaces. Voici quelques-unes des menaces les répandues :

- La visite de sites Internet dont le contenu peut provoquer une perte de temps (chats, jeux) ou d'argent (magasins en ligne, sites d'enchères) ;
- L'accès à des sites Web réservés aux adultes (contenu pornographique, extrémiste, contenu extrême faisant l'apologie des armes, de la drogue, de la violence, etc.) ;
- Le téléchargement de fichiers infectés par des programmes malveillants ;
- Une trop longue utilisation de l'ordinateur, ce qui pourrait nuire à la santé ;
- Les contacts avec des inconnus qui, en se faisant passer pour des amis, peuvent obtenir des informations personnelles de l'utilisateur (nom véridique, adresse, heure à laquelle il n'y a personne à la maison).

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

- Restriction de l'utilisation de l'ordinateur et d'Internet dans le temps ;
- Composition de listes d'applications dont l'exécution est autorisée ou interdite et restriction temporaire sur l'exécution d'applications autorisées ;
- Composition de listes de sites dont la visite est autorisée ou interdite et sélection de catégories de contenu ne pouvant être consulté ;
- Activation du mode de recherche sécurisée à l'aide des moteurs de recherche (dans ce cas, les liens de sites au contenu douteux n'apparaissent pas dans les résultats de la recherche) ;
- Restriction du téléchargement de fichiers depuis Internet ;
- Composition de listes de contacts avec lesquels les communications sont autorisées ou interdites dans les clients de messagerie instantanée ou dans les réseaux sociaux ;
- Consultation du texte des communications via les clients de messagerie et dans les réseaux sociaux ;
- Interdiction du transfert de certaines données personnelles ;
- Recherche de mots clés définis dans les communications.

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

Pour administrer le composant, il faut saisir le mot de passe d'administrateur (cf. rubrique "Comment restreindre l'accès aux paramètres de Kaspersky PURE" à la page 77). Si vous n'avez pas encore défini un mot de passe pour l'administration de Kaspersky PURE, vous pourrez le faire maintenant.

DANS CETTE SECTION

Configuration du Contrôle Parental de l'utilisateur 178

Consultation des rapports sur les actions de l'utilisateur 185

CONFIGURATION DU CONTROLE PARENTAL DE L'UTILISATEUR

Vous pouvez activer et configurer le Contrôle Parental pour chaque compte utilisateur de manière individuelle et définir différentes restrictions pour différents utilisateurs, par exemple en fonction de l'âge. Vous pouvez désactiver le Contrôle Parental pour les utilisateurs dont les actions ne doivent pas être contrôlées.

Pour administrer le composant, vous devez vous identifier. Après avoir saisi le mot de passe d'administrateur, vous pourrez activer, suspendre ou désactiver Mon Contrôle Parental et modifier sa configuration.

ACTIVATION ET DESACTIVATION DU CONTROLE

Vous pouvez activer ou désactiver le Contrôle Parental de manière individuelle pour chaque compte utilisateur. Par exemple, les actions d'un utilisateur adulte doté d'un compte d'administrateur n'ont pas besoin d'être contrôlées. Vous pouvez désactiver le Contrôle Parental pour un tel utilisateur. Pour les autres utilisateurs dont les actions doivent être contrôlées, il faut activer le Contrôle Parental, puis le configurer, par exemple en chargeant des paramètres de configuration standard depuis un modèle.

Vous pouvez activer ou désactiver le Contrôle Parental pour le compte utilisateur en cours au départ de la fenêtre principale depuis le menu contextuel de l'icône de l'application

Pour activer Mon Contrôle Parental, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**.
2. Dans la fenêtre qui s'ouvre, choisissez la section **Utilisateurs**, puis, dans la partie supérieure de la fenêtre, cliquez sur le bouton **Activer**.

Pour suspendre Mon Contrôle Parental, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**.
2. Dans la fenêtre qui s'ouvre, choisissez la section **Utilisateurs**, puis, dans la partie supérieure de la fenêtre, cliquez sur le bouton **Suspendre**.
3. Dans la fenêtre **Suspension de Mon Contrôle Parental**, sélectionnez le mode de reprise.

Vous pouvez également suspendre ou reprendre Mon Contrôle Parental pour le compte utilisateur actif via la fenêtre principale de Kaspersky PURE (cf. page 45) ou via le menu contextuel de l'icône de l'application (cf. page 44)

VOIR EGALEMENT :

Enregistrement et chargement des paramètres de Mon Contrôle Parental..... 179

ENREGISTREMENT ET CHARGEMENT DES PARAMETRES DE MON CONTROLE PARENTAL

Si vous avez configuré les paramètres du Contrôle Parental pour un compte utilisateur, vous pouvez les enregistrer dans un fichier distinct. Plus tard, vous pourrez importer les paramètres depuis ce fichier afin de procéder à une configuration rapide. De plus, vous pouvez appliquer les paramètres de contrôle d'un autre compte ou utiliser un modèle de configuration (ensemble préconfiguré de règles pour divers types d'utilisateurs en fonction de leur âge, de leur expérience et d'autres caractéristiques).

Après l'importation, les paramètres des différents comptes utilisateur pourront être modifiés.

- *Pour enregistrer les paramètres de contrôle dans un fichier, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**.
  2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**, sélectionnez le compte dont les paramètres de contrôle doivent être enregistrés, puis cliquez sur le bouton **Configurer**.
  3. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Exporter les paramètres** dans la partie supérieure de la fenêtre et enregistrez le fichier de configuration.

- *Pour charger les paramètres de contrôle depuis un fichier, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**
  2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Utilisateurs**, sélectionnez le compte utilisateur dont les paramètres de contrôle doivent être importés, puis cliquez sur le bouton **Configurer**.
  3. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Importer les paramètres** dans la partie supérieure de la fenêtre.
  4. Dans la fenêtre **Chargement des paramètres du contrôle** qui s'ouvre, choisissez l'option **Fichier avec les paramètres enregistrés** au préalable et indiquez l'emplacement du fichier.

- *Pour appliquer les paramètres d'un autre compte utilisateur, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**
  2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Utilisateurs**, sélectionnez le compte utilisateur auquel les paramètres de contrôle doivent être appliqués, puis cliquez sur le bouton **Configurer**.
  3. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Importer les paramètres** dans la partie supérieure de la fenêtre.
  4. Dans la fenêtre **Chargement des paramètres du contrôle** qui s'ouvre, choisissez l'option **Autre utilisateur** et désignez le compte utilisateur dont les paramètres doivent être utilisés.

- *Pour utiliser un modèle de configuration, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**.
  2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Utilisateurs**, sélectionnez le compte utilisateur auquel les paramètres de contrôle prédéfinis être appliqués, puis cliquez sur le bouton **Configurer**.
  3. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Importer les paramètres** dans la partie supérieure de la fenêtre.
  4. Dans la fenêtre **Chargement des paramètres du contrôle** qui s'ouvre, sélectionnez l'option **Modèle** et désignez le modèle dont les paramètres doivent être utilisés.

REPRESENTATION DU COMPTE UTILISATEUR DANS KASPERSKY PURE

Vous pouvez sélectionner le pseudonyme et l'image utilisés pour représenter le compte utilisateur dans Kaspersky PURE.

Pour configurer le pseudonyme et la photo associée au compte, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**, sélectionnez le compte dont les paramètres d'affichage doivent être configurés, puis cliquez sur le bouton **Configurer**.

3. Dans la fenêtre qui s'ouvre, sélectionnez le groupe **Avancé** et choisissez le composant **Profil**. Saisissez le pseudonyme du compte utilisateur et choisissez la photo pour la représentation.

DUREE D'UTILISATION DE L'ORDINATEUR

Vous pouvez configurer l'horaire d'accès à l'ordinateur (jours de la semaine et heures de la journée) ainsi que limiter la durée globale d'utilisation de l'ordinateur par jour.

Entre 15 et 5 minutes avant l'expiration de la durée d'utilisation autorisée de l'ordinateur Kaspersky PURE prévient l'utilisateur de l'arrêt prochain de l'ordinateur. L'utilisateur a ainsi le temps de terminer son travail et d'enregistrer les données requises. À l'issue de la période d'utilisation autorisée, Kaspersky PURE affiche une notification sur la violation de l'horaire d'utilisation de l'ordinateur et arrête celui-ci.

Pour limiter l'utilisation de l'ordinateur dans le temps, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**, sélectionnez le compte pour lequel des restrictions doivent être définies, puis cliquez sur **Configurer**.

3. Dans la fenêtre qui s'ouvre, sélectionnez le groupe **Ordinateur** et choisissez le composant **Temps d'utilisation**.

4. Dans la fenêtre **Contrôle du temps d'utilisation de l'ordinateur** qui s'ouvre, cochez la case **Activer le contrôle** et définissez les restrictions dans le temps.

LANCEMENT DES APPLICATIONS

Vous pouvez autoriser ou interdire le lancement d'applications en particulier ainsi que limiter l'exécution des applications autorisées dans le temps.

Pour restreindre le lancement des applications et des jeux, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**, sélectionnez le compte pour lequel des restrictions doivent être définies, puis cliquez sur **Configurer**.

3. Dans la fenêtre qui s'ouvre, sélectionnez le groupe **Ordinateur** et choisissez le composant **Lancement des applications**.

4. Dans la fenêtre **Contrôle des applications exécutées** qui s'ouvre, cochez la case **Activer le contrôle**.

5. Les onglets **Autorisés** et **Interdits** permettent de constituer des listes d'applications dont le lancement est autorisé ou interdit et de définir un horaire pour l'utilisation des applications autorisées.

DUREE D'UTILISATION D'INTERNET

Vous pouvez limiter le temps que peut passer un utilisateur sur Internet. Pour ce faire, il faut configurer un horaire d'accès à Internet (jours de la semaine et heures auxquelles l'accès sera autorisé ou interdit) ainsi que limiter la durée totale d'utilisation d'Internet par jour.

Dix minutes avant l'expiration de la durée d'utilisation d'Internet autorisée, Kaspersky PURE signale à l'utilisateur que la connexion va être coupée. L'utilisateur a ainsi le temps de terminer son travail et d'enregistrer les données requises. À l'issue de la durée autorisée, Kaspersky PURE affiche la notification sur la violation de l'horaire d'utilisation d'Internet et interrompt la connexion.

Pour limiter l'utilisation d'Internet dans le temps, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**, sélectionnez le compte pour lequel des restrictions doivent être définies, puis cliquez sur **Configurer**.
3. Dans la fenêtre qui s'ouvre, sélectionnez le groupe **Internet** et choisissez le composant **Temps d'utilisation**.
4. Dans la fenêtre **Contrôle du temps d'utilisation d'Internet** qui s'ouvre, cochez la case **Activer le contrôle** et définissez les restrictions dans le temps.

CONSULTATION DE SITES

Vous pouvez limiter l'accès à certains sites Web en fonction du contenu. Pour ce faire, composez des listes d'URL autorisées ou interdites et sélectionnez les catégories de site qui ne pourront être consultés.

Pour limiter l'accès aux sites Web, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**, sélectionnez le compte pour lequel des restrictions doivent être définies, puis cliquez sur **Configurer**.
3. Dans la fenêtre qui s'ouvre, dans le groupe **Internet**, sélectionnez le composant **Filtrage par catégories**.
4. Dans la fenêtre **Contrôle de la visite des sites Web** qui s'ouvre, cochez la case **Activer le contrôle** et définissez les restrictions pour la visite de sites.

   Les onglets **URL interdites** et **URL autorisées** permettent de saisir les adresses des sites Web qui pourront être consultés ou non. L'onglet **Non recommandés** permet de sélectionner les catégories de sites Web à bloquer.
5. Si vous souhaitez autoriser l'accès uniquement aux sites Web autorisés cités, cochez la case **Interdire l'accès à tous les sites ne faisant pas partie de la liste des URL Autorisées**.

Si vous avez coché la case **Interdire l'accès à tous les sites ne faisant pas partie de la liste des URL Autorisées**, il faudra ajouter l'adresse du serveur proxy à la liste des **URL autorisées** pour pouvoir se connecter à Internet via un serveur proxy.

TELECHARGEMENT

Vous pouvez également imposer des restrictions sur les types de fichiers qui peuvent être téléchargés depuis Internet.

Pour restreindre le téléchargement de fichiers depuis Internet, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**, sélectionnez le compte pour lequel des restrictions doivent être définies, puis cliquez sur **Configurer**.

3. Dans la fenêtre qui s'ouvre, sélectionnez le groupe **Internet** et choisissez le composant **Téléchargement**.

4. Dans la fenêtre **Contrôle du téléchargement de fichiers depuis Internet** qui s'ouvre, cochez la case **Activer le contrôle** et sélectionnez la catégorie de fichiers dont le chargement est autorisé.

MODE DE RECHERCHE SECURISEE

Certains moteurs de recherche veulent protéger les utilisateurs contre des sites au contenu inacceptable. Pour ce faire, les mots clés et les expressions, les adresses et les catégories de ressources sont analysées lors de l'indexation des sites Web. Lorsque le mode de recherche sécurisée est activé, tous les sites web appartenant aux catégories indésirables (pornographie, apologie des drogues et de la violence, autre contenu qui ne convient pas aux mineurs d'âges) seront exclus des résultats de la recherche.

Le Contrôle Parental permet d'activer le mode de Recherche sécurisée simultanément pour les moteurs de recherche Google et Bing.

Pour activer le mode de recherche sécurisée, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**, sélectionnez le compte pour lequel des restrictions doivent être définies, puis cliquez sur **Configurer**.

3. Dans la fenêtre qui s'ouvre, sélectionnez le groupe **Internet** et choisissez le composant **Recherche sécurisée**.

4. Dans la fenêtre **Contrôle des résultats de la recherche** qui s'ouvre, cochez la case **Activer le mode de recherche sécurisée**.

COMMUNICATION A L'AIDE DE CLIENTS DE MESSAGERIE INSTANTANEE

Le contrôle des conversations via clients de messagerie instantanée consiste à contrôler les contacts avec lesquels les communications sont autorisées ainsi que le contenu de ces conversations. Vous pouvez créer une liste de contacts autorisés ou interdits, définir des mots clés (cf. rubrique "Recherche de mots clés" à la page 185), dont la présence dans les messages sera vérifiée et désigner les données personnelles (cf rubrique "Transfert de données personnelles" à la page 185), dont le transfert sera interdit.

Si l'échange de messages instantanés avec un contact est interdit, tous les messages envoyés à ce contact ou par celui-ci seront bloqués. Les informations relatives aux messages bloqués, ainsi que la présence de mots clés dans les messages, sont consignées dans un rapport. Le rapport complet reprend également le texte des messages échangés avec le contact.

Le contrôle de la correspondance possède les limites suivantes :

- Si le client de messagerie instantanée a été lancé avant l'activation du Contrôle Parental, aucun contrôle de la correspondance n'aura lieu tant que le client de messagerie n'aura pas été redémarré.

- Il n'y aura pas de contrôle de la correspondance en cas d'utilisation d'un proxy HTTP.

La version actuelle du Contrôle Parental prend en charge le contrôle des échanges via les clients de messagerie suivants :

- ICQ ;
- QIP
- Windows Live Messenger (MSN) ;
- Yahoo Messenger ;

- GoogleTalk ;
- mIRC ;
- Mail.Ru Agent ;
- Psi ;
- Miranda ;
- AOL Instant Messenger (AIM) ;
- Jabber.

Certains clients de messagerie instantanée utilisent des connexions cryptées. Pour contrôler les échanges entre ces applications, il faut activer l'analyse des connexions sécurisées (cf. page 157).

Pour limiter le nombre de contacts avec lesquels l'utilisateur pourra communiquer en utilisant un client de messagerie instantanée, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**, sélectionnez le compte pour lequel des restrictions doivent être définies, puis cliquez sur **Configurer**.
3. Dans la fenêtre qui s'ouvre, sélectionnez-le composant **Messageries instantanées** dans la rubrique **Messageries (Chat, ...)**.
4. Dans la fenêtre **Contrôler la correspondance via les clients de messagerie instantanée** qui s'ouvre, cochez la case **Activer le contrôle**.
5. Sous les onglets **Autorisés** et **Interdits**, constituez la liste des contacts autorisés ou interdits.
6. Dans la liste déroulante **Action**, sélectionnez l'action par défaut pour les contacts qui ne sont pas repris dans les listes.

Vous pouvez également autoriser ou interdire la correspondance avec un contact en particulier depuis le rapport détaillé des événements pour ce compte utilisateur.

Pour parcourir les statistiques sommaires, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**
2. Dans la fenêtre qui s'ouvre, sélectionnez le groupe **Rapports** et dans la liste déroulante à droite, choisissez le compte utilisateur pour lequel vous souhaitez afficher le rapport.

   Le groupe **Messageries (Chat, ...)** présente de brèves statistiques sur la correspondance via les clients de messagerie instantanée pour le compte utilisateur choisi.

Pour obtenir le rapport détaillé, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**
2. Dans la fenêtre qui s'ouvre, sélectionnez le groupe **Rapports** et dans la liste déroulante à droite, choisissez le compte utilisateur pour lequel vous souhaitez afficher le rapport. Cliquez sur le lient **Rapport complet**.
3. Dans la fenêtre qui s'ouvre, sélectionnez-le composant **Messageries instantanées** dans la rubrique **Messageries (Chat, ...)**.

   Le rapport apparaîtra dans la fenêtre **Messageries instantanées** qui s'ouvre.

Vous pouvez également ouvrir le rapport détaillé dans la rubrique **Utilisateurs** en cliquant sur le bouton **Rapport complet**.

COMMUNICATIONS DANS LES RESEAUX SOCIAUX

Le contrôle de la communication dans les réseaux sociaux recouvre le contrôle des contacts avec lesquels la communication est autorisée ainsi que le contrôle du contenu de la communication. Vous pouvez créer une liste de contacts autorisés ou interdits, définir des mots clés (cf. rubrique "Recherche de mots clés" à la page 185), dont la présence dans les messages sera vérifiée et désigner les données personnelles (cf rubrique "Transfert de données personnelles" à la page 185), dont le transfert sera interdit.

Si l'échange de messages instantanés avec un contact est interdit, tous les messages envoyés à ce contact ou par celui-ci seront bloqués. Les informations relatives aux messages bloqués, ainsi que la présence de mots clés dans les messages, sont consignées dans un rapport. Le rapport complet reprend également le texte des messages échangés avec le contact.

Certains réseaux sociaux, par exemple, Twitter utilisent une connexion sécurisée. Pour analyser le trafic de ces applications, il faut activer l'analyse des connexions cryptées (cf. page 157).

La version actuelle de Mon Contrôle Parental permet de contrôler les communications dans les réseaux sociaux suivants :

- Facebook ;
- Twitter ;
- MySpace.

Pour limiter le nombre de contacts avec lesquels l'utilisateur pourra communiquer dans les réseaux sociaux, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**, sélectionnez le compte pour lequel des restrictions doivent être définies, puis cliquez sur **Configurer**.
3. Dans la fenêtre qui s'ouvre, sélectionnez-le composant **Réseaux sociaux** dans la rubrique **Messageries (Chat, ...)**.
4. Dans la fenêtre **Réseaux sociaux** qui s'ouvre, cochez la case **Activer le contrôle**.
5. Dans la liste déroulante **Action**, sélectionnez l'action par défaut pour les contacts qui ne sont pas repris dans les listes.

   Vous pouvez également autoriser ou interdire la correspondance avec un contact en particulier depuis le rapport détaillé des événements pour ce compte utilisateur.

6. Fermez la fenêtre de configuration, puis cliquez sur le bouton **Rapport détaillé**.
7. Dans la fenêtre qui s'ouvre, sélectionnez-le composant **Réseaux sociaux** dans la rubrique **Messageries (Chat, ...)**.

   La partie droite de la fenêtre reprend la liste des contacts qui ont envoyé un message ou auxquels un message a été envoyé.

8. Indiquez l'action (autoriser ou interdire la correspondance) pour les contacts sélectionnés.

   Les contacts seront ajoutés automatiquement à la liste des contacts à contrôler. Cette liste est consultable dans la fenêtre **Configuration**, dans la section **Réseaux sociaux**.

TRANSFERT D'INFORMATIONS CONFIDENTIELLES

Vous pouvez interdire le transfert de données contenant des informations personnelles via les clients de messagerie instantanée, les réseaux sociaux et lors de l'envoi des données sur des sites Web. Pour ce faire, il faut composer une liste d'entrées contenant des données confidentielles (par exemple, adresse du domicile, téléphone).

Les tentatives de transfert des données de la liste sont bloquées et les informations relatives aux messages bloqués sont consignées dans le rapport.

Pour bloquer le transfert des données personnelles, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**, sélectionnez le compte pour lequel des restrictions doivent être définies, puis cliquez sur **Configurer**.
3. Dans la fenêtre qui s'ouvre, sélectionnez-le composant **Données personnelles** dans la rubrique **Messageries (Chat, ...)**.
4. Dans la fenêtre **Contrôle de l'envoi de données personnelles** qui s'ouvre, cochez la case **Activer le contrôle**. Cliquez sur le lien **Ajouter** afin d'ajouter à la liste les données dont l'envoi sera interdit.

RECHERCHE DE MOTS CLES

Vous pouvez vérifier si la correspondance de l'utilisateur via les clients de messagerie instantanée, les réseaux sociaux et lors de l'envoi des données sur les sites Web contient des mots ou des expressions déterminés.

La présence de mots clés de la liste dans la correspondance est signalée dans le rapport.

La recherche des mots clés n'est pas possible si le contrôle des communications via les clients de messagerie instantanée ou les réseaux sociaux et le contrôle des visites de sites est désactivé.

Pour vérifier la présence de mots clés dans la correspondance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Utilisateurs**, sélectionnez le compte pour lequel des restrictions doivent être définies, puis cliquez sur **Configurer**.
3. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Mots clés** dans la rubrique **Messageries (Chat, ...)**.
4. Dans la fenêtre **Contrôle des mots clés utilisés** qui s'ouvre, cochez la case **Activer le contrôle**. Cliquez sur le lien **Ajouter** pour ajouter à la liste les mots clés dont la présence devra être vérifiée dans la correspondance.

CONSULTATION DES RAPPORTS SUR LES ACTIONS DE L'UTILISATEUR

Pour chaque utilisateur pour lequel Mon Contrôle Parental a été configuré, vous pouvez consulter des statistiques succinctes et un rapport détaillé par catégorie d'événement contrôlé.

Pour parcourir les statistiques sommaires, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Contrôle Parental**.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Rapports** et sélectionnez, dans la liste déroulante à droite, le compte utilisateur pour lequel vous souhaitez afficher les statistiques sommaires.
3. La fenêtre propose des statistiques succinctes pour le compte utilisateur sélectionné.

Pour obtenir le rapport détaillé, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, sélectionnez le groupe **Rapports** et dans la liste déroulante à droite, choisissez le compte utilisateur pour lequel vous souhaitez afficher le rapport. Cliquez sur le lient **Rapport complet**.

3. La fenêtre qui s'ouvre affiche un rapport détaillé par catégorie pour le compte utilisateur sélectionné.

Vous pouvez également ouvrir le rapport détaillé dans la rubrique **Utilisateurs** en cliquant sur le bouton **Rapport complet**.

MES COFFRES-FORTS

Le composant Mes Coffres-forts assure la protection des données confidentielles contre l'accès non autorisé. Les informations sont cryptées et conservées dans un conteneur spécial appelé coffre-fort.

Le *coffre-fort* est un objet crypté créé par l'utilisateur à l'aide de la fonction de cryptage de données. Les fichiers et les dossiers sont placés dans le coffre-fort. L'accès aux informations contenues dans le coffre-fort requiert un mot de passe. De plus, Kaspersky PURE doit être installé sur l'ordinateur.

Avant de pouvoir utiliser les données du coffre-fort, il faut les déchiffrer. Kaspersky PURE requiert pour ce faire la saisie d'un mot de passe. Une fois le mot de passe correct saisi, le coffre-fort apparaît dans le système sous la forme d'un disque amovible virtuel sur lequel il est possible de copier et de déplacer des fichiers et des dossiers.

DANS CETTE SECTION

Création et connexion d'un coffre-fort déjà créé 187

Interdiction et autorisation de l'accès aux données du coffre-fort 188

Ajout de fichiers à un coffre-fort 189

Configuration des paramètres du coffre-fort 189

Création d'un lien pour accéder rapidement au coffre-fort 190

CREATION ET CONNEXION D'UN COFFRE-FORT DEJA CREE

Pour pouvoir conserver des données sous forme cryptée, il faut créer un coffre-fort. Le coffre-fort peut être créé sur un disque local ou un disque amovible.

La création du coffre-fort est réalisée à l'aide d'un Assistant. Au moment de créer un coffre-fort, il faut définir son nom, sa taille, le mot de passe d'accès et l'emplacement du fichier du coffre-fort.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Il est également possible de naviguer entre les étapes de l'Assistant à l'aide des boutons situés dans la partie supérieure de la fenêtre.

De plus, il est possible de connecter un coffre-fort créé préalablement s'il n'est pas accessible sur l'ordinateur (par exemple, après la réinstallation du système ou après une copie depuis un autre ordinateur). Dans ce cas, le coffre-fort apparaît dans la liste mais l'accès aux données est bloqué. Avant de pouvoir utiliser les données du coffre-fort, il faut les déchiffrer (cf. rubrique "Interdiction et autorisation de l'accès aux données du coffre-fort" à la page 188).

Pour créer un coffre-fort, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Coffres-forts**.
2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Créer...**.
3. L'Assistant de création d'un coffre-fort crypté sera lancé. Voici, en détails, les étapes de l'Assistant :
    a. Saisissez le nom du coffre-fort, la taille et le mot de passe d'accès dans la fenêtre **Paramètres généraux**.
    b. Indiquez l'emplacement du fichier du coffre-fort dans la fenêtre **Source**.

c. Sélectionnez la lettre du disque virtuel pour le déverrouillage du coffre-fort, définissez les paramètres complémentaires, si nécessaire, et confirmez la création du coffre-fort avec les paramètres indiqués dans la fenêtre **Résumé**.

Pour connecter un coffre-fort créé au préalable, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Coffres-forts**.
2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Connecter le coffre-fort**.
3. Dans la fenêtre qui s'ouvre, indiquez l'emplacement du fichier du coffre-fort.

INTERDICTION ET AUTORISATION DE L'ACCES AUX DONNEES DU COFFRE-FORT

Après que le coffre-fort a été créé, l'accès aux données est autorisé. En cas de connexion d'un coffre-fort déjà crée, l'accès aux données qu'il renferme est interdit par défaut. Avant de pouvoir utiliser les données du coffre-fort, il faut les déchiffrer. Cette opération peut être réalisée via l'interface de Kaspersky PURE ou via le menu contextuel de Microsoft Windows.

Si le coffre-fort est enregistré sur un support amovible, vous pouvez configurer l'octroi automatique de l'accès aux données du coffre-fort quand le support est connecté.

Quand l'accès au coffre-fort est autorisé, celui-ci est accessible à tous les comptes utilisateur de l'ordinateur, sous la forme d'un disque amovible dans la liste des périphériques. Par conséquent, il est conseillé d'interdire l'accès (chiffrer les données) quand vous n'utilisez pas les données. Le chiffrement des données peut être réalisé via l'interface de Kaspersky PURE ou via le menu contextuel de Microsoft Windows.

Pour déchiffrer les données du coffre-fort via l'interface de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Coffres-forts**.
2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Déchiffrer les données**.
3. Dans la fenêtre qui s'ouvre, saisissez les paramètres de déchiffrement des données et confirmez l'octroi de l'accès.

Pour déchiffrer les données via le menu contextuel, procédez comme suit :

1. Cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel du fichier du coffre-fort ou le raccourci pour l'accès au conteneur (cf. la rubrique "Création d'un lien pour accéder au coffre-fort" à la page 190) sur le bureau ou le disque amovible.
2. Dans le menu déroulant, choisissez l'option **Déchiffrer les données**.

Pour octroyer automatiquement l'accès aux données du coffre-fort lors de la connexion du support, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Coffre-fort**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le coffre-fort auquel l'accès est autorisé, puis cliquez sur le bouton **Configurer**.
3. Dans la fenêtre qui s'ouvre, cochez la case **Déchiffrer à la connexion**.

Pour chiffrer les données via l'interface de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Coffres-forts**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le coffre-fort auquel l'accès est autorisé, puis cliquez sur le bouton **Chiffrer les données**.

Pour chiffrer les données via le menu contextuel, procédez comme suit :

1. Cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel du fichier du coffre-fort ou le raccourci pour l'accès au conteneur (cf. la rubrique "Création d'un lien pour accéder au coffre-fort" à la page 190) sur le bureau ou le disque amovible.
2. Dans le menu déroulant, choisissez l'option **Chiffrer les données**.

AJOUT DE FICHIERS AU COFFRE-FORT

Une fois débloqué (cf. rubrique "Interdiction et autorisation de l'accès aux données du coffre-fort" à la page 188) le coffre-fort apparaît dans le système en tant que disque amovible virtuel et il est accessible à tous les utilisateurs du système d'exploitation. Vous pouvez ouvrir le coffre-fort et y placer les fichiers et les dossiers à crypter. Pour garantir la sécurité de vos données, il est conseillé de chiffrer les données quand vous avez terminé votre travail. Par la suite, il faudra saisir un mot de passe afin de pouvoir accéder aux données chiffrées du coffre-fort.

Pour ouvrir le coffre-fort via l'interface de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Coffres-forts**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le coffre-fort auquel l'accès est autorisé et ouvrez-le d'un double-clique.
3. Placez dans le coffre-fort les données qui doivent être cryptées.

Pour ouvrir le coffre-fort via le menu contextuel, procédez comme suit :

1. Cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel du fichier du coffre-fort ou le raccourci pour l'accès au conteneur (cf. la rubrique "Création d'un lien pour accéder au coffre-fort" à la page 190) sur le bureau ou le disque amovible.
2. Dans le menu qui s'ouvre, choisissez l'option **Ouvrir le coffre-fort**.

CONFIGURATION DES PARAMETRES DU COFFRE-FORT

Le nom du coffre-fort et le mot de passe d'accès sont modifiables.

Seuls les paramètres du coffre-fort auquel l'accès est autorisé peuvent être modifiés.

Pour renommer un coffre-fort, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Coffres-forts**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le coffre-fort et cliquez sur le bouton **Configurer**.
3. Dans la fenêtre qui s'ouvre, saisissez le mot de passe d'accès au coffre-fort.
4. Dans la fenêtre **Paramètres du coffre-fort** qui s'ouvre, indiquez le nouveau nom du coffre-fort.

Pour modifier le mot de passe d'accès au coffre-fort, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Coffres-forts**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le coffre-fort et cliquez sur le bouton **Configurer**.
3. Dans la fenêtre qui s'ouvre, saisissez le mot de passe d'accès au coffre-fort.
4. Dans la fenêtre **Paramètres du coffre-fort** qui s'ouvre, cliquez sur le lien **Modifier le mot de passe**.

5. Saisissez le mot de passe dans la fenêtre **Modification du mot de passe**.

CREATION D'UN LIEN POUR ACCEDER RAPIDEMENT AU COFFRE-FORT

Pour simplifier l'accès aux données, vous pouvez créer un raccourci d'accès au coffre-fort sur le Bureau. Ce raccourci permet d'ouvrir le coffre-fort et de chiffrer ou déchiffrer les données quel que soit l'endroit où se trouve le fichier du coffre-fort (si vous avez accès au coffre-fort depuis votre ordinateur). Vous pouvez créer le raccourci pour l'accès rapide lors de la création du coffre-fort ou n'importe quand après la création de celui-ci.

