Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG Standard Edition

MANUEL D'ADMINISTRATEUR

VERSION DE L'APPLICATION: 8.0

Chers utilisateurs !

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

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

Date d'édition du document : 15.10.2010

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

TABLE DES MATIÈRES

DISPONIBILITE

Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG Standard Edition (par la suite, Kaspersky Anti-Virus) est disponible chez nos distributeurs ainsi que dans notre boutique en ligne (par exemple, http://www.kaspersky.ru, rubrique "Boutique en ligne"). Kaspersky Anti-Virus fait partie de Kaspersky Total Space Security (http://www.kaspersky.com/fr/total_space_security) et de Kaspersky Security for Internet Gateway (http://www.kaspersky.com/fr/kaspersky_security_internet_gateway). Une fois que vous aurez acheté la licence pour Kaspersky Anti-Virus, vous recevrez par courrier électronique un lien d'où vous pourrez télécharger l'application depuis le site de la société ainsi qu'un fichier de licence pour l'activation de la licence.

DANS CETTE SECTION DE L'AIDE

CONTRAT DE LICENCE

Le contrat de licence est l'accord légal conclu entre vous et Kaspersky Lab qui précise les conditions d'utilisation du logiciel que vous venez d'acquérir.

Lisez attentivement le contrat de licence !

Si vous n'acceptez pas les dispositions du contrat de licence, vous pouvez refuser d'utiliser l'application et vous serez remboursé.

SERVICES POUR LES UTILISATEURS ENREGISTRES

Kaspersky Lab offre à ses utilisateurs légitimes un vaste éventail de services qui leur permettent d'accroître l'efficacité de l'utilisation de l'application.

En obtenant une licence, vous devenez un utilisateur enregistré et vous pouvez bénéficier des services suivants pendant la durée de validité de la licence :

- Mise à jour toutes les heures des bases de l'application et accès aux nouvelles versions de ce logiciel ;
- Consultation par téléphone ou courrier électronique sur des questions liées à l'installation, à la configuration et à l'exploitation du logiciel ;
- Notifications de la sortie de nouveaux logiciels de Kaspersky Lab ou de 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/).

Aucune aide n'est octroyée pour les questions relatives au fonctionnement et à l'utilisation des systèmes d'exploitation, de logiciels tiers ou de diverses technologies.

KASPERSKY ANTI-VIRUS 8.0 FOR MICROSOFT ISA SERVER AND FOREFRONT TMG STANDARD EDITION

Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG Standard Edition protège tous les employés de la société exposés au trafic qui transite via le pare-feu en bloquant automatiquement les objets malveillants et potentiellement malveillants dans le flux de données des protocoles HTTP, FTP, SMTP et POP3.

DANS CETTE SECTION DE L'AIDE

PRINCIPALES FONCTIONNALITÉS DE L'APPLICATION

Kaspersky Anti-Virus offre les fonctionnalités suivantes :

- Analyse en temps réel du trafic des protocoles HTTP, FTP, SMTP et POP3.
- Analyse du trafic entrant du protocole HTTPS (uniquement pour Forefront TMG).
- Large choix de paramètres de filtrage du trafic avec utilisation de groupe d'entitées réseau et de règles d'analyse.
- Maintien de l'actualité de la protection grâce à la mise à jour à intervalle régulier des bases de Kaspersky Anti-Virus.
- Identification des riskwares.
- Contrôle en temps réel du fonctionnement de Kaspersky Anti-Virus.
- Obtention d'informations sur le fonctionnement de Kaspersky Anti-Virus grâce aux rapports intégrés.
- Conservation des copies des objets bloqués dans la sauvegarde.
- Configuration détaillée des performances de l'analyse antivirus en fonction de la puissance du serveur et de la bande passante du canal Internet.
- Répartition de la charge entre les processeurs du serveur.
- Administration à distance de Kaspersky Anti-Virus à l'aide de la console d'administration qui se présente sous la forme d'un composant logiciel enfichable de console.

CONFIGURATIONS LOGICIELLE ET MATERIELLE

La configuration logicielle de l'ordinateur sur lequel Kaspersky Anti-Virus est installée:

1. Tout système d'exploitation parmi ceux énumérés ci-après :

- Pour utiliser Kaspersky Anti-Virus avec Microsoft ISA Server 2006 Standard Edition :
  - Microsoft Windows Server 2003 SP2.
  - Microsoft Windows Server 2003 R2.
- Pour utiliser Kaspersky Anti-Virus avec Forefront TMG Standard Edition :
  - Microsoft Windows Server x64 2008 SP2.
  - Microsoft Windows Server x64 2008 R2.

2. Microsoft Management Console 3,0.
3. Microsoft .NET Framework 3,5 SP1.
4. Microsoft ISA Server 2006 Standard Edition/ Forefront TMG Standard Edition Console.

Lors de l'utilisation de Kaspersky Anti-Virus avec Microsoft ISA Server 2006 Enterprise Edition ou Forefront TMG Enterprise Edition, l'exécution des conditions suivantes est requise :

- Uniquement un seul massif doit être utilisé dans la configuration corporative ;
- Le massif doit contenir uniquement un seul serveur ;
- Le stockage de la configuration doit être installé sur le même serveur que Kaspersky Anti-Virus.

Dans le cas de la connexion du serveur isolé Forefront TMG Enterprise Edition au massif autonome (standalone) ou corporatif (EMS-managed), Kaspersky Anti-Virus perd son fonctionnement ; avec cela, la possibilité de supprimer l'antivirus à l'aide des moyens standards du système d'exploitation sera perdue. La suppression du serveur depuis le massif ne va pas aider à rétablir ni à supprimer correctement Kaspersky Anti-Virus.

Un tel schéma du fonctionnement est spécifié par les particularités techniques de réalisation Forefront TMG Enterprise Edition.

Configuration logicielle de l'ordinateur sur lequel la Kaspersky Anti-Virus de gestion est installée :

1. Pour utiliser Kaspersky Anti-Virus avec Microsoft ISA Server 2006 Standard Edition :
   - Processeur 1 GHz ;
   - 1 Go de mémoire vive ;
   - 2.5 Go d'espace libre sur le disque dur.
2. Pour utiliser Kaspersky Anti-Virus avec Forefront TMG Standard Edition :
   - Processeur 64 bits, dual-core ;
   - 2 Go de mémoire vive ;
   - 2.5 Go d'espace libre sur le disque dur.

Configuration logicielle de l'ordinateur sur lequel la Console de gestion est installée :

1. Tout système d'exploitation parmi ceux énumérés ci-après :
   - Microsoft Windows 7 x64 Professional / Enterprise / Ultimate Edition ;
   - Microsoft Windows 7 Professional / Enterprise / Ultimate Edition ;

- Microsoft Windows Server 2008 x64 Enterprise / Standard Edition ;
- Microsoft Windows Server 2008;
- Microsoft Windows Server 2003 x64 R2 Enterprise / Standard Edition ;
- Microsoft Windows Server 2003 x64 Enterprise / Standard Edition ;
- Microsoft Windows Server 2003 x64 SP2 ;
- Microsoft Windows Server 2003 SP2 ;
- Microsoft Windows Vista x64 ;
- Microsoft Windows Vista.

2. Microsoft Management Console 3,0.
3. Microsoft .NET Framework 3.5 SP1.
4. Microsoft ISA Server 2006 Standard Edition/ Forefront TMG Standard Edition Console.

Configuration matérielle de l'ordinateur sur lequel la Console de gestion est installée :

- Processeur 1 GHz ;
- 1 Go de mémoire vive.

ARCHITECTURE DE L'APPLICATION

Kaspersky Anti-Virus est installé sur un serveur Microsoft ISA Server / Forefront TMG et protèges les ordinateurs clients contre les objets malveillants en interceptant le trafic qui transite sur Microsoft ISA Server / Forefront TMG via les protocoles HTTP, FTP, SMTP et POP3.

S'agissant de Forefront TMG, il est possible également d'analyser le trafic entrant via le protocole HTTPS. Il n'y a pas de configuration spéciale pour l'analyse du trafic HTTPS. Les paramètres d'analyse du protocole HTTP sont appliqués. Pour que Kaspersky Anti-Virus puisse analyser le trafic HTTPS, il faut activer l'inspection du trafic dans la console d'administration Forefront TMG (cf. rubrique "Activation de l'inspection du trafic HTTPS" à la page 66).

Kaspersky Anti-Virus comprend les composants suivants :

- **Filtres de Kaspersky Anti-Virus** : le composant est intégré à Microsoft ISA Server/Forefront TMG lors de l'installation. Les filtres suivants sont proposés :
  - Web : intercepte le trafic entrant du protocole HTTP ;
  - FTP : intercepte le trafic entrant du protocole FTP ;
  - SMTP : intercepte le trafic entrant et sortant du protocole SMTP ;
  - POP3 : intercepte le trafic entrant et sortant du protocole POP3.