La création d'un raccourci est uniquement possible pour un coffre-fort auquel l'accès est autorisé.

Pour créer un raccourci d'accès au coffre-fort, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Coffres-forts**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le coffre-fort et cliquez sur le bouton **Configurer**.
3. Dans la fenêtre qui s'ouvre, saisissez le mot de passe d'accès au coffre-fort.
4. Dans la fenêtre **Paramètres du coffre-fort** qui s'ouvre, cliquez sur le lien **Créer un raccourci sur le bureau**.

MON RESEAU

Les fonctions de Mon Réseau sont prévues pour l'administration à distance de l'application Kaspersky PURE installée sur les ordinateurs du réseau local depuis le poste de travail de l'administrateur.

Grâce à Mon Réseau, l'administrateur du réseau peut exécuter les actions suivantes :

- Analyser le niveau de protection des ordinateurs du réseau ;
- Rechercher la présence éventuelle de menaces dans le réseau et sur des ordinateurs distincts ;
- Réaliser la mise à jour centralisée des bases antivirus ;
- Configurer les paramètres de protection des ordinateurs du réseau ;
- Exercer le contrôle parental ;
- Réaliser une copie de sauvegarde des données sur les ordinateurs du réseau ;
- Consulter les rapports sur le fonctionnement des sous-systèmes de la protection.

Pour lancer Mon Réseau, procédez comme suit :

Dans la partie inférieure de la fenêtre de Kaspersky PURE, cliquez sur le bouton **Mon Réseau**.

Au premier lancement, l'Assistant de configuration d'administration à distance s'ouvre automatiquement (cf. la rubrique "Configuration de l'administration à distance" à la page 191). Lors des lancements suivants, il faudra saisir le mot de passe d'administrateur.

Pour l'administration à distance de l'application sur les ordinateurs du réseau, Mon Réseau doit être protégé par le même mot de passe d'administrateur sur tous les ordinateurs.

DANS CETTE SECTION

Configuration de l'administration à distance 191

Recherche de virus et de vulnérabilités dans le réseau domestique 192

Mise à jour à distance sur les ordinateurs du réseau 192

Activation/désactivation des composants de la protection sur les ordinateurs du réseau 193

Administration à distance de Mon Contrôle Parental 194

Lancement de la copie de sauvegarde sur les ordinateurs du réseau 194

Administration à distance des licences sur les ordinateurs du réseau 195

CONFIGURATION DE L'ADMINISTRATION A DISTANCE

Un Assistant permet de configurer l'administration à distance. Au premier lancement de Mon Réseau, l'Assistant de configuration s'ouvre automatiquement. Plus tard, vous pourrez lancer l'Assistant de configuration manuellement.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Il est également possible de naviguer entre les étapes de l'Assistant à l'aide des boutons situés dans la partie supérieure de la fenêtre.

Pour configurer Mon Réseau, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre pour lancer l'Assistant de configuration de l'administration à distance. Voici, en détails, les étapes de l'Assistant :

   a. Saisissez ou modifiez le mot de passe d'administration dans la fenêtre **Protection par mot de passe**.

   b. Sélectionnez les ordinateurs pour l'administration à distance dans la fenêtre **Recherche des ordinateurs**.

   c. Sélectionnez le mode de mise à jour des bases dans la fenêtre **Mode de mise à jour**.

   d. Confirmez les paramètres sélectionnés dans la fenêtre **Résumé**.

RECHERCHE DE VIRUS ET DE VULNERABILITES DANS LE RESEAU DOMESTIQUE

Mon Réseau permet de lancer à distance la tâche de recherche d'éventuels virus sur tout le réseau et sur des ordinateurs en particulier.

Pour rechercher la présence éventuelle de virus sur tout le réseau, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Exécuter la recherche de virus** du menu **Actions sur le réseau** dans la partie supérieure de la fenêtre.

3. Dans la fenêtre **Lancement groupé de l'analyse** qui s'ouvre, sélectionnez le type d'analyse et les ordinateurs à analyser.

Pour rechercher la présence éventuelle de virus et de vulnérabilités sur un ordinateur en particulier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Réseau** dans la partie inférieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez l'ordinateur dans la partie supérieure, puis passez à la rubrique **Analyse**.

3. Sélectionnez la tâche d'analyse requise dans la partie droite.

MISE A JOUR A DISTANCE SUR LES ORDINATEURS DU RESEAU

Mon Réseau permet d'administrer à distance la mise à jour de Kaspersky PURE sur les ordinateurs du réseau.

Vous pouvez sélectionner une des méthodes suivantes pour la mise à jour :

- Mise à jour des bases sur les ordinateurs, indépendamment les uns des autres.

- Chargement des mises à jour depuis un ordinateur sélectionné dans le réseau. Dans ce cas, un des ordinateurs du réseau doit être désigné en tant que serveur de mises à jour. Les autres ordinateurs téléchargeront les mises à jour depuis cet ordinateur.

Pour modifier le mode de mise à jour des bases sur les ordinateurs du réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Réseau** dans la partie inférieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
3. Dans l'Assistant de configuration de **Mon Réseau** qui s'ouvre, passez à l'étape Mode de mise à jour et sélectionnez le mode de mise à jour requis.

Pour désigner un ordinateur en tant que serveur de mises à jour, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le bouton **Mon Réseau** dans la partie inférieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez l'ordinateur dans la partie supérieure de la fenêtre et passez à la rubrique **Mise à jour**.
3. Cliquez sur le bouton **Désigner comme source des mises à jour**.

Vous pouvez lancer la tâche de mise à jour à distance pour tout le réseau ou pour un ordinateur en particulier.

Pour lancer la mise à jour pour tous les ordinateurs du réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Réseau** dans la partie inférieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Exécuter la mise à jour** du menu **Actions sur le réseau** dans la partie supérieure de la fenêtre.
3. Dans la fenêtre **Lancement groupé de la mise à jour**, sélectionnez les ordinateurs sur lesquels il faut installer la mise à jour.

Pour lancer la mise à jour sur un ordinateur distinct, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Réseau** dans la partie inférieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez l'ordinateur dans la partie supérieure de la fenêtre et passez à la rubrique **Mise à jour**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Exécuter la mise à jour**.

ACTIVATION/DESACTIVATION DES COMPOSANTS DE LA PROTECTION SUR LES ORDINATEURS DU RESEAU

Mon Réseau permet d'activer/de désactiver à distance divers composants de la protection sur les ordinateurs du réseau.

Pour activer/désactiver à distance un composant de la protection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Réseau** dans la partie inférieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez l'ordinateur dont vous souhaitez administrer la protection, puis passez à la rubrique **Informations**.
3. Dans la partie droite de la fenêtre, choisissez l'option **Composants de la protection**.

4. Dans la fenêtre **Composants de la protection** qui s'ouvre, activez/désactivez le composant de la protection souhaité d'un clic de la souris sur l'icône d'état située à droite du nom du composant.

ADMINISTRATION A DISTANCE DE MON CONTROLE PARENTAL

Mon Réseau permet de définir à distance des restrictions et de consulter les statistiques des événements liés à l'utilisation des ordinateurs dans le réseau et sur Internet.

Pour configurer à distance Mon Contrôle Parental, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Réseau** dans la partie inférieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez l'ordinateur dans la partie supérieure de la fenêtre et passez à la rubrique **Mon Contrôle Parental**.

3. Sélectionnez le compte utilisateur dans la partie droite de la fenêtre, puis cliquez sur le bouton **Configurer**.

Pour parcourir les statistiques, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Réseau** dans la partie inférieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez l'ordinateur dans la partie supérieure de la fenêtre et passez à la rubrique **Mon Contrôle Parental**.

3. Sélectionnez le compte utilisateur dans la partie droite de la fenêtre, puis cliquez sur le bouton **Rapport complet**.

LANCEMENT DE LA COPIE DE SAUVEGARDE SUR LES ORDINATEURS DU RESEAU

Mon Réseau permet de lancer à distance une tâche de copie de sauvegarde sur les ordinateurs du réseau et de consulter le rapport sur les tâches exécutées de copie de sauvegarde et de restauration des données.

Pour exécuter une copie de sauvegarde à distance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mon Réseau** dans la partie inférieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez l'ordinateur dans la partie supérieure de la fenêtre et passez à la rubrique **Mes Sauvegardes**.

3. Dans la partie droite de la fenêtre, sélectionnez la tâche de copie de sauvegarde, puis cliquez sur **Exécuter**.

   Vous pouvez suspendre ou annuler l'exécution de la tâche à l'aide des boutons correspondants de la partie supérieure de la fenêtre.

Pour obtenir le rapport sur les tâches de copie de sauvegarde et de restauration des données, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, sélectionnez l'ordinateur dans la partie supérieure de la fenêtre et passez à la rubrique **Mes Sauvegardes**.

3. Cliquez sur le bouton **Voir le rapport** dans la partie supérieure de la fenêtre.

4. Dans la fenêtre **Rapport** qui s'ouvre, configurez les paramètres d'affichage des informations sur les événements.

ADMINISTRATION A DISTANCE DES LICENCES SUR LES ORDINATEURS DU RESEAU

Mon Réseau permet de vérifier à distance l'état des licences sur les ordinateurs du réseau, de renouveler les licences et d'en activer de nouvelles.

Pour administrer les licences sur les ordinateurs du réseau, procédez comme suit :

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

2. Dans la fenêtre qui s'ouvre, sélectionnez l'ordinateur pour lequel vous souhaitez afficher la liste des problèmes, puis passez à la rubrique **Informations**.

3. Dans la partie droite de la fenêtre qui s'ouvre, sélectionnez l'option **Gestionnaire de licences**.

4. Dans la fenêtre **Gestion des licences** qui s'ouvre, réalisez les opérations requises.

MON GESTIONNAIRE DE MOTS DE PASSE

Mon Gestionnaire de mots de passe conserve et protège toutes vos données personnelles (par exemple mots de passe, noms d'utilisateur, identifiants de messageries instantanées, données de contact, numéros de téléphone, etc.). Mon Gestionnaire de mots de passe établit un lien entre vos mots de passe et vos comptes et les applications Microsoft Windows ou pages Web dans lesquelles ils sont utilisés. Toutes les informations stockées sont cryptées dans une base de mots de passe dont l'accès est protégé au moyen d'un Mot de passe principal. Les informations sont accessibles uniquement si la base des mots de passe est déverrouillée. Après avoir lancé la page Web ou l'application, Mon Gestionnaire de mots de passe introduit à votre place le mot de passe, l'identifiant et les autres données personnelles dans les champs correspondants. De cette manière, il vous suffit de retenir un seul mot de passe.

Par défaut, Mon Gestionnaire de mots de passe est chargé au lancement du système d'exploitation. Le composant s'intègre dans les applications qui permettent de gérer des données personnelles directement depuis la fenêtre de l'application.

Mon Gestionnaire de mots de passe surveille l'activité des applications utilisant des mots de passe et offre une protection contre l'interception et le vol de données personnelles. Le composant analyse les programmes qui utilisent des mots de passe ou interrogent le mot de passe d'autres programmes et vous propose ensuite de décider d'autoriser ou d'interdire l'action suspecte.

De plus, Mon Gestionnaire de mots de passe permet de :

- enregistrer et utiliser vos mots de passe (cf. page 207) ;
- rechercher des comptes utilisateur, des mots de passe, des noms d'utilisateur et d'autres informations personnelles dans la base de mots de passe (cf. page 208) ;
- générer des mots de passe robustes (cf. page 225) lors de la création de comptes utilisateur ;
- conserver tous les mots de passe sur un disque amovible (cf. page 226) ;
- restaurer la base de mots de passe depuis la copie de sauvegarde (cf. page 210) ;
- protéger les mots de passe contre l'accès non autorisé (cf. page 198).

Pour ouvrir Mon Gestionnaire de mots de passe depuis la fenêtre principale de Kaspersky PURE,

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

Pour ouvrir Mon Gestionnaire de mots de passe depuis le menu contextuel,

Choisissez l'option **Mon Gestionnaire de mots de passe** dans le menu contextuel de Mon Gestionnaire de mots de passe.

Vous pouvez aussi configurer l'ouverture de la fenêtre principale de Mon Gestionnaire de mots de passe d'un double-clique de la souris (cf. page 225) sur l'icône de Mon Gestionnaire de mots de passe dans la zone de notification de la barre des tâches.

DANS CETTE SECTION

Gestion de la base de mots de passe 198

Configuration des paramètres de l'application 212

Création de mots de passe fiables 225

Utilisation d'une version portable de Mon Gestionnaire de mots de passe 226

GESTION DE LA BASE DE MOTS DE PASSE

La base de mots de passe conserve tous les comptes des programmes et pages Web ainsi qu'un ou plusieurs noms d'utilisateurs et même vos identités (contenant p.ex. des données de contact, numéros de téléphone, identifiants de messageries, etc.).

La base de mots de passe ne peut être utilisée que lorsqu'elle est déverrouillée (cf. page 198). Avant toute modification de la base de mots de passe, il est recommandé de configurer les paramètres de copie de sauvegarde de la base (cf. page 218). Si vos données ont été malencontreusement modifiées ou supprimées, utilisez la fonction de restauration de la base de mots de passe (cf. page 210).

Vous pouvez exécuter les opérations suivantes :

- ajouter (cf. page 199), modifier, supprimer (cf. page 208) des données personnelles ;
- importer/exporter (cf. page 209), restaurer (cf. page 210) la base de mots de passe.

DANS CETTE SECTION

Accès à la base de mots de passe 198

Ajout de données personnelles 199

Utilisation des données personnelles 207

Recherche de mots de passe 208

Suppression de données personnelles 208

Importation / exportation de données 209

Copie de sauvegarde/restauration de la base de mots de passe 210

ACCES A LA BASE DE MOTS DE PASSE

Pour accéder à la base de mots de passe, vous pouvez choisir parmi les méthodes d'authentification suivantes :

- **Protection par Mot de passe principal**. L'accès à la base de mots de passe s'effectue via le Mot de passe principal.
- **Périphérique USB**. L'accès à la base de mots de passe s'effectue via un périphérique à interface USB connecté à l'ordinateur. Lorsque le périphérique USB est déconnecté, la base de mots de passe est automatiquement verrouillée.
- **Périphérique Bluetooth**. L'accès à la base de mots de passe s'effectue via un périphérique Bluetooth connecté à l'ordinateur. Lorsque le périphérique Bluetooth est déconnecté, la base de mots de passe est automatiquement verrouillée.
- **Sans authentification**. L'accès à la base de mots de passe n'est pas protégé.

La protection activée par défaut est celle par Mot de passe principal qui vous permet de ne retenir qu'un seul mot de passe pour accéder à tous les autres.

Mot de passe principal – il s'agit de la méthode de base pour protéger vos données personnelles. Si vous avez opté pour la méthode d'authentification par périphérique et que par la suite vous n'avez pas ce périphérique sous la main (ou par exemple qu'il a été perdu), vous pouvez utiliser le Mot de passe principal pour accéder à vos données personnelles.

Mon Gestionnaire de mots de passe verrouille par défaut la base de mots de passe au lancement de l'application et après une période d'inactivité définie de l'ordinateur (cf. page 220). L'utilisation de l'application n'est possible que lorsque la base de mots de passe est déverrouillée.

Vous pouvez également déverrouiller / verrouiller la base de mots de passe par les moyens suivants :

- Dans la fenêtre Mon Gestionnaire de mots de passe (à la page 50) ;
- périphérique USB ou Bluetooth – uniquement possible lorsque le mode d'authentification par périphérique USB ou Bluetooth est activé ;
- double-clique sur l'icône de l'application (cf. page 225) ; pour ce faire, la fonction d'activation par double-clique doit être activée ;
- Dans le menu contextuel de Mon Gestionnaire de mots de passe (cf. page 51) ;
- combinaison de touches CTRL+ALT+L (cf. page 216).

Pour saisir le Mot de passe principal, vous pouvez utiliser Mon Clavier virtuel. Celui-ci vous permet d'introduire des mots de passe sans risque d'interception des frappes sur le clavier.

Pour verrouiller l'application depuis le menu contextuel, procédez comme suit :

1. Dans la zone de notification de la barre des tâches, cliquez avec le bouton droit de la souris sur l'icône de Mon Gestionnaire de mots de passe.
2. Dans le menu qui s'ouvre, sélectionnez l'entrée **Verrouiller**.

Pour déverrouiller l'application depuis le menu contextuel, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur l'icône de Mon Gestionnaire de mots de passe dans la zone de notification de la barre des tâches.
2. Dans le menu qui s'ouvre, sélectionnez le point **Débloquer**.
3. Introduisez le Mot de passe principal dans la boîte de dialogue.

AJOUT DE DONNEES PERSONNELLES

L'ajout de données personnelles est possible si la base de mots de passe n'est pas verrouillée (cf. page 198). Lors du lancement d'une application / d'une page Web, un nouveau compte est automatiquement identifié lorsqu'il ne se trouve pas dans la base de mots de passe. Après vous être authentifié dans l'application / sur la page Web, Mon Gestionnaire de mots de passe vous propose d'ajouter automatiquement vos données personnelles dans la base de mots de passe.

Les types de données personnelles suivants sont accessibles dans la base de mots de passe :

- **Compte**. Combinaison d'identifiants et de mots de passe pour l'autorisation d'accès sur certains sites Web ou dans des applications.
- **Groupe de Comptes**. S'utilise pour organiser de manière plus commode les comptes dans la base de mots passe.
- **Identifiant**. Par défaut, Mon Gestionnaire de mots de passe vous propose de créer un compte avec un seul identifiant. Les noms d'utilisateurs multiples s'utilisent lorsque les programmes ou pages Web permettent de créer plusieurs noms d'utilisateur pour accéder à leurs ressources.
- **Identité**. Les Identités permettent de conserver des données telles que le sexe, la date de naissance, les données de contact, le numéro de téléphone, le lieu de travail, l'identifiant de messagerie instantanée, l'URL de votre page d'accueil, etc. Afin de séparer les informations professionnelles et privées, vous pouvez créer plusieurs identités.
- **Note personnelle**. Utilisé pour la conservation de tout type d'informations.

COMPTE

Mon Gestionnaire de mots de passe identifie automatiquement le nouveau compte lorsqu'il ne le trouve pas dans la base de mots de passe. Après vous être authentifié dans l'application / sur la page Web, Mon Gestionnaire de mots de passe vous propose d'enregistrer les données dans la base de mots de passe. Vous pouvez également ajouter manuellement un Compte dans la base de mots de passe.

Un Compte se compose des données suivantes :

- type de compte utilisateur (compte utilisateur d'application ou compte utilisateur Internet) ;
- nom / plusieurs noms d'utilisateur ;
- mot de passe ;
- chemin d'accès à l'application/URL de la page Web (en fonction du type de compte utilisateur) ;
- paramètres du lien entre le compte utilisateur et l'objet ;
- paramètres d'activation du compte utilisateur ;
- commentaires ;
- paramètres de remplissage des champs complémentaires de la page Web.

Mon Gestionnaire de mots de passe permet d'utiliser un ou plusieurs comptes utilisateur pour l'autorisation sur l'application ou sur le site Web.

Mon Gestionnaire de mots de passe permet de spécifier la zone d'utilisation de chaque compte utilisateur sur la base de l'emplacement de l'application/de l'URL de la page Web.

Il existe plusieurs manières d'ajouter un Compte :

- via le Bouton d'accès rapide – pour ce faire, sélectionnez l'entrée **Ajouter un Compte** dans le menu du Bouton d'accès rapide ;
- via le menu contextuel de Mon Gestionnaire de mots de passe : il faut pour cela sélectionner l'option **Ajouter compte utilisateur** dans le menu contextuel de Mon Gestionnaire de mots de passe ;
- via la fenêtre principale de Mon Gestionnaire de mots de passe.

Pour ajouter un nouveau compte utilisateur depuis la fenêtre principale, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.
4. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**, puis choisissez l'option **Ajouter un compte**.
5. Dans la fenêtre de l'Assistant de création de compte utilisateur qui s'ouvre, sélectionnez le type de compte utilisateur (compte utilisateur Internet, compte utilisateur d'application ou mode utilisateur), puis cliquez sur **Suivant**.
   - Si vous avez choisi l'option compte utilisateur Internet ou d'application, indiquez le site Web ou l'application pour laquelle le compte utilisateur sera utilisé, puis cliquez sur **Suivant**.

- Si vous avez sélectionné le mode utilisateur, sous l'onglet **Association** de la fenêtre qui s'ouvre, indiquez le chemin d'accès à l'application/à la page Web et définissez les paramètres d'utilisation du compte utilisateur.

6. Dans la partie supérieure de la fenêtre, dans le champ **Nom**, saisissez ou modifiez le nom du nouveau compte utilisateur.

7. Sous l'onglet **Identifiant**, introduisez l'Identifiant et le mot de passe.

   L'Identifiant peut se composer d'un ou plusieurs caractères. Pour spécifier les mots-clés (cf. page 201) associés au nom d'utilisateur, cliquez sur le bouton .

   Pour copier l'identifiant/le mot de passe dans le Presse-papiers, cliquez sur le bouton .

   Pour copier l'identifiant d'un autre compte, cliquez sur le lien **Utiliser l'identifiant d'un autre compte**.

   Pour créer automatiquement un mot de passe, cliquez sur le lien **Nouveau mot de passe** (cf. page 225).

8. Sous l'onglet **Modification avancée**, configurez si nécessaire les paramètres de remplissage des champs complémentaires de la page Web.

9. Sous l'onglet **Commentaires**, introduisez si nécessaire un texte complémentaire décrivant le compte. Pour afficher les commentaires dans les notifications après activation du compte, cochez la case **Afficher les commentaires dans les notifications**.

DEFINITION DE MOTS-CLES POUR LA RECHERCHE

Pour rechercher rapidement des données personnelles dans la base de mots de passe, vous pouvez utiliser des mots-clés. Vous pouvez en spécifier pour chaque Identifiant. Il est conseillé de définir des mots clés lors de l'ajout d'un compte utilisateur (cf. page 200) / nom d'utilisateur (cf. page 205).

Pour associer des mots-clés à un Identifiant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.

4. Sélectionnez l'identifiant dans la liste **Mes Mots de passe** et dans la partie supérieure de la fenêtre, cliquez sur le bouton **Modifier**.

5. Dans la fenêtre qui s'ouvre, cliquez sur le bouton en regard du champ **Identifiant** et complétez le champ **Description**.

   En cas de sélection d'un Compte associé à un seul Identifiant, cliquez sur le bouton sous l'onglet **Identifiant** de la fenêtre **Compte associé à un seul Identifiant** .

AJOUT DE L'EMPLACEMENT DE L'APPLICATION / DE LA PAGE WEB

Pour associer un compte à une application ou à une page Web, il faut créer un lien. S'agissant des pages Web, le lien se présente sous la forme d'une URL et pour les applications, il prend la forme du chemin d'accès au fichier exécutable de l'application sur l'ordinateur. Sans ces données, le Compte ne peut être associé au programme / à la page Web.

Pour associer un Compte à un programme / à une page Web, vous pouvez procéder de différentes manières :

- sélectionnez le lien en cliquant sur le bouton dans les favoris de votre navigateur Internet ou dans la liste des programmes installés sur votre ordinateur ;

- spécifiez manuellement l'emplacement de l'application / de la page Web ;

- utilisez le pointeur de Mon Gestionnaire de mots de passe.

Pour vérifier que le lien introduit est correct, ouvrez le programme / la page Web via le bouton .

Pour choisir un lien dans la liste, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.
4. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**, puis choisissez l'option **Ajouter un compte**.
5. Dans le champ **Lien** de l'onglet **Liens** de la boîte de dialogue, cliquez sur le bouton .
6. Dans le champ **Lien** de la boîte de dialogue, saisissez l'emplacement de l'application / de la page Web.

   Pour désigner la page Web dans la liste des pages Web enregistrées (Sélection), sélectionnez dans la liste **Onglets** la page Web, puis cliquez sur le lien **Copier le lien de la Sélection**. Pour copier l'emplacement de la page Web depuis la fenêtre du navigateur Internet, cliquez sur le lien **Utiliser le chemin à l'application couplée**.

   Pour créer un lien vers une application, dans le champ **Lien**, cliquez sur le bouton et désignez le chemin d'accès au fichier exécutable de l'application.

Pour désigner le chemin d'accès à l'application / à la page Web manuellement, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.
4. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**, puis choisissez l'option **Ajouter un compte**.
5. Dans le champ **Lien** de l'onglet **Liens** de la boîte de dialogue, saisissez l'emplacement de l'application / l'URL de la page Web . L'URL de la page Web doit commencer par http://www.

Pour désigner le chemin d'accès à l'application / à la page Web via l'index de Mon Gestionnaire de mots de passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.
4. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**, puis choisissez l'option **Ajouter un compte**.
5. Dans le champ **Lien** de l'onglet **Liens** de la fenêtre qui s'ouvre, indiquez l'emplacement de l'application/l'URL de la page Web en déplaçant le pointeur de Mon Gestionnaire de mots de passe dans la fenêtre de l'application/du navigateur Internet.

SELECTION DU MODE DE LIAISON DU COMPTE

Pour déterminer le compte dont les données doivent être utilisées pour le remplissage automatique lors du lancement d'un programme/d'une page Web, Mon Gestionnaire de mots de passe utilise le chemin d'accès à l'application/l'URL de la page Web.

Étant donné que Mon Gestionnaire de mots de passe permet d'utiliser plusieurs comptes utilisateur pour un seul programme/site Web, la zone d'utilisation de chaque compte utilisateur doit être définie.

Mon Gestionnaire de mots de passe permet de spécifier la zone d'utilisation du compte utilisateur sur la base de l'emplacement de l'application/de l'URL de la page Web. Les paramètres de la zone sont configurés lors de la création d'un compte utilisateur (cf. page 200). Il est toutefois possible d'en modifier ultérieurement la valeur.

En fonction de l'objet (programme ou site Web), l'utilisation du Compte est différente.

Pour un programme, les options possibles sont les suivantes :

- Utiliser le Compte pour le programme. Le Compte sera utilisé pour toutes les fenêtres de l'application prévoyant l'introduction de données personnelles.
- Identifier selon le titre de la fenêtre. Le Compte ne sera utilisé que pour la fenêtre spécifiée de l'application.

  Par exemple, un programme peut utiliser plusieurs Comptes. Au sein de ce programme, le seul élément permettant de distinguer le compte à utiliser est le titre de la fenêtre. Mon Gestionnaire de mots de passe complétera automatiquement les données du compte utilisateur en fonction du titre de la fenêtre de l'application.

Pour une page Web, les utilisations possibles du Compte sont les suivantes :

- Uniquement pour la page Web spécifiée. Mon Gestionnaire de mots de passe ajoutera automatiquement l'identifiant et le mot de passe dans les champs d'identification uniquement pour l'URL définie.

  Par exemple, si le compte utilisateur est associé à l'URL http://www.web-site.com/login.html, celui-ci ne sera pas actif pour les autres pages du même site (par exemple pour l'URL http://www.web-site.com/index.php).

- Pour les pages Web d'un répertoire. Mon Gestionnaire de mots de passe ajoutera automatiquement l'identifiant et le mot de passe dans les champs d'identification pour toutes les pages Web du dernier répertoire.

  Par exemple, si l'URL introduite est http://www.web-site.com/cgi-bin/login.html, le compte utilisateur spécifié sera utilisé pour toutes les pages Web situées dans le répertoire *cgi-bin*.

- Pour un site Web: <nom de domaine de troisième niveau et inférieur>. Le Compte spécifié est utilisé pour n'importe quelle page du domaine (domaine de troisième niveau et inférieur).

  Par exemple, Mon Gestionnaire de mots de passe complète automatiquement les données d'identification pour les pages Web: http://www.domain1.domain2.web-site.com/login.html ou http://www.domain1.domain2.web-site.com/index.php. Cependant, le compte utilisateur spécifié ne sera pas utilisé pour les pages Web dont les URL ont un domaine de quatrième niveau différent : http://www.domain3.domain2.web-site.com/index.php ou http://www.domain4.domain2.web-site.com/index.php.

- Pour un site Web: <nom du site Web>. Le Compte spécifié sera utilisé pour toutes les pages du site Web prévoyant l'introduction d'un Identifiant et d'un mot de passe.

  Par exemple, Mon Gestionnaire de mots de passe complétera automatiquement les données d'identification pour les pages Web : http://www.domain1.domain2.web-site.com/login.html, http://www.domain2.domain2.web-site.com/index.php, http://www.domain3.domain2.web-site.com/index.php ou http://www.domain4.domain2.web-site.com/index.php.

➧ *Pour spécifier les paramètres d'utilisation d'un Compte, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.

4. Sélectionnez le compte dans la liste **Mes Mots de passe**, puis cliquez sur **Modifier**.

5. Sous l'onglet **Liens** de la boîte de dialogue, sélectionnez l'une des options d'utilisation du compte.

ACTIVATION AUTOMATIQUE D'UN COMPTE

L'option d'activation automatique d'un Compte est activée par défaut. Mon Gestionnaire de mots de passe saisit uniquement l'identifiant et le mot de passe dans les champs d'identification. Vous pouvez configurer des paramètres complémentaires d'activation du compte utilisateur (cf. page 200).

Pour les pages Web, il est en outre possible de spécifier une série d'URL pour lesquelles l'activation automatique doit s'appliquer.

Les différentes possibilités d'activation d'un Compte sont les suivantes :

- Pour la page Web sélectionnée. Le Compte ne sera activé que pour la page Web spécifiée.
- Pour un site Web. Le Compte sera activé pour toutes les pages du site Web.

Pour sélectionner l'activation automatique d'un Compte, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.

4. Sélectionnez le compte dans la liste **Mes Mots de passe**, puis cliquez sur **Modifier**.

5. Sous l'onglet **Liens** de la boîte de dialogue, cochez la case **Activation automatique du Compte**.

   Choisissez également l'un des modes d'activation du compte pour la page Web.

REMPLISSAGE DE CHAMPS COMPLEMENTAIRES

Lors de l'authentification sur une page Web, des données autres que l'Identifiant et le mot de passe doivent parfois être complétées. Mon Gestionnaire de mots de passe permet d'utiliser le remplissage automatique des champs complémentaires. Vous avez la possibilité de configurer les paramètres de remplissage des champs complémentaires pour un Compte.

La configuration des paramètres de remplissage des champs complémentaires est possible lorsque l'emplacement de l'application / l'URL de la page Web est spécifiée pour le Compte.

Pour configurer ces champs, Mon Gestionnaire de mots de passe télécharge provisoirement la page Web et en analyse ensuite tous les champs et boutons. Les champs et boutons sont inclus dans un groupe propre à chaque page Web.

Lors du traitement de la page Web téléchargée, Mon Gestionnaire de mots de passe stocke temporairement les fichiers et images sur votre ordinateur.

Pour configurer les paramètres de remplissage automatique des champs complémentaires, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.

4. Sélectionnez le compte dans la liste **Mes Mots de passe**, puis cliquez sur **Modifier**.

5. Sous l'onglet **Modification avancée** de la boîte de dialogue, cliquez sur le lien **Ouvrez l'édition avancée de formulaire**.