  Les filtres interceptent le trafic du protocole indiqué, téléchargent les objets sollicités par les ordinateurs clients et dirigent l'objet téléchargé vers le sous-système d'analyse. Les filtres transmettent les objets téléchargés aux ordinateurs clients après l'analyse ou envoient une notification sur le blocage de l'objet.
- **Moteur d'analyse** : ce composant est chargé de la recherche d'éventuels virus dans les objets. Les filtres de Kaspersky Anti-Virus transmettent les objets téléchargés au moteur d'analyse afin d'identifier d'éventuels virus. Lors de cette opération, le moteur compare les signatures des objets aux entrées des bases de Kaspersky Anti-Virus. Il utilise également l'analyseur heuristique pour identifier les virus toujours inconnus. Chaque objet reçoit un état à l'issue de l'analyse. Cet état détermine la suite des opérations. Avant de bloquer n'importe quel objet ou d'y introduire des modifications, il est possible d'en créer une copie de sauvegarde afin de pouvoir rétablir son état initial, le cas échéant. Les informations relatives aux objets analysés sont conservées dans une base de données utilisées par les modules de contrôle et de création de rapports.
- **Module de mises à jour** : ce composant est chargé de la mise à jour des bases de Kaspersky Anti-Virus. Il les télécharge depuis les serveurs de mise à jour de Kaspersky Lab ou depuis d'autres sources définies par l'utilisateur. La recherche de nouvelles bases et le téléchargement de celles-ci peuvent avoir lieu automatiquement selon un programme défini ou manuellement.
- **Sauvegarde** : base de données sur l'ordinateur doté de tous les modules de Kaspersky Anti-Virus qui contient les copies des objets dangereux réalisées avant le traitement ainsi que les informations sur les objets. Les objets sont conservés sous un format spécial et ne présentent aucun danger pour l'ordinateur de l'utilisateur. Les objets de la sauvegarde pourront être restaurés ultérieurement ou supprimés.
- **Rapports** : ce composant permet de créer des rapports sur les résultats de la protection. Les informations sont obtenues selon un programme défini ou à la demande (création manuelle des rapports).
- **Protection en temps réel** : composant prévu pour l'affichage en temps réel des informations relatives de l'état de l'application : description des fonctionnalités de l'application, état du fonctionnement des filtres et du sous-système d'analyse. De plus, le contrôle permet de consulter des données statistiques sur les objets analysés.
- **Diagnostic** : ce composant est responsable des journaux de fonctionnement de tous les composants de l'application. Les informations sont consignées dans des fichiers texte.
- **Console d'administration** : application distincte qui permet d'administrer et de contrôler le fonctionnement de Kaspersky Anti-Virus. La console d'administration doit être installée sur un ordinateur doté de Microsoft ISA

Server / Forefront TMG ou sur un ordinateur distinct qui a accès au serveur. Toutefois, lorsque plusieurs administrateurs travaillent simultanément, il est possible d'installer la console d'administration sur l'ordinateur de chaque administrateur.

Voici une représentation schématique du fonctionnement de l'application (cf. illustration ci-dessous) : .

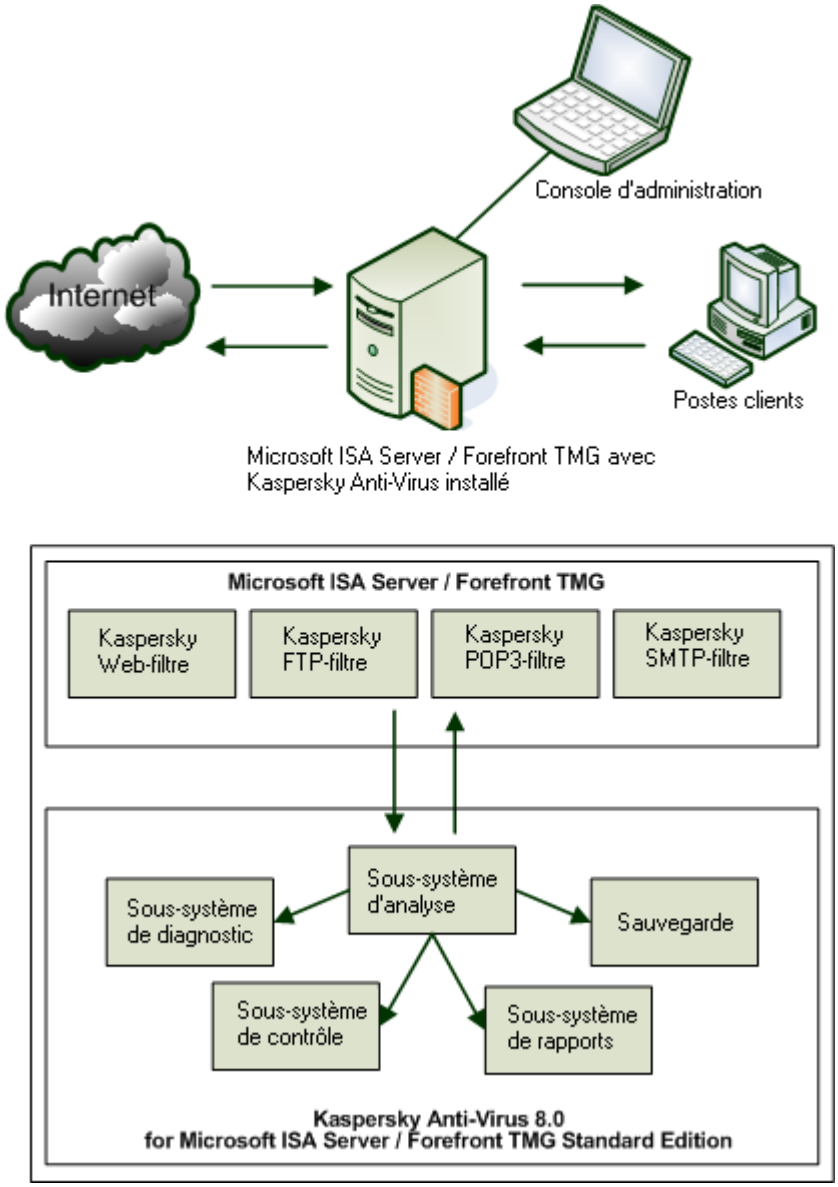

Illustration 1. Schéma de fonctionnement de l'application

DEPLOIEMENT DE LA PROTECTION DES POSTES CLIENTS

Afin de mettre en place un système de protection des ordinateurs clients du réseau contre les programmes malveillants, procédez comme suit :

1. Installez Kaspersky Anti-Virus sur le serveur Microsoft ISA Server / Forefront TMG.
2. Connectez la console d'administration au serveur (cf. rubrique "Connexion de la console d'administration au serveur" à la page 29).
3. Installez la licence (cf. rubrique "Activation de l'application" à la page 22).
4. Configurez le système de protection :
   - Définissez les paramètres de la mise à jour des bases (à la page 33).
   - Configurez les paramètres de l'analyse antivirus (cf. rubrique "Analyse antivirus" à la page 38).
   - Configurez les stratégies de traitement des objets (cf. rubrique "Stratégies de l'analyse antivirus" à la page 42).
   - Configurez les paramètres de fonctionnement des journaux des événements (cf. rubrique "Diagnostic" à la page 63).
5. Vérifiez l'exactitude de la configuration des paramètres et le bon fonctionnement de l'application à l'aide du virus de test EICAR (cf. rubrique "Contrôle de l'exactitude de la configuration de l'application" à la page 30).

La protection du serveur contre les programmes malveillants sera activée automatiquement au démarrage de Microsoft ISA Server / Forefront TMG.

Pour garantir la protection du trafic des postes clients, les mesures suivantes sont prévues :

- la mise à jour à intervalle régulier des bases de Kaspersky Anti-Virus (cf. rubrique "Mise à jour des bases" à la page 33) ;
- le contrôle du fonctionnement de Kaspersky Anti-Virus (cf. rubrique "Contrôle du fonctionnement de l'application" à la page 55) ;
- la vérification à intervalle régulier des rapports sur le fonctionnement de l'application (cf. rubrique "Rapports" à la page 51) ;
- le traitement des notifications ;
- le traitement et la purge de la sauvegarde (cf. rubrique "Sauvegarde" à la page 58).

INSTALLATION DE L'APPLICATION

L'installation de Kaspersky Anti-Virus s'opère à l'aide d'un Assistant d'installation (cf. rubrique "Procédure d'installation de l'application" à la page 13). Avant de commencer, il est conseillé de lire les informations relatives aux préparatifs de l'installation (cf. rubrique "Préparatifs pour l'installation de l'application" à la page 13).

DANS CETTE SECTION DE L'AIDE

PREPARATIONS DE L'INSTALLATION DE L'APPLICATION

Avant d'installer Kaspersky Anti-Virus, assurez-vous que le système répond complètement à la configuration matérielle et logicielle requise (cf. rubrique "Configurations logicielle et matérielle" à la page 7). Assurez-vous également que le compte utilisateur sous lequel vous accédez au système possède les autorisations d'écriture dans la configuration de Microsoft ISA Server/Forefront TMG.

MISE A JOUR DE LA VERSION ANTERIEURE DE L'APPLICATION

La mise à jour depuis la version antérieure de l'application n'est pas prévue. Si l'une des versions précédentes est installée sur votre ordinateur, désinstallez-la avant d'installer la nouvelle version.

PROCEDURE D'INSTALLATION DE L'APPLICATION

Pour installer Kaspersky Anti-Virus sur votre ordinateur, lancez le fichier exécutable repris dans la distribution. Si le déploiement a lieu dans un système d'exploitation qui pratique le contrôle des comptes utilisateur (User Account Control, UAC), il faudra exécuter le fichier sous les privilèges d'administrateur.

Le programme d'installation se présente sous la forme d'un Assistant. Chaque fenêtre contient plusieurs boutons pour contrôler la procédure :

- **Suivant** : confirme l'action et passe au point suivant dans le processus d'installation ;

- **Précédent** : revient à l'étape antérieure de l'installation ;
- **Annuler** : interrompt l'installation ;
- **Installer** : lance la copie des fichiers sur le disque dur et l'enregistrement des composants de l'application ;
- **Terminer** : termine la procédure d'installation de l'application.