6. Dans la partie supérieure de la fenêtre **Modification avancée** qui s'ouvre, cochez le champ/le bouton requis.

7. Activez le champ **Valeur** pour le champ / bouton sélectionné par un double-clique de la souris et saisissez ensuite la valeur du champ.

CREATION D'UN GROUPE DE COMPTES

Les groupes de Comptes permettent d'organiser les informations dans la base de mots de passe. Un groupe se compose d'un dossier dans lequel sont ajoutés des Comptes.

Les groupes créés sont affichés dans le menu contextuel de Mon Gestionnaire de mots de passe : option **Comptes** → **<Intitulé du groupe>**.

Pour créer un groupe de Comptes, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.

4. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**, puis choisissez l'option **Ajouter un groupe**.

5. Saisissez le nom du nouveau groupe.

6. Glissez-déposez les Comptes à ajouter depuis la liste **Base de données** vers le dossier créé.

IDENTIFIANT

Certaines applications / pages Web utilisent plusieurs noms d'utilisateur. Mon Gestionnaire de mots de passe permet d'enregistrer plusieurs noms d'utilisateur pour un compte utilisateur. Mon Gestionnaire de mots de passe détecte automatiquement le nouvel identifiant lors de sa première utilisation et vous propose de l'ajouter au compte utilisateur pour l'application/la page Web concernée. Vous pouvez ajouter manuellement un nouvel Identifiant pour un Compte et par la suite le modifier. Vous pouvez également utiliser le même identifiant pour différents comptes.

Il existe plusieurs manières d'ajouter un Identifiant pour un Compte déterminé :

- Via le Bouton d'accès rapide. Pour ce faire, sélectionnez l'entrée **Modifier le Compte** → **Ajouter l'Identifiant** dans le menu du Bouton d'accès rapide.

- Au départ de la fenêtre principale du logiciel.

Pour ajouter un nouvel Identifiant pour un Compte déterminé, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.

4. Sélectionnez un compte dans la liste **Mes Mots de passe**, cliquez sur le bouton **Ajouter** et choisissez l'option **Ajouter un identifiant**.

5. Dans la boîte de dialogue, spécifiez l'Identifiant et le mot de passe. L'Identifiant peut se composer d'un ou plusieurs caractères. Pour spécifier les mots-clés associés à l'Identifiant, cliquez sur le bouton et complétez ensuite le champ **Description**.

   Pour copier l'Identifiant / mot de passe dans le Presse-papiers, utilisez le bouton . Pour créer un mot de passe automatiquement, cliquez sur le lien **Nouveau mot de passe** (cf. page 225).

   Pour copier l'identifiant d'un autre compte, cliquez sur le lien **Utiliser l'identifiant d'un autre compte**.

IDENTITE

Outre l'Identifiant et le mot de passe, certaines données personnelles sont souvent nécessaires pour s'enregistrer sur un site Web, par exemple le nom complet, l'année de naissance, le sexe, l'adresse de courrier électronique, le numéro de téléphone, la ville de résidence, etc. Mon Gestionnaire de mots de passe permet de conserver toutes ces données de manière cryptée dans la base de mots de passe sous la forme d'identité. Lorsque vous vous enregistrez sur un nouveau site Web, Mon Gestionnaire de mots de passe complète automatiquement le formulaire d'enregistrement en se basant sur les données de l'identité sélectionnée. Afin de séparer les informations professionnelles et privées, il est possible d'utiliser plusieurs identités. Les paramètres de l'Identité sont modifiables.

Pour créer une identité, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.
4. Dans la partie supérieure de la fenêtre, cliquez sur le bouton **Ajouter une identité**.
5. Dans le champ **Nom** de la boîte de dialogue, introduisez l'intitulé de l'Identité.
6. Saisissez la valeur pour les champs requis en les activant d'un double-clique dans la colonne **Valeur**.

NOTE PERSONNELLE

Les notes personnelles permettent de conserver des informations textuelles sous forme cryptée (par exemple, les données du passeport, des numéros de comptes en banque, etc.) et d'accéder rapidement aux données enregistrées. Pour pouvoir manipuler le texte des notes personnelles, Mon Gestionnaire de mots de passe propose une série d'outils standards d'un éditeur de texte. Lors de la création d'une note personnelle, vous pouvez utiliser des modèles avec des sélections de données standard (cf. page 222).

Vous pourrez modifier par la suite les paramètres de la note personnelle.

Pour créer une note personnelle à partir de zéro, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.
4. Dans la partie supérieure de la fenêtre, cliquez sur le bouton **Ajouter une note personnelle**.
5. Dans le champ **Nom** de la boîte de dialogue, introduisez l'intitulé de la note personnelle.
6. Saisissez les informations requises dans l'éditeur de texte.

Pour créer une note personnelle sur la base d'un modèle, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.

4. Dans la partie supérieure de la fenêtre, cliquez sur le bouton **Ajouter une note personnelle**.

5. Dans le champ **Nom** de la boîte de dialogue, introduisez l'intitulé de la note personnelle.

6. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Sélectionner un modèle** et choisissez le modèle requis.

7. Saisissez les données requises et réalisez la mise en page selon vos besoins.

Pour consulter une note personnelle,

ouvrez le menu contextuel de Mon Gestionnaire de mots de passe et choisissez l'option **Notes personnelles** → **<nom du groupe>** →**<nom de la note personnelle>**.

UTILISATION DES DONNEES PERSONNELLES

Mon Gestionnaire de mots de passe établit un lien entre vos comptes et les applications ou pages Web dans lesquelles ils sont utilisés. Lors du lancement d'une application / d'une page Web, Mon Gestionnaire de mots de passe recherche automatiquement un Compte associé dans la base de mots de passe. En cas de recherche fructueuse, les données personnelles sont complétées automatiquement. Si aucun compte utilisateur n'est trouvé dans la base de mots de passe, Mon Gestionnaire de mots de passe vous propose de l'ajouter (cf. page 200).

Certaines applications / pages Web peuvent utiliser plusieurs noms d'utilisateur. Mon Gestionnaire de mots de passe permet d'enregistrer plusieurs noms d'utilisateur pour un compte utilisateur. En cas d'introduction d'un nouveau nom d'utilisateur lors de l'authentification, Mon Gestionnaire de mots de passe vous propose de l'ajouter au compte utilisateur (cf. page 205) pour l'application / la page Web en cours d'utilisation. Par la suite, lors du lancement de l'application / de la page Web, une fenêtre reprenant la liste des noms d'utilisateur correspondant au Compte s'affiche en regard des champs de saisie des données personnelles.

Outre l'Identifiant et le mot de passe permettant l'identification, les sites Web utilisent souvent d'autres données personnelles (par exemple le nom complet, le sexe, le pays, la ville, l'adresse de courrier électronique, etc.). Mon Gestionnaire de mots de passe conserve ces données sous forme cryptée dans la base des mots de passe sous la forme d'une identité. Afin de séparer les informations professionnelles et privées, il est possible de créer plusieurs identités (cf. page 206). De cette manière, lorsque vous vous enregistrez dans l'application / sur un site Web, Mon Gestionnaire de mots de passe complète automatiquement les champs du formulaire d'enregistrement en se basant sur l'identité sélectionnée. L'utilisation d'une identité fait gagner du temps au moment de remplir des formulaires identiques.

Lorsque vous vous authentifiez dans une application / sur une page Web, Mon Gestionnaire de mots de passe ne complétera automatiquement les données personnelles que si la base de mots de passe est déverrouillée.

Vous pouvez utiliser le Compte d'une des manières suivantes :

- Lancer l'application / la page Web. Le formulaire d'authentification sera automatiquement complété sur la base des données du Compte.

- Appliquer le pointeur de Mon Gestionnaire de mots de passe. Pour ce faire, déplacez le curseur sur l'icône de l'application située dans la zone de notification de la barre des tâches et activez le Compte en "glissant-déposant" le pointeur de Mon Gestionnaire de mots de passe dans la fenêtre de l'application / sur la page Web concernée.

- Choisir le Compte dans la liste des comptes favoris. Pour ce faire, accédez au menu contextuel de Mon Gestionnaire de mots de passe et choisissez le compte approprié dans le groupe des comptes favoris.

- Utiliser le menu contextuel de Mon Gestionnaire de mots de passe. Pour ce faire, accédez au menu contextuel de Mon Gestionnaire de mots de passe et choisissez l'option **Comptes utilisateur** → **<Intitulé du compte>**.

Pour utiliser une Identité, procédez comme suit :

1. Dans la fenêtre de l'application /du navigateur Internet, cliquez sur le bouton d'accès rapide.

2. Dans le menu qui s'ouvre, choisissez l'option **Identités** → **<Nom de l'identité>**. Mon Gestionnaire de mots de passe complète automatiquement les champs du formulaire d'enregistrement de la page Web en se basant sur les données de l'identité.

RECHERCHE DE MOTS DE PASSE

La recherche de données personnelles peut être difficile dans les cas suivants :

- certains mots de passe ne sont pas liés à des programmes / pages Web ;
- la base de mots de passe contient un nombre important de comptes.

Mon Gestionnaire de mots de passe permet de trouver rapidement des mots de passe selon les paramètres suivants :

- intitulé du Compte ;
- nom de l'utilisateur ;
- mots-clés (cf. page 201) (les paramètres de recherche sur mots-clés sont accessoires et propres à chaque nom d'utilisateur) ;
- URL (pour les pages Web).

La recherche est lancée aussi bien sur un nom complet que sur les premières lettres ou sur n'importe quel caractère dans le nom du compte utilisateur ou dans le lien.

Pour trouver le compte utilisateur /le mot de passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.

4. Saisissez le texte dans la barre de recherche de la partie supérieure de la fenêtre.

SUPPRESSION DE DONNEES PERSONNELLES

Avant toute modification de vos données personnelles, Mon Gestionnaire de mots de passe crée automatiquement une copie de sauvegarde de la base de mots de passe. Si vos données ont été malencontreusement modifiées ou supprimées, utilisez la fonction de restauration de la base de mots de passe (cf. page 210). Il est possible de supprimer un élément ou tous les éléments de la base de mots de passe.

Pour supprimer un élément de la base de mots passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.

4. Choisissez un élément dans la liste **Mes Mots de passe**, cliquez sur le bouton **Supprimer** et choisissez l'option **Supprimer**.

Pour supprimer tous les éléments de la base de mots passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.
4. Choisissez un élément dans la liste **Mes Mots de passe**, cliquez sur le bouton **Supprimer** et choisissez l'option **Supprimer tout**.

IMPORTATION / EXPORTATION DE DONNEES

Mon Gestionnaire de mot de passe permet d'importer et d'exporter la base de mots de passe ainsi que des objets distincts (identités, comptes utilisateur ou notes personnelles).

Vous pouvez importer des mots de passe depuis d'autres applications de gestion de mots de passe (par exemple, Internet Explorer, Mozilla FireFox, KeePass) ou des mots de passe que vous aviez enregistrés à l'aide de Mon Gestionnaire de mots de passe. L'importation de mots de passe s'effectue depuis des fichiers au format xml ou ini.

Mon Gestionnaire de mots de passe permet d'exporter la base de mots de passe dans un fichier au format xml, html ou txt. La fonction d'exportation des mots de passe dans un fichier peut s'avérer utile lorsque vous devez partager les mots de passe, imprimer la base de mots de passe ou en effectuer une copie de sauvegarde dans un fichier d'un format différent de celui de Mon Gestionnaire de mots de passe.

Les mots de passe exportés sont sauvegardés dans des fichiers non cryptés et par conséquent non protégés contre l'accès non autorisé. C'est pourquoi il est recommandé de réfléchir préalablement aux moyens de protéger les données exportées.

Lors de l'importation, la base de mots de passe subit des modifications. Vous aurez alors la possibilité de choisir parmi différentes actions :

- **Écraser**. La base de mots de passe actuelle est remplacée par la base importée (tous les mots de passe sauvegardés dans la base de Mon Gestionnaire de mots de passe avant l'importation seront supprimés).
- **Fusionner**. Les mots de passe importés sont ajoutés à la base de mots de passe. Lors d'une fusion, il vous est proposé de choisir les comptes utilisateur à importer dans Mon Gestionnaire de mots de passe.
- **Annuler**. L'importation des mots de passe est annulée.

Pour importer les mots de passe depuis un fichier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.
4. Dans la partie inférieure de la fenêtre de l'application, cliquez sur le lien **Charger les mots de passe**.
5. Dans la boîte de dialogue **Chargement des mots de passe**, sélectionnez l'application depuis laquelle seront importés les mots de passe. Cliquez ensuite sur le bouton **Charger les mots de passe**.
6. Dans la fenêtre qui s'ouvre, désignez le fichier contenant les mots de passe que vous souhaitez importer, puis cliquez sur **Ouvrir**.
7. Dans la fenêtre qui s'ouvre, sélectionnez l'action à exécuter sur la base des mots de passe.

Pour enregistrer la base de mots de passe dans un fichier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.
4. Dans la partie inférieure de la fenêtre de l'application, cliquez sur le lien **Enregistrer les mots de passe**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le mode d'enregistrement (enregistrement de toute la base de mots de passe ou de certains objets), puis cliquez sur le bouton **Suivant**.
6. Dans la fenêtre qui s'ouvre, sélectionnez les paramètres d'enregistrement.
   - Si vous souhaitez protéger les données enregistrées, choisissez l'option **Enregistrement sécurisé** et saisissez un mot de passe pour la protection des données.
   - Si vous souhaitez enregistrer les données dans un fichier non crypté, choisissez l'option **Enregistrement sans cryptage** et désignez le format du fichier.
   - Afin de programmer le changement de mot de passe pour les données enregistrées, cochez la case **Programmer le changement de mot de passe pour les objets enregistrés**, puis sélectionnez la date à laquelle le mot de passe sera mis hors fonction. Mon Gestionnaire de mots de passe vous signalera la nécessité de remplacer le mot de passe.
7. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès pour l'enregistrement du fichier, puis cliquez sur le bouton **Suivant**.
8. Dans la fenêtre qui s'ouvre, vérifiez les paramètres d'enregistrement des données, puis lancez l'enregistrement.

COPIE DE SAUVEGARDE/RESTAURATION DE LA BASE DE MOTS DE PASSE

Avant toute modification de la base de mots de passe, une copie de sauvegarde est automatiquement créée. Un emplacement par défaut est défini pour l'enregistrement des copies de sauvegarde mais vous avez la possibilité de le modifier (cf. page 218). La sauvegarde des mots de passe peut s'avérer utile dans les cas suivants :

- pour annuler les dernières modifications ;
- lorsque la base de mots de passe a été écrasée ou supprimée ;
- lorsque la base de mots de passe est inaccessible / endommagée après une erreur matériel ou système.

Les données de la copie de sauvegarde sont entièrement cryptées. Mon Gestionnaire de mots de passe enregistre toutes les modifications dans la base de mots de passe. Dans l'application, les copies de sauvegarde sont affichées dans une liste et triées par date de création, la plus récente en premier. Les informations suivantes sont spécifiées pour chaque copie de sauvegarde:

- emplacement ;
- date et heure de création ;
- modifications apportées par rapport à la version précédente.

Les différentes actions possibles sont les suivantes :

- sauvegarde de la base de mots de passe depuis une copie de sauvegarde spécifique ;
- suppression d'anciennes copies de sauvegarde ;

- modification de l'emplacement de l'enregistrement des copies de sauvegarde (cf. page 218).

Pour restaurer la base de mots passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.
4. Dans la partie inférieure de la fenêtre, cliquez sur le lien **Restaurer la base des mots de passe**.
5. Dans la fenêtre **Restauration** qui s'ouvre, sélectionnez la date de la copie de sauvegarde dans la liste, puis cliquez sur le bouton **Restauration** dans la partie supérieure de la fenêtre.
6. Dans la boîte de dialogue qui s'affiche, confirmez la sauvegarde à l'aide du bouton **OK**.

Pour supprimer une ancienne copie de sauvegarde devenue inutile, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.
4. Dans la partie inférieure de la fenêtre, cliquez sur le lien **Restaurer la base des mots de passe**.
5. Dans la boîte de dialogue **Sauvegarde**, sélectionnez dans la liste la copie de sauvegarde à supprimer. Pour sélectionner plusieurs versions, maintenez enfoncée la touche **CTRL**.
6. Cliquez sur le bouton **Supprimer**.
7. Dans la boîte de dialogue qui s'affiche, confirmez la suppression des copies de sauvegarde à l'aide du bouton **OK**.

CONFIGURATION DES PARAMETRES DE L'APPLICATION

La configuration des paramètres de l'application n'est possible que lorsque la base de mots de passe est déverrouillée (cf. page 198). La modification des paramètres recouvre les actions suivantes :

- définir le type de démarrage de l'application (cf. page 224) ;
- définir le nom d'utilisateur (cf. page 213), utilisé par défaut lors de la création d'un compte utilisateur ;
- définir la durée de conservation du mot de passe dans le Presse-papiers (cf. page 224) ;
- configurer la liste des comptes souvent utilisés (cf. page 214) ;
- établir la liste des sites Web interdits (cf. p 215) pour lesquels les fonctions de Mon Gestionnaire de mots de passe doivent être désactivées ;
- établir la liste des sites Web de confiance (cf. page 215) pour lesquels Mon Gestionnaire de mots de passe autorise le réadressage ;
- configurer les touches de raccourci pour l'appel des fonctions de Mon Gestionnaire de mots de passe (cf. page 216) ;
- modifier le chemin d'accès à la base des mots de passe (cf. page 216), aux copies de sauvegarde (cf. page 218) ;
- modifier la méthode de cryptage des données (cf. page 219) ;
- configurer le verrouillage automatique de la base des mots de passe (cf. page 220) ;
- modifier le mot de passe principal (cf. page 221) ;
- configurer l'accès à la base de mots de passe (cf. page 220) ;
- modifier la position du Bouton d'accès rapide, établir la liste des applications, supportant le Bouton d'accès rapide (cf. page 223) ;
- composer la liste des applications prises en charge (cf. page 222).

Afin de modifier les paramètres de fonctionnement du Mon Gestionnaire de mots de passe, procédez comme suit :

1. Ouvrez l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la fenêtre qui s'ouvre, sélectionnez la section relative aux paramètres à modifier.
5. Dans la partie droite de la fenêtre, effectuez les modifications nécessaires au groupe de paramètres souhaité.

DANS CETTE SECTION

Assistant de Configuration des paramètres 213

Utilisation d'un Identifiant par défaut 213

Comptes favoris 214

URL ignorées 215

URL de confiance 215

Touches de raccourci 216

Emplacement du fichier de la base de mots de passe 216

Création d'une nouvelle base de mots de passe 217

Emplacement de la copie de sauvegarde 218

Sélection du mode de cryptage 219

Verrouillage automatique la base de mots de passe 220

Modification du mode d'authentification de Mon Gestionnaire de mots de passe 220

Autorisation à l'aide d'un périphérique USB ou Bluetooth 221

Modification du Mot de passe principal 221

Navigateurs compatibles 222

Administration des modèles des notes personnelles 222

Affichage du bouton d'accès rapide 223

Définir la durée de conservation d'un mot de passe dans le Presse-papiers 224

Notifications 224

Fonction d'activation par double-clique 225

ASSISTANT DE CONFIGURATION DES PARAMETRES

L'Assistant de configuration des paramètres de l'application est lancé à la première exécution de Mon Gestionnaire de mots de passe. Son rôle est de vous aider à réaliser la configuration initiale des paramètres de Mon Gestionnaire de mots de passe en fonction de vos préférences personnelles et des tâches que vous devrez effectuer.

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**.

Nous détaillerons plus loin chaque étape de l'assistant.

UTILISATION D'UN IDENTIFIANT PAR DEFAUT

Mon Gestionnaire de mots de passe permet de spécifier l'Identifiant qui sera automatiquement affiché dans le champ **Identifiant** lors de la création d'un compte (cf. page 200).

Pour spécifier l'Identifiant par défaut, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre, sélectionnez la section **Général**.
5. Dans la partie droite de la fenêtre, complétez le champ **Identifiant par défaut**.

COMPTES FAVORIS

Mon Gestionnaire de mots de passe garantit un accès rapide aux comptes utilisateur. La liste des comptes favoris apparaît dans la fenêtre principale de l'application, ainsi que dans le menu contextuel et dans le menu du bouton d'accès rapide. Elle présente le nom des programmes / pages Web que vous lancez le plus souvent. Les éléments de la liste peuvent être triés par ordre alphabétique ou par fréquence d'utilisation.

La liste des Comptes favoris n'est accessible depuis le menu que si la base de mots de passe est déverrouillée (cf. page 198).

Vous pouvez spécifier les paramètres de liste suivants :

- **Quantité d'éléments dans la liste** – nombre maximum de Comptes favoris pouvant être affichés dans le menu de l'application ;
- **Afficher la liste dans le menu de l'application** : la liste des comptes utilisateur favoris sera accessible depuis le menu contextuel de Mon Gestionnaire de mots de passe ;
- **Afficher les Comptes favoris dans le menu du Bouton d'accès rapide** – la liste des Comptes favoris sera accessible depuis le menu du Bouton d'accès rapide (dans la fenêtre de l'application / du navigateur Internet).

Pour afficher les comptes favoris dans le menu contextuel, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre sélectionnez la rubrique **Comptes favoris**.
5. Dans la partie droite de la fenêtre, cochez la case **Afficher la liste dans le menu de la barre des tâches**.

   Pour afficher la liste des comptes favoris dans le menu du Bouton d'accès rapide, cochez en plus la case **Afficher les Comptes favoris dans le menu du Bouton d'accès rapide**.

   Si la case **Afficher les Comptes favoris dans le menu de la barre des tâches** n'est pas cochée, les autres paramètres de liste ne pourront être modifiés.

6. Spécifiez le nombre de Comptes dans le champ **Taille de la liste**.
7. Si nécessaire, modifiez manuellement la composition de la liste. Pour retirer un élément de la liste, sélectionnez le Compte souhaité et cliquez sur le bouton **Supprimer.** Pour supprimer tous les éléments de la liste, cliquez sur le bouton **Purger**.

URL IGNOREES

Vous pouvez configurer la liste des URL pour lesquelles les fonctions de Mon Gestionnaire de mots de passe ne seront pas utilisées. La fonction de remplissage automatique de l'Identifiant et du mot de passe sera inactive pour tous les sites Web appartenant à cette liste. De plus, pour celles-ci, Mon Gestionnaire de mots de passe ne proposera pas automatiquement la création d'un compte (cf. page 200) / identifiant (cf. page 205).

Pour constituer la liste des URL ignorées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre sélectionnez la rubrique **URL à ignorer**.
5. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ajouter**, saisissez l'URL et appuyez sur la touche **ENTER**.

   Pour modifier une URL, sélectionnez-la dans la liste et cliquez sur le bouton **Modifier**. Pour supprimer une URL de la liste, sélectionnez-la et cliquez sur le bouton **Supprimer**.

URL DE CONFIANCE

Mon Gestionnaire de mots de passe protège vos données personnelles contre les attaques d'hameçonnage. Si lors d'une tentative d'authentification vous êtes redirigé vers un autre site Web, le programme vous en avise.

Les individus mal intentionnés utilisent souvent le réadressage à partir de sites Web qui accèdent à des comptes bancaires (il peut par exemple s'agir de banques sur Internet, de systèmes de paiement, etc.). Une fois sur la page d'authentification du site Web officiel de la société, un réadressage est effectué vers un site Web contrefait qui est visuellement identique à la page Web officielle. Toutes les données encodées sur la page contrefaite sont transmises aux individus mal intentionnés.

Souvent l'échange d'adresse est officiellement installé sur les sites Web. Pour éviter que Mon Gestionnaire de mots de passe ne considère ce type de réadressage comme des tentatives d'hameçonnage, vous avez la possibilité d'établir une liste des URL de confiance. Cette liste doit contenir les sites Web vers lesquels sont transmises des données personnelles. Lors d'une autorisation, Mon Gestionnaire de mots de passe n'affiche pas de notification si les données personnelles sont transmises vers un site Web de confiance.

Mon Gestionnaire de mots de passe autorise l'envoi de données personnelles depuis d'autres sites vers un site Web de confiance. Avant d'ajouter un site Web dans la liste des URL de confiance, assurez-vous de sa fiabilité.

Vous pouvez ajouter un site Web dans la liste des URL de confiance de plusieurs manières :

- directement lors de l'authentification sur un site Web ;
- manuellement depuis la fenêtre **Configuration de Mon Gestionnaire de mots de passe**.

Pour ajouter un site Web à la liste des URL de confiance durant le processus d'autorisation sur le site, attendez le réadressage d'un site Web à l'autre et cochez ensuite la case **Toujours faire confiance au site Web <intitulé du site Web>** dans la boîte de dialogue de Mon Gestionnaire de mots de passe.

Pour constituer manuellement la liste des URL de confiance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.

4. Dans la partie gauche de la fenêtre sélectionnez la rubrique **URL de confiance**.

5. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ajouter**. Un champ devient accessible dans la liste **URL de confiance**. Saisissez l'URL et appuyez sur la touche **ENTER**.

   Pour modifier une URL, sélectionnez-la dans la liste et cliquez sur le bouton **Modifier**. Pour supprimer une URL, sélectionnez-la dans la liste et cliquez sur le bouton **Supprimer**.

TOUCHES DE RACCOURCI

L'utilisation de combinaisons de touches du clavier permet de lancer rapidement diverses fonctions de l'application.

Vous pouvez spécifier une combinaison de touches pour les actions suivantes :

- Verrouillage/déverrouillage de Mon Gestionnaire de mots de passe (cf. page 198).
- Saisissez le mot de passe.

Un raccourci peut se composer d'une touche ou d'une combinaison de deux ou trois touches.

N'attribuez pas au lancement des fonctions de Mon Gestionnaire de mots de passe les combinaisons de touches utilisées dans Microsoft Windows.

Pour attribuer une combinaison de touches, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre, sélectionnez la section **Raccourcis**.
5. Dans la partie droite de la fenêtre, spécifiez la combinaison de touches à associer à chaque action.

EMPLACEMENT DU FICHIER DE LA BASE DE MOTS DE PASSE

Base de mots de passe de Mon Gestionnaire de mots de passe : il s'agit d'un fichier crypté (cf. page 219) dans lequel sont conservées toutes vos données personnelles (comptes, noms d'utilisateur, mots de passe et identité).

Par défaut, le chemin d'accès à la base de mots de passe est le suivant (diffère selon la version de Microsoft Windows):

- pour Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Passwords Database\ ;
- pour Microsoft Windows Vista: C:\Users\User_name\Documents\Passwords Database\ ;
- pour Microsoft Windows 7: C:\Users\User_name\My Documents\Passwords Database\.

Votre base de mots de passe peut être stockée sur plusieurs supports différents: disque amovible, disque local ou disque réseau.

Lors de la modification du chemin d'accès à la base de mots de passe ou du nom de celle-ci, plusieurs actions sont possibles:

- **Copier** : une copie de la base de mots de passe est créée à l'emplacement indiqué. Cette copie devient la base de mots de passe active.
- **Replacer** : la base de mots de passe active est sauvegardée à l'emplacement indiqué.

- **Créer une base de mots de passe** : une copie vide de la base de mots de passe est créée, laquelle devient la base active.

Pour déplacer la base de mots de passe et modifier son nom, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre, sélectionnez la section **Mes mots de passe**.
5. Dans la partie droite de la fenêtre, dans le groupe **Source**, cliquez sur le bouton situé à droite du champ **Chemin**.
6. Dans la fenêtre **Sélection de la base de mots de passe**, spécifiez le chemin du fichier ainsi que son nom et cliquez ensuite sur le bouton **Ouvrir**.
7. Dans la fenêtre **Emplacement des bases de mots de passe** qui s'ouvre, sélectionnez l'action requise à exécuter sur la base de mots de passe.
8. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, sélectionnez le mot de passe principal pour la confirmation des modifications.

Pour modifier la base de mots passe active, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre, sélectionnez la section **Mes mots de passe**.
5. Dans la partie droite de la fenêtre, dans le groupe **Source**, cliquez sur le bouton situé à droite du champ **Chemin**.
6. Dans la fenêtre **Sélection de base des mots de passe** sur le bouton **Ouvrir**.
7. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, saisissez le mot de passe principal pour accéder à la base de mots de passe sélectionnée.

CREATION D'UNE NOUVELLE BASE DE MOTS DE PASSE

Mon Gestionnaire de mots de passe permet de travailler avec plusieurs bases de mots de passe. La création d'une nouvelle base de mots de passe permet de séparer vos données personnelles en les répartissant dans deux ou plusieurs bases. Si nécessaire, il est possible de restaurer une ancienne base de mots de passe. Mon Gestionnaire de mots de passe vous propose de créer une base de mots de passe lorsque la base actuelle est endommagée ou qu'une copie de sauvegarde ne peut être restaurée.

Pour créer une nouvelle base de mots passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre, sélectionnez la section **Mes mots de passe**.

5. Dans la partie droite de la fenêtre, dans le groupe **Source**, cliquez sur le bouton situé à droite du champ **Chemin**.

6. Dans la fenêtre **Sélection de la base de mots de passe**, définissez l'emplacement et le nom du fichier de la base de mots de passe et cliquez ensuite sur le bouton **Ouvrir**.

7. Dans la fenêtre **Emplacement des bases de mots de passe** qui s'ouvre, choisissez l'action **Créer une base de mots de passe**.

8. Dans le groupe **Mot de passe** de la fenêtre **Nouvelle base de mots de passe**, spécifiez le mot de passe permettant d'accéder à la nouvelle base et confirmez celui-ci dans le champ **Confirmation du mot de passe**.

   Si le mot de passe introduit ne correspond pas au mot de passe de confirmation, ce dernier apparaîtra en rouge.

   Dans le groupe **Cryptage**, sélectionnez le fournisseur de services cryptographiques ainsi que le mode de cryptage souhaité (cf. page 219).

9. Dans la boîte de dialogue, introduisez le nouveau Mot de passe principal afin de confirmer la création de la nouvelle base de mots de passe.

EMPLACEMENT DE LA COPIE DE SAUVEGARDE

Avant d'enregistrer les modifications apportées à vos données personnelles, Mon Gestionnaire de mots de passe effectue automatiquement une copie de sauvegarde de la base de mots de passe. Cela permet de prévenir les pertes de données en cas de problèmes système ou techniques. Mon Gestionnaire de mots de passe effectue une copie complète de la base de mots de passe juste avant l'introduction des modifications les plus récentes. Si la base de mots de passe est endommagée, vous avez la possibilité de restaurer les données de la dernière copie de sauvegarde (cf. page 210).

La copie de sauvegarde de votre base de mots de passe peut être stockée sur un disque local, un disque amovible ou un disque réseau.

L'emplacement par défaut de la copie de sauvegarde est le suivant (dépend du système d'exploitation):

- Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Passwords Database\ ;
- Microsoft Windows Vista: C:\Users\User_name\Documents\Passwords Database\ ;
- Microsoft Windows 7: C:\Users\User_name\My Documents\Passwords Database\.

Pour modifier l'emplacement de la copie de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre, sélectionnez la section **Mes mots de passe**.
5. Dans la partie droite de la fenêtre, dans le groupe **Mes Sauvegardes**, cliquez sur le bouton situé à droite du champ **Chemin**.
6. Dans la boîte de dialogue **Parcourir**, sélectionnez le dossier de sauvegarde de la copie de sauvegarde de la base de mots de passe.

SELECTION DU MODE DE CRYPTAGE

But de la cryptographie – protéger vos informations de l'accès et de la diffusion non autorisés. Principale fonction du cryptage – brouiller la communication sur les canaux non protégés.

Les fonctions de cryptage et décryptage nécessitent des clés. Clé – paramètre indispensable pour le cryptage. Lorsque les fonctions de cryptage et décryptage mettent en œuvre une clé unique, l'algorithme est dit symétrique. Lorsqu'elles utilisent deux clés, on parle d'algorithme asymétrique. Le cryptage symétrique peut à son tour être par bloc ou par flot. Toute information (quel que soit le format des données originales) est interprétée en code binaire. Le cryptage par bloc part du principe que les données sont scindées en blocs et que chaque bloc est ensuite transformé de manière indépendante. Avec le cryptage par flot, l'algorithme de transformation s'applique à chaque bit d'information.

Mon Gestionnaire de mots de passe utilise les algorithmes symétriques de cryptage suivants :

- **DES**. Cryptage par bloc avec clé standard de 56 bits. Comparativement aux standards actuels, le DES n'offre pas un niveau de sécurité élevé. Cet algorithme s'utilise lorsque la fiabilité ne constitue pas l'exigence principale.
- **3DES**. Algorithme par bloc se basant sur le DES Cette version résout le principal défaut de l'algorithme précédent – la clé de petite taille. La clé du 3DES est trois fois plus grande que celle du DES (56*3=168 bits). Sa vitesse d'exécution est trois fois moins importante que celle du DES mais la sécurité est considérablement plus élevée. Le 3DES est plus fréquent que le DES car ce dernier n'est plus suffisamment complexe face aux technologies actuelles de piratage.
- **3DES TWO KEY**. Algorithme par bloc se basant sur le DES Algorithme 3DES avec clé de 112 bits (56*2).
- **RC2**. Algorithme de cryptage par bloc avec longueur de clé variable capable de traiter rapidement un grand volume d'informations. Algorithme plus rapide que le DES. Il équivaut au 3DES en termes de fiabilité et de résistance.
- **RC4**. Cryptage par flot avec longueur de clé variable. Celle-ci peut être comprise entre 40 et 256 bits. Avantages de cet algorithme – vitesse de traitements élevés et longueur de clé variable. Le gestionnaire de paroles utilise par défaut RC4 pour le Mes Coffres-forts.
- **AES**. Algorithme symétrique à cryptage par bloc et clés de 128, 192 et 256 bits. Cet algorithme garantit un niveau de sécurité élevé et fait partie des algorithmes les plus répandus.

Sous Microsoft Windows, les opérations de cryptographie sont effectuées au moyen de fournisseurs de services cryptographiques. Chaque fournisseur supporte plusieurs algorithmes de cryptage avec une longueur de clé déterminée. Mon Gestionnaire de mots de passe utilise les fournisseurs de cryptage suivants intégrés à Microsoft Windows :

- Microsoft Base Cryptographic Provider ;
- Microsoft Enhanced Cryptographic Provider ;
- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype) ;
- Microsoft RSA/Schannel Cryptographic Provider ;
- Microsoft Strong Cryptographic Provider.

Pour modifier l'algorithme de cryptage, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre, sélectionnez la section **Mes mots de passe**.
5. Dans la partie droite de la fenêtre, dans le groupe **Chiffrement**, cliquez sur **Modifier**.

6. Dans la boîte de dialogue **Algorithme de cryptage**, spécifiez les paramètres de cryptage.

VERROUILLAGE AUTOMATIQUE LA BASE DE MOTS DE PASSE

Mon Gestionnaire de mots de passe verrouille automatiquement la base de mots de passe après le lancement de l'application ainsi qu'après une durée déterminée d'inactivité de l'ordinateur. Vous pouvez déterminer vous-même la durée après laquelle se verrouille la base de mots de passe. Elle peut être comprise entre 1 et 60 minutes. Il est recommandé de verrouiller la base de mots de passe après 5-20 minutes d'inactivité de l'ordinateur. Vous pouvez également désactiver verrouillage automatique de la base de mots de passe.

Mon Gestionnaire de mots de passe verrouille automatiquement la base des mots de passe après une durée d'inactivité déterminée de l'ordinateur. Si vous désactivez le verrouillage automatique de l'ordinateur, vos données personnelles ne seront pas protégées dans le cas où vous vous absenteriez de l'ordinateur sans verrouillage manuel préalable.

Pour modifier la durée après laquelle se verrouille la base de mots de passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre, sélectionnez la section **Mes mots de passe**.
5. Dans la partie droite de la fenêtre, dans le groupe **Verrouillage automatique**, sélectionnez dans la liste déroulante la durée d'inactivité de l'ordinateur après laquelle base de mots de passe sera verrouillée.

   Pour désactiver le verrouillage de la base de mots de passe, sélectionnez la valeur **Jamais**.

MODIFICATION DU MODE D'AUTHENTIFICATION DE MON GESTIONNAIRE DE MOTS DE PASSE

L'authentification permet de contrôler l'accès à vos données personnelles. Le mode d'autorisation est sélectionné à la première exécution de Mon Gestionnaire de mots de passe. Ceci étant dit, le mode d'autorisation peut être modifié le cas échéant.

Pour modifier le mode d'authentification, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre sélectionnez la section **Mode d'autorisation**.
5. Dans la partie droite de la fenêtre, dans le groupe **Mode d'authentification**, sélectionnez l'une des options d'authentification depuis le menu déroulant.

VOIR EGALEMENT :

Autorisation à l'aide d'un périphérique USB ou Bluetooth 221

AUTORISATION A L'AIDE D'UN PERIPHERIQUE USB OU BLUETOOTH

Pour accéder à la base de mots de passe (cf. page 220), Mon Gestionnaire de mots de passe permet d'utiliser divers périphériques USB et Bluetooth.

Afin de pouvoir utiliser un périphérique USB pour accéder à la base de mots de passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre sélectionnez la section **Mode d'autorisation**.
5. Dans la partie droite de la fenêtre, dans le groupe **Mode d'authentification**, sélectionnez la valeur **Périphérique USB** depuis le menu déroulant.
6. Connectez le périphérique portable à l'ordinateur.
7. Sélectionnez un périphérique dans la liste **Périphériques à disque** et cliquez sur le bouton **Installer**.
   L'icône apparaît en regard du périphérique sélectionné. Si le périphérique connecté n'est pas affiché dans la liste, cochez la case **Afficher tous les périphériques**. Si nécessaire, vous pouvez modifier le périphérique d'authentification en cliquant sur le bouton **Réinitialiser**.

Pour utiliser un périphérique Bluetooth pour accéder à la base de mots de passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre sélectionnez la section **Mode d'autorisation**.
5. Dans la partie droite de la fenêtre, dans le groupe **Mode d'authentification**, sélectionnez la valeur **Périphérique Bluetooth** depuis le menu déroulant.
6. Activez la fonction Bluetooth sur votre ordinateur et ensuite sur votre périphérique.
7. Sélectionnez un périphérique dans la liste **Téléphones et modems** et cliquez sur le bouton **Installer**.
   L'icône apparaît en regard du périphérique sélectionné. Si nécessaire, il est possible de modifier le périphérique d'authentification en cliquant sur le bouton **Réinitialiser**.

MODIFICATION DU MOT DE PASSE PRINCIPAL

Par défaut, le mot de passe principal est créé au premier lancement de Mon Gestionnaire de mots de passe. Il est toutefois possible de le modifier ultérieurement.

Lors de la modification du mot de passe principal, Mon Gestionnaire de mots de passe exige une confirmation du mot de passe saisi (double introduction). Il est impossible d'enregistrer le nouveau mot de passe sans cette confirmation. Si le mot de passe introduit ne correspond pas au mot de passe de confirmation, ce dernier apparaîtra en rouge. Avant de mémoriser le nouveau mot de passe, un message d'avertissement est affiché.

Pour modifier le Mot de passe principal, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre sélectionnez la section **Mode d'autorisation**.
5. Dans la partie droite de la fenêtre, dans le groupe **Protection par mot de passe**, cliquez sur **Modifier**.
6. Dans la fenêtre **Protection par mot de passe** qui s'ouvre, saisissez le nouveau mot de passe dans les champs **Mot de passe** et **Confirmation du mot de passe**.

NAVIGATEURS COMPATIBLES

Pour garantir le bon fonctionnement de l'activation automatique du compte utilisateur et du bouton de lancement rapide (cf. page 223) Mon Gestionnaire de mots de passe requiert l'installation d'extensions complémentaires (modules externes) pour certains navigateurs Internet. Par défaut, l'installation des extensions a lieu lors de la première exécution de Mon Gestionnaire de mots de passe. Vous pouvez également installer le module externe requis.

Mon Gestionnaire de mots de passe contient une liste de navigateurs et de clients de messagerie possédant chacun l'état **Installé** / **Non installé**, selon que le module externe est installé ou non pour celui-ci.

Avant d'installer des modules externes pour une application en particulier, il est conseillé de quitter celle-ci.

Pour installer un module externe pour un navigateur ou un client de messagerie, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre sélectionnez la rubrique **Navigateurs pris en charge**.
5. Dans la partie droite de la fenêtre, sélectionnez l'application dans la liste **Navigateurs pris en charge et extensions disponibles**, puis cliquez sur le bouton **Installer**.
6. Suivez les instructions de l'**Assistant d'installation**. Lorsque le module externe sera installé, le nom de l'application sera automatiquement repris dans le groupe **Installés**. Elle reçoit alors l'état **Installé**. Vous pouvez désinstaller une extension en cliquant sur le bouton **Supprimer**.

ADMINISTRATION DES MODELES DES NOTES PERSONNELLES

Vous pouvez modifier les modèles de notes personnelles (cf. page 206) proposés, créer des modèles, voire utiliser une note existante en guise de modèle.

Pour modifier un modèle proposé de note personnelle, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Administration des modèles**.
5. Dans la partie droite de la fenêtre, sélectionnez le modèle, puis cliquez sur **Modifier**.
6. Introduisez les modifications requises dans l'éditeur de texte.

Pour créer un modèle de note personnelle, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Administration des modèles**.
5. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ajouter**.
6. Dans le champ **Nom** de la fenêtre qui s'ouvre, introduisez le nom de la nouvelle note personnelle.
7. Saisissez les informations requises dans l'éditeur de texte.

Pour utiliser une note personnelle existante en guise de modèle, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre **Mon Gestionnaire de mots de passe** qui s'ouvre, cliquez sur le bouton **Base de mots de passe**.
4. Dans la fenêtre qui s'ouvre, sélectionnez la note personnelle requise dans la liste et dans la partie supérieure de la fenêtre, cliquez sur le bouton **Modifier**.
5. Dans la partie inférieure de la fenêtre qui s'ouvre, cliquez sur le bouton **Enregistrer en tant que modèle**.
6. Dans le champ **Nom** de la fenêtre qui s'ouvre, introduisez le nom de la nouvelle note personnelle.

AFFICHAGE DU BOUTON D'ACCES RAPIDE

Si le programme que vous utilisez intègre le menu d'autres applications que Mon Gestionnaire de mots de passe, vous avez la possibilité de spécifier la position du bouton d'accès rapide par rapport aux autres boutons. Par ailleurs, il est possible de définir manuellement la liste des navigateurs Internet devant intégrer le Bouton d'accès rapide (cf. page 53).

Pour modifier les paramètres du Bouton d'accès rapide, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Bouton de lancement rapide**.
5. Dans la partie droite de la fenêtre, dans le groupe **Affichage du Bouton d'accès rapide**, configurez les paramètres requis en fonction de la tâche à effectuer:
   - Pour modifier l'emplacement du bouton d'accès rapide, saisissez le numéro de position du bouton (combien de boutons à droite avant le bouton d'accès rapide) dans le champ **Déplacer le bouton à gauche** ;
   - Pour que le bouton d'accès rapide n'apparaisse pas quand la base de mots de passe est verrouillée, cochez la case **Masquer le bouton d'accès rapide si le Gestionnaire de mots de passe est verrouillé** ;
   - Pour établir la liste des navigateurs Internet dans lesquels le Bouton d'accès rapide doit apparaître, cochez dans la liste du groupe **Afficher le Bouton d'accès rapide dans les navigateurs Internet suivants** la case en regard des navigateurs Internet concernés.

DEFINIR LA DUREE DE CONSERVATION D'UN MOT DE PASSE DANS LE PRESSE-PAPIERS

Mon Gestionnaire de mots de passe vous permet de copier un mot de passe dans le Presse-papiers pour un laps de temps déterminé. Cela peut s'avérer intéressant lorsque le mot de passe ne doit être exploité que pour une courte durée (par exemple lors de l'enregistrement sur un site Web / dans un programme). Vous pouvez spécifier la durée de conservation du mot de passe dans le Presse-papiers. Une fois ce temps écoulé, le mot de passe est automatiquement supprimé du Presse-papiers. Cela permet d'éviter l'interception et le vol du mot de passe puisque celui-ci ne peut plus être récupéré dans le Presse-papiers après la durée définie.

Pour modifier la durée de conservation du mot de passe dans le Presse-papiers, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre sélectionnez la section **Général**.
5. Dans la partie droite de la fenêtre, dans le groupe **Presse-papiers**, spécifiez-la durée en secondes.

NOTIFICATIONS

Pendant le fonctionnement de Mon Gestionnaire de mots de passe, divers types d'événement à caractère généralement informatif sont générés. Pour être informé de ces événements, utilisez le service de notification. Les utilisateurs sont notifiés par le biais d'avertissements et de messages contextuels.

Le programme prévoit les types de notification suivants :

- **Lancement de l'application**. Ce message apparaît lorsque le programme est lancé et que la base de mots de passe est déverrouillée.
- **Activation du compte**. Ce message apparaît lorsque le Compte est activé.
- **Purge du Presse-papiers**. Mon Gestionnaire de mots de passe permet de conserver temporairement le mot de passe dans le Presse-papiers. Cela peut s'avérer utile lorsque des données doivent être copiées d'un champ à un autre. A la fin de la période définie (cf. page 224), le mot de passe sera supprimé du Presse-papiers.
- **Verrouillage automatique de Mon Gestionnaire de mots de passe**. Le message apparaît lorsque Mon Gestionnaire de mots de passe verrouille automatiquement la base de mots de passe. Par défaut, la base de mots de passe est automatiquement verrouillée au démarrage du système d'exploitation ainsi qu'après une durée définie (cf. page 220) d'inactivité de l'ordinateur.
- **Exportation de données dans un fichier non protégé**. Message d'avertissement spécifiant que la fonction d'exportation sauvegardera vos mots de passe dans un fichier non crypté et qu'ils seront par conséquent accessibles par n'importe quel utilisateur travaillant sur votre ordinateur. Nous vous recommandons de réfléchir à la manière de protéger le fichier contenant les mots de passe avant de procéder à l'exportation des données.
- **Modification avancée**. Avant de modifier la configuration de champs complémentaires, le programme demande l'authentification d'utiliser le navigateur Internet par défaut. Ce message vous avertit que des images et fichiers système (cookies) seront sauvegardés sur votre ordinateur.
- **Problèmes lors du remplissage automatique de l'Identifiant pour le Compte**. Ce message vous avertit que les données n'ont pu être automatiquement complétées lors de l'authentification.

Pour recevoir les notifications, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre sélectionnez la section **Général**.
5. Dans la partie droite de la fenêtre, dans le groupe **Général**, cliquez sur le bouton **Notifications...**.
6. Dans la boîte de dialogue, cochez / décochez la case en regard des types de notification souhaités.

FONCTION D'ACTIVATION PAR DOUBLE-CLIQUE

Mon Gestionnaire de mots de passe permet de sélectionner l'action exécutée après le double-clique sur l'icône de l'application dans la zone de notification de la barre des tâches de Microsoft Windows (cf. page 51). Vous avez le choix entre les options suivantes :

- ouvrir la fenêtre principale de Mon Gestionnaire de mots de passe (cf. page 50) ;
- bloquer/débloquer Mon Gestionnaire de mots de passe (action définie par défaut).

Pour modifier la tâche à lancer lors d'un double-clique sur l'icône de l'application situé dans la zone de notification de la barre des tâches, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres**.
4. Dans la partie gauche de la fenêtre sélectionnez la section **Général**.
5. Dans la partie droite de la fenêtre, sélectionnez l'action à exécuter dans le menu déroulant **Double-clique sur l'icône**.

CREATION DE MOTS DE PASSE FIABLES

La sécurité des données dépendent directement de la fiabilité des mots de passe. Les données sont sujettes à un risque dans les cas suivants :

- utilisation d'un mot de passe unique pour tous les comptes ;
- mot de passe simpliste ;
- mot de passe composé à partir de données faciles à deviner (par exemple, nom d'un membre de la famille ou date de naissance).

Pour garantir la sécurité des données, Mon Gestionnaire de mots de passe permet de créer des mots de passe uniques et robustes pour les comptes utilisateur à l'aide du générateur de mots de passe.

Un mot de passe est considéré comme complexe lorsqu'il se compose de plus de quatre caractères et qu'il mélange des caractères spéciaux, des chiffres, des lettres majuscules et des lettres minuscules.

Les paramètres suivants déterminent la fiabilité d'un mot de passe :

- **Longueur** – nombre de caractères composant le mot de passe. Elle peut être comprise entre 4 et 99 caractères. On considère que plus le mot de passe est long, plus il est complexe.
- **A-Z** – utilisation de lettres majuscules.
- **A-Z** – utilisation de lettres majuscules.

- **0-9** – utilisation de chiffres.
- **Caractères spéciaux** – utilisation de caractères spéciaux.
- **Ne pas utiliser deux fois le même caractère** – défense d'utiliser des caractères identiques dans le mot de passe.

Pour créer un mot de passe robuste à l'aide du générateur de mots de passe, procédez comme suit :

1. Ouvrez le menu contextuel de Mon Gestionnaire de mots de passe et sélectionnez l'option **Générateur de mots de passe**.
2. Dans le champ **Longueur du mot de passe** de la fenêtre **Générateur de mots de passe**, spécifiez le nombre de caractères devant composer le mot de passe.
3. Si vous le souhaitez, vous pouvez configurer les paramètres avancés du générateur de mots de passe. Pour ce faire, cochez / décochez la case en regard des paramètres à modifier dans le groupe **Paramètres avancés**.
4. Cliquez sur le bouton **Générer**. Le mot de passe généré s'affiche dans le champ **Mot de passe**. Pour visualiser le mot de passe créé, cochez la case **Afficher le mot de passe**.
5. Copiez le mot de passe dans le Presse-papiers à l'aide du bouton , puis collez le mot de passe dans le champ de saisie dans l'application/sur la page Web à l'aide de la combinaison de touches **CTRL+V**. Le mot de passe créé est conservé dans le Presse-papiers.
6. Afin de conserver les paramètres utilisés pour la fois suivante, cochez la case **Par défaut**.

UTILISATION D'UNE VERSION PORTABLE DE MON GESTIONNAIRE DE MOTS DE PASSE

Mon Gestionnaire de mots de passe permet de sauvegarder tous vos mots de passe sur un support amovible (par exemple une unité de mémoire flash ou un téléphone portable si celui-ci peut être utilisé comme unité de mémoire flash). Pour ce faire, il faut créer une version portable de Mon Gestionnaire de mots de passe sur le disque amovible. La version portable de l'application est créée sur votre ordinateur où est installée la version complète de Mon Gestionnaire de mots de passe. La version portable de l'application possède toutes les fonctionnalités de Mon Gestionnaire de mots de passe.

La version portable permet d'utiliser Mon Gestionnaire de mots de passe sur un ordinateur public (par exemple, dans un cybercafé) qui n'est pas équipé de l'application. Mon Gestionnaire de mots de passe sera lancé automatiquement à la connexion du disque amovible. Dès que le support amovible est déconnecté, Mon Gestionnaire de mots de passe se ferme automatiquement en ne laissant aucune trace de vos données sur l'ordinateur public.

De plus, la version portable permet de synchroniser les bases de mots de passe quand Mon Gestionnaire de Mots de passe est installé et utilisé en parallèle sur différents ordinateurs (par exemple, l'ordinateur au bureau et celui à la maison).

DANS CETTE SECTION

Création et connexion de la version portable 227

Synchronisation de la base de mots de passe 228

CREATION ET CONNEXION DE LA VERSION PORTABLE

Pour garantir le bon fonctionnement de la version portable de Mon Gestionnaire de mots de passe sur un ordinateur partagé, il est conseillé d'installé des plug-ins complémentaires pour le navigateur.

Il est possible d'installer le module externe de plusieurs manières :

- Depuis l'assistant d'installation du module externe. Pour ce faire, suivez les étapes de l'Assistant d'installation du module externe qui se lance lors du premier démarrage de la version portable de Mon Gestionnaire de mots de passe.

- Depuis le menu du Bouton d'accès rapide situé dans la fenêtre du navigateur Internet. Pour ce faire, sélectionnez l'entrée **Module externe de remplissage automatique non installé** dans le menu du bouton d'accès rapide.

L'Assistant d'installation de la version portable de Mon Gestionnaire de mots de passe se lance automatiquement lors du premier démarrage sur l'ordinateur public. Vous avez alors la possibilité de modifier certains paramètres avancés de la version portable :

- créer sur le bureau un raccourci vers la version portable - permet de lancer ultérieurement le programme depuis le bureau de l'ordinateur en cours d'utilisation ;

- utiliser Mon Clavier virtuel – affiche un Mon Clavier virtuel pour l'introduction des données personnelles.

Pour créer la version portable de Mon Gestionnaire de mots de passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.

3. Dans la fenêtre qui s'ouvre, cliquez sur **Version portable**.

4. Dans la fenêtre qui s'ouvre, sélectionnez le périphérique sur lequel vous souhaitez installer la version portable de Mon Gestionnaire de mots de passe, puis cliquez sur **Suivant**.

5. Définissez les paramètres de la version portable dans la fenêtre qui s'ouvre :

   - Pour éviter de devoir introduire le mot de passe principal pour accéder à la version portable de Mon Gestionnaire de mots de passe, cochez la case **Ne jamais demander le Mot de passe principal**.

   - Pour configurer l'exécution automatique de la version portable lors de la connexion du disque amovible à l'ordinateur, cochez la case **Activer le lancement automatique de Mon Gestionnaire de mots de passe depuis le disque amovible**.

6. Cliquez sur **Exécuter**. Une fois l'installation achevée, cliquez sur le bouton **Terminer**.

Pour utiliser la version portable de l'application, procédez comme suit :

1. Connectez le périphérique amovible à l'ordinateur.

2. Lancez la version portable de Mon Gestionnaire de mots de passe depuis le disque amovible sélectionné si le lancement automatique n'a pas eu lieu.

3. Lors du premier lancement de la version portable, vous serez invité à installer les plug-ins de remplissage automatique et à désactiver les gestionnaires de mots de passe intégrés aux navigateurs installés.

4. Introduisez le Mot de passe principal dans la boîte de dialogue.

   La version portable de Mon Gestionnaire de mots de passe est prête à l'emploi.

SYNCHRONISATION DE LA BASE DE MOTS DE PASSE

Si vous utilisez Mon Gestionnaire de mots de passe sur plusieurs ordinateurs, il est nécessaire de maintenir l'actualité de toutes les bases de mots de passe. Grâce à la version portable de l'application, vous pourrez synchroniser les données et utiliser la base actuelle de mots de passe sur tous les ordinateurs où Mon Gestionnaire de mots de passe est installé. Pour ce faire, synchroniser la base de mots de passe de la version portable avec la base de mots de passe sur un des ordinateurs, puis reproduisez la synchronisation sur un autre ordinateur.

Pour synchroniser la base de mots de passe de la version portable avec la base de mots de passe sur un des ordinateurs, procédez comme suit :

1. Connectez le périphérique amovible à l'ordinateur.
2. Ouvrez la fenêtre principale de l'application.
3. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mon Gestionnaire de mots de passe**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **Version portable**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le périphérique sur lequel la version portable de Mon Gestionnaire de mots de passe est installée, puis cliquez sur le bouton **Suivant**.
6. Dans la fenêtre qui s'ouvre, sélectionnez le mode de synchronisation de la base de mots de passe.
   - Pour ajouter les données de la base de Mon Gestionnaire de mots de passe installé sur l'ordinateur à la base de mots de passe de la version portable, choisissez l'option **Fusionner les bases de mot de passe**.

     Dans ce cas, la base de Mon Gestionnaire de mots de passe installé sur l'ordinateur ne sera pas modifiée. Pour y ajouter les données fusionnées, répétez la synchronisation en choisissant l'option **Utiliser la base de mots de passe de la version portable**.
   - Pour remplacer la base de mots de passe de la version portable par la base de Mon Gestionnaire de mots de passe installée su l'ordinateur, choisissez, dans la version portable, l'option **Utilisez la base de Mon Gestionnaire de mots de passe installée sur cet ordinateur**.
   - Pour remplacer la base de Mon Gestionnaire de mots de passe installée sur l'ordinateur par la base de mots de passe de la version portable, choisissez l'option **Utiliser la base de mots de passe de la version portable**.
7. Cliquez sur **Suivant**.
8. Définissez les paramètres de la version portable dans la fenêtre qui s'ouvre :
   - Pour éviter de devoir introduire le mot de passe principal pour accéder à la version portable de Mon Gestionnaire de mots de passe, cochez la case **Ne jamais demander le Mot de passe principal**.
   - Pour configurer l'exécution automatique de la version portable lors de la connexion du disque amovible à l'ordinateur, cochez la case **Activer le lancement automatique de Mon Gestionnaire de mots de passe depuis le disque amovible**.
9. Cliquez sur **Exécuter**. Une fois la synchronisation achevée, cliquez sur le bouton **Terminer**.

PERFORMANCES ET COMPATIBILITE AVEC D'AUTRES APPLICATIONS

Dans le contexte de Kaspersky PURE, les performances désignent le spectre des menaces détectées ainsi que la consommation d'énergie et l'utilisation des ressources de l'ordinateur.

Kaspersky PURE permet de configurer avec souplesse le spectre de la protection et de sélectionner diverses catégories de menaces (cf. section "Sélection des catégories de menaces identifiées" à la page 229) que l'application découvrira durant son fonctionnement.

Dans le cadre de l'utilisation d'un ordinateur portable, la consommation en énergie des applications est un élément particulièrement important. En particulier, la recherche d'éventuels virus sur l'ordinateur et la mise à jour des bases de Kaspersky PURE requièrent des ressources importantes. Le mode spécial de fonctionnement de Kaspersky PURE sur un ordinateur portable (cf. page 231) permet de reporter automatiquement les tâches d'analyse et de mise à jour programmées lorsque l'ordinateur fonctionne sur la batterie afin d'économiser celle-ci.

L'utilisation des ressources de l'ordinateur par Kaspersky PURE peut avoir un effet sur les performances des autres applications. Pour résoudre les problèmes liés au fonctionnement simultané en cas d'augmentation de la charge du processeur et des sous-système de disque, Kaspersky PURE suspend l'exécution des tâches d'analyse et cède des ressources aux autres applications (cf. page 230) qui tournent sur l'ordinateur.

En Mode Jeux, l'affichage des notifications sur le fonctionnement de Kaspersky PURE est automatiquement désactivé quand les autres applications sont lancées en mode plein écran.

La procédure de désinfection avancée en cas d'infection active du système requiert le redémarrage de l'ordinateur, ce qui peut également avoir un effet sur le fonctionnement des autres applications. Le cas échéant, vous pouvez suspendre l'application de la technologie de réparation d'une infection active (cf. page 230) afin d'éviter le redémarrage inopportun de l'ordinateur.

DANS CETTE SECTION

Sélection des catégories de menaces identifiées 229

Technologie de réparation de l'infection active 230

Répartition des ressources de l'ordinateur pendant la recherche de virus 230

Paramètres de l'application en cas d'utilisation du mode plein écran. Mode jeux 231

Économie d'énergie en cas d'alimentation via la batterie 231

SELECTION DES CATEGORIES DE MENACES IDENTIFIEES

Les menaces qui peuvent être découvertes par Kaspersky PURE sont réparties en différentes catégories selon diverses caractéristiques. L'application détecte toujours les virus, les chevaux de Troie et les utilitaires malveillants. Il s'agit des programmes qui peuvent occasionner les dégâts les plus graves. Pour garantir une plus grande sécurité à l'ordinateur, il est possible d'élargir la liste de menaces découvertes en activant le contrôle des actions des applications légitimes qui pourraient être utilisées par un individu malintentionné pour nuire à l'ordinateur ou aux données de l'utilisateur.

Pour sélectionner les catégories de menaces à identifier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez la sous-section **Menaces et exclusions**.

4. Dans la partie droite de la fenêtre, dans le groupe **Menaces**, cliquez sur **Configuration**.

5. Dans la fenêtre **Menaces** qui s'ouvre, cochez la case en regard de la catégorie de menace qu'il faut détecter.

TECHNOLOGIE DE REPARATION DE L'INFECTION ACTIVE

Les programmes malveillants actuels peuvent s'introduire au niveau le plus bas du système d'exploitation, ce qui vous prive en pratique de la possibilité de les supprimer. En cas de découverte d'une action malveillante dans le système, Kaspersky PURE propose la réalisation d'une procédure élargie de réparation qui permet de neutraliser la menace ou de la supprimer de l'ordinateur.

L'ordinateur redémarrera à la fin de la procédure. Une fois que l'ordinateur a redémarré, il est conseillé de lancer une analyse complète (cf. section "Procédure d'exécution d'une analyse complète de l'ordinateur" à la page 67).

Pour que Kaspersky PURE applique la procédure de réparation élargie, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Compatibilité** dans la rubrique **Paramètres avancés**.

4. Dans la partie droite de la fenêtre, cochez la case **Appliquer la technologie de désinfection avancée**.

REPARTITION DES RESSOURCES DE L'ORDINATEUR PENDANT LA RECHERCHE DE VIRUS

Afin de limiter la charge appliquée au processeur central et aux sous-systèmes du disque, vous pouvez reporter les tâches liées à la recherche de virus.

L'exécution des tâches d'analyse augmente la charge du processeur central et des sous-systèmes du disque, ce qui ralentit le fonctionnement d'autres programmes. Lorsqu'une telle situation se présente, Kaspersky PURE arrête par défaut l'exécution des tâches d'analyse et libère des ressources pour les applications de l'utilisateur.

Il existe cependant toute une série de programmes qui sont lancés lors de la libération des ressources du processeur et qui travaillent en arrière-plan. Pour que l'analyse ne dépende pas du fonctionnement de tels programmes, il ne faut pas leur céder des ressources.

Remarquez que ce paramètre peut être défini individuellement pour chaque tâche d'analyse. Dans ce cas, la configuration des paramètres pour une tâche particulière a une priorité supérieure.

Pour que Kaspersky PURE reporte l'exécution des tâches d'analyse lorsque le fonctionnement des autres applications ralentit, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Compatibilité** dans la rubrique **Paramètres avancés**.

4. Dans la partie droite de la fenêtre, cochez la case **Céder les ressources aux autres applications**.

PARAMETRES DE L'APPLICATION EN CAS D'UTILISATION DU MODE PLEIN ECRAN. MODE JEUX

L'utilisation de certaines applications (principalement des jeux) en mode plein écran peut créer des problèmes avec certaines fonctionnalités de Kaspersky PURE : par exemple, les fenêtres de notification n'ont pas leur place dans ce mode. Bien souvent, ces applications requièrent également des ressources considérables du système et c'est la raison pour laquelle l'exécution de certaines tâches de Kaspersky PURE peut ralentir ces applications.