Examinons en détail chacune des étapes de la procédure d'installation de l'application.

DANS CETTE SECTION DE L'AIDE

ETAPE 1. VERIFICATION DU RESPECT DES CONDITIONS REQUISES POUR L'INSTALLATION DE KASPERSKY ANTI-VIRUS

Lors de la première étape de l'installation, l'Assistant vérifie si le système d'exploitation et les services packs installés répondent à la configuration logicielle requise pour l'installation de Kaspersky Anti-Virus. L'Assistant vérifie également si les applications indispensables au fonctionnement de Kaspersky Anti-Virus sont installées sur l'ordinateur. L'Assistant d'installation vérifie si Microsoft ISA Server / Forefront TMG est installé sur l'ordinateur et lance les services Microsoft ISA Server Control (isactrl) et Microsoft ISA Server Storage (isastg), au cas où ils seraient installés, mais pas exécutés.

Si une des conditions n'est pas remplie, une notification s'affiche. Avant d'installer Kaspersky Anti-Virus, il est conseillé d'installer les mises à jour requises via le service Windows Update, ainsi que les programmes indispensables.

ETAPE 2. ACCUEIL DE L'ASSISTANT D'INSTALLATION

Si votre système répond complètement aux conditions, la fenêtre d'accueil de l'Assistant s'ouvre après l'exécution du fichier d'installation. Elle présente des informations sur le début de l'installation de Kaspersky Anti-Virus sur l'ordinateur. Cliquez sur **Suivant** pour poursuivre l'installation. Cliquez sur **Annuler** pour quitter le programme d'installation.

ETAPE 3. EXAMEN DU CONTRAT DE LICENCE

La fenêtre suivante d'installation de l'application présente le contrat de licence conclu entre vous et Kaspersky Lab. Lisez-le attentivement. Si vous en acceptez tous les points, cochez la case **J'accepte les termes du contrat de licence**, puis cliquez sur **Suivant**. L'installation passera à l'étape suivante.

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

ETAPE 4. SELECTION DU TYPE D'INSTALLATION

Cette étape correspond à la sélection du type d'installation de l'application. Deux options s'offrent à vous :

- **Complet**. Sélectionnez cette option pour installer tous les composants de l'application. Dans ce cas, les composants de Kaspersky Anti-Virus, intégrés au serveur Microsoft ISA Server / Forefront TMG, et la console d'administration seront installés. Cette option est accessible uniquement si Microsoft ISA Server / Forefront TMG est installé sur l'ordinateur sur lequel l'Assistant d'installation est lancé.

- **Console d'administration**. Sélectionnez cette option si vous devez installer uniquement la console d'administration sans les composants de Kaspersky Anti-Virus intégrés au serveur Microsoft ISA Server/Forefront TMG. Cette option est pratique pour installer sur l'ordinateur local les outils d'administration de Kaspersky Anti-Virus installé sur un ordinateur distant.

Pour sélectionner le type d'installation, cliquez sur le mode souhaité.

ETAPE 5. L'INSTALLATION PERSONNALISEE

Si vous aviez choisi l'option **Complet** à l'étape précédente, la fenêtre **Installation personnalisée** reprendra automatiquement tous les composants de l'application à installer sur le disque dur local.

L'arborescence des composants propose les nœuds suivants :

- **Service** : nœud contenant des informations sur les composants de Kaspersky Anti-Virus chargés de la protection des données transmises via Microsoft ISA Server / Forefront TMG. Pour que la protection fonctionne, il faut intégrer à Microsoft ISA Server / Forefront TMG les filtres d'interception des données transmises via les différents protocoles. Sélectionnez un ou plusieurs filtres dans le composant **Service**.

- **Filtres** : permet de choisir les filtres de Kaspersky Anti-Virus à installer. Vous avez le choix entre les filtres suivants :

  - **Web** : le filtre intercepte le trafic transmis via le protocole HTTP ;

  - **FTP** : le filtre intercepte le trafic transmis via le protocole FTP ;

  - **SMTP** : le filtre intercepte le trafic transmis via le protocole SMTP ;

  - **POP3** : le filtre intercepte le trafic transmis via le protocole POP3.

- **Console d'administration** : le nœud permet d'installer le composant logiciel enfichable de la console d'administration pour administrer Kaspersky Anti-Virus.

> La console d'administration est une partie essentielle du bon fonctionnement de l'application et elle est installée quelle que soit la sélection du type d'installation. Il est impossible d'installer Kaspersky Anti-Virus sans la console d'administration.

Pour choisir le dossier d'installation des composants sélectionnés, procédez comme suit :

1. Choisissez le nœud racine de l'arborescence des composants **Tous les composants**.

2. Cliquez sur **Parcourir** pour ouvrir la fenêtre de modification du dossier d'installation.

3. Dans le champ **Nom du dossier**, saisissez le chemin d'accès au dossier où les composants sélectionnés devront être installés. L'application doit être installée sur le même disque que Microsoft ISA Server / Forefront TMG.

4. Cliquez sur **OK**.

Vous pouvez obtenir les informations relatives à l'espace disque nécessaire pour l'installation d'un composant en particulier en sélectionnant ce-dernier dans l'arborescence. La partie droite de la fenêtre de l'Assistant d'installation affichera les informations relatives à l'espace requis ainsi qu'une brève description du rôle du composant sélectionné.

Pour consulter les informations détaillées sur l'espace disponible sur les disques logiques de votre ordinateur, procédez comme suit :

1. Cliquez sur le bouton **Disques**.
2. Les informations seront reprises dans la fenêtre **Espace disque requis**.
3. Pour fermer la fenêtre, cliquez sur **OK**.

Pour sélectionner un composant en vue de son installation, procédez comme suit :

1. Ouvrez le menu du nœud du composant en cliquant sur le bouton gauche de la souris.
2. Sélectionnez l'option **Sera installé en vue d'une exécution depuis le disque dur** ou **Tous les composants**.

   Si vous choisissez l'option **Tous les composants**, le composant et tous ses sous-composants seront préparés pour l'installation.

Si vous ne souhaitez pas installer un composant, choisissez l'option **Le composant ne sera pas accessible** dans le menu contextuel.

Pour continuer à utiliser l'Assistant, il faut cliquer sur **Suivant**. Si vous avez choisi l'option d'installation de la console d'administration uniquement à l'étape précédente, la description de la suite de l'installation reprend à l'étape 9.

ETAPE 6. SELECTION DES DOSSIERS D'ENREGISTREMENT DES DONNEES

Au cours de cette étape, vous devez sélectionner sur le disque dur le dossier dans lequel les données générées par l'application seront conservées. Les données suivantes sont sauvegardées dans ce dossier :

- Journaux de fonctionnement et de la protection antivirus ;
- Données de service et temporaires indispensables au bon fonctionnement de l'application et à la fiabilité de la protection en continu ;
- Bases de Kaspersky Anti-Virus utilisées pour identifier les programmes malveillants et les virus connus ;
- Rapports ;
- Base de données des statistiques ;
- Base de données de la banque de fichiers ;
- Base de données de la sauvegarde ;
- Diverses données assurant l'interaction avec le serveur Microsoft ISA Server/Forefront TMG.

Le champ **Dossier des données** indique le chemin d'accès au dossier de conservation des données par défaut.

Pour modifier le chemin d'accès au dossier de sauvegarde des données de Kaspersky Anti-Virus,

saisissez le chemin d'accès dans le champ **Dossier des données** ou sélectionnez le dossier requis dans la fenêtre **Modification du dossier cible actuel** en cliquant sur le bouton **Modifier**.

Le cas échéant, vous pourrez, après l'installation de Kaspersky Anti-Virus, modifier l'emplacement du dossier des données de l'application (cf. rubrique "Modification de l'emplacement du dossier des données de l'application" à la page 65).

Cliquez sur **Suivant** pour poursuivre l'installation.

ETAPE 7. CONFIGURATION DES REGLES D'ADMINISTRATION A DISTANCE

Vous devez indiquer au cours de cette étape le port de connexion à Kaspersky Anti-Virus pour l'administration de l'application à l'aide de la console installée sur un ordinateur distant.

Saisissez le numéro dans le champ **Port TCP**. La valeur par défaut est de 5000.

Si la case **Activer la règle** est cochée, cela signifie que l'Assistant d'installation créera dans la stratégie du pare-feu du serveur Microsoft ISA Server / Forefront TMG une règle d'utilisateur qui autorisera les connexions entrantes sur le port du serveur indiqué. La possibilité de réaliser l'administration de Kaspersky Anti-Virus à distance sera activée automatiquement. Décochez la case si vous n'avez pas l'intention d'autoriser l'administration à distance après l'installation de l'application.

Cliquez sur **Suivant** pour poursuivre l'installation.

ETAPE 8. COPIE DES FICHIERS ET ENREGISTREMENT DES COMPOSANTS

Cette étape correspond à la copie des fichiers sur l'ordinateur dans le dossier d'installation de l'application sélectionné dans la fenêtre de sélection des composants (cf. rubrique "Etape 5 Installation personnalisée" à la page 15), à l'enregistrement des composants installés dans le système d'exploitation et à leur intégration au serveur Microsoft ISA Server / Forefront TMG.

Cliquez sur **Installer** pour poursuivre l'installation. L'Assistant commence la procédure d'installation de l'application. Cliquez sur le bouton **Précédent** s'il faut modifier les paramètres sélectionnés aux étapes antérieures de l'Assistant.