Pour ne pas devoir désactiver manuellement les notifications ou suspendre les tâches chaque fois que vous utilisez le mode plein écran, Kaspersky PURE permet de modifier temporairement les paramètres grâce au mode Jeux. Quand le Mode Jeux est utilisé, les paramètres de tous les composants sont automatiquement modifiés quand l'utilisateur passe en mode plein écran afin de garantir le fonctionnement optimal dans ce mode. Au moment de quitter le mode plein écran, les paramètres de l'application reprennent les valeurs en vigueur au moment de passer en mode plein écran.

Pour activer le mode jeu, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Paramètres généraux**, sélectionnez la sous-section **Mode Jeux**.
4. Dans la partie droite de la fenêtre, cochez la case **Utiliser le mode Jeux** et dans le groupe **Paramètres du mode** en-dessous, définissez les paramètres requis pour l'utilisation du mode Jeux.

ÉCONOMIE D'ENERGIE EN CAS D'ALIMENTATION VIA LA BATTERIE

Afin d'économiser les batteries des ordinateurs portables, vous pouvez reporter l'exécution des tâches d'analyse antivirus et de mises à jour programmées. Le cas échéant, il est possible d'actualiser Kaspersky PURE ou de lancer la recherche de virus manuellement.

Pour activer le mode d'économie d'énergie en cas d'alimentation via la batterie, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Paramètres généraux**; sélectionnez la sous-section **Economie d'énergie**.
4. Dans la partie droite de la fenêtre, cochez la case **Ne pas lancer l'analyse programmée en cas d'alimentation via les batteries**.

AUTODEFENSE DE KASPERSKY PURE

Dans la mesure où Kaspersky PURE protège les ordinateurs contre les programmes malveillants, ceux-ci tentent, une fois qu'ils se sont infiltrés dans l'ordinateur, de bloquer le fonctionnement de Kaspersky PURE, voire de supprimer l'application de l'ordinateur.

La stabilité du système de protection de l'ordinateur est garantie par des mécanismes d'autodéfense et de protection contre l'interaction à distance intégrés à Kaspersky PURE.

L'autodéfense de Kaspersky PURE empêche la modification et la suppression des fichiers de l'application sur le disque, des processus dans la mémoire et des enregistrements dans la base de registres. La protection contre l'interaction à distance permet de bloquer toutes les tentatives d'administration à distance des services de l'application.

Sous les systèmes d'exploitation 64 bits et sous Microsoft Windows Vista, seule l'administration du mécanisme d'autodéfense de Kaspersky PURE contre la modification et la suppression de ses propres fichiers sur le disque ou contre la modification ou la suppression des clés dans la base de registres est accessible.

DANS CETTE SECTION

Activation et désactivation de l'autodéfense 232

Protection contre l'administration externe 232

ACTIVATION ET DESACTIVATION DE L'AUTODEFENSE

L'autodéfense de Kaspersky PURE est activée par défaut. Le cas échéant, vous pouvez désactiver l'autodéfense.

Pour activer ou désactiver l'autodéfense de Kaspersky PURE, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Autodéfense** dans la rubrique **Paramètres généraux**.
4. Dans la partie droite de la fenêtre, décochez la case **Activer l'Autodéfense** si vous souhaitez désactiver l'autodéfense de Kaspersky PURE. Cochez cette case pour activer l'autodéfense.

PROTECTION CONTRE L'ADMINISTRATION EXTERNE

La protection contre l'administration externe est activée par défaut. Le cas échéant, vous pouvez désactiver cette protection.

Il arrive parfois que le recours à la protection contre les interventions à distance entraîne l'impossibilité d'utiliser les programmes d'administration à distance (par exemple, RemoteAdmin). Pour garantir leur fonctionnement, il faut ajouter ces applications à la liste des applications de confiance (cf. section "Composition de la liste des applications de confiance" à la page 162) et activer le paramètre **Ne pas surveiller l'activité de l'application**.

Pour désactiver la protection contre l'administration externe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Autodéfense** dans la rubrique **Paramètres généraux**.
4. Dans la partie droite de la fenêtre, dans le groupe **Administration externe**, décochez la case **Interdire l'administration externe du service système**.

APPARENCE DE L'APPLICATION

Vous pouvez modifier l'aspect de Kaspersky PURE à l'aide de skins. Il est également possible de configurer l'utilisation d'éléments actifs de l'interface (icône de l'application dans la zone de notification de la barre des tâches de Microsoft Windows et fenêtres contextuelles).

DANS CETTE SECTION

Eléments actifs de l'interface 233

Graphisme de Kaspersky PURE 233

Kiosque d'informations 234

ELEMENTS ACTIFS DE L'INTERFACE

Vous pouvez configurer l'affichage des éléments actifs de l'interface : par exemple, la fenêtre des notifications, l'icône Kaspersky PURE de la barre des tâches.

Pour configurer les éléments actifs de l'interface, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Apparence** dans la rubrique **Paramètres généraux**.
4. Dans la partie droite de la fenêtre, groupe **Icône de la barre des tâches**, cochez ou décochez les cases correspondantes.

GRAPHISME DE KASPERSKY PURE

Tous les couleurs, les caractères, les icônes et les textes utilisés dans l'interface de Kaspersky PURE peuvent être modifiés. Vous pouvez créer votre propre environnement graphique pour le logiciel et localiser l'interface de l'application dans la langue de votre choix.

Pour utilisez un autre skin, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Apparence** dans la rubrique **Paramètres généraux**.
4. Dans le groupe Skins, cochez la case **Utiliser un skin personnalisé** pour activer un skin. Dans le champ de saisie, indiquez le catalogue avec les paramètres des skins et cliquez sur le bouton **Parcourir** pour trouver ce catalogue.

KIOSQUE D'INFORMATIONS

Grâce au *kiosque d'informations*, Kaspersky Lab vous maintient au courant des événements importants qui concernent Kaspersky PURE en particulier et la protection contre les menaces informatiques en général.

L'application vous signalera l'existence de nouvelles informations par le biais d'une fenêtre contextuelle dans la zone de notification de la barre des tâches. L'aspect de l'icône de l'application changera (cf. ci-dessous).

Vous pouvez lire les nouvelles par un des moyens suivants :

- Cliquez sur l'icône dans la zone de notification de la barre des tâches ;
- Cliquez sur le lien **Lire les nouvelles** dans la fenêtre contextuelle présentant l'information.

Pour désactiver la réception des nouvelles, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Apparence** dans la rubrique **Paramètres généraux**.
4. Dans la partie droite de la fenêtre, groupe **Icône de la barre des tâches**, décochez la case **M'avertir des informations de Kaspersky Lab**.

MES OUTILS D'OPTIMISATION

Afin d'exécuter des tâches spécifiques à la protection de l'ordinateur, Kaspersky PURE propose une série d'Assistants et d'outils.

- L'Assistant de création de disque de dépannage est prévu pour la création d'un disque de dépannage qui permettra de restaurer le système après une attaque de virus en lançant le système depuis un disque amovible. Le disque de dépannage intervient dans les cas d'infection qui rendent la réparation de l'ordinateur impossible à l'aide des logiciels antivirus ou des outils de réparation.

- L'Assistant de suppression des traces d'activité est prévu pour la recherche et la suppression des traces d'activité de l'utilisateur dans le système ainsi que des paramètres du système d'exploitation qui permettent d'accumuler des données sur l'activité de l'utilisateur.

- L'Assistant de Nettoyage du disque permet de rechercher et de supprimer les fichiers temporaires et les fichiers non utilisés sur l'ordinateur et d'optimiser le fonctionnement du système.

- L'Assistant de restauration du système permet de supprimer les corruptions et les traces laissées par des objets malveillants dans le système.

- L'Assistant de Configuration du navigateur est prévu pour l'analyse et la configuration des paramètres de Microsoft Internet Explorer dans le but de supprimer les vulnérabilités potentielles.

- L'outil de suppression irréversible des données permet de supprimer les données confidentielles sans possibilité de restauration ultérieure.

Tous les problèmes découverts par les Assistants (sauf l'Assistant de création du disque de dépannage) sont regroupés en fonction du danger qu'ils représentent pour le système. Pour chaque groupe de problèmes, les experts de Kaspersky Lab proposent un ensemble d'actions dont l'exécution permettra de supprimer les vulnérabilités et les points problématiques du système. Il existe trois groupes de problèmes et par conséquent, trois groupes d'actions exécutées.

- *Les actions vivement recommandées* permettent de supprimer les problèmes qui constituent une menace sérieuse pour la sécurité. Il est conseillé d'exécuter dans les plus brefs délais toutes les actions de ce groupe pour supprimer la menace.

- *Les actions recommandées* visent à supprimer les problèmes qui peuvent présenter un danger potentiel. Il est également conseillé d'exécuter les actions de ce groupe pour garantir une protection optimale.

- *Les actions complémentaires* sont prévues pour supprimer les problèmes qui ne présentent actuellement aucun danger mais qui à l'avenir pourraient menacer la sécurité de l'ordinateur. L'exécution de ces actions garantit la protection totale de l'ordinateur mais peut, dans certains cas, entraîner la suppression de certains paramètres définis par l'utilisateur (par exemple, les cookies).

DANS CETTE SECTION

Suppression permanente des données 236

Suppression des traces d'activité 237

Nettoyage du disque 238

Configuration du navigateur 240

SUPPRESSION PERMANENTE DES DONNEES

La sécurité de vos données est garantie non seulement par la protection contre les virus, les chevaux de Troie et autres programmes malveillants, mais également par la protection contre la restauration non autorisée des informations supprimées.

La suppression des données à l'aide des méthodes Windows standard ne garantit pas une suppression fiable des informations et la possibilité de restauration demeure. Lors de la suppression, les données ne sont pas supprimées du disque dur : les secteurs du disque qu'elles occupaient sont tout simplement marqués comme libres. Seul l'enregistrement relatif au fichier dans le tableau de fichiers est supprimé. Le formatage du support (disque dur, mémoire flash ou clé USB) n'est pas non plus une garantie de la suppression définitive des données. On estime que ce n'est qu'après un écrasement répété que les données disparaissent pour toujours. Mais même dans ce cas de figure, il est toujours possible de récupérer les données à l'aide de puissants outils.

Kaspersky PURE propose un Assistant de suppression permanente des données. Cet Assistant permet de supprimer les données confidentielles tout en privant les individus mal intentionnés de la possibilité de les restaurer et de les utiliser ultérieurement. La suppression définitive des données exclut les cas qui permettent de restaurer les données à l'aide d'outils logiciels traditionnels. L'Assistant peut être utilisé aussi bien avec les objets de petite taille que de grande taille (plusieurs gigaoctets).

L'Assistant prend en charge la suppression des données des supports suivants :

- Disques locaux. La suppression est possible si l'utilisateur possède les privilèges d'écriture et de suppression des informations.

- Disques amovibles ou autres périphériques identifiés comme disque amovible (par exemple, disquettes, cartes Flash, cartes USB ou téléphones mobiles). La suppression des données sur une carte Flash est possible si le mode de protection mécanique contre l'écriture n'est pas activé (mode Lock).

Avant de lancer la procédure de suppression définitive des données, l'application vérifie s'il est possible de supprimer les données du support. La procédure de suppression sera exécutée uniquement si la suppression des données est prise en charge par l support sélectionné. Dans le cas contraire, la suppression définitive des données ne sera pas possible.

Vous pouvez supprimer uniquement les données auxquelles vous avez accès sous votre compte utilisateur. Avant de supprimer les données, assurez-vous que le fichier ou le dossier n'est pas ouvert et qu'il n'est pas utilisé par d'autres applications.

Il est possible de supprimer un fichier ou un dossier. Pour éviter la suppression accidentelle de fichiers nécessaires en une seule fois, vous ne pouvez supprimer qu'un objet (sachez toutefois que le dossier sélectionné pour la suppression peut contenir plusieurs fichiers ou sous-dossiers).

Le dossier sélectionné pour la suppression peut contenir des fichiers système dont la disparition pourrait entraîner des problèmes pour le système. Si des fichiers et des dossiers système figurent parmi les données sélectionnées, l'Assistant demandera à l'utilisateur de confirmer la suppression.

Les méthodes de suppression définitive des données personnelles sont normalisées. Elles reposent toutes sur l'écrasement répétés des informations supprimées par des unités et des zéros ou des caractères aléatoires. La vitesse et la qualité de la suppression des données varient en fonction du nombre de cycles.

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

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mes outils d'optimisation**.

3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Suppression permanente des données**.

4. Dans la fenêtre **Suppression permanente des données** qui s'ouvre, sélectionnez l'objet à l'aide du bouton **Parcourir** puis, dans la fenêtre **Sélection du répertoire** qui s'ouvre, sélectionnez l'objet à supprimer.

   Dans la liste déroulante **Méthode de suppression des données**, sélectionnez l'algorithme requis de suppression des données.

5. Dans la boîte de dialogue qui s'affiche, confirmez la suppression des données à l'aide du bouton **OK**. Si certains fichiers n'ont pas été supprimés, répétez l'opération en cliquant sur le bouton **Réessayer** dans la fenêtre qui s'ouvre. Pour sélectionner un autre objet à supprimer, cliquez sur le bouton **Terminer**.

SUPPRESSION DES TRACES D'ACTIVITE

Lorsque vous utilisez votre ordinateur, vos activités sont enregistrées dans le système. Les données relatives aux recherches lancées par l'utilisateur et aux sites visités sont conservées, tout comme les données relatives à l'exécution d'applications et à l'ouverture et à l'enregistrement de fichiers, les entrées du journal système Microsoft Windows, les fichiers temporaires et bien d'autres encore.

Toutes ces sources d'informations sur l'activité de l'utilisateur peuvent contenir des données confidentielles (y compris des mots de passe) que les individus malintentionnés pourraient analyser. Bien souvent, l'utilisateur ne possède pas les connaissances suffisantes pour empêcher le vol d'informations depuis ces sources.

Kaspersky PURE propose un Assistant de suppression des traces d'activité. Cet Assistant recherche les traces d'activité de l'utilisateur dans le système ainsi que les paramètres du système d'exploitation qui permettent de récolter des informations sur cette activité.

Il ne faut pas oublier que des informations sur l'activité de l'utilisateur dans le système sont accumulées sans cesse. L'exécution du moindre fichier ou l'ouverture de n'importe quel document est enregistrée dans l'historique et le journal de Microsoft Windows enregistre une multitude d'événements qui surviennent dans le système. Ceci veut dire qu'une nouvelle exécution de l'Assistant de suppression des traces d'activité peut découvrir des traces supprimées lors de l'exécution antérieure de l'Assistant. Certains fichiers, par exemple le fichier de rapport de Microsoft Windows, peuvent être utilisés par le système au moment où les traces sont supprimées par l'Assistant. Afin de pouvoir supprimer ces fichiers, l'Assistant propose de redémarrer le système. Toutefois, ces fichiers peuvent être recréés lors du redémarrage, ce qui signifie qu'ils seront à nouveau découverts en tant que trace d'activité

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

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mes outils d'optimisation**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Suppression des traces d'activité**.

Examinons en détails les étapes de l'Assistant.

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

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

Etape 2. Recherche de traces d'activité

L'Assistant recherche les traces d'activité sur votre ordinateur. La recherche peut durer un certain temps. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

Etape 3. Sélection des actions pour la suppression des traces d'activité

A la fin de la recherche, l'Assistant indique les traces d'activité trouvées et les moyens proposés pour s'en débarrasser. Le rapport sur le fonctionnement de l'Assistant est présenté sous forme de la liste (cf. section "Outils d'optimisation" à la page 235).

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

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

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

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

Etape 4. Suppression des traces d'activité

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

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

Etape 5. Fin de l'Assistant

Si vous souhaitez que la suppression des traces d'activité soit réalisée automatiquement à l'avenir au moment de quitter Kaspersky PURE, cochez la case **Supprimer les traces d'activité à chaque arrêt de Kaspersky PURE à la dernière étape de l'Assistant**. Si vous avez l'intention de supprimer vous-même les traces d'activité à l'aide de l'Assistant, sans cochez cette case.

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

NETTOYAGE DU DISQUE

Au fil du temps, des fichiers inutilisés s'accumulent dans le système d'exploitation et nuisent aux performances de celui-ci. Ces fichiers peuvent occuper beaucoup de place dans la mémoire et ils peuvent également être utilisés par des programmes malveillants.

Les fichiers temporaires sont créés au lancement de n'importe quel système d'exploitation ou application. Une fois l'application fermée, tous ces fichiers ne sont pas automatiquement supprimés.

Les fichiers suivants appartiennent aux informations non utilisées :

- journaux d'événement du système où sont consignés les noms de toutes les applications ouvertes ;
- journaux d'événements de différentes applications (par exemple, Microsoft Office, Microsoft Visio, Macromedia Flash Player) ou d'utilitaires de mise à jour (par exemple Windows Updater, Adobe Updater) ;
- journaux des connexions système ;
- fichiers temporaires des navigateurs Internet (cookies) ;
- fichiers temporaires qui restent après l'installation ou la suppression d'applications ;
- le contenu de la corbeille ;
- les fichiers du dossier TEMP dont la taille peut quelque fois atteindre plusieurs gigaoctets.

Kaspersky PURE contient un assistant de suppression des informations non utilisées. La tâche de l'Assistant est de contribuer à l'optimisation du système. Outre la suppression des fichiers inutiles dans le système, l'Assistant nettoie les fichiers qui pourraient contenir des données confidentielles (mots de passe, noms d'utilisateur et informations dans les formulaires). Ceci étant dit, pour une suppression complète de ces données, il est conseillé d'utiliser l'Assistant de suppression des traces d'activité (cf. page 237)

Au moment de la purge du système, certains fichiers (par exemple, fichier journal de Microsoft Windows, journal des événements de Microsoft Office) peuvent être utilisés par le système. Afin de pouvoir supprimer ces fichiers, l'Assistant propose de redémarrer le système.

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

Pour lancer l'Assistant de Nettoyage du disque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mes outils d'optimisation**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Suppression des données non utilisées**.

Examinons en détails les étapes de l'Assistant.

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

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

Etape 2. Recherche des informations inutiles

L'Assistant recherche les fichiers temporaires et les fichiers non utilisés 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 fichiers non utilisés

À la fin de la recherche, l'Assistant signale les fichiers non utilisés découverts et les actions proposées pour les supprimer. Le rapport sur le fonctionnement de l'Assistant est présenté sous forme de la liste (cf. section "Outils d'optimisation" à la page 235).

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

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

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

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

Etape 4. Nettoyage du disque

L'Assistant exécute les actions sélectionnées à l'étape précédente. La suppression des informations non utilisées peut durer un certain temps. La suppression de certains fichiers nécessitera peut-être le redémarrage de l'ordinateur. L'Assistant vous préviendra.

Une fois la suppression de ces fichiers terminée, l'Assistant passera automatiquement à l'étape suivante.

Etape 5. Fin de l'Assistant

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

CONFIGURATION DU NAVIGATEUR

Dans certains cas, le navigateur Microsoft Internet Explorer requiert une analyse et une configuration spéciales des paramètres car certaines valeurs, définies par les utilisateurs ou présentes par défaut peuvent entraîner des problèmes au niveau de la sécurité.

Voici quelques exemples d'objets et de paramètres utilisés par le navigateur et qui constituent une menace potentielle pour la sécurité.

- **Cache de fonctionnement de Microsoft Internet Explorer**. Le cache conserve les données téléchargées depuis Internet, ce qui permet de ne pas les télécharger de nouveaux par la suite. Ceci diminue le temps de téléchargement des pages web et diminue le trafic Internet. Par ailleurs, le cache contient les données confidentielles et offre la possibilité de connaître les ressources visitées par l'utilisateur. Nombreux sont les objets malveillants qui, lors du balayage du disque, balaient également le cache, ce qui signifie que les individus malintentionnés peuvent obtenir, par exemple, les adresses de messagerie des utilisateurs. Pour augmenter la protection, il est recommandé de purger le cache après la fin du fonctionnement du navigateur.

- **Affichage de l'extension pour les fichiers de format connu**. Pour faciliter la modification des noms des fichiers, il est possible de ne pas afficher leurs extensions. Cependant, il est utile par fois pour l'utilisateur de voir l'extension réelle du fichier. Les noms de fichier de nombreux objets malveillants utilisent des combinaisons de caractères qui imitent une extension supplémentaire avant l'extension réelle (par exemple, exemple.txt.com). Si l'extension réelle du fichier n'est pas affichée, l'utilisateur voit uniquement la partie du fichier avec l'imitation de l'extension et peut considérer l'objet malveillant comme un objet ne présentant aucun danger. Pour augmenter la protection, il est recommandé d'activer l'affichage des extensions pour les fichiers de formats connus.

- **Liste des sites Web de confiance**. Pour le fonctionnement correct de certains sites web, il faut les ajouter dans la liste de confiance. Par ailleurs, les objets malveillants peuvent ajouter à cette liste les liens sur les sites web créés par les malfaiteurs.

Il ne faut pas oublier que certaines valeurs des paramètres peuvent entraîner des problèmes d'affichage de certains sites web (par exemple, si ces sites utilisent des éléments ActiveX). Vous pouvez résoudre ce problème en ajoutant ces sites web à la zone de confiance.

L'analyse et la configuration du navigateur sont confiées à l'Assistant de configuration du navigateur. L'Assistant vérifie si les mises à jour les plus récentes du navigateur ont été installées et si les valeurs des paramètres définies ne rendent pas le système vulnérable aux actions des individus malintentionnés. Pour conclure, l'Assistant rédige un rapport qui peut être envoyé à Kaspersky Lab pour analyse.

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

Avant de lancer le diagnostic, fermez toutes les fenêtres de Microsoft Internet Explorer.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Mes outils d'optimisation**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Configuration du navigateur**.

Examinons en détails les étapes de l'Assistant.

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

Assurez-vous que l'option **Analyser Microsoft Internet Explorer** a été sélectionnée, puis appuyez sur le bouton **Suivant** pour lancer l'Assistant.

Etape 2. Analyse de la configuration de Microsoft Internet Explorer

L'Assistant analyse les paramètres du navigateur Microsoft Internet Explorer. La recherche de problèmes dans les paramètres peut prendre un certain temps. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

Etape 3. Sélection des actions pour la configuration du navigateur

Tous les problèmes identifiés à l'étape antérieure sont regroupés selon le niveau de danger qu'ils présentent pour le système (cf. section "Outils d'optimisation" à la page 235).

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

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

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

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

Etape 4. Configuration du navigateur

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

Etape 5. Fin de l'Assistant

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

RAPPORTS

Les événements survenus pendant le fonctionnement des composants de la protection ou lors de l'exécution des tâches de Kaspersky PURE sont consignés dans des rapports. Vous pouvez composer un rapport détaillé pour chaque composant de la protection ou chaque tâche et configurer l'affichage des données dans une mise en page pratique. De plus, vous pouvez filtrer les données (cf. section "Filtrage des données" à la page 242) et lancer une recherche (cf. section "Recherche d'événements" à la page 243) sur tous les événements du rapport.

Le cas échéant, vous pouvez enregistrer les données du rapport (cf. section "Enregistrement du rapport dans un fichier" à la page 244) dans un fichier texte. Vous pouvez également purger les rapports (cf. section "Purge des rapports" à la page 245) contenant des données qui ne vous sont plus nécessaires et configurer les paramètres de composition (cf. section "Entrées relatives aux événements non critiques" à la page 245) et de conservation (cf. section "Conservation des rapports" à la page 244) des rapports.

DANS CETTE SECTION

Composition du rapport pour le composant sélectionné 242

Filtrage des données 242

Recherche d'événements 243

Enregistrement du rapport dans un fichier 244

Conservation des rapports 244

Purge des rapports 245

Entrées relatives aux événements non critiques 245

Configuration de la notification sur la disponibilité du rapport 245

COMPOSITION DU RAPPORT POUR LE COMPOSANT SELECTIONNE

Vous pouvez obtenir un rapport détaillé sur les événements survenus pendant le fonctionnement de chaque composant ou de chaque tâche de Kaspersky PURE.

Pour le confort d'utilisation des rapports, vous pouvez gérer la représentation des données à l'écran : regrouper les événements selon divers paramètres, sélectionner la période couverte par le rapport, trier les événements dans chaque colonne ou selon l'importance et masquer des colonnes du tableau.

Pour obtenir un rapport pour le composant ou la tâche, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Le lien **Rapport** permet d'accéder à la fenêtre des rapports de Kaspersky PURE.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.

   La fenêtre **Rapport détaillé** s'ouvre.

4. Dans la liste déroulante de la partie supérieure gauche de la fenêtre, sélectionnez le composant ou la tâche pour laquelle il faut composer un rapport. Si vous choisissez l'option **Protection**, le rapport sera produit pour tous les composants de la protection.

FILTRAGE DES DONNEES

Les rapports de Kaspersky PURE permettent de filtrer les événements selon une ou plusieurs valeurs dans les colonnes du tableau, voire de définir des conditions de filtrage complexe.

Pour filtrer les événements selon des valeurs, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Le lien **Rapport** permet d'accéder à la fenêtre des rapports de Kaspersky PURE.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.

La fenêtre **Rapport détaillé** s'ouvre.

4. Dans la partie droite de la fenêtre, placez le curseur sur le coin supérieur gauche de l'en-tête de la colonne, puis ouvrez le menu du filtre en cliquant sur le bouton gauche de la souris.

5. Dans le menu du filtre, choisissez la valeur à utiliser pour filtrer les données.

6. Le cas échéant, répétez la procédure pour une autre colonne du tableau.

Pour définir des conditions de filtrage complexe, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Le lien **Rapport** permet d'accéder à la fenêtre des rapports de Kaspersky PURE.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.

   La fenêtre **Rapport détaillé** s'ouvre.

4. Dans la partie droite de la fenêtre, cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la colonne du rapport requise, puis choisissez l'option **Filtre**.

5. Dans la fenêtre **Filtre complexe**, définissez les conditions nécessaires du filtrage.

   a. Dans la partie droite de la fenêtre, définissez la limite de la sélection.

   b. Dans la partie gauche de la fenêtre, dans la liste déroulante **Condition**, choisissez la condition de sélection (par exemple, supérieure à ou inférieure à, égale à ou différente de la valeur indiquée en tant que limite de la sélection).

   c. Le cas échéant, ajoutez une deuxième valeur à l'aide d'un opérateur logique de conjonction (ET) ou de disjonction (OU). Si vous souhaitez que la sélection des données vérifie les deux conditions définies, sélectionnez **ET**. Si une condition minimum suffit, sélectionnez **OU**.

RECHERCHE D'EVENEMENTS

Vous pouvez rechercher l'événement souhaité dans le rapport à l'aide d'un mot clé via la barre de recherche ou à l'aide d'une fenêtre de recherche spéciale.

Pour trouver l'événement, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Le lien **Rapport** permet d'accéder à la fenêtre des rapports de Kaspersky PURE.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.

   La fenêtre **Rapport détaillé** s'ouvre.

4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du titre de la colonne qui vous intéresse, puis choisissez l'option **Recherche**.

5. Dans la fenêtre **Recherche** qui s'ouvre, définissez les critères de la recherche.

   a. Dans le champ **Ligne**, saisissez le mot clé pour la recherche.

b. Dans la liste déroulante **Colonne**, sélectionnez le nom de la colonne dans laquelle il faudra rechercher le mot clé saisi.

c. Le cas échéant, cochez les cases pour des paramètres de recherche complémentaires.

6. Cliquez sur le bouton **Recherche avancée**.

ENREGISTREMENT DU RAPPORT DANS UN FICHIER

Le rapport obtenu peut être enregistré dans un fichier texte.

Pour enregistrer le rapport dans un fichier, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.

2. Le lien **Rapport** permet d'accéder à la fenêtre des rapports de Kaspersky PURE.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.

   La fenêtre **Rapport détaillé** s'ouvre.

4. Composez le rapport souhaité, puis cliquez sur le bouton **Exporter**.

5. Dans la fenêtre qui s'ouvre, désignez le répertoire dans lequel il faut enregistrer le fichier du rapport et saisissez le nom du fichier.

CONSERVATION DES RAPPORTS

La durée maximale de conservation des rapports sur les événements est limitée à 30 jours. Les données sont supprimées à l'issue de cette période. Vous pouvez annuler la restriction sur la durée de conservation ou la modifier.

De plus, vous pouvez également indiquer la taille maximale du fichier du rapport. Par défaut, la taille maximale est limitée à 1 024 Mo. Une fois que la taille maximale est atteinte, le contenu du fichier est remplacé par de nouveaux enregistrements. Vous pouvez supprimer les restrictions sur la taille du rapport ou attribuer une autre valeur.

Pour configurer la durée maximale de conservation des rapports, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dans la section **Paramètres généraux**, sélectionnez la sous-section **Rapports et stockages**.

4. Dans la partie droite de la fenêtre, dans le groupe **Conservation**, cochez la case **Supprimer les rapports après** et indiquez la durée maximale de la conservation des rapports.

Pour configurer la taille maximale du fichier de rapport, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.

3. Dans la partie gauche de la fenêtre, dans la section **Paramètres généraux**, sélectionnez la sous-section **Rapports et stockages**.

4. Dans la partie droite de la fenêtre, dans le groupe **Conservation**, cochez la case **Taille maximale de fichier** et indiquez la taille maximale du fichier de rapport.

PURGE DES RAPPORTS

Vous pouvez purger les rapports dont les données ne vous sont plus utiles.

Pour purger les rapports*, procédez comme suit* :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Paramètres généraux**, sélectionnez la sous-section **Rapports et stockages**.
4. Dans la partie droite de la fenêtre, dans le groupe **Purge des rapports**, cliquez sur **Purger**.
5. Dans la fenêtre **Suppression** des informations des rapports qui s'ouvre, cochez les cases en regard des rapports que vous souhaitez purger.

ENTREES RELATIVES AUX EVENEMENTS NON CRITIQUES

Par défaut, les entrées relatives aux événements non critiques, aux événements du registre ou aux événements du système de fichiers ne sont pas ajoutées. Vous pouvez inclure ces entrées dans les rapports sur la protection.

Pour ajouter au rapport des entrées relatives aux événements non critiques, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, dans la section **Paramètres généraux**, sélectionnez la sous-section **Rapports et stockages**.
4. Dans la partie droite de la fenêtre, groupe **Evénements repris dans les rapports**, cochez la case en regard des types d'événement à inclure dans le rapport.

CONFIGURATION DE LA NOTIFICATION SUR LA DISPONIBILITE DU RAPPORT

Vous pouvez programmer la fréquence selon laquelle Kaspersky PURE vous rappellera la disponibilité des rapports.

Pour réaliser la programmation, procédez comme suit :

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

   La fenêtre **Ma Protection** s'ouvre.
2. Le lien **Rapport** permet d'accéder à la fenêtre des rapports de Kaspersky PURE.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cochez la case **Rappeler le rapport** et ouvrez la fenêtre de configuration de la programmation en cliquant sur le temps indiqué.
4. Dans la fenêtre **Rapport : programmation** qui s'ouvre, définissez les paramètres de la programmation.

NOTIFICATIONS

Par défaut, lorsqu'un événement se produit pendant l'utilisation de Kaspersky PURE vous prévient. Si vous devez exécuter une action quelconque, une fenêtre de notification apparaît (cf. section "Fenêtre de notification et messages contextuels" à la page 55). Les événements qui ne requièrent pas la sélection d'une action sont signalés à l'aide d'une notification sonore, de messages électronique ou de messages contextuels dans la zone de notification de la barre des tâches (cf. section "Fenêtre de notification et messages contextuels" à la page 55).

Vous pouvez sélectionner les modes de notification (cf. section "Configuration des modes de notification" à la page 246) sur les événements qui ne requièrent pas la sélection d'une action, voire désactiver la remise des notifications (cf. section "Activation et désactivation des notifications" à la page 246).

VOIR EGALEMENT :

Configuration des modes de notification 246

ACTIVATION ET DESACTIVATION DES NOTIFICATIONS

Par défaut Kaspersky PURE vous signale les événements importants liés au fonctionnement de l'application de différentes manières (cf. section "Configuration des modes de notification" à la page 246). Vous pouvez désactiver l'affichage des notifications.

Que la remise des notifications soit activée ou non, les informations relatives aux événements survenus pendant le fonctionnement de Kaspersky PURE sont consignées dans le rapport sur le fonctionnement de l'application.

La désactivation de la remise des notifications n'a aucune influence sur l'affichage des fenêtres de notification. Pour réduire au minimum l'affichage de fenêtre de notification, utilisez le mode de protection automatique (cf. section "Utilisation du mode de protection interactif" à la page 60).

Pour activer ou désactiver la remise des notifications, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Notifications** dans la rubrique **Paramètres avancés**.
4. Dans la partie droite de la fenêtre, décochez la case **Activer les notifications** si vous devez désactiver les notifications. Cochez cette case pour activer les notifications.

CONFIGURATION DES MODES DE NOTIFICATION

L'application vous signale les événements d'une des méthodes suivantes :

- message contextuel dans la zone de notification de la barre des tâches ;
- notification sonore ;
- messages électroniques.

Vous pouvez configurer les modes de notification pour chaque type d'événement.

Par défaut, les notifications critiques et les notifications sur les violations du fonctionnement de l'application sont accompagnées d'une notification sonore. Les notifications sonores utilisent la gamme de sons de Microsoft Windows. Vous pouvez changer la gamme de sons ou désactiver la notification sonore.

Pour configurer les modes de notification pour différents types d'événements, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Notifications** dans la rubrique **Paramètres avancés**.
4. Dans la partie droite de la fenêtre, cochez la case **Activer les notifications**, puis cliquez sur **Configuration**, situé à droite.
5. Dans la fenêtre **Notifications** qui s'ouvre, cochez les cases en fonction des modes de notification que vous voulez utiliser pour les divers événements : par courrier électronique, dans un message contextuel ou via une notification sonore. Pour ne recevoir aucune notification sur un type d'événement en particulier, décochez toutes les cases dans la ligne pour cet événement.

   Pour que Kaspersky PURE puisse vous signaler les événements par courrier électronique, il faut configurer les paramètres du courrier électronique pour la remise des notifications.

Pour configurer les paramètres du courrier électronique pour l'envoi des notifications, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Notifications** dans la rubrique **Paramètres avancés**.
4. Dans la partie droite de la fenêtre, cochez la case **Activer les notifications par courriers**, puis cliquez sur le bouton **Configuration**, situé à droite.
5. Dans la fenêtre **Configuration des notifications par courrier** qui s'ouvre, définissez les paramètres de livraison.

Pour modifier la gamme de sons des notifications, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Notifications** dans la rubrique **Paramètres avancés**.
4. Dans la partie droite de la fenêtre, cochez la case **Utiliser les sons standard de Windows par défaut** et modifiez la gamme de sons utilisée du système d'exploitation.

   Si la case est décochée, c'est la sélection de sons de la version antérieure de l'application qui sera utilisée.

Pour désactiver l'accompagnement sonore, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Notifications** dans la rubrique **Paramètres avancés**.
4. Dans la partie droite de la fenêtre, décochez la case **Activer les sons**.

PARTICIPATION AU KASPERSKY SECURITY NETWORK

Chaque jour dans le monde, une multitude de nouveaux virus apparaît. Afin de contribuer à la collecte efficace de données sur les types et les sources des nouvelles menaces et dans le but d'accélérer le développement de moyens de neutralisation, vous pouvez participer au Kaspersky Security Network.

Kaspersky Security Network (KSN) est un ensemble de services en ligne qui permet d'accéder à la base de connaissances de Kaspersky Lab sur la réputation des fichiers, des sites et des applications. L'utilisation des données de Kaspersky Security Network permet à l'application de réagir plus rapidement aux nouvelles formes de menace, améliore l'efficacité de certains composants de la protection et réduit la probabilité de faux positifs.

La participation au Kaspersky Security Network signifie que certaines statistiques obtenues pendant l'utilisation de Kaspersky PURE sur votre ordinateur sont envoyées automatiquement à Kaspersky Lab.

Les données relatives à l'utilisateur ne sont ni recueillies, ni traitées, ni enregistrées.

La participation au Kaspersky Security Network est volontaire. Vous prenez cette décision pendant l'installation de Kaspersky PURE, mais vous pouvez la changer à tout moment.

Pour activer l'utilisation de Kaspersky Security Network, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre qui s'ouvre, cliquez sur le lien **Configuration**.
3. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Retour d'informations** dans la rubrique **Paramètres généraux**.
4. Dans la partie droite de la fenêtre, cochez la case **J'accepte de rejoindre le Kaspersky Security Network**.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE KASPERSKY PURE

Une fois que Kaspersky PURE a été installé et configuré, vous pouvez vérifier si la configuration est correcte à l'aide d'un virus d'essai et de ses modifications. La vérification doit être réalisée séparément pour chaque composant de la protection/protocole.

DANS CETTE SECTION

Virus d'essai EICAR et ses modifications 249

Test de la protection du trafic HTTP 250

Test de la protection du trafic SMTP 251

Vérification de l'exactitude de la configuration d'Antivirus Fichiers 251

Vérification de l'exactitude de la configuration de la tâche d'analyse antivirus 252

Vérification de l'exactitude de la configuration de la protection contre le courrier indésirable 252

VIRUS D'ESSAI EICAR ET SES MODIFICATIONS

Ce "virus" d'essai a été développé spécialement par l'organisation EICAR (The European Institute for Computer Antivirus Research) afin de tester les logiciels antivirus.

Le "virus" d'essai N'EST PAS un programme malveillant et il ne contient pas de code qui pourrait nuire à votre ordinateur. Toutefois, la majorité des logiciels antivirus considère EICAR comme un virus.

N'utilisez jamais d'authentiques virus pour vérifier le fonctionnement de votre antivirus.

Vous pouvez télécharger le "virus" d'essai depuis le site officiel de l'organisation EICAR : http://www.eicar.org/anti_virus_test_file.htm.

Avant de lancer le téléchargement, il faut suspendre la protection antivirus, puisque le "virus" d'essai, chargé depuis la page anti_virus_test_file.htm, sera identifié et traité par l'application en tant qu'objet infecté transmis par le protocole HTTP.

Le fichier téléchargé depuis le site de la société EICAR est identifié par l'application comme un objet infecté par un virus qui ne peut être réparé et l'action définie pour ce genre d'objet est exécutée.

Vous pouvez également utiliser une modification du virus d'essai standard afin de vérifier le bon fonctionnement de l'application. Pour ce faire, il faut modifier le contenu du virus d'essai standard en ajoutant un des préfixes présentés dans le tableau ci-après. Pour créer une modification du virus d'essai, vous pouvez utiliser n'importe quel éditeur de fichier texte ou éditeur hypertexte tel que le Bloc-Notes de Microsoft ou UltraEdit32.

La première colonne du tableau (cf. ci-dessous) contient les préfixes qu'il faut ajouter en tête de la ligne du "virus" d'essai traditionnel afin de pouvoir créer sa modification. La deuxième colonne reprend toute les valeurs possibles de l'état attribué par application à la fin de l'analyse. La troisième colonne contient les informations relatives au traitement que réservera l'application aux objets de l'état indiqué. N'oubliez pas que les actions à réaliser sur les objets sont définies par les paramètres de l'application.

Après avoir ajouté le préfixe au "virus" d'essai, enregistrez le fichier obtenu sous le nom présentant la modification du virus : par exemple, si vous avez ajouté le préfixe DELE-, enregistrez le fichier obtenu sous le nom eicar_dele.com.

N'oubliez pas de restaurer la protection antivirus dès que le téléchargement du "virus" d'essai et la création de sa modification seront terminés..

Tableau 2. Modifications du virus d'essai

Préfixe	Etat de l'objet	Informations relatives au traitement de l'objet
Pas de préfixe, "virus" d'essai standard	**Infecté**. L'objet contient le code d'un virus connu. Réparation impossible.	L'application identifie l'objet en tant que virus qui ne peut être réparé. Une erreur se produit en cas de tentative de réparation de l'objet ; l'action définie pour les objets qui ne peuvent être réparés est appliquée.
CORR-	**Corrompu**.	L'application a pu accéder à l'objet mais n'a pas pu l'analyser car l'objet est corrompu (par exemple, sa structure est endommagée ou le format du fichier est invalide) Les informations relatives au traitement de l'objet figure dans le rapport sur le fonctionnement de l'application.
WARN-	**Suspect**. L'objet contient le code d'un virus inconnu. Réparation impossible.	L'objet est considéré comme suspect. Au moment de la découverte, les bases de l'application ne contenaient pas la description de la réparation de cet objet. Vous serez averti de la découverte d'un tel objet.
SUSP-	**Suspect**. L'objet contient le code modifié d'un virus connu. Réparation impossible.	L'application a découvert une équivalence partielle entre un extrait du code de l'objet et un extrait du code d'un virus connu. Au moment de la découverte, les bases de l'application ne contenaient pas la description de la réparation de cet objet. Vous serez averti de la découverte d'un tel objet.
ERRO-	**Erreur d'analyse**.	Une erreur s'est produite lors de l'analyse de l'objet. L'application ne peut accéder à l'objet car l'intégrité de celui-ci a été violée (par exemple : il n'y a pas de fin à une archive multivolume) ou il n'y a pas de lien vers l'objet (lorsque l'objet se trouve sur une ressource de réseau). Les informations relatives au traitement de l'objet figurent dans le rapport sur le fonctionnement de l'application.
CURE-	**Infecté**. L'objet contient le code d'un virus connu. Réparable.	L'objet contient un virus qui peut être réparé. L'application répare l'objet et le texte du corps du virus est remplacé par CURE. Vous serez averti de la découverte d'un tel objet.
DELE-	**Infecté**. L'objet contient le code d'un virus connu. Réparation impossible.	L'application identifie l'objet en tant que virus qui ne peut être réparé. Une erreur se produit en cas de tentative de réparation de l'objet ; l'action définie pour les objets qui ne peuvent être réparés est appliquée. Vous serez averti de la découverte d'un tel objet.

TEST DE LA PROTECTION DU TRAFIC HTTP

- *Pour vérifier l'identification de virus dans le flux de données transmises par le protocole HTTP :*

  essayez de télécharger le "virus" d'essai depuis le site officiel de l'organisation **EICAR** : http://www.eicar.org/anti_virus_test_file.htm.

Lors d'une tentative de téléchargement du virus d'essai, Kaspersky PURE découvre l'objet, l'identifie comme étant infecté et ne pouvant être réparé puis exécute l'action définie dans les paramètres d'analyse du trafic HTTP pour ce type d'objet. Par défaut, la connexion avec le site est coupée à la moindre tentative de téléchargement du virus d'essai et un message indiquera dans le navigateur que l'objet en question est infecté par le virus EICAR-Test-File.

TEST DE LA PROTECTION DU TRAFIC SMTP

Pour vérifier l'identification des virus dans le flux de données transmises via le protocole SMTP, vous pouvez utiliser le système de messagerie qui exploite ce protocole pour le transfert des données.

Il est conseillé de tester la détection de virus dans les parties différentes du courrier sortant : aussi bien sur le corps des messages que les pièces jointes. Pour le test, utilisez le fichier du virus d'essai EICAR (cf. section "Virus d'essai EICAR et ses modifications" à la page 249).

Pour tester la détection de virus dans le flux de données envoyées par le protocole SMTP, procédez comme suit :

1. Composez le message au format "Texte normal" à l'aide du client de messagerie installé sur l'ordinateur.

   Les messages contenant le "virus" d'essai dans le corps et rédigés au format RTF et HTML ne seront pas analysés !

2. En fonction de la partie du message où l'application doit détecter un virus, procédez comme suit :

   - Pour détecter le virus dans le corps du message, placez le texte du "virus" d'essai standard ou modifié EICAR dans le début du message ;
   - Pour détecter le virus dans les pièces jointes, ajoutez au message le fichier contenant le "virus" d'essai EICAR.

3. Envoyez ce message à l'adresse de l'administrateur.

L'application découvre l'objet, l'identifie en tant qu'objet infecté et bloque l'envoie du message.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION D'ANTIVIRUS FICHIERS

Pour vérifier l'exactitude de la configuration de l'Antivirus Fichiers, procédez comme suit :

1. Créez un répertoire sur le disque, copiez-y le virus d'essai récupéré sur le site officiel de l'organisation **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) ainsi que les modifications de ce virus que vous avez créé.
2. Autorisez la consignation de tous les événements afin que le rapport reprenne les données sur les objets corrompus ou les objets qui n'ont pas été analysés suite à un échec.
3. Exécutez le fichier du virus d'essai ou une de ses modifications.

Antivirus Fichiers intercepte la requête adressée au fichier, la vérifie et exécute l'action définie dans les paramètres. En sélectionnant diverses actions à réaliser sur les objets infectés, vous pouvez vérifier le fonctionnement du composant dans son ensemble.

Les informations complètes sur les résultats du fonctionnement d'Antivirus Fichiers sont consultables dans le rapport sur l'utilisation du composant.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE LA TACHE D'ANALYSE ANTIVIRUS

Pour vérifier l'exactitude de la configuration de la tâche d'analyse, procédez comme suit :

1. Créez un répertoire sur le disque, copiez-y le virus d'essai récupéré sur le site officiel de l'organisation **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) ainsi que les modifications de ce virus que vous avez créées.

2. Créez une nouvelle tâche d'analyse antivirus et en guise d'objet à analyser sélectionnez le dossier, contenant la sélection de virus d'essai.

3. Autorisez la consignation de tous les événements dans le rapport afin de conserver les données relatives aux objets corrompus ou aux objets qui n'ont pas été analysés suite à l'échec.

4. Lancez la tâche d'analyse antivirus.

Lors de l'analyse, les actions définies dans les paramètres de la tâche seront exécutées au fur et à mesure que des objets suspects ou infectés sont découverts. En sélectionnant diverses actions à réaliser sur les objets infectés, vous pouvez vérifier le fonctionnement du composant dans son ensemble.

Toutes les informations relatives aux résultats de l'exécution de la tâche d'analyse sont consultables dans le rapport de fonctionnement du composant.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE LA PROTECTION CONTRE LE COURRIER INDESIRABLE

Pour vérifier la protection contre le courrier indésirable, vous pouvez utiliser un message d'essai qui sera considéré comme indésirable par l'application.

Le message d'essai doit contenir dans le corps la ligne suivante :

```
Spam is bad do not send it
```

Une fois que ce message est arrivé sur l'ordinateur, Kaspersky PURE l'analyse, lui attribue l'état de courrier indésirable et exécute l'action définie pour les objets de ce type.

CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

En cas de problème d'utilisation de Kaspersky PURE, vérifiez d'abord si la solution n'est pas expliquée dans la documentation, dans l'aide, dans la banque de solutions du support technique de Kaspersky Lab ou dans le forum des utilisateurs.

Si vous ne trouvez pas la réponse à votre question, vous pouvez contacter le support technique de Kaspersky Lab d'une des manières suivantes :

- Envoyez une demande depuis Mon Espace Personnel sur le site Web du support technique ;
- Appelez par téléphone.

Les experts du support technique répondront à vos questions sur l'installation, l'activation et l'utilisation de l'application. En cas d'infection de votre ordinateur, ils vous aideront à supprimer les conséquences de l'action des programmes malveillants.

Avant de contacter le service d'assistance technique, veuillez prendre connaissance des règles d'assistance (http://support.kaspersky.com/fr/support/rules).

Si vous contactez les experts du support technique, ceux-ci peuvent vous demander de générer un rapport sur l'état du système et un fichier de trace et de les envoyer au support technique. Après l'analyse des données envoyées, les experts du support technique pourront créer le script AVZ et vous l'envoyer. Celui-ci vous aidera à supprimer les problèmes rencontrés.

DANS CETTE SECTION

Mon Espace Personnel 253

Assistance technique par téléphone 254

Création d'un rapport sur l'état du système 254

Création d'un fichier de trace 255

Envoi des rapports 255

Exécution du script AVZ 257

MON ESPACE PERSONNEL

Comme son nom l'indique, *Mon Espace Personnel* est un espace qui vous est réservé sur le site du Support technique. Vous pouvez y réaliser les opérations suivantes :

- Envoyer des demandes au 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.

Pour accéder à la page d'accueil de Mon Espace Personnel, réalisez une des opérations suivantes :

- Cliquez sur le lien **Mon espace personnel** dans la fenêtre principale de Kaspersky PURE ;
- Saisissez l'URL https://my.kaspersky.com/en/index.html?LANG=fr dans la barre d'adresse du navigateur.

Si vous n'êtes pas enregistré dans Mon Espace Personnel, vous pouvez réaliser la procédure d'enregistrement à la page d'enregistrement https://my.kaspersky.com/ru/registration?LANG=fr. Vous devrez saisir votre adresse de messagerie et un mot de passe d'accès à Mon Espace Personnel. L'envoi de questions sur l'utilisation de Kaspersky PURE requiert le code d'activation.

N'oubliez pas que certaines demandes doivent être envoyées non pas au support technique mais au laboratoire d'étude des virus. Il s'agit des demandes du type suivant :

- Programme malveillant inconnu. Vous pensez qu'un objet quelconque est malveillant mais Kaspersky PURE ne confirme pas vos soupçons ;
- Faux positif du logiciel antivirus. Kaspersky PURE considère un certain fichier comme un virus mais vous êtes convaincu que ce n'est pas le cas ;
- Demande de description d'un programme malveillant. Vous souhaitez obtenir la description d'un virus quelconque.

L'envoi de demandes au laboratoire d'étude des virus ne requiert pas le code d'activation.

Vous pouvez également envoyer des demandes au laboratoire d'étude des virus sans vous enregistrer dans Mon Espace Personnel. Utilisez pour ce faire le formulaire de demande en ligne (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr).

ASSISTANCE TECHNIQUE PAR TELEPHONE

Si le problème est urgent, vous pouvez téléphoner au support technique dans votre ville. Si vous contactez l'assistance technique russe (http://support.kaspersky.ru/support/support_local) ou internationale (http://support.kaspersky.com/fr/support/international) veuillez fournir l'information (http://support.kaspersky.com/fr/support/details Nos experts pourront ainsi vous venir en aide plus rapidement.

CREATION D'UN RAPPORT SUR L'ETAT DU SYSTEME

Afin de pouvoir résoudre vos problèmes, il se peut que les experts du Support technique de Kaspersky Lab aient besoin d'un rapport sur l'état du système. Ce rapport contient des informations détaillées sur les processus exécutés, les modules et les pilotes chargés, les modules externes de Microsoft Internet Explorer et de l'Assistant Microsoft Windows, les ports ouverts, les objets suspects décelés, etc.

Aucune donnée personnelle relative à l'utilisateur n'est recueillie durant la création du rapport.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur le lien **Assistance technique**.
3. Dans la fenêtre **Assistance technique** qui s'ouvre, cliquez sur le lien **Outils d'assistance**.
4. Dans la **fenêtre** Informations pour le service d'assistance technique, cliquez sur le bouton **Créer le rapport sur l'état du système**.

Le rapport sur l'état du système est généré au format HTML et XML et il est enregistré dans l'archive sysinfo.zip. Une fois que la collecte des informations sur le système est terminée, vous pouvez consulter le rapport.

Pour parcourir le rapport, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur le lien **Assistance technique**.
3. Dans la fenêtre **Assistance technique** qui s'ouvre, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, cliquez sur le bouton **Voir**.
5. Ouvrez l'archive sysinfo.zip contenant le fichier du rapport.

CREATION D'UN FICHIER DE TRACE

Le système d'exploitation et certaines applications peuvent connaître des échecs après l'installation de Kaspersky PURE. Dans ce cas, il s'agit généralement d'un conflit entre Kaspersky PURE et des applications installées ou des pilotes sur l'ordinateur. Afin de résoudre ce problème, les experts du Support technique de Kaspersky Lab pourraient vous demander de créer un fichier de trace.

Pour créer un fichier de trace, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur le lien **Assistance technique**.
3. Dans la fenêtre **Assistance technique** qui s'ouvre, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, dans le groupe **Traçages** sélectionnez le niveau du traçage dans la liste déroulante.

   Il est recommandé de demander au spécialiste du Support technique le niveau du traçage requis. Faute d'indication du Support technique, il est conseillé d'établir le niveau du traçage à **500**.
5. Afin de lancer le traçage, cliquez sur le bouton **Activer**.
6. Reproduisez la situation qui entraîne le problème.
7. Pour arrêter le traçage, cliquez sur le bouton **Désactiver**.

Vous pouvez passer au transfert des résultats du traçage (cf. section "Envoi des fichiers de données" à la page 255) sur le serveur de Kaspersky Lab.

ENVOI DES RAPPORTS

Une fois que les fichiers de traçage et le rapport sur l'état du système ont été créés, il faut les envoyer aux experts du Support technique de Kaspersky Lab.

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

Pour télécharger les fichiers de données sur le serveur du service d'Assistance technique, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur le lien **Assistance technique**.
3. Dans la fenêtre **Assistance technique** qui s'ouvre, cliquez sur le lien **Outils d'assistance**.

4. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, dans le groupe **Actions**, cliquez sur le bouton **Envoyer les informations au service d'assistance technique**.

5. Dans la fenêtre **Chargement des informations pour l'assistance sur le serveur** qui s'ouvre, cochez les cases en regard des fichiers que vous souhaitez envoyer au service d'assistance technique, puis cliquez sur **Envoyer**.

6. Dans la fenêtre **Numéro de requête** qui s'ouvre, indiquez le numéro attribué à votre demande lors du remplissage du formulaire électronique sur le site du service d'Assistance technique.

Les fichiers de données sélectionnés seront compactés et envoyés sur le serveur du Support technique.

S'il n'est pas possible pour une raison quelconque de contacter le Support technique, vous pouvez enregistrer les fichiers de données sur votre ordinateur et les envoyer plus tard depuis Mon Espace Personnel.

Pour enregistrer les fichiers de données sur le disque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur le lien **Assistance technique**.

3. Dans la fenêtre **Assistance technique** qui s'ouvre, cliquez sur le lien **Outils d'assistance**.

4. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, dans le groupe **Actions**, cliquez sur le bouton **Envoyer les informations au service d'assistance technique**.

5. Dans la fenêtre **Chargement des informations pour l'assistance sur le serveur** qui s'ouvre, cochez les cases en regard des fichiers que vous souhaitez envoyer au service d'assistance technique, puis cliquez sur **Envoyer**.

6. Dans la fenêtre **Numéro de requête** qui s'ouvre, cliquez sur **Annuler** et dans la fenêtre qui s'ouvre, confirmez l'enregistrement des fichiers sur le disque en cliquant sur le bouton **Oui**.

7. Dans la fenêtrer qui s'ouvre, définissez le nom de l'archive et confirmez l'enregistrement.

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

EXECUTION DU SCRIPT AVZ

Les experts de Kaspersky Lab analysent votre problème sur la base du fichier de trace et du rapport sur l'état du système. Cette analyse débouche sur une séquence d'actions à exécuter pour supprimer les problèmes identifiés. Le nombre de ces actions peut être très élevé.

Pour modifier la procédure de résolution des problèmes, des scripts AVZ sont utilisés. Le script AVZ est un ensemble d'instructions qui permettent de modifier les clés du registre, de mettre des fichiers en quarantaine, de lancer des recherches de catégories avec possibilité de mise en quarantaine des fichiers en rapport, de bloquer les intercepteurs UserMode et KernelMode, etc.

Pour exécuter les scripts inclus dans l'application, utilisez *l'Assistant d'exécution des scripts AVZ*.

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

Il est déconseillé de modifier le texte du script envoyé par les experts de Kaspersky Lab. En cas de problème lors de l'exécution du script, contactez le service d'assistance technique.

Pour lancer l'assistant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur le lien **Assistance technique**.
3. Dans la fenêtre **Assistance technique** qui s'ouvre, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, cliquez sur le bouton **Exécuter le script AVZ**.

Si l'exécution du script réussi, l'Assistant termine. Si un échec se produit durant l'exécution du script, l'Assistant affiche le message correspondant.

ANNEXES

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

DANS CETTE SECTION

Etats de l'abonnement 258

Utilisation de l'application au départ de la ligne de commande 259

Liste des notifications Kaspersky PURE 269

ETATS DE L'ABONNEMENT

L'état de l'abonnement se caractérise par un des états suivants :

- *En cours*. La demande sur l'abonnement n'a pas encore été traitée (pour traiter la demande sur le serveur, un certain temps est requis). Kaspersky PURE est totalement opérationnel. Si à l'expiration d'une certaine période la demande sur l'abonnement n'a pas été traitée, vous recevez une notification que la mise à jour de l'état de l'abonnement n'a pas été exécutée. Les bases de l'application ne seront plus actualisées (pour les licences avec abonnement pour la mise à jour) et l'ordinateur ne sera plus protégé (pour les licences avec abonnement pour la mise à jour et la protection).

- *Activé*. L'abonnement a été activé pour une durée indéterminée ou non (la date de fin de validité est alors précisée).

- *Renouvelé*. L'abonnement a été renouvelé pour une durée indéterminée ou non.

- *Erreur*. Lors de la mise à jour de l'état de l'abonnement, une erreur s'est produite.

- *Expiré. Période de grâce.* La durée de validité de l'abonnement ou la durée pour la mise à jour de l'état a expiré. Si la durée de validité pour la mise à jour de l'état a expiré, actualisez l'état de l'abonnement à la main. Si la durée de validité de l'abonnement a expiré, vous pouvez renouveler l'abonnement en contactant la boutique en ligne où vous avez acheté Kaspersky PURE. Pour utiliser un autre code d'activation, il faut d'abord supprimer l'abonnement utilisé.

- *Expiré. Période de grâce expirée.* La durée de validité de l'abonnement ou la période de grâce pour le renouvellement de la licence est écoulée. Contactez votre fournisseur de l'abonnement pour obtenir un nouvel abonnement ou renouveler l'abonnement actuel.

  Si la durée de validité de l'abonnement est écoulée ainsi que la période complémentaire durant laquelle le renouvellement est possible (état *Expiré*), Kaspersky PURE vous le signale et cesse de tenter d'obtenir le renouvellement depuis le serveur. Dans le cas des licences avec abonnement pour la mise à jour, les fonctions de l'application sont préservées à l'exception de la mise à jour des bases de l'application. Dans le cas d'une licence avec abonnement pour la mise à jour et la protection, les bases de l'application ne seront plus actualisées, l'ordinateur ne sera plus protégé et les analyses ne seront plus exécutées.

- *Refus de l'abonnement*. Vous avez refusé l'abonnement pour renouveler automatiquement la licence.

- *Mise à jour requise*. L'état de l'abonnement n'a pas été actualisé à temps pour une raison quelconque.

  Si l'abonnement n'a pas été renouvelé à temps (par exemple, l'ordinateur n'était pas allumé pendant la période où le renouvellement de la licence était possible), vous pouvez actualiser son état manuellement dans la fenêtre de Gestionnaire de licences (cf. section "Consultation des informations sur la licence" à la page 41). Avant le renouvellement de l'abonnement, Kaspersky PURE n'actualise plus les bases de l'application (pour les licences

avec abonnement pour la mise à jour) et cesse de protéger l'ordinateur et de lancer l'analyse (pour les licences commerciales avec abonnement pour la mise à jour et la protection).

- *Suspendu*. L'abonnement pour renouveler la licence est suspendu.
- *Restauré*. L'abonnement est restauré.

Dans certains cas pour la licence avec abonnement, l'affichage des informations supplémentaires sur l'état de l'abonnement est possible.

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

Vous pouvez utiliser Kaspersky PURE à l'aide de la ligne de commande. Ce mode vous permet d'exécuter les opérations suivantes :

- Activation de l'application ;
- Lancement et arrêt de l'application ;
- Lancement et arrêt des composants de l'application ;
- Lancement et arrêt des tâches ;
- Obtention d'informations relatives à l'état actuel des composants et aux tâches et à leur statistiques ;
- lancement et arrêt de l'exécution des tâches d'analyse antivirus ;
- Analyse des objets sélectionnés ;
- Mise à jour des bases et des modules de l'application, retour à l'état antérieur à la mise à jour ;
- Exportation et importation des paramètres de la protection ;
- Affichage de l'aide sur la syntaxe de la ligne de commande pour l'ensemble des instructions ou pour des instructions individuelles.

Syntaxe de la ligne de commande :

```
avp.com <instruction> [paramètres]
```

La requête adressée à l'application via la ligne de commande doit être réalisée depuis le répertoire d'installation du logiciel ou en indiquant le chemin d'accès complet à avp.com.

La liste des instructions utilisées pour l'administration de l'application et de ses composants est reprise dans le tableau ci-dessous.

START	Lancement du composant ou de la tâche
STOP	Arrêt du composant ou de la tâche (l'exécution de l'instruction est possible uniquement après saisie du mot de passe défini via l'interface de Kaspersky PURE)
STATUS	Affichage de l'état actuel du composant ou de la tâche
STATISTICS	Affichage des statistiques du composant ou de la tâche
HELP	Affichage de la liste des instructions et des informations sur la syntaxe de l'instruction

SCAN	Recherche d'éventuels virus dans les objets
UPDATE	Lancement de la mise à jour de l'application
ROLLBACK	Annulation de la dernière mise à jour réalisée (l'exécution de l'instruction est possible uniquement après saisie du mot de passe défini via l'interface de Kaspersky PURE)
EXIT	Arrêt du logiciel (l'exécution de l'instruction est possible uniquement avec la saisie du mode passe défini via l'interface de l'application)
IMPORT	Importation des paramètres de protection de Kaspersky PURE (l'exécution de l'instruction est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
EXPORT	Exportation des paramètres de la protection de l'application

Chaque instruction possède ses propres paramètres, propres à chaque composant de l'application.

DANS CETTE SECTION

Activation de l'application 260

Lancement de l'application 261

Arrêt de l'application 261

Administration des composants de l'application et des tâches 261

Recherche de virus 263

Mise à jour de l'application 265

Annulation de la dernière mise à jour 266

Exportation des paramètres de protection 266

Importation des paramètres de protection 267

Obtention du fichier de trace 267

Consultation de l'aide 268

Codes de retour de la ligne de commande 268

ACTIVATION DE L'APPLICATION

Kaspersky PURE peut être activé à l'aide du fichier de licence.

Syntaxe de l'instruction :

```
avp.com ADDKEY <nom_du_fichier>
```

La description des paramètres d'exécution de l'instruction est reprise dans le tableau ci-dessous.