Lors de l'installation et de l'enregistrement des filtres, il faut relancer les services du serveur Microsoft ISA Server / Forefront TMG. Cliquez sur **OK** dans la notification pour relancer automatiquement les services et garantir la bonne intégration de Kaspersky Anti-Virus sur le serveur Microsoft ISA Server / Forefront TMG.

Lors de l'installation de Kaspersky Anti-Virus, certains services de Microsoft ISA Server / Forefront TMG seront relancés. Cela pourrait interrompre les connexions établies par les ordinateurs clients.

Si vous cliquez sur **Annuler** dans la fenêtre de demande confirmation de redémarrage des services, l'installation sera interrompue et le système reviendra à l'état antérieur au déploiement de Kaspersky Anti-Virus. L'installation de l'application sera interrompue.

ETAPE 9. FIN DE LA PROCEDURE D'INSTALLATION

La fenêtre **Fin de l'installation** signale que l'installation de Kaspersky Anti-Virus est terminée.

Cochez la case **Lancer l'Assistant de configuration** pour lancer l'Assistant de configuration finale de l'application (cf. rubrique "Assistant de configuration finale" à la page 20) après la fermeture de la fenêtre de l'Assistant d'installation. L'Assistant de configuration finale permet d'ajouter les fichiers de licence de l'application suite à l'installation. L'exécution de l'Assistant n'est pas obligatoire. Les paramètres définis à l'aide de l'Assistant peuvent être modifiés ultérieurement à l'aide de la console d'administration.

Cliquez sur **Terminer** pour fermer la fenêtre de l'Assistant d'installation.

Le menu de l'application **Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG Standard Edition** apparaît dans le menu "Démarrer". Il permet de lancer la console d'administration et d'ouvrir le système d'aide de l'application.

ACTIVATION DE L'APPLICATION. INFORMATIONS SUR LES MODES D'ACTIVATION DE L'APPLICATION

Pour que Kaspersky Anti-Virus protége les ordinateurs clients à l'aide des bases de l'Antivirus les plus récentes, il faut activer l'application. L'activation de l'application signifie l'ajout du fichier de licence.

Deux modes s'offrent à vous pour activer l'application :

- Utilisation de l'Assistant de configuration finale (cf. rubrique "Assistant de configuration finale" à la page 20).
- Utilisation de la console d'administration (cf. rubrique "Administration des licences" à la page 22).

MODIFICATIONS DANS LE SYSTEME SUITE A L'INSTALLATION DE L'APPLICATION

Les dossiers suivants sont créés lors de l'installation :

- **Dossier d'installation** : <ProgramFiles>\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG Standard Edition, où <ProgramFiles> peut prendre une des valeurs suivantes :
  - si Microsoft ISA / Forefront TMG est installé sur le même disque que Microsoft Windows, alors <ProgramFiles> est le dossier standard Program Files, dont le chemin d'accès est conservé dans la variable %ProgramFiles% pour les systèmes 32 bits ou dans %ProgramFiles(x86)% pour les systèmes 64 bits ;
  - si Microsoft ISA / Forefront TMG est installé sur un autre disque, <ProgramFiles> désigne <Disque avec Microsoft ISA / Forefront TMG>:\Program Files.
- **Le dossier de données** : <CommonAppDataFolder>\Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG Standard Edition\data, où <CommonAppDataFolder> est le dossier **Common AppData** pour les données de l'application utilisée par tous les utilisateurs. La valeur **Common AppData** peut être précisée dans la clé du registre :
  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders]
- **Dossier des composants partagés (ISD)**: <CommonFilesFolder>\Kaspersky Lab\ISD>,
  où <CommonFilesFolder> est le dossier standard Common Files pour les applications 32 bits pour l'utilisateur actuel. Le chemin d'accès au dossier est conservé dans la variable %CommonProgramFiles% pour les systèmes 32 bits et dans la variable %CommonProgramFiles(x86)%pour les systèmes 64 bits.
- **Dossier du menu Démarrer :** <ProgramMenuFolder>\Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG Standard Edition où <ProgramMenuFolder> est le dossier **Common Programs** contenant les éléments du menu **Démarrer** pour tous les utilisateurs. La valeur **Common Programms** peut être précisée dans la clé du registre :
  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders].
- **Dossier dans Downloaded Installations** : <DownloadedInstallationsFolder>\{0D40E22B-2FB4-4237-AB63-3FFA9A4CE2EA}, où <DownloadedInstallationsFolder> est le dossier standard Downloaded Installations pour la conservation des fichiers d'installation dont le chemin d'accès est %WinDir%\Downloaded où %WinDir% désigne le dossier d'installation de Microsoft Windows.

Les actions suivantes ont également lieu durant l'installation :

- Les applications suivantes sont installées : Microsoft Windows Installer 3.1, Microsoft Visual C++ 2005 Redistributable Package (x86).
- Le service **Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG SE** est enregistré dans le système (kavisasrv.exe).
- Sur le serveur Microsoft ISA Server / Forefront TMG, une règle d'accès est créée dans le pare-feu permettant à la Console de gestion d'accéder à distance à l'ordinateur sur lequel Kaspersky Anti-Virus est installé.
- Deux groupes de compteurs de performances sont installés : **Kav for ISA and TMG Filters** et **Kav for ISA and TMG Service**.
- Le processus de notifications des événements de Kaspersky Anti-Virus dans Microsoft ISA Server / Forefront TMG est enregistré.

Les modifications dans le registre pour les applications 32 et 64 bits sont reprises dans l'annexe 1.

PREPARATIFS POUR L'UTILISATION

Une fois l'installation terminée, Kaspersky Anti-Virus commence à fonctionner selon une sélection minime de paramètres définis par défaut et recommandés par les experts de Kaspersky Lab. Le cas échéant, vous pouvez introduire les modifications nécessaires en tenant compte des particularités du réseau et des caractéristiques de l'ordinateur sur lequel Microsoft ISA Server / Forefront TMG est installé.

La configuration des paramètres de fonctionnement de l'application est réalisée depuis le poste de travail de l'administrateur, c.-à-d. l'ordinateur sur lequel la **Console d'administration** est installée.

Il est vivement recommandé de configurer la mise à jour automatique des bases toutes les heures (cf. rubrique "Mise à jour automatique des bases" à la page 34).

Pour confirmer le bon fonctionnement de l'application, vous pouvez tester la protection à l'aide du virus de test (cf. rubrique "Contrôle de l'exactitude de la configuration de l'application" à la page 30).

Pour contrôler le fonctionnement de Kaspersky Anti-Virus, cliquez sur le nœud **Contrôle** (cf. rubrique "**Contrôle du fonctionnement de l'application**" à la page 55).

RESTAURATION DE L'APPLICATION

La restauration de Kaspersky Anti-Virus a lieu si la première installation s'est soldée sur une erreur ou si l'intégrité des fichiers exécutables ou l'enregistrement des composants de l'application a été compromis.

Pour installer à nouveau l'application, lancez le fichier exécutable repris dans le paquet d'installation. Vous pouvez utiliser également l'Assistant d'ajout et de suppression de programmes de Microsoft Windows.

Pour utiliser l'Assistant d'ajout et de suppression de programmes de Microsoft Windows, procédez comme suit :

1. Ouvrez la fenêtre des **Ajout/suppression de programmes**. Vous pouvez ouvrir cette fenêtre d'une des manières suivantes :
   a. Utilisez la combinaison de touches **WINDOWS + R** ;
   b. Dans la boîte de dialogue **Exécuter** qui s'ouvre, saisissez l'instruction "*appwiz.cpl*", puis appuyez sur la touche **ENTRÉE**.
2. Dans la fenêtre **Ajout / suppression de programmes**, trouvez l'enregistrement correspondant à Kaspersky Anti-Virus et supprimez-le.

3. Cliquez sur le bouton **Modifier / Supprimer**.

4. Dans la fenêtre de l'Assistant qui s'ouvre, cliquez sur **Suivant**.

5. Cliquez sur le bouton **Restaurer** dans la fenêtre suivante de l'Assistant.

6. Cliquez sur **Modifier** dans la fenêtre suivante de l'Assistant d'installation de Kaspersky Anti-Virus et attendez la fin de la nouvelle installation de l'application. L'Assistant écrase automatiquement les fichiers de l'application installés en réalisant un nouvel enregistrement des composants de Kaspersky Anti-Virus et leur intégration à Microsoft ISA Server / Forefront TMG.

SUPPRESSION DE L'APPLICATION

La suppression de Kaspersky Anti-Virus s'opère selon la méthode standard d'installation et de suppression des applications Microsoft Windows ou via le fichier d'installation. Dans ce cas, tous les composants installés de l'application seront supprimés.

ASSISTANT DE CONFIGURATION FINALE

L'Assistant de configuration finale permet d'ajouter les fichiers de licence de l'application suite à l'installation. L'Assistant de configuration finale est lancé automatiquement à la fin de l'installation si la case **Lancer l'Assistant de configuration finale** a été cochée à la dernière étape de l'Assistant.

Chaque fenêtre de l'Assistant contient plusieurs boutons pour contrôler la procédure :

- **Suivant** : confirme l'action et passe à l'étape suivante de l'Assistant ;
- **Précédent** : revient à l'étape antérieure de l'Assistant ;
- **Annuler** : ferme la fenêtre de l'Assistant sans enregistrer les modifications apportées ;
- **Terminer** : quitte l'Assistant, enregistre les modifications apportées et ferme la fenêtre.

La première fenêtre de l'Assistant de configuration finale **Ajout du fichier de licence principale** permet d'ajouter le fichier de licence principale.

Pour ajouter le fichier de licence principale à l'application, procédez comme suit :

1. Cliquez sur le bouton **Ajouter / remplacer** et dans la fenêtre qui s'ouvre, désignez le fichier de licence actif (fichier avec extension *.key).

2. Les informations suivantes seront ajoutées après l'ajout du fichier de licence :

   - type de licence ;
   - le propriétaire de la licence ;
   - le nombre d'utilisateurs ;
   - fin de validité de la licence.
   - le numéro de série de la licence.

La deuxième fenêtre de l'Assistant de configuration finale **Ajout du fichier de licence de réserve** permet d'ajouter un fichier de licence de réserve.

Pour ajouter le fichier de licence de réserve à l'application, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**, puis désignez le fichier de licence de réserve (fichier avec extension : *.key).
2. Les informations suivantes seront ajoutées après l'ajout du fichier de licence :
   - le nombre d'utilisateurs ;
   - fin de validité de la licence.
   - le numéro de série de la licence.
3. Le fichier de licence de réserve devient le fichier de licence actif automatiquement à l'échéance de la licence active.

ADMINISTRATION DES LICENCES

Pour que Kaspersky Anti-Virus protège les ordinateurs clients à l'aide des bases de l'Antivirus les plus récentes, la licence est indispensable (cf. rubrique "Activation de l'application" à la page 22).

En l'absence de licence, le trafic transite via Microsoft ISA Server / Forefront TMG sans analyse et la mise à jour des bases de l'Antivirus n'a pas lieu.

Si la licence est périmée, Kaspersky Anti-Virus analyse le trafic à l'aide des bases de l'Antivirus disponibles, mais il ne les mettra plus à jour. Il est conseillé de configurer les notifications sur l'expiration des fichiers de licence (cf. rubrique "Configuration des notifications sur l'expiration des licences24" à la page).

Si la licence appartient à la liste noire, le trafic transite via Microsoft ISA Server / Forefront TMG sans analyse, mais la mise à jour des bases de l'Antivirus a lieu.

Deux licences peuvent être ajoutées simultanément à l'application : une licence active et une licence de réserve. Une fois que la licence active arrive à échéance, la licence de réserve devient automatiquement la licence active (cf. rubrique "Ajout d'une licence de réserve" à la page 23).

DANS CETTE SECTION DE L'AIDE

ACTIVATION DE L'APPLICATION

Pour activer l'application, afin que Kaspersky Anti-Virus commence à protéger les postes clients, vous devez ajouter le fichier de licence.

En l'absence de licence, le trafic transite via Microsoft ISA Server / Forefront TMG sans analyse et la mise à jour des bases de l'Antivirus n'a pas lieu.

Si la licence est périmée, Kaspersky Anti-Virus analyse le trafic à l'aide des bases de l'Antivirus disponibles, mais il ne les mettra plus à jour. Il est conseillé de configurer les notifications sur l'expiration des fichiers de licence (cf. rubrique "Configuration des notifications sur l'expiration des licences" à la page 24).

Si la licence appartient à la liste noire, le trafic transite via Microsoft ISA Server / Forefront TMG sans analyse, mais la mise à jour des bases de l'Antivirus a lieu.

Pour activer l'application, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console.
2. Cliquez sur le bouton **Paramètres généraux**.
3. Dans la fenêtre **Paramètres généraux** qui s'ouvre, ouvrez l'onglet **Licences** (cf. illustration ci-dessous).
4. Cliquez sur le bouton **Ajouter / remplacer**, dans la fenêtre qui s'ouvre, désignez le fichier de licence actif (fichier avec extension *.key).
5. Les informations suivantes seront ajoutées après l'ajout du fichier de licence :
   - type de licence ;

- le propriétaire de la licence ;
- le nombre d'utilisateurs ;
- fin de validité de la licence.
- le numéro de série de la licence.

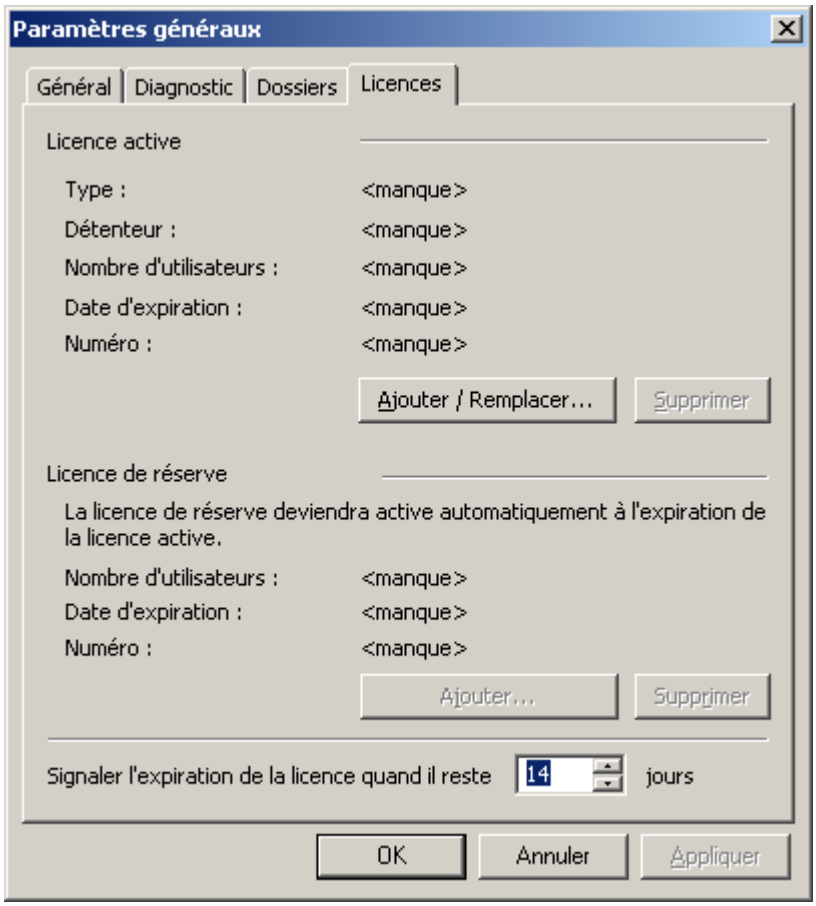

Illustration 2. Onglet "Licences"

AJOUT D'UN FICHIER DE LICENCE DE RESERVE

Pour ajouter le fichier de licence de réserve, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console.
2. Cliquez sur le bouton **Paramètres généraux**.
3. Dans la fenêtre **Paramètres généraux** qui s'ouvre, ouvrez l'onglet **Licences**.
4. Cliquez sur le bouton **Ajouter**, puis désignez le fichier de licence de réserve (fichier avec l'extension *.key).
5. Les informations suivantes seront ajoutées après l'ajout du fichier de licence :
   - le nombre d'utilisateurs ;
   - fin de validité de la licence.
   - le numéro de série de la licence.

6. Le fichier de licence de réserve devient le fichier de licence actif automatiquement à l'échéance de la licence active.

CONFIGURATION DES NOTIFICATIONS SUR L'EXPIRATION DES LICENCES

Pour configurer la notification sur l'expiration de la licence, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console.
2. Cliquez sur le bouton **Paramètres généraux**.
3. Dans la fenêtre **Paramètres généraux** qui s'ouvre, ouvrez l'onglet **Licences**.
4. Saisissez le nombre de jours requis dans le champ **Rappeler l'expiration de la licence N jours avant**.
5. Cliquez sur **OK** pour enregistrer les modifications introduites puis fermez la fenêtre.

INTERFACE DE L'APPLICATION

La console d'administration de l'application est un composant logiciel enfichable de la console (MMC) Microsoft Windows (cf. rubrique "Fenêtre principale de l'application" à la page 25).

Les paramètres de fonctionnement de Kaspersky Anti-Virus sont configurés dans des fenêtres de configuration spéciales (cf. rubrique "Fenêtres de configuration de l'application" à la page 26).

DANS CETTE SECTION DE L'AIDE

FENETRE PRINCIPALE DU PROGRAMME

La fenêtre principale de l'application se présente sous la forme d'une console de composant logiciel enfichable (MMC) (cf. illustration ci-dessous). Pour ouvrir la fenêtre de l'application, cliquez sur le raccourci de la **Console d'administration** sur le Bureau.