<nom_du_fichier>	Nom du fichier de licence avec l'extension .key

Exemple :

```
avp.com ADDKEY 1AA111A1.key
```

LANCEMENT DE L'APPLICATION

Syntaxe de l'instruction :

```
avp.com
```

ARRET DE L'APPLICATION

Syntaxe de l'instruction :

```
avp.com EXIT /password=<votre_mot_de_passe>
```

La description des paramètres est reprise dans le tableau ci-dessous.

<votre_mot_de_passe>	Mot de passe d'accès à l'application, défini dans l'interface

N'oubliez pas que l'instruction ne s'exécutera pas sans la saisie du mot de passe.

ADMINISTRATION DES COMPOSANTS DE L'APPLICATION ET DES TACHES

Syntaxe de l'instruction :

```
avp.com <instruction> <profil|nom_de_la_tâche> [/R[A]:<fichier_de_rapport>]
avp.com STOP <profil|nom_de_la_tâche> /password=<votre_mot_de_passe>
[/R[A]:<fichier_de_rapport>]
```

Les instructions et les paramètres sont décrits dans le tableau ci-après.

<instruction>	L'administration des composants et des tâches de Kaspersky PURE via la ligne de commande s'opère à l'aide des instructions suivantes : START : lancement du composant de la protection en temps réel ou d'une tâche. STOP : arrêt du composant de la protection en temps réel ou d'une tâche. STATUS : affichage de l'état actuel du composant de la protection ou d'une tâche. STATISTICS : affichage des statistiques du composant de la protection ou d'une tâche. N'oubliez pas que l'instruction STOP ne peut être exécutée sans la saisie préalable du mot de passe.
<profil|nom_de_la_tâche>	En guise de valeur pour le paramètre **<profil>**, vous pouvez indiquer n'importe quel composant de la protection en temps réel de Kaspersky PURE ainsi que les modules qui sont repris dans les composants des tâches d'analyse à la demande ou de mise à jour composées (les valeurs standard utilisées par l'application sont reprises dans le tableau ci-après). En guise de valeur pour le paramètre **<nom_de_la_tâche>**, vous pouvez indiquer le nom de n'importe quelle tâche d'analyse à la demande ou de mise à jour configurée par l'utilisateur.
<votre_mot_de_passe>	Mot de passe d'accès à l'application, défini dans l'interface.
/R[A]:<fichier_de_rapport>	**/R:<fichier_de_rapport>** : consigner dans le rapport uniquement les événements importants. **/RA:<fichier_de_rapport>** : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

Le paramètre **<profil>** prend une des valeurs du tableau ci-après.

RTP	Tous les composants de la protection. L'instruction **avp.com START RTP** lance tous les composants de la protection, si la protection avait été arrêtée. Si le composant a été arrêté via l'instruction **STOP** de la ligne de commande, il ne pourra être redémarré via l'instruction **avp.com START RTP**. Pour ce faire, il faut exécuter la commande **avp.com START <profil>** où le paramètre **<profil>** représente un composant concret de la protection, par exemple **avp.com START FM**.
FW	Pare-feu.
HIPS	Contrôle des Applications.
pdm	Défense Proactive.
FM	Antivirus Fichiers.
EM	Antivirus Courrier.
WM	Antivirus Internet. Valeurs pour les sous-composants de l'Antivirus Internet : **httpscan (HTTP)** : analyse du trafic HTTP ; **sc** : analyse des scripts.
IM	Antivirus IM ("Chat").
AB	Anti-bannière.
AS	Anti-Spam.
PC	Contrôle Parental.
AP	Anti-Phishing.
ids	Prévention des intrusions.
Updater	Mise à jour.
Rollback	Annulation de la dernière mise à jour.
Scan_My_Computer	Analyse de l'ordinateur.
Scan_Objects	Analyse des Objets.
Scan_Quarantine	Analyse de la quarantaine.
Scan_Startup (STARTUP)	Analyse des objets de démarrage.
Scan_Vulnerabilities (SECURITY)	Recherche de vulnérabilités.

Les composants et les tâches lancés via la ligne de commande sont exécutés selon les paramètres définis dans l'interface du logiciel.

Exemples :

- *Pour activer l'Antivirus Fichiers, saisissez l'instruction :*

```
avp.com START FM
```

- *Pour arrêter l'analyse de l'ordinateur, saisissez l'instruction :*

```
avp.com STOP Scan_My_Computer /password=<votre_mot_de_passe>
```

RECHERCHE DE VIRUS

La ligne de commande utilisée pour lancer l'analyse antivirus d'un secteur quelconque et pour lancer le traitement des objets malveillants découverts ressemble à ceci :

```
avp.com SCAN [<objet à analyser>] [<action>] [<types de fichiers>] [<exclusions>]
[<fichier de configuration>] [<paramètres du rapport>] [< paramètres complémentaires
>]
```

Pour analyser les objets, vous pouvez également utiliser les tâches créées dans l'application en lançant la tâche requise via la ligne de commande. Dans ce cas, la tâche sera réalisée selon les paramètres définis dans l'interface de Kaspersky PURE.

La description des paramètres est reprise dans le tableau ci-dessous.

<objet à analyser> : ce paramètre définit la liste des objets qui seront soumis à la recherche de code malveillant. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.	
<files>	Liste des chemins d'accès aux fichiers et aux répertoires à analyser. La saisie d'un chemin relatif ou absolu est autorisée. Les éléments de la liste doivent être séparés par un espace. Remarque : • Mettre le nom de l'objet entre guillemets s'il contient un espace ; • Lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.
/MEMORY	Objets de la mémoire vive.
/STARTUP	Objets de démarrage.
/MAIL	Boîtes aux lettres.
/REMDRIVES	Tous les disques amovibles.
/FIXDRIVES	Tous les disques locaux.
/NETDRIVES	Tous les disques de réseau.
/QUARANTINE	Objets en quarantaine.

/ALL	Analyse complète de l'ordinateur.
/@:<filelist.lst>	Chemin d'accès au fichier de la liste des objets et répertoires inclus dans l'analyse. La saisie d'un chemin d'accès relatif ou absolu au fichier est autorisée. Le chemin doit être saisi sans guillemets, même s'il contient un espace. Le fichier contenant la liste des objets doit être au format texte. Chaque objet à analyser doit se trouver sur une nouvelle ligne. Il est conseillé de saisir dans le fichier les chemins d'accès absolu aux objets à analyser. Si un chemin d'accès relatif est saisi, le chemin est indiqué par rapport au fichier exécutable de l'application et non pas par rapport au fichier contenant la liste des objets à analyser.
<action> : ce paramètre définit les actions exécutées sur les objets malveillants découverts lors de l'analyse. Si le paramètre n'est pas défini, l'action exécutée par défaut sera l'action définie par la valeur **/i8**. Si vous travaillez en mode automatique, alors Kaspersky PURE appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. L'action définie par la valeur du paramètre **<action>** sera ignorée.	
/i0	Aucune action n'est exécutée, les informations sont consignées dans le rapport.
/i1	Réparer les objets infectés, si la réparation est impossible, les ignorer.
/i2	Réparer les objets infectés, si la réparation est impossible, supprimer les objets simples; ne pas supprimer les objets infectés au sein d'un conteneur (fichiers composés); supprimer les conteneurs avec un en-tête exécutable (archive sfx).
/i3	Réparer les objets infectés, si la réparation est impossible, supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
/i4	Supprimer les objets infectés ; supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
/i8	Confirmer l'action auprès de l'utilisateur en cas de découverte d'un objet infecté.
/i9	Confirmer l'action auprès de l'utilisateur à la fin de l'analyse.
Le paramètre **<types de fichiers>** définit les types de fichiers qui seront soumis à l'analyse antivirus. Si le paramètre n'est pas défini, seuls seront analysés par défaut les objets pouvant être infectés en fonction du contenu.	
/fe	Analyser uniquement les fichiers qui peuvent être infectés selon l'extension.
/fi	Analyser uniquement les fichiers qui peuvent être infectés selon le contenu.
/fa	Analyser tous les fichiers.
Le paramètre **<exclusions>** définit les objets exclus de l'analyse. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.	
-e:a	Ne pas analyser les archives.
-e:b	Ne pas analyser les bases de messagerie.
-e:m	Ne pas analyser les messages électroniques au format plain text.
-e:<filemask>	Ne pas analyser les objets en fonction d'un masque.
-e:<secondes>	Ignorer les objets dont l'analyse dure plus que la valeur attribuée au paramètre **<secondes>**.
-es:<taille>	Ignorer les objets dont la taille (en Mo) est supérieure à la valeur définie par le paramètre **<taille>**. Le paramètre s'applique uniquement aux fichiers composés (par exemple, aux archives).

Le paramètre **<fichier de configuration>** définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par l'application pour l'analyse. Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour l'analyse antivirus. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs définies dans l'interface de l'application qui seront utilisées.	
/C:<nom_du_fichier>	Utiliser les valeurs des paramètres définies dans le fichier de configuration **<nom_du_fichier>**.
Le paramètre **<paramètres du rapport>** définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.	
/R:<fichier_de_rapport>	Consigner uniquement les événements importants dans le fichier indiqué.
/RA:<fichier_de_rapport>	Consigner tous les événements dans le fichier de rapport indiqué.
<paramètres complémentaires> : paramètres qui définissent l'utilisation de technologies de recherche de virus.	
/iChecker=<on|off>	Active/désactive l'utilisation de la technologie iChecker.
/iSwift=<on|off>	Active/désactive l'utilisation de la technologie iSwift.

Exemples :

- *Lancer l'analyse de la mémoire vive, des objets de démarrage, des boîtes aux lettres et des répertoires My Documents, Program Files et du fichier test.exe :*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" "C:\Downloads\test.exe"
```

- *Analyser les objets dont la liste est reprise dans le fichier object2scan.txt. Utiliser le fichier de configuration scan_settings.txt. À la fin de l'analyse, rédiger un rapport qui reprendra tous les événements :*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Exemple de fichier de configuration :

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

MISE A JOUR DE L'APPLICATION

L'instruction pour la mise à jour des modules de Kaspersky PURE et des bases de l'application possède la syntaxe suivante :

```
avp.com UPDATE [<source_de_la_mise_à_jour>] [/R[A]:<fichier_de_rapport>] [/C:<nom_du_fichier>]
```

La description des paramètres est reprise dans le tableau ci-dessous.

<source_de_la_mise_à_jour>	Serveur HTTP, serveur FTP pou répertoire de réseau pour le chargement de la mise à jour. Ce paramètre accepte en tant que valeur le chemin d'accès complet à la source des mises à jour ou une URL. Si le chemin d'accès n'est pas indiqué, la source de la mise à jour sera définie par les paramètres du service de mise à jour de l'application.
/R[A]:<fichier_de_rapport>	**/R:<fichier_de_rapport>** : consigner dans le rapport uniquement les événements importants. **/RA:<fichier_de_rapport>** : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran ; portent sur tous les événements.

/C:<nom_du_fichier>	Chemin d'accès au fichier de configuration contenant les paramètres de fonctionnement de Kaspersky PURE pour la mise à jour. Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour la mise à jour de l'application. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs des paramètres définies dans l'interface de l'application qui seront utilisées.

Exemples :

- *Mettre à jour les bases de l'application et consigner tous les éléments dans le rapport :*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Mettre à jour les modules de Kaspersky PURE en utilisant les paramètres du fichier de configuration updateapp.ini :*

```
avp.com UPDATE /C:updateapp.ini
```

Exemple de fichier de configuration :

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ANNULATION DE LA DERNIERE MISE A JOUR

Syntaxe de l'instruction :

```
avp.com ROLLBACK [/R[A]:<fichier_de_rapport>][/password=<votre_mot_de_passe>]
```

La description des paramètres est reprise dans le tableau ci-dessous.

/R[A]:<fichier_de_rapport>	**/R:<fichier_de_rapport>** : consigner dans le rapport uniquement les événements importants. **/RA:<fichier_de_rapport>** : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran ; portent sur tous les événements.
<votre_mot_de_passe>	Mot de passe d'accès à l'application, défini dans l'interface.

N'oubliez pas que l'instruction ne s'exécutera pas sans la saisie du mot de passe.

Exemple :

```
avp.com ROLLBACK /RA:rollback.txt/password=<votre mot de passe>
```

EXPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de l'instruction :

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

La description des paramètres d'exécution de l'instruction est reprise dans le tableau ci-dessous.

<profil>	Composant ou tâche dont les paramètres sont exportés. Le paramètre **<profil>** peut prendre n'importe quelle des valeurs indiquées au point "Administration des composants de l'application et des tâches".
<nom_du_fichier>	Chemin d'accès au fichier vers lequel sont exportés les paramètres de Kaspersky PURE. Vous pouvez indiquer un chemin relatif ou absolu. Le fichier de configuration est enregistré au format binaire (dat), si aucun autre format n'est indiqué ou si le format n'est pas précisé, et il peut être ensuite utilisé pour transférer les paramètres de l'application vers d'autres ordinateurs. De plus, vous pouvez enregistrer le fichier de configuration au format texte. Dans ce cas, ajoutez l'extension txt. N'oubliez pas que l'importation de paramètres de la protection depuis un fichier texte n'est pas prise en charge. Ce fichier peut être utilisé uniquement pour consulter les paramètres de fonctionnement principaux de Kaspersky PURE.

Exemple :

```
avp.com EXPORT RTP c:\settings.dat
```

IMPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de l'instruction :

```
avp.com IMPORT <nom_du_fichier > [/password=< votre_mot_de_passe >
```

La description des paramètres d'exécution de l'instruction est reprise dans le tableau ci-dessous.

<nom_du_fichier>	Chemin d'accès au fichier d'où sont importés les paramètres de Kaspersky PURE. Vous pouvez indiquer un chemin relatif ou absolu.
<votre_mot_de_passe>	Mot de passe pour Kaspersky PURE défini via l'interface de l'application. L'importation des paramètres de la protection est possible uniquement depuis un fichier au format binaire.

N'oubliez pas que l'instruction ne s'exécutera pas sans la saisie du mot de passe.

Exemple :

```
avp.com IMPORT c:\settings.dat /password=<mot de passe>
```

OBTENTION DU FICHIER DE TRACE

La création du fichier de trace s'impose parfois lorsque des problèmes se présentent dans le fonctionnement de Kaspersky PURE. Cela aidera les spécialistes du Support technique à détecter plus précisément les problèmes.

Il est conseillé d'activer la création de ces fichiers uniquement pour le diagnostic d'un problème particulier. L'activation permanente de cette fonction peut entraîner une réduction des performances de l'ordinateur et un débordement du disque dur.

Syntaxe de l'instruction :

```
avp.com TRACE [file] [on|off] [<niveau_de_trace>]
```

La description des paramètres est reprise dans le tableau ci-dessous.

[on|off]	Active/désactive la création d'un fichier de trace.
[file]	Réception de la trace dans un fichier.
<niveau_de_trace>	Pour ce paramètre, il est possible de saisir un chiffre compris entre 0 (niveau minimum, uniquement les événements critiques) et 700 (niveau maximum, tous les messages). Lorsque vous contactez le support technique, l'expert doit vous préciser le niveau qu'il souhaite. Si le niveau n'a pas été indiqué, il est conseillé d'utiliser la valeur 500.

Exemples :

- *Désactiver la constitution de fichiers de trace :*

  ```
  avp.com TRACE file off
  ```

- *Créer un fichier de trace avec le niveau maximum de détails défini à 500 en vue d'un envoi à l'assistance technique :*

  ```
  avp.com TRACE file on 500
  ```

CONSULTATION DE L'AIDE

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

```
avp.com [ /? | HELP ]
```

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