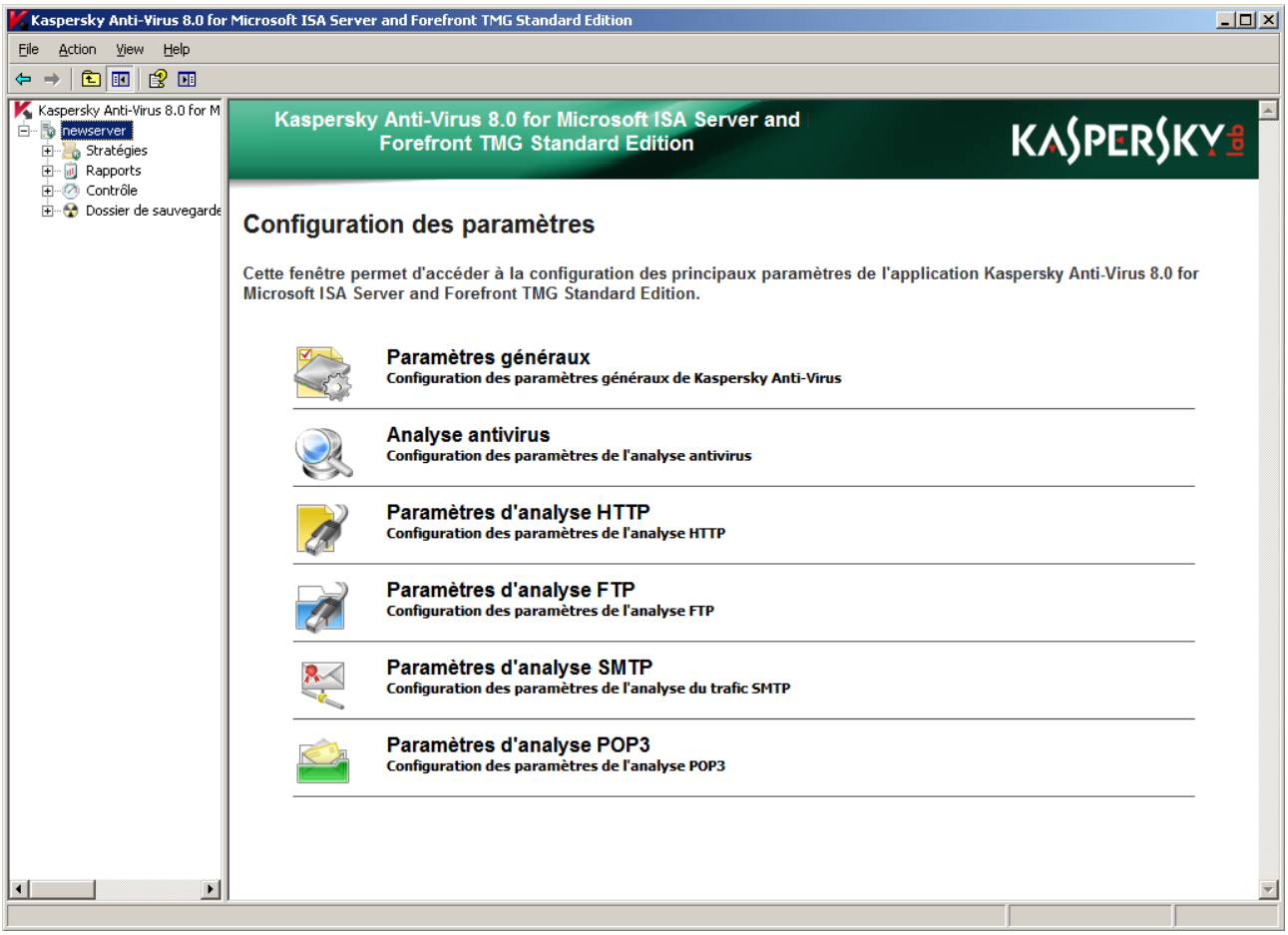

Illustration 3. Fenêtre principale de l'application

La fenêtre est scindée en deux parties : *arborescence de la console* et *zone des résultats*.

L'*arborescence de la console* a une structure hiérarchique reprise dans la partie gauche de la fenêtre de la MMC. L'arborescence de la console contient des nœuds qui représentent la fonction principale de l'application. L'arborescence de la console peut être masquée ou affichée.

Un *nœud* désigne n'importe quel élément de l'arborescence de la console auquel des objets sont ajoutés. Double-cliquez sur le signe "+" pour déployer le nœud et afficher son contenu ou double-cliquez sur le signe "-" pour réduire le nœud.

La *zone des résultats* est la partie droite du composant logiciel enfichable de la console. Elle affiche les objets ou les informations relatives à l'élément sélectionné. La zone des résultats est toujours visible, quelle que soit la configuration.

Vous pouvez configurer l'affichage du composant en masquant ou en affichant les zones de la fenêtre.

Pour configurer l'affichage du composant logiciel enfichable de la console, procédez comme suit :

1. Ouvrez la **Console d'administration**.
2. Dans le menu **Apparence**, choisissez l'option **Configurer**.
3. Dans la boîte de dialogue **Configuration de l'apparence** qui s'ouvre, affichez les éléments en cochant les cases correspondantes ou supprimez des éléments en désélectionnant des cases.

Pour obtenir de plus amples informations sur l'interface du composant logiciel enfichable, procédez comme suit :

1. Ouvrez la **Console d'administration**.
2. Choisissez l'option **Aide** du menu.

FENETRES DE CONFIGURATION DE L'APPLICATION

Les principaux paramètres de fonctionnement de Kaspersky Anti-Virus sont définis dans les fenêtres de configuration. Pour accéder aux fenêtres de configuration, sélectionnez le nœud correspondant au serveur dans la console d'administration et la zone des résultats présentera les boutons d'ouverture des fenêtres de configuration suivantes (cf. illustration ci-dessous) :

- **Paramètres généraux** : paramètres des journaux de fonctionnement de l'application (cf. rubrique "Diagnostic" à la page 63), paramètres de fonctionnement de la licence (cf. rubrique "Administration des licences" à la page 22).
- **Analyse antivirus** : paramètres de mise à jour des bases de Kaspersky Anti-Virus et des performances du moteur antivirus (cf. rubrique "Analyse antivirus" à la page 38).
- **Paramètres d'analyse HTTP** : modification des modèles de remplacement pour les objets bloqués, configuration des paramètres d'analyse du trafic HTTP :
  - Temps maximal avant le transfert de données
  - Volume de données non envoyées au client avant la fin de l'analyse ;
  - Vitesse de transfert d'objet non analysé vers un client.
- **Paramètres d'analyse FTP** : temps maximal avant le début du transfert des données au client et nombre de données non envoyé au client avant la fin du transfert.
- **Paramètres d'analyse SMTP** : modification des modèles de remplacement pour les objets bloqués et le corps du message.

- **Paramètres d'analyse POP3** : modification des modèles de remplacement pour les objets bloqués et le corps du message.

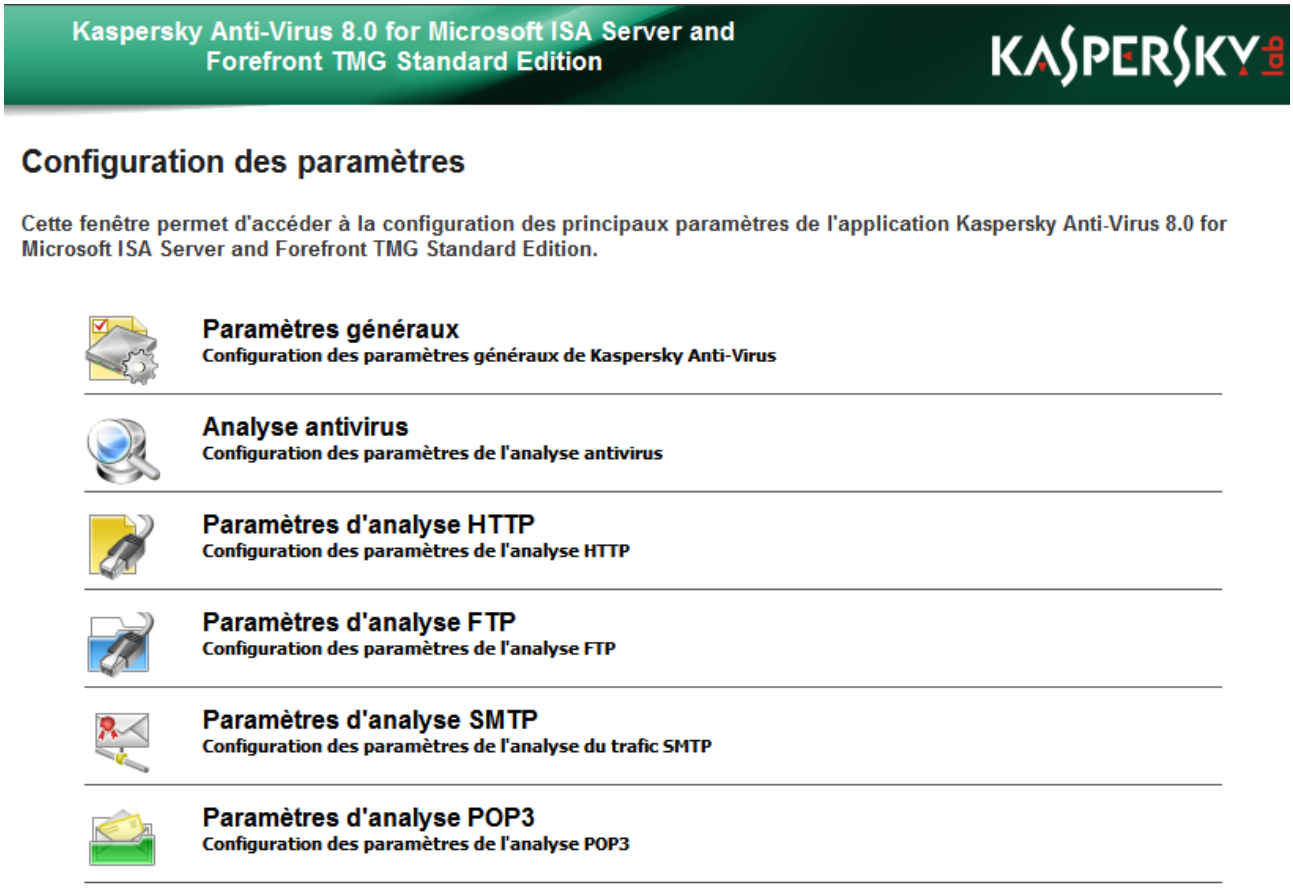

Illustration 4. Fenêtre de configuration de l'application

LANCEMENT ET ARRET DE L'APPLICATION

Une fois l'application installée, le service **Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG SE** (kavisasrv.exe) est lancé automatiquement et garantit le fonctionnement de Kaspersky Anti-Virus.

Pour arrêter Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez la console d'administration **Microsoft ISA Server / Forefront TMG**.
2. Dans l'arborescence de la console d'administration, choisissez le nœud du serveur puis **Configuration** > **Add-ins** pour Microsoft ISA Server ou le nœud **System** pour Forefront TMG. La liste des filtres installés s'affiche dans la partie droite de la fenêtre.
3. Sous l'onglet **Web Filters**, désactivez le filtre **Filtre Web de Kaspersky Anti-Virus**.
4. Sous l'onglet **Application Filters**, désactivez le fonctionnement des filtres de l'application : **Filtre FTP de Kaspersky Anti-Virus**, **Filtre POP3 de Kaspersky Anti-Virus**, **Filtre SMTP de Kaspersky Anti-Virus**.
5. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites. Dans la boîte de dialogue qui s'ouvre, choisissez l'option d'enregistrement des modifications avec redémarrage des services.
6. Arrêtez le service **Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG** dans le gestionnaire de services de Microsoft Windows.

   Le fonctionnement de Kaspersky Anti-Virus sera arrêté.

Si vous désactivez le service de Kaspersky Anti-Virus sans désactiver les filtres dans Microsoft ISA Server / Forefront TMG, le service sera lancé automatiquement quelques minutes après l'arrêt.

Pour lancer Kaspersky Anti-Virus après l'arrêt, procédez comme suit :

1. Ouvrez la Console d'administration **Microsoft ISA Server / Forefront TMG**.
2. Dans l'arborescence de la console d'administration, choisissez le nœud du serveur puis **Configuration** > **Add-ins** pour Microsoft ISA Server ou le nœud **System** pour Forefront TMG. La liste des filtres installés s'affiche dans la partie droite de la fenêtre.
3. Sous l'onglet **Application Filters**, activez le fonctionnement des filtres de l'application : **Filtre FTP de Kaspersky Anti-Virus**, **Filtre POP3 de Kaspersky Anti-Virus**, **Filtre SMTP de Kaspersky Anti-Virus**.
4. Sous l'onglet **Web Filters**, activez le filtre **Filtre Web de Kaspersky Anti-Virus**.
5. Une fois les filtres activés, le service **Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG** démarre automatiquement.

CONNEXION DE LA CONSOLE D'ADMINISTRATION AU SERVEUR

Pour connecter la console d'administration au serveur, procédez comme suit :

1. Lancez la Console d'administration. La fenêtre de connexion au serveur s'ouvre (cf. illustration ci-dessous).

2. Cochez la case **Ordinateur local** si la console est lancée depuis un ordinateur sur lequel Kaspersky Anti-Virus est installé ou cochez la case **Autre ordinateur** et saisissez dans le champ **Nom** son nom dans le réseau Microsoft Windows, l'adresse IP ou le nom de domaine de l'ordinateur sur lequel Kaspersky Anti-Virus est installé. Vous pouvez également sélectionner un ordinateur distant à l'aide du bouton **Parcourir**.

3. Cochez la case **Données du compte utilisateur actuel** si l'accès au serveur s'opère sous le compte utilisateur actuel. Ou cochez la case **Définir un autre compte utilisateur** et saisissez le nom de l'utilisateur, le domaine et le mot de passe dans les champs correspondants. Cette option est offerte uniquement pour les connexions à distance.

   Pour une connexion distante à valeur requise de la Console d'administration au serveur, utilisez le compte Administrateur intégré par défaut dans le système d'exploitation installé sur le serveur, où désactivez le Contrôle des comptes (UAC) sur le serveur. Dans le cas contraire, la surveillance du fonctionnement de l'application et l'administration des licences seront inaccessibles.

4. Cliquez sur **Terminer** pour vous connecter au serveur.

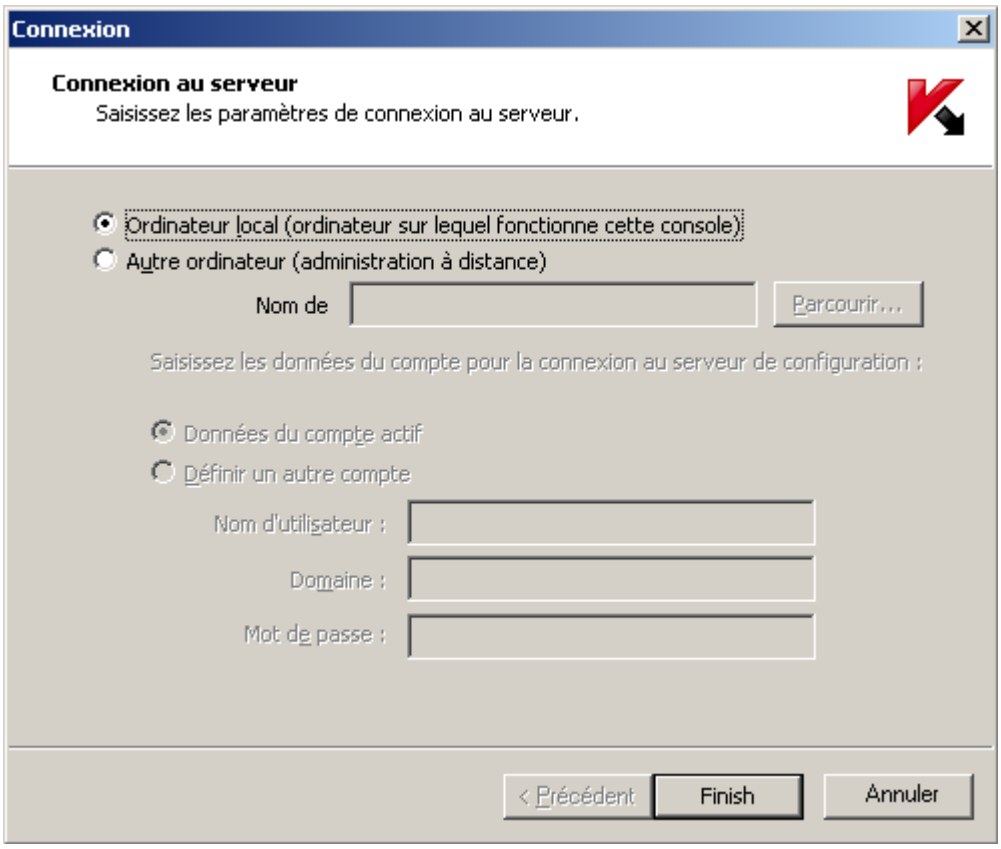

Illustration 5. Fenêtre de connexion au serveur.

VALIDATION DE LA CONFIGURATION DE L'APPLICATION

Une fois l'installation et la configuration de Kaspersky Anti-Virus terminée, il est conseillé de vérifier l'exactitude de la configuration des paramètres et le bon fonctionnement de l'application à l'aide d'un "virus" de test et de ses modifications.

Ce virus de test a été développé spécialement par l'organisation EICAR (The European Institute for Computer Antivirus Research) afin de vérifier le bon fonctionnement des logiciels antivirus. Il ne s'agit pas d'un programme malveillant et il ne contient aucun code qui puisse nuire à votre ordinateur. Néanmoins, la majorité des logiciels antivirus le considère comme un virus.

Vous pouvez télécharger le "virus" depuis le site officiel de l'organisation EICAR : http://www.eicar.org/anti_virus_test_file.htm.

Le fichier téléchargé sur le site de la société EICAR contient le corps d'un "virus" de test standard. Kaspersky Anti-Virus le détecte, lui attribue le statut "infecté" et effectue l'action établie par l'administrateur pour les objets de ce type.

Afin de vérifier le comportement de l'application lors de la découverte d'objets d'un autre type, vous pouvez modifier le contenu du "virus" en ajoutant un des préfixes repris dans le tableau ci-dessous. Vous pouvez utiliser n'importe quel éditeur de fichiers texte ou html pour le modifier.

Tableau 1. Préfixes du "virus" de test

Préfixe	Type d'objet
Pas de préfixe, "virus" de test standard	Infecté. Une erreur se produit lors de la tentative de réparation de l'objet ; l'action définie pour les objets irréparables est exécutée.
CORR-	Endommagé.
SUSP-	Suspect (code d'un virus inconnu).
WARN-	Suspect (code modifié d'un virus connu).
ERRO-	Entraîne une erreur d'analyse correspondant à la découverte d'un objet endommagé.
CURE-	Infecté (réparable). L'objet sera réparé et le texte du corps du "virus" sera remplacé par CURED.
DELE-	Infecté (irréparable). L'action prévue pour les objets irréparables est appliquée.

La première colonne du tableau contient les préfixes qu'il faut ajouter en tête de la ligne du virus de test traditionnel.

Une fois que vous aurez ajouté le préfixe, enregistrez le fichier sous le nom eicar_dele.com par exemple (utilisez la même convention pour toutes les modifications du virus).

La deuxième colonne reprend la description des types d'objet identifiés par l'antivirus suite à l'ajout des différents préfixes. Les actions exécutées sur chacun des objets sont définies par les paramètres de l'analyse antivirus déterminés par l'administrateur.

DANS CETTE SECTION DE L'AIDE

VALIDATION DE LA PROTECTION DU TRAFIC HTTP

Pour valider la protection du trafic HTTP, procédez comme suit :

1. Ouvrez dans le navigateur le lien avec le virus de test http://www.eicar.org/download/eicar.com. Si Kaspersky Anti-Virus est configuré correctement, le virus de test ne sera pas chargé et le navigateur affichera une notification indiquant que le lien contient un objet malveillant.