```
avp.com <instruction> /?
avp.com HELP <instruction>
```

CODES DE RETOUR DE LA LIGNE DE COMMANDE

Cette section décrit les codes de retour de la ligne de commande (dans le tableau ci-dessous). Les codes généraux peuvent être renvoyés par n'importe quelle instruction de la ligne de commande. Les codes de retour des tâches concernent les codes généraux et les codes spécifiques à un type de tâche en particulier.

CODES DE RETOUR GENERAUX	
0	Opération réussie
1	Valeur de paramètre invalide
2	Erreur inconnue
3	Erreur d'exécution de la tâche
4	Annulation de l'exécution de la tâche
CODES DE RETOUR DES TACHES D'ANALYSE ANTIVIRUS	
101	Tous les objets dangereux ont été traités
102	Des objets dangereux ont été découverts

LISTE DES NOTIFICATIONS KASPERSKY PURE

Cette rubrique reprend les notifications qui peuvent apparaître à l'écran pendant le fonctionnement de Kaspersky PURE.

DANS CETTE SECTION

La réparation de l'objet est impossible 269

Serveur de mises à jour inaccessible 270

Un objet malveillant a été identifié 270

Un objet dangereux a été découvert dans le trafic 271

Objet suspect détecté 271

Une activité dangereuse a été découverte dans le système 272

Détection de processus cachés 273

Une tentative d'accès à la base de registres système a été découverte 273

Une activité réseau de l'application a été découverte 274

Un nouveau réseau a été découvert 274

Une tentative de phishing a été découverte 275

Lien suspect découvert 275

Découverte d'un certificat incorrect 276

Restriction sur la durée d'utilisation de l'application 276

Une procédure spéciale de réparation est requise 276

Le fichier existe déjà 276

LA REPARATION DE L'OBJET EST IMPOSSIBLE

Dans certains cas, il est impossible de réparer l'objet malveillant. Par exemple, si l'objet est corrompu à un tel point qu'il est impossible d'en supprimer le code malveillant ou de le restaurer. De plus il existe certains types d'objets malicieux comme les chevaux de Troie qui ne peuvent pas être réparés.

Dans ce cas, un message spécial contenant les informations suivantes s'affiche :

- Le type de menace (par exemple : *virus*, *cheval de Troie*) et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet malveillant se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte dans le système.

- Le nom complet de l'objet malveillant et son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Effacer** : supprime l'objet malveillant. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudrait le restaurer ou reproduire le scénario de l'infection.

- **Ignorer** : bloque l'accès à l'objet mais n'exécute aucune action, sauf consigner les informations à son sujet dans le rapport.

  Vous pourrez revenir au traitement des objets malveillants ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche d'analyse antivirus depuis son lancement jusque sa fin.

SERVEUR DE MISES A JOUR INACCESSIBLE

Si un ou plusieurs ordinateurs du réseau utilisés en tant que serveur de mises à jour sont inaccessibles en ce moment, il est impossible de réaliser la mise à jour de Kaspersky PURE. Dans ce cas, la sécurité du réseau est menacée et Kaspersky PURE affiche le message correspondant dans le rapport sur l'état de la protection du réseau.

Pour garantir la sécurité, il faut allumer l'ordinateur qui n'est pas accessible ou désigner une autre source pour les mises à jour.

UN OBJET MALVEILLANT A ETE IDENTIFIE

Lorsque l'Antivirus Fichiers, l'Antivirus Courrier ou une tâche d'analyse découvre un objet malveillant, un message spécial apparaît.

Il indique :

- Le type de menace (par exemple : *virus*, *cheval de Troie*) et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet malveillant se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte dans le système.

- Le nom complet de l'objet malveillant et son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Réparer** : tentative de réparation de l'objet malveillant. Une copie de sauvegarde est créée avant la suppression au cas où il faudrait restaurer l'objet ou le scénario de l'infection.

- **Effacer** : supprime l'objet malveillant. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudrait le restaurer ou reproduire le scénario de l'infection.

- **Ignorer** : bloque l'accès à l'objet mais n'exécute aucune action sur ce dernier. L'application se contente de consigner les informations relatives à l'objet dans le rapport.

  Vous pourrez revenir au traitement des objets malveillants ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

UN OBJET DANGEREUX A ETE DECOUVERT DANS LE TRAFIC

Lorsqu'Antivirus Internet découvre un objet dangereux dans le trafic, un message spécial s'affiche.

Celui-ci contient :

- Le type de menace (par exemple : *modification d'un virus*) et le nom de l'objet dangereux tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte.

- Le nom complet de l'objet dangereux et le chemin vers la ressource Internet.

Vous aurez le choix entre les actions suivantes :

- **Autoriser** : continue à télécharger l'objet.

- **Interdire** : bloque le téléchargement de l'objet depuis le site Internet.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

OBJET SUSPECT DETECTE

Lorsque l'Antivirus Fichiers, l'Antivirus Courrier ou la recherche d'éventuels virus découvre un objet qui contient le code d'un virus inconnu ou le code modifié d'un virus connu, un message spécial s'affiche.

Il indique :

- Le type de menace (par exemple : *virus*, *cheval de Troie*) et le nom de l'objet tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet malveillant se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte dans le système.

- Le nom complet de l'objet et son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Quarantaine** : place l'objet en quarantaine. L'objet placé en quarantaine est déplacé et non pas copié : l'objet est supprimé du disque ou du message et il est enregistré dans le répertoire de quarantaine. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

  Lors des analyses ultérieures de la quarantaine à l'aide de signatures des menaces actualisées, il est possible que l'état de l'objet change. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  > En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son statut après l'analyse ne deviendra pas automatiquement *OK*. Cela se passe uniquement si l'analyse a été réalisée (dans les trois jours maximum) après la mise en quarantaine du fichier.

- **Supprimer** : supprime l'objet. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudra par la suite le restaurer ou reproduire le scénario de l'infection.

- **Ignorer** : bloque l'accès à l'objet mais n'exécute aucune action sur ce dernier. L'application se contente de consigner les informations relatives à l'objet dans le rapport.

Vous pourrez revenir au traitement des objets ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

Si vous êtes convaincu que l'objet découvert n'est pas malveillant, il est conseillé de l'ajouter à la zone de confiance pour éviter tout nouveau déclenchement de l'activation lors d'une prochaine manipulation de cet objet.

UNE ACTIVITE DANGEREUSE A ETE DECOUVERTE DANS LE SYSTEME

Lorsque la Protection proactive découvre une activité dangereuse en provenance d'une application quelconque du système, un message spécial apparaît avec les informations suivantes :

- Nom de la menace, tel qu'il figure dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte.
- Le nom complet du fichier du processus à l'origine de l'activité dangereuse et son chemin d'accès.
- Sélection des actions possibles :
  - **Quarantaine** : arrêter le processus et mettre son fichier exécutable en quarantaine. Un objet qui est mis en quarantaine est déplacé et non pas copié. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

    Lors des analyses ultérieures de la quarantaine à l'aide de signatures des menaces actualisées, il est possible que l'état de l'objet change. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

    En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son statut après l'analyse ne deviendra pas automatiquement *OK*. Cela se passe uniquement si l'analyse a été réalisée (dans les trois jours maximum) après la mise en quarantaine du fichier.

  - **Terminer** : terminer le processus.
  - **Autoriser** : autorise l'exécution du processus.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

Si vous êtes convaincu que l'application découverte ne représente aucun danger, il est conseillé de l'ajouter à la zone de confiance pour éviter un nouveau déclenchement de Kaspersky PURE.

DETECTION DE PROCESSUS CACHES

Lorsque la Défense Proactive découvre un processus caché dans le système, un message spécial s'affiche et fournit les informations suivantes :

- Nom de la menace, tel qu'il figure dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte.
- Le nom complet du processus caché et son chemin d'accès.
- Sélection des actions possibles :
  - **Quarantaine** : place le fichier exécutable du processus en quarantaine. Un objet qui est mis en quarantaine est déplacé et non pas copié. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

    Lors des analyses ultérieures de la quarantaine à l'aide de signatures des menaces actualisées, il est possible que l'état de l'objet change. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

    En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son statut après l'analyse ne deviendra pas automatiquement *OK*. Cela se produira uniquement si l'analyse a eu lieu un certain temps (au moins trois jours) après la mise du fichier en quarantaine.
  - **Terminer** : terminer le processus.
  - **Autoriser** : autorise l'exécution du processus.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

Si vous êtes convaincu que l'application découverte ne représente aucun danger, il est conseillé de l'ajouter à la zone de confiance pour éviter un nouveau déclenchement de Kaspersky PURE.

UNE TENTATIVE D'ACCES A LA BASE DE REGISTRES SYSTEME A ETE DECOUVERTE

Lorsque la Défense Proactive découvre une tentative d'accès aux clés de la base de registres, un message spécial s'affiche et fournit les informations suivantes :

- La clé du registre exposée à la tentative d'accès.
- Le nom complet du fichier du processus à l'origine de la tentative d'accès à la clé du registre et son chemin d'accès.
- Sélection des actions possibles :
  - **Autoriser** : autorise une fois l'exécution de l'action dangereuse ;
  - **Interdire** : bloque une fois l'exécution de l'action dangereuse.

Pour que l'action que vous avez sélectionnée soit exécutée automatiquement chaque fois qu'une telle activité sera lancée sur l'ordinateur, cochez la case **Créer règle**.

Si vous estimez que l'activité de l'application qui a envoyé une requête aux clés de la base de registre système n'est pas dangereuse, ajoutez-la à la liste des applications de confiance.

UNE ACTIVITE RESEAU DE L'APPLICATION A ETE DECOUVERTE

Lors de la détection de l'activité de réseau de l'application (par défaut, pour les applications incluses dans le groupe **Restrictions faibles** ou **Restrictions élevées**) une notification apparaîtra sur votre écran.

La notification s'affichera, si Kaspersky Internet Security fonctionne en mode interactif (cf. section "Sélection du mode de protection" à la page 60), et si aucune règle pour les paquets (cf. page) n'a été créée pour l'application dont l'activité de réseau a été détectée.

La notification contient les informations suivantes :

- Nom de l'application et brève description de la connexion qu'elle établit ;
- Informations sur la connexion (type de connexion, port distant et local, adresse à partir d'où la connexion est établie) ;
- Séquence de lancement de l'application.

Vous aurez le choix entre les actions suivantes :

- **Autoriser maintenant**.
- **Interdire maintenant**.
- **Créer une règle**. Le choix de cette option entraîne l'ouverture de la fenêtre **Pare-feu** qui permet de créer une règle qui régit l'activité de réseau de l'application.

Vous pouvez autoriser ou interdire l'activité de réseau d'une application une fois ou pour une durée plus longue. Pour ce faire, réalisez une des opérations suivantes :

- Pour autoriser ou interdire une fois l'activité de réseau d'une application, choisissez l'action **Autoriser maintenant** ou **Bloquer maintenant**.
- Pour enregistrer l'action sélectionnée pour la durée de la session de fonctionnement de l'application à l'origine de l'activité de réseau, sélectionnez **Autoriser maintenant** ou **Bloquer maintenant**, puis cochez la case **Enregistrer pour la session de l'application**.

  Si la case **Enregistrer pour toujours** apparaît dans la fenêtre, cochez-la, puis cliquez sur **pour toujours** pour changer le texte en **Enregistrer pour la session de l'application**.
- Pour enregistrer l'action sélectionnée pour l'application pour toujours, choisissez l'option **Autoriser maintenant** ou **Bloquer maintenant**, puis cochez la case **Enregistrer pour toujours**.

  Si la case **Enregistrer pour la session de l'application** apparaît dans la fenêtre, cochez-la, puis cliquez sur le lien **pour la session de l'application** afin que le texte devienne **Enregistrer pour toujours**.

UN NOUVEAU RESEAU A ETE DECOUVERT

Chaque fois que l'ordinateur se connecte à une nouvelle zone (réseau), un message spécial s'affiche.

La partie supérieure de ce message reprend une brève description du réseau avec l'adresse IP et le masque de sous-réseau.

La partie inférieure de la fenêtre vous propose d'attribuer un état à la nouvelle zone. Cet état permettra d'autoriser ou non telle ou telle activité de réseau.

- **Réseau public (interdire l'accès à l'ordinateur depuis l'extérieur)**. Ce réseau présente un très grand risque car une fois que l'ordinateur y est connecté, il est exposé à toutes les menaces possibles et imaginables. Cet état doit être sélectionné pour les réseaux qui ne sont protégés par aucun logiciel antivirus, pare-feu, filtre, etc. Ce choix offre la protection maximale de l'ordinateur dans cet environnement.

- **Réseau local (autoriser l'accès aux fichiers et aux imprimantes)**. Cet état est recommandé pour les zones présentant un risque moyen (par exemple, le réseau interne d'une entreprise).

- **Réseau de confiance (autoriser toutes les activités de réseau)**. Cet état doit être réservé aux zones qui, d'après vous, ne présentent aucun danger car l'ordinateur ne risque pas d'être attaqué ou victime d'un accès non autorisé.

UNE TENTATIVE DE PHISHING A ETE DECOUVERTE

Lorsque Kaspersky PURE découvre une tentative d'ouverte d'un site de phishing, un message spécial s'affiche.

Celui-ci contient :

- Le nom de la menace, *attaque de phishing*, sous la forme de lien qui vous renvoie à la description détaillée de la menace dans l'Encyclopédie des virus de Kaspersky Lab.

- L'URL du site de phishing.

- Sélection des actions possibles :

  - **Autoriser** : continue à télécharger le site de phishing.

  - **Interdire** : bloque le téléchargement du site de phishing.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

LIEN SUSPECT DECOUVERT

Lorsque Kaspersky PURE découvre une tentative d'ouverture d'un site Web dont l'adresse figure dans la liste des URL suspectes, il affiche un message spécial.

Celui-ci contient :

- L'URL du site.

- Sélection des actions possibles :

  - **Autoriser** : poursuit le chargement du site Web.

  - **Interdire** : bloque le chargement du site Web.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

DECOUVERTE D'UN CERTIFICAT INCORRECT

L'analyse de la sécurité de la connexion via le protocole SSL aura lieu à l'aide du certificat installé. En cas de tentative de connexion avec le serveur avec un certificat incorrect (par exemple, dans le cas de substitution par les malfaiteurs), un message spécial s'affiche.

L'information sur les causes possibles d'erreur, ainsi que le port et l'adresse à distance s'affichent dans la notification. Vous serez invité à décider de la nécessité d'établir la connexion en cas d'utilisation d'un certificat non valide.

- **Accepter le certificat** : poursuivre la connexion à une ressource en ligne ;
- **Rejeter le certificat** : rompre la connexion à une ressource en ligne ;
- **Consulter le certificat** : profiter de la possibilité de consulter l'information sur le certificat.

RESTRICTION SUR LA DUREE D'UTILISATION DE L'APPLICATION

Si une restriction sur la durée d'utilisation d'une application a été définie dans Mon Contrôle Parental, un message spécial s'affichera à l'issue du temps autorisé.

Le message reprend les informations suivantes :

- Nom de l'application ;
- Le temps restant avant l'arrêt de l'application ou la cause de l'arrêt.

UNE PROCEDURE SPECIALE DE REPARATION EST REQUISE

Suite à la découverte d'une menace active en ce moment dans le système (par exemple, un processus malveillant dans la mémoire vive ou dans les objets de démarrage), un message vous invitant à lancer la procédure de réparation élargie s'affiche.

Les experts de Kaspersky Lab recommandent vivement d'accepter de lancer cette procédure de réparation. Pour ce faire, cliquez sur le bouton **OK**. Toutefois, n'oubliez pas que l'ordinateur sera redémarré à la fin de la procédure et par conséquent, il est conseillé d'enregistrer tous les travaux en cours et de quitter toutes les applications avant de lancer la procédure.

Lors de la procédure de réparation, il est interdit de lancer les clients de messagerie ou de modifier les bases de registres du système d'exploitation. Une fois que l'ordinateur a redémarré, il est conseillé de lancer une analyse complète.

LE FICHIER EXISTE DEJA

Si un fichier portant le même nom existe déjà dans le dossier où va être restauré un fichier depuis la copie de sauvegarde, un message spécial s'affichera.

La partie supérieure de la notification reprend le nom et l'emplacement du fichier.

La partie inférieure de la fenêtre permet de sélectionner le mode de restauration :

- **Remplacer**. Le fichier restauré remplace le fichier existant.
- **Ignorer**. La version actuelle du fichier sera enregistrée.
- **Enregistrer les deux fichiers**. Le fichier restauré recevra un autre nom.

GLOSSAIRE

A

Activation de l'application

L'application devient entièrement fonctionnelle. L'utilisateur doit avoir une licence pour activer l'application.

Analyse du trafic

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

Analyseur heuristique

Technologie d'identification des menaces qui n'ont pas été identifiées à l'aide des bases des applications de Kaspersky Lab. Celle-ci permet d'identifier les objets soupçonnés d'être infectés par un virus inconnu ou par une nouvelle modification d'un virus connu.

L'analyseur heuristique permet d'identifier jusqu'à 92% des nouvelles menaces. Ce mécanisme est assez efficace et entraîne rarement des faux-positifs.

Les fichiers identifiés à l'aide de l'analyseur heuristique sont considérés comme des fichiers suspects.

Application incompatible

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

Archive

Fichier qui contient un ou plusieurs autres objets qui peuvent être des archives.

Attaque virale

Tentatives multiples d'infection virale d'un ordinateur.

B

Base des URL de phishing

Liste des URL de sites identifiés par les experts de Kaspersky Lab comme des sites de phishing. La base est actualisée régulièrement et elle est livrée avec l'application de Kaspersky Lab.

Base des URL suspectes

Liste des URL dont le contenu pourrait constituer une menace. La liste est rédigée par les experts de Kaspersky Lab. Elle est actualisée régulièrement et est livrée avec l'application de Kaspersky Lab.

Bases

Les bases de données sont créées par les experts de Kaspersky Lab et elles contiennent une description détaillée de toutes les menaces informatiques qui existent à l'heure actuelle ainsi que les moyens de les identifier et de les neutraliser. Les bases sont actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouvelles menaces sont découvertes.

Bases de donnees de messagerie

Bases contenant les messages stockés sur votre ordinateur et possédant un format spécifique. Chaque message entrant/sortant est inscrit dans la base de données de messagerie après sa réception/son envoi. Ces bases sont analysées lors de l'analyse complète de l'ordinateur.

Si la protection en temps réel est activée, les messages entrants/sortants sont directement analysés lors de leur réception/envoi.

BLOCAGE D'UN OBJET

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

C

CERTIFICAT DU SERVEUR D'ADMINISTRATION

Certificat qui intervient dans l'authentification du serveur d'administration lors de la connexion à celui-ci de la console d'administration et de l'échange de données avec les postes client. Le certificat du serveur d'administration est créé lors de l'installation du serveur d'administration et il est enregistré dans le sous-répertoire Cert du répertoire d'installation.

COFFRE-FORT

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

L'application Kaspersky PURE doit être installée sur l'ordinateur pour pouvoir utiliser les coffres-forts.

COMPTEUR D'EPIDEMIE DE VIRUS

Modèle qui sert à prévenir les utilisateurs en cas de menace d'épidémie de virus. Le compteur d'épidémie de virus renferme un ensemble de paramètres qui déterminent un seuil d'activité de virus, les modes de diffusions et le texte des messages.

COURRIER INDESIRABLE

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

D

DEGRE D'IMPORTANCE DE L'EVENEMENT

Caractéristique de l'événement consignée dans le fonctionnement de l'application de Kaspersky Lab. Il existe 14 degrés d'importance:

Evénement critique.

Refus de fonctionnement.

Avertissement.

Information.

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

DOSSIER DE SAUVEGARDE

Le stockage spécial est conçu pour l'enregistrement des copies de sauvegarde des objets, créées avant leur première réparation ou suppression.

DUREE DE VALIDITE DE LA LICENCE

Durée pendant laquelle vous pouvez utiliser toutes les fonctions de l'application de Kaspersky Lab. Généralement, la durée de validité d'une licence est d'une année calendrier à partir de la date d'installation. Une fois que la durée de validité est écoulée, les fonctions de l'application sont bloquées : vous ne pourrez plus actualiser les bases de l'application.

E

EN-TETE

L'information, qui est contenue dans le début du fichier ou du message, se compose des données de faibles niveaux selon l'état et le traitement du fichier (message). En particulier, l'en-tête du courrier électronique contient des renseignements, tels que, les données de l'expéditeur, du destinataire et la date.

ETAT DE LA PROTECTION

Etat actuel de la protection caractérisé par le niveau de sécurité de l'ordinateur.

EXCLUSION

Objet exclu de l'analyse de l'application de Kaspersky Lab. Vous pouvez exclure de l'analyse des fichiers d'un format défini, des fichiers selon un masque, certains secteurs (par exemple :un répertoire ou un programme), des processus ou des objets selon un type de menace conforme à la classification de l'encyclopédie des virus. Des exclusions peuvent être définies pour chaque tâche.

F

FAUX-POSITIFS

Situation qui se présente lorsqu'un objet sain est considéré par l'application de Kaspersky Lab comme étant infecté car son code évoque celui d'un virus.

FICHIERS COMPACTE

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

FLUX NTFS ALTERNATIFS

Flux de données du système de fichiers NTFS (alternate data streams), prévus pour contenir des attributs complémentaires ou des informations relatives au fichier.

Chaque fichier dans le système de fichiers NTFS présente un ensemble de flux (streams). Un des flux renferme le contenu du fichier que nous pouvons voir une fois que le fichier a été ouvert. Les autres flux (alternatifs) sont prévus pour les méta-informations et garantissent, par exemple, la compatibilité du système NTFS avec d'autres systèmes tels que l'ancien système de fichiers Macintosh – Hierarchical File System (HFS). Les flux peuvent être créés, supprimés, enregistrés séparément, renommer ou lancer comme processus.

Les flux alternatifs peuvent être exploités par des individus mal intentionnés dans le but de dissimuler l'envoi ou la réception de données de l'ordinateur.

I

INSTALLATION A L'AIDE D'UN SCRIPT D'ENTREE

Méthode d'installation à distance des applications de Kaspersky Lab qui permet d'associer le lancement d'une tâche d'installation à distance à un compte utilisateur particulier (ou pour plusieurs comptes). Lorsque l'utilisateur s'enregistre dans le domaine, une tentative d'installation de l'application sur le poste client d'où s'est connecté l'utilisateur est lancé. Cette méthode est conseillée pour l'installation d'applications sur des ordinateurs tournant sous Microsoft Windows 98/Me.

INTERCEPTEUR

Sous-composant de l'application chargé de l'analyse de certains types de messages électroniques. La sélection d'intercepteurs installés dépend du rôle ou de la combinaison de rôles de l'application.

L

LES SERVEURS DE MISE A JOUR DE KASPERSKY LAB

Liste de serveurs HTTP et FTP de Kaspersky Lab d'où l'application peut récupérer les bases et les mises à jour des modules.

LICENCE COMPLEMENTAIRE

Licence ajoutée pour le fonctionnement de l'application de Kaspersky Lab mais qui n'a pas été activée. La licence complémentaire entre en vigueur lorsque la licence active est arrivée à échéance.

LISTE DES URL ANALYSEES

Liste des masques et des URL soumises obligatoirement à la recherche d'objets malveillants par l'application de Kaspersky Lab.

LISTE DES URL AUTORISEES

Liste des masques et des URL dont l'application de Kaspersky Lab bloque l'accès. La liste des adresses est composée par les utilisateurs lors de la configuration de l'application.

LISTE DES URL DE CONFIANCE

Liste des masques et URL dont le contenu est jugé fiable par l'utilisateur. L'application de Kaspersky Lab ne recherche pas la présence éventuelle d'objets malveillants dans les pages qui correspondent à un élément de la liste.

LISTE DES URL INTERDITES

Liste des masques et des URL dont l'application de Kaspersky Lab bloque l'accès. La liste des adresses est composée par les utilisateurs lors de la configuration de l'application.

LISTE DES EXPEDITEURS AUTORISES

(également liste blanche des adresses)

Liste des adresses électroniques des messages du courrier entrant qui ne seront pas analysés par l'application de Kaspersky Lab.

LISTE DES EXPEDITEURS INTERDITS

(également liste noire des adresses)

Liste des adresses de messagerie électronique bloquées par l'application de Kaspersky Lab, quel que soit le contenu des messages.

LISTE NOIRE DES LICENCES

Base de données contenant des informations relatives aux clés de licence Kaspersky Lab bloquées. Le contenu du fichier avec la liste "noire" est mis à jour en même temps que les bases.

M

MASQUE DE FICHIER

Représentation du nom et de l'extension d'un fichier par des caractères génériques. Les deux caractères principaux utilisés à cette fin sont * et ? (où * représente n'importe quel nombre de n'importe quels caractères et ? représente un caractère unique). A l'aide de ces caractères, il est possible de représenter n'importe quel fichier. Attention! le nom et l'extension d'un fichier sont toujours séparés par un point.

MASQUE DE SOUS-RESEAU

Le masque de sous-réseau et l'adresse réseau permettent d'identifier un ordinateur au sein d'un réseau informatique.

MESSAGE INDECENT

Message électronique contenant un vocabulaire non normatif.

MESSAGE SUSPECT

Message qui ne peut être catégorisé comme indésirable de manière certaine mais dont l'analyse donne lieu à des soupçons (par exemple, certains types d'envois et de messages publicitaires).

MISE EN QUARANTAINE D'OBJETS

Mode de traitement d'un objet potentiellement infecté empêchant tout accès à celui-ci et engendrant son déplacement vers le dossier de quarantaine où il est conservé de manière cryptée afin de prévenir toute action malveillante.

MISE A JOUR

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules logiciels), récupérés des serveurs de mise à jour de Kaspersky Lab.

MISE A JOUR DES BASES

Une des fonctions de l'application de Kaspersky Lab qui permet de garantir l'actualité de la protection. Dans ce scénario, les bases sont copiées depuis les serveurs de mise à jour de Kaspersky Lab sur l'ordinateur et elles sont installées automatiquement.

MISE A JOUR DISPONIBLE

Ensemble de mises à jour des modules de l'application de Kaspersky Lab qui reprend les mises à jour urgentes rassemblées au cours d'un intervalle de temps défini ainsi que les modifications de l'architecture de l'application.

MISE A JOUR URGENTE

Mise à jour critique des modules de l'application de Kaspersky Lab.

MODULES LOGICIELS

Fichiers faisant partie de la distribution de l'application de Kaspersky Lab et responsables de ses principales tâches. Chaque type de tâche réalisée par l'application (Protection en temps réel, Analyse à la demande, Mise à jour) possède son propre module exécutable. En lançant l'analyse complète depuis la fenêtre principale, vous démarrez le module lié à cette tâche.

MODELE DE NOTIFICATION

Modèle utilisé pour signaler la découverte d'objets infectés lors de l'analyse. Le modèle de notification contient un ensemble de paramètres qui définissent l'ordre des notifications, les moyens de diffusion et le texte du message.

N

NIVEAU DE PROTECTION

Le niveau de protection est l'ensemble de paramètres prédéfinis de fonctionnement du composant.

NIVEAU RECOMMANDE

Niveau de protection qui repose sur les paramètres de fonctionnement définis par les experts de Kaspersky Lab et qui garantit la protection optimale de votre ordinateur. Ce niveau de protection est activé par défaut à l'installation.

O

OBJET OLE

Objet uni ou intégré à un autre fichier. L'application de Kaspersky Lab permet de rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Excel dans un document Microsoft Office Word, ce tableau sera analysé comme un objet OLE.

OBJET CONTROLE

Fichier transmis via le protocole HTTP, FTP ou SMTP par le pare-feu et envoyer à l'application de Kaspersky Lab pour analyse.

OBJET DANGEREUX

Objet contenant un virus. Nous vous déconseillons de manipuler de tels objets car ils pourraient infecter votre ordinateur. Suite à la découverte d'un objet infecté, il est conseillé de le réparer à l'aide d'une application de Kaspersky Lab ou de le supprimer si la réparation est impossible.

OBJET INFECTE POTENTIELLEMENT

Objet qui, en raison de son format ou de sa structure, peut être utilisé par un individu mal intentionné en tant que "conteneur" pour abriter et diffuser un objet malveillant. En règle générale, il s'agit d'objets exécutables avec, par exemple, les extensions com, exe, dll, etc. Le risque d'infection par un code malveillant est très élevé pour ces fichiers.

OBJET POTENTIELLEMENT INFECTE

Objet dont le code contient le code modifié d'un virus connu ou un code semblable à celui d'un virus mais inconnu de Kaspersky Lab. Les objets potentiellement infectés sont identifiés à l'aide de l'analyseur heuristique.

OBJET SUSPECT

Objet dont le code contient le code modifié d'un virus connu ou un code semblable à celui d'un virus mais inconnu de Kaspersky Lab. Les objets suspects sont détectés grâce à l'analyseur heuristique.

OBJETS DE DEMARRAGE

Série de programmes indispensables au lancement et au bon fonctionnement du système d'exploitation et des applications installés sur votre ordinateur. Ces objets sont exécutés à chaque démarrage du système d'exploitation. Il existe des virus qui s'attaquent en particulier à ces objets, ce qui peut par exemple provoquer le blocage du système d'exploitation.

P

PAQUET DE MISE A JOUR

Ensemble de fichiers provenant d'Internet et s'installant sur votre ordinateur afin de mettre à jour une application.

PARAMETRES DE L'APPLICATION

Paramètres de fonctionnement de l'application communs à tous les types de tâche, responsables du fonctionnement de l'application dans son ensemble, par exemple les paramètres de performance de l'application, les paramètres de création des rapports, les paramètres de la sauvegarde.

PARAMETRES DE LA TACHE

Paramètres de fonctionnement de l'application propres à chaque type de tâche.

PASSERELLE A DEUX CANAUX

Ordinateur doté de deux cartes de réseau, chacune d'entre elles connectée à un réseau différent et transmettant les informations d'un réseau à l'autre.

PORT DE RESEAU

Paramètre des protocoles TCP et UDP déterminant la destination des paquets de données IP transmis vers l'hôte via le réseau et permettant aux divers programmes utilisés sur ce même hôte de recevoir des données indépendamment les uns des autres. Chaque programme traite les données envoyées sur un port bien défini (en d'autres termes, le programme "écoute" ce port).

Certains ports standards sont destinés aux protocoles réseau les plus courants (par exemple, les serveurs Web réceptionnent généralement les données envoyées via le protocole HTTP sur le port TCP 80). Néanmoins, un programme peut utiliser n'importe quel protocole et n'importe quel port. Valeurs possibles: de 1 à 65535.

PORT ENTREE-SORTIE

Utilisé dans les microprocesseurs (par exemple Intel) lors de l'échange de données avec les périphériques. Le port entrée-sortie est comparé à l'un ou l'autre périphérique et permet aux applications de le contacter pour l'échange de données.

PORT MATERIEL

Connexion pour un périphérique matériel quelconque via un câble ou une fiche (port LPT, port série, USB).

PROCESSUS DE CONFIANCE

Processus d'une application dont les opérations sur les fichiers ne sont pas contrôlées par l'application de Kaspersky Lab dans le cadre de la protection en temps réel. Tous les objets lancés, ouverts ou conservés par un processus de confiance ne sont pas analysés.

PROTECTION EN TEMPS REEL

Mode de fonctionnement pendant lequel l'application analyse en temps réel la présence de code malveillant.

L'application intercepte toutes les tentatives d'ouverture d'un objet en lecture, écriture et exécution et recherche la présence éventuelle de menaces. Les objets sains sont ignorés alors que les objets (potentiellement) malveillants sont traités conformément aux paramètres de la tâche (réparation, suppression, mise en quarantaine).

PROTOCOLE

Ensemble de règles clairement définies et standardisées, régulant l'interaction entre un client et un serveur. Parmi les protocoles les plus connus et les services liés à ceux-ci, on peut noter: HTTP (WWW), FTP et NNTP (news).

PROTOCOLE INTERNET (IP)

Protocole de base du réseau Internet, inchangé depuis son lancement en 1974. Il exécute les opérations principales liées au transfert de données d'un ordinateur à un autre et est à la base de protocoles plus haut niveau tels que le TCP et l'UDP. Il gère la connexion ainsi que la correction d'erreurs. Grâce à des technologies tels que le NAT et le masquerading, il est possible de dissimuler d'importants réseaux privés derrière quelques adresses IP (parfois même derrière une seule adresse). Cela permet de satisfaire la demande sans cesse croissante d'adresses IP dont la plage IPv4 est relativement limitée.

Q

QUARANTAINE

Répertoire défini dans lequel sont placés tous les objets potentiellement infectés découverts pendant l'analyse ou par la protection en temps réel.

R

RESTAURATION

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

REPARATION D'OBJETS

Mode de traitement des objets infectés qui débouche sur la restauration totale ou partielle des données ou sur le constat de l'impossibilité de réparer les objets. La réparation des objets s'opère sur la base des enregistrements des bases. Une partie des données peut être perdue lors de la réparation.

REPARATION D'OBJETS LORS DU REDEMARRAGE

Mode de traitement des objets infectés utilisés par d'autres applications au moment de la réparation. Il consiste à créer une copie de l'objet infecté, à réparer cette copie et à remplacer l'objet original infecté par cette copie lors du redémarrage suivant de l'ordinateur.

S

SOCKS

Protocole de serveur proxy permettant une connexion à deux points entre des ordinateurs du réseau interne et des ordinateurs de réseaux externes.

SCRIPT

Petit programme informatique ou partie indépendante d'un programme (fonction) écrit, en règle générale, pour exécuter une petite tâche particulière. Ils interviennent le plus souvent lors de l'exécution de programmes intégrés à de l'hypertexte. Les scripts sont exécutés, par exemple, lorsque vous ouvrez certains sites Web.

Si la protection en temps réel est activée, l'application surveille l'exécution des scripts, les intercepte et vérifie s'ils contiennent des virus. En fonction des résultats de l'analyse, vous pourrez autoriser ou bloquer l'exécution du script.

SECTEUR D'AMORÇAGE DU DISQUE

Le secteur d'amorçage est un secteur particulier du disque dur de l'ordinateur, d'une disquette ou d'un autre support de stockage informatique. Il contient des informations relatives au système de fichier du disque ainsi qu'un programme de démarrage s'exécutant au lancement du système d'exploitation.

Certains virus, appelés virus de boot ou virus de secteur d'amorçage, s'attaquent aux secteurs d'amorçage des disques. L'application de Kaspersky Lab permet d'analyser les secteurs d'amorçage afin de voir s'ils contiennent des virus et des les réparer en cas d'infection.

SERVEUR PROXY

Service dans les réseaux informatiques qui permet aux clients de réaliser des requêtes indirectes vers d'autres ressources du réseau. Le client se connecte d'abord au serveur proxy et envoi une requête vers une ressource quelconque (par exemple, un fichier) situé sur un autre serveur. Ensuite, le serveur proxy se connecte au serveur indiqué et obtient la ressource demandée ou récupère la ressource dans son cache (si le serveur proxy possède son propre cache). Dans certains cas, la requête du client ou la réponse du serveur peut être modifiée par le serveur proxy à des fins déterminées.

SERVICE DE NOMS DE DOMAINE (DNS)

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

SEUIL D'ACTIVITE VIRALE

Nombre d'événements d'un type donné et générés dans un intervalle de temps déterminé qui, une fois dépassé, permettra à l'application de considérer qu'il y a augmentation de l'activité virale et développement d'un risque d'attaque virale. Ce paramètre est d'une importance capitale en cas d'épidémie de virus car il permet à l'administrateur d'anticiper l'attaque.

SUPPRESSION D'UN MESSAGE

Mode de traitement d'un message électronique considéré comme indésirable. Il se caractérise par la suppression physique du message. Cette méthode est recommandée lorsqu'il ne fait aucun doute que le message est indésirable ou qu'il contient un objet malveillant. Une copie du message supprimé est conservée dans le dossier de sauvegarde (pour autant que cette fonctionnalité ne soit pas désactivée).

SUPPRESSION D'UN OBJET

Mode de traitement de l'objet qui entraîne sa suppression physique de l'endroit où il a été découvert par l'application (disque dur, répertoire, ressource de réseau). Ce mode de traitement est recommandé pour les objets dangereux dont la réparation est impossible pour une raison quelconque.

T

TECHNOLOGIE ICHECKER

Technologie qui permet d'accélérer l'analyse antivirus en excluant les objets qui n'ont pas été modifiés depuis l'analyse antérieure pour autant que les paramètres de l'analyse (bases antivirus et paramètres) n'aient pas été modifiés. Ces informations sont conservées dans une base spéciale. La technologie est appliquée aussi bien pendant la protection en temps réel que dans les analyses à la demande.

Admettons que vous possédez une archive qui a été analysée par une application de Kaspersky Lab et qui a reçu l'état sain. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases antivirus, l'archive sera analysée à nouveau.

Limitations technologiques d'iChecker :

la technologie ne fonctionne pas avec les fichiers de grande taille car dans ce cas il est plus rapide d'analyser tout le fichier que de vérifier s'il a été modifié depuis la dernière analyse ;

la technologie est compatible avec un nombre restreint de formats (exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

TACHE

Fonctions exécutées par l'application de Kaspersky Lab sous la forme d'une tâche, par exemple : Protection en temps réel des fichiers, Analyse complète de l'ordinateur, Mise à jour des bases.

V

VIRUS DE BOOT (AMORÇAGE)

Virus affectant les secteurs d'amorçage du disque de l'ordinateur. Au redémarrage du système, le virus force le système à inscrire en mémoire et à exécuter du code malveillant au lieu du code d'amorçage original.

VIRUS INCONNU

Nouveau virus pour lequel aucune information ne figure dans les bases. En règle générale, les virus inconnus sont découverts dans les objets à l'aide de l'analyse heuristique et ces objets reçoivent l'état potentiellement infecté.

KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, dans les pays du Benelux, en Chine, en Pologne, en Roumanie et aux États-Unis (Californie). Un nouveau service de la compagnie, le centre européen de recherches anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les experts principaux de Kaspersky Lab siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Grâce à l'analyse en continu de l'activité virale, nous pouvons prévoir les tendances dans le développement des programmes malveillants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Grâce à des années de travail assidu, la société est devenue leader en développement de systèmes de défense antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Antivirus : il assure la protection de tous les objets qui peuvent être pris pour cible par les virus, à savoir les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux d'entreprise. De nombreux fabricants reconnus utilisent le moteur antivirus de Kaspersky Anti-Virus : Nokia ICG (États-Unis), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui répondent à la moindre de leurs attentes. Nous élaborons, mettons en ouvre et accompagnons les dispositifs de protection antivirale pour entreprise. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez une réponse complète à vos questions.

Site Web de Kaspersky Lab :	http://www.kaspersky.com/fr
L'Encyclopédie des virus :	http://www.securelist.com/fr/
Laboratoire antivirus :	newvirus@kaspersky.com (envoi uniquement d'objets suspects sous forme d'archive) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr (pour les questions aux experts antivirus)
Forum de Kaspersky Lab :	http://forum.kaspersky.fr

INFORMATIONS SUR LE CODE TIERS

Du code développé par des éditeurs tiers a été utilisé pour créer l'application.

DANS CETTE SECTION

Code d'application 287

Autres informations 311

CODE D'APPLICATION

Informations sur le code tiers d'application développé par des éditeurs tiers a été utilisé pour créer l'application.

DANS CETTE SECTION

AGG (ANTI-GRAIN GEOMETRY) 2.4 289

BISON PARSER SKELETON 2.3 289

BOOST 1.30.0, 1.39.0, 1.43.0 290

BZIP2/LIBBZIP2 1.0.5 290

EXPAT 1.2, 2.0.1 290

FASTSCRIPT 1.9 290

GECKO SDK 1.8 290

INFO-ZIP 5.51 290

LIBJPEG 6B 291

LIBNKFM 2.0.5 292

LIBPNG 1.2.8, 1.2.29 292

LIBSPF2 1.2.9 292

LIBUNGIF 3.0 293

LIBXDR 293

NDIS INTERMEDIATE MINIPORTDRIVER SAMPLE 294

NDIS SAMPLE NDIS LIGHTWEIGHT FILTER DRIVER 294

NETWORK CONFIGURATION SAMPLE 294

OPENSSL 0.9.8D 294

PCRE 3.0, 7.4, 7.7 295

PROTOCOL BUFFER 296

QT 4.6.1 297

RFC1321-BASED (RSA-FREE) MD5 LIBRARY 302

TINICONV 1.0.0 302

WINDOWS TEMPLATE LIBRARY 7.5 308

WINDOWS TEMPLATE LIBRARY 8.0 310

ZLIB 1.2, 1.2.2 310

AGG (ANTI-GRAIN GEOMETRY) 2.4

Copyright (C) 2002-2005, Maxim Shemanarev

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BISON PARSER SKELETON 2.3

Copyright (C) GNU Project

---

http://ftp.gnu.org/gnu/bison/

As a special exception, you may create a larger work that containspart or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

BOOST 1.30.0, 1.39.0, 1.43.0

Copyright (C) Beman Dawes

BZIP2/LIBBZIP2 1.0.5

Copyright (C) 1996-2007, Julian R Seward

EXPAT 1.2, 2.0.1

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

FASTSCRIPT 1.9

Copyright (C) Fast Reports Inc

GECKO SDK 1.8

Copyright (C) Mozilla Foundation

---

http://www.mozilla.org/MPL/MPL-1.1.html

INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip, "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

LIBJPEG 6B

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

LIBNKFM 2.0.5

Copyright (C) KUBO Takehiro

LIBPNG 1.2.8, 1.2.29

Copyright (C) 2004, 2006-2008, Glenn Randers-Pehrson

LIBSPF2 1.2.9

Copyright (C) 2005, Shevek and Wayne Schlitt

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBUNGIF 3.0

Copyright (C) 1997, Eric S. Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBXDR

Copyright (C) Sun Microsystems, Inc

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

NDIS INTERMEDIATE MINIPORTDRIVER SAMPLE

Copyright (C) 1992-2000, Microsoft Corporation

NDIS SAMPLE NDIS LIGHTWEIGHT FILTER DRIVER

Copyright (C) 2004-2005, Microsoft Corporation

NETWORK CONFIGURATION SAMPLE

Copyright (C) 1997, Microsoft Corporation

OPENSSL 0.9.8D

Copyright (C) 1998-2007, The OpenSSL Project

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:"This product includes cryptographic software written byEric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence

[including the GNU Public Licence.]

PCRE 3.0, 7.4, 7.7

Copyright (C) University of Cambridge

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PROTOCOL BUFFER

Copyright (C) 2008, Google Inc

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

QT 4.6.1

Copyright (C) 2009, Nokia Corporation and/or its subsidiary(-ies)

GNU LESSER GENERAL PUBLIC LICENSE v.2.1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more

frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright

notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the

Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

RFC1321-BASED (RSA-FREE) MD5 LIBRARY

Copyright (C) 1999, 2002, Aladdin Enterprises

TINICONV 1.0.0

Copyright (C) Free Software Foundation, Inc

----

http://sourceforge.net/projects/tiniconv/

GNU LESSER GENERAL PUBLIC LICENSE v.2.1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work

containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

WINDOWS TEMPLATE LIBRARY 7.5

Copyright (C) 2005, Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

WINDOWS TEMPLATE LIBRARY 8.0

Copyright (C) Microsoft Corporation

ZLIB 1.2, 1.2.2

Copyright (C) Jean-loup Gailly and Mark Adler

AUTRES INFORMATIONS

Informations supplémentaire sur le code tiers.

La bibliothèque du programme "Agava-C", développée par OOO "R-Alpha", est utilisée pour vérifier une signature numérique.

Le Logiciel peut comprendre des programmes concédés à l'utilisateur sous licence (ou sous-licence) dans le cadre d'une licence publique générale GNU (General Public License, GPL) ou d'autres licences de logiciel gratuites semblables, qui entre autres droits, autorisent l'utilisateur à copier, modifier et redistribuer certains programmes, ou des portions de ceux-ci, et à accéder au code source ("Logiciel libre"). Si une licence prévoit l'octroi du code source à l'utilisateur qui a reçu l'application sous la forme d'un fichier exécutable binaire, ce code sera fourni sur demande envoyée à l'adresse source@kaspersky.com ou accompagne le logiciel.

INDEX

A

Anti-bannière
liste "blanche" 137
liste des adresses de bannières autorisées 137
Anti-Spam
extension Microsoft Office Outlook 134
extension Microsoft Outlook Express 134
extension The Bat! 135
extension Thunderbird 136
filtrage des messages sur le serveur 132
liste des expéditeurs autorisés 128
liste des expressions autorisées 126

C

Catégories de menaces à identifier 229
Contrôle des Applications
héritage des restrictions 144
règles du Contrôle des Applications 142
Création d'un raccourci
environnement protégé 165

E

Environnement protégé
création d'un raccourci 165
sélection du mode 165

G

Gestionnaire de messages
Anti-Spam 132

H

Héritage des restrictions
Contrôle des Applications 144

L

Licence
contrat de licence 40

M

Mes Coffres-forts
ajout de fichiers à un coffre-fort 189
configuration des paramètres du coffre-fort 189
création d'un coffre-fort 187
création et connexion d'un coffre-fort 188
Mes Outils d'optimisation
configuration du navigateur 240
l'Assistant de suppression des traces d'activités 237
nettoyage du disque 238
suppression permanente des données 236
Mes Sauvegardes
consultation des données de la copie de sauvegarde 175
consultation du rapport sur les événements 176
création de l'espace de sauvegarde 170
création d'une tâche de copie de sauvegarde 172

exécution de la tâche de copie de sauvegarde....173
purge de l'espace de sauvegarde....171
recherche des copies de sauvegarde....174
restauration des données....173
sélection de l'espace de sauvegarde....171
suppression de l'espace de sauvegarde....172
Mise à jour
annulation de la dernière mise à jour....97
depuis un répertoire local....96
paramètres régionaux....95
selon la programmation....96
serveur proxy....98
source des mises à jour....95
Mise à jour de l'application....93
Mon Contrôle Parental
activation et configuration des paramètres....178
communication à l'aide de clients de messagerie instantanée....182
envoi de données personnelles....185
exportation/importation des paramètres....179
lancement des applications et des jeux....180
mode de recherche sécurisée....182
recherche de mots clés....185
restriction de l'utilisation de l'ordinateur....180
restriction temporelle de l'utilisation de l'Internet....181
téléchargement....181
visite de sites Web....181
Mon Gestionnaire de mots de passe
accès à la base de mots de passe....198
algorithme de cryptage....219
bouton de lancement rapide....223
Compte....200
données personnelles....207
générateur de mots de passe....225
groupe de Comptes....205
identifiant....205
identité....206
importation / exportation de mots de passe....209
lancement rapide de fonctions....216
modification du Mot de passe principal....221
recherche de mots de passe....208
version portable....226
Mon Réseau
administration de Mon Contrôle Parental....194
administration des composants de la protection....193
administration des licences....195
analyse de la sécurité de réseau....68
configuration de l'administration à distance....191
mes Sauvegardes....194
mise à jour....192
recherche de virus et de vulnérabilités....192

P

Pare-feu
Assistant de création d'une règle....153
extension de la plage d'adresses du réseau....152
Prévention des intrusions
types d'attaques de réseau identifiées....155

R

Rapports....241
Règles du Contrôle des Applications
Contrôle des Applications....142

S

Sélection du mode
environnement protégé.....165