2. La fenêtre **Contrôle** de la console d'administration de Kaspersky Anti-Virus permet de consulter les statistiques des objets analysés : le virus de test doit apparaître dans la colonne **HTTP**. Assurez-vous que le virus de test a été traité conformément aux paramètres définis dans la fenêtre **Paramètres de l'analyse HTTP** de la console d'administration de Kaspersky Anti-Virus.

VALIDATION DE LA PROTECTION DU TRAFIC FTP

Pour valider la protection du trafic FTP, procédez comme suit :

1. Essayez de télécharger le virus de test à l'aide du client FTP de votre choix. Si Kaspersky Anti-Virus est correctement configuré, le virus de test sera bloqué.

2. La fenêtre **Contrôle** de la console d'administration de Kaspersky Anti-Virus permet de consulter les statistiques des objets analysés : le virus de test doit apparaître dans la colonne **FTP**.

VALIDATION DE LA PROTECTION DU TRAFIC SMTP / POP3

Pour valider la protection du trafic SMTP, vous devez envoyer un message avec le virus de test en pièce jointe à l'aide d'un client de messagerie utilisant le protocole SMTP. Le virus de test sera remplacé conformément aux paramètres définis dans les **Paramètres d'analyse SMTP** de la console d'administration de Kaspersky Anti-Virus. La fenêtre **Contrôle** de la console d'administration de Kaspersky Anti-Virus permet de consulter les statistiques des objets analysés : le virus test doit apparaître dans la colonne **SMTP / POP3**.

Pour valider la protection du trafic POP3, vous devez recevoir un message avec le virus de test en pièce jointe à l'aide d'un client de messagerie utilisant le protocole POP3. Pour ce faire, vous pouvez envoyer un message avec le virus test à votre adresse, en ayant désactivé l'analyse du trafic SMTP. Le virus d'essai sera remplacé conformément aux paramètres définis dans les **Paramètres d'analyse POP3** de la console d'administration de Kaspersky Anti-Virus. La fenêtre **Contrôle** de la console d'administration de Kaspersky Anti-Virus permet de consulter les statistiques des objets analysés : le virus test doit apparaître dans la colonne **SMTP / POP3**.

PROTECTION DU TRAFIC PAR DEFAUT

Une fois installé, Kaspersky Anti-Virus commence à protéger le trafic des ordinateurs clients selon les paramètres par défaut. L'analyse porte sur le trafic des protocoles HTTP, FTP, POP3 et SMTP. Kaspersky Anti-Virus bloque les objets malveillants et suspects trouvés et remplace les objets par des modèles de messages sur la menace identifiée.

Les stratégies de l'analyse antivirus sont définies pour tous les ordinateurs.

VOIR EGALEMENT

MISE A JOUR DES BASES

Chaque jour, de nouveaux virus et autres programmes malveillants apparaissent dans le monde. Pour garantir la fiabilité de la protection du trafic, il faut utiliser des informations fraîches sur les menaces et les moyens de les neutraliser. Ces données sont reprises dans les bases de l'Antivirus qui permettent à l'application d'offrir la protection. Pour maintenir la protection au niveau le plus élevé, il faut réaliser une mise à jour fréquente des bases.

Il est conseillé de réaliser la mise à jour directement suite à l'installation de l'application car les bases de l'Antivirus présentes dans le paquet d'installation sont dépassées au moment de l'installation.

Les bases antivirus sont mises à jour toutes les heures sur les serveurs de Kaspersky Lab. Il est conseillé de configurer la mise à jour automatiquement selon le même intervalle (cf. rubrique "Mise à jour automatique des bases" à la page 34).

La mise à jour des bases de l'Antivirus peut avoir lieu depuis les sources suivantes :

- Depuis les serveurs de mises à jour de Kaspersky Lab sur Internet (cf. rubrique "Configuration des paramètres de mise à jour des bases via Internet" à la page 36) ;
- Depuis une source de mise à jour locale, à savoir un dossier local ou réseau (cf. rubrique "Sélection de la source de mise à jour des bases" à la page 34).

Lors de la mise à jour, les bases actuelles sont comparées aux bases de la source des mises à jour. S'il existe des différences, la partie manquante des bases est installée. La copie complète des bases n'a pas lieu, ce qui permet d'augmenter sensiblement la vitesse de la mise à jour et de réduire le volume du trafic.

La mise à jour des bases peut avoir lieu automatiquement selon une programmation ou manuellement. Après la copie des fichiers depuis la source de mises à jour définie, l'application utilise automatiquement les bases récupérées et effectue son analyse à l'aide de celles-ci.

Vous pouvez à tout moment vérifier le fonctionnement de la mise à jour automatique des bases en consultants les informations relatives au statut des bases (cf. rubrique "Consultation des informations relatives à l'état des bases" à la page 33).

DANS CETTE SECTION DE L'AIDE

CONSULTATION DES INFORMATIONS RELATIVES AU STATUT DES BASES

Pour consulter les informations relatives au statut des bases utilisées, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console.
2. Cliquez sur **Analyse antivirus**. Ouvrez la fenêtre **Analyse antivirus** sous l'onglet **Mettre à jour**.

Les informations relatives aux bases utilisées sont reprises dans le champ **Informations sur les bases utilisées**. Vous pouvez ainsi obtenir la date et l'heure de création des bases et le nombre d'enregistrements.

MISE A JOUR MANUELLE DES BASES

La mise à jour manuelle des bases permet une actualisation immédiate de celles-ci.

Pour mettre à jour manuellement les bases de Kaspersky Anti-Virus, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console.
2. Cliquez sur **Analyse antivirus**. Ouvrez la fenêtre **Analyse antivirus** sous l'onglet **Mettre à jour**.
3. Cliquez sur le bouton **Mettre à jour maintenant**. La mise à jour des bases sera lancée. L'état de l'exécution de la tâche apparaîtra dans le champ à droite du bouton.

MISE A JOUR AUTOMATIQUE DES BASES

Les bases antivirus sont mises à jour toutes les heures sur les serveurs de Kaspersky Lab. Il est conseillé de réaliser la mise à jour automatique selon la même fréquence. Cette valeur est sélectionnée par défaut.

Pour configurer la mise à jour automatique des bases, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console.
2. Cliquez sur **Analyse antivirus**. Ouvrez la fenêtre **Analyse antivirus** sous l'onglet **Mettre à jour**.
3. Assurez-vous que la case **Mettre à jour les bases automatiquement** est cochée (si la case n'est pas cochée, la mise à jour automatique n'aura pas lieu).
4. Sélectionnez la fréquence de la mise à jour parmi les options suivantes :
   - **Tous les N jours à T1 et T2** où N représente le nombre de jours entre chaque lancement de la mise à jour des bases et T1 et T2 représentent l'heure à laquelle la mise à jour aura lieu. Si vous définissez les valeurs suivantes : N = 3, T1 = 23:15, T2 = 05:00, alors la mise à jour aura lieu tous les trois jours, deux fois par jour aux heures indiquées. Le paramètre T2 est facultatif. Vous pouvez le désactiver en décochant la case correspondante.
   - **Une fois toutes les T3** où T3 représente le temps qui s'écoulera entre chaque lancement de la mise à jour. Si T3 = 4 heures, alors la mise à jour aura lieu toutes les quatre heures.
5. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications des paramètres ou sur **OK** pour enregistrer les modifications et fermer la fenêtre.
6. Sélectionnez la source de la mise à jour (cf. rubrique "Sélection de la source de la mise à jour" à la page 34).
7. Configurez les paramètres de la mise à jour via Internet (cf. la rubrique "Configuration des paramètres de la mise à jour des bases via Internet" à la page 36) ou depuis un dossier réseau (cf. la rubrique "Mise à jour des bases depuis un répertoire réseau" à la page 36).

SELECTION DE LA SOURCE DE LA MISE A JOUR DES BASES

La source des mises à jour est une ressource qui contient les mises à jour des bases de Kaspersky Anti-Virus. La mise à jour est téléchargée par défaut des serveurs de mises à jour de Kaspersky Lab. Il s'agit de sites Internet spéciaux qui hébergent les mises à jour des bases et des modules de programme pour toutes les applications de Kaspersky Lab. Vous pouvez configurer la récupération des mises à jour depuis un serveur HTTP ou FTP ou depuis un dossier local ou

réseau. La source sélectionnée sera utilisée aussi bien pour la mise à jour manuelle que pour la mise à jour programmée.

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

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console.

2. Cliquez sur **Analyse antivirus**. La fenêtre **Analyse antivirus** s'ouvre sur l'onglet de **Mise à jour** (cf. illustration ci-dessous).

3. Dans le groupe de paramètres **Source**, sélectionnez une des options suivantes :

   - **Serveurs de mises à jour de Kaspersky Lab** : serveurs HTTP et FTP de Kaspersky Lab en ligne sur lesquels les mises à jour des bases sont publiées toutes les heures (option choisie par défaut) ;

   - **Dossier local ou réseau** : dossier local ou réseau qui héberge les mises à jour téléchargées depuis Internet. Si vous choisissez cette option, saisissez le chemin d'accès manuellement ou dans la fenêtre standard de l'Assistant Microsoft Windows. Pour ouvrir la fenêtre de l'Assistant, cliquez sur le bouton **Parcourir**. Le cas échéant, configurez les autres paramètres de la mise à jour (cf. rubrique "Mise à jour des bases depuis un répertoire réseau" à la page 36).

4. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications des paramètres ou sur **OK** pour enregistrer les modifications et fermer la fenêtre.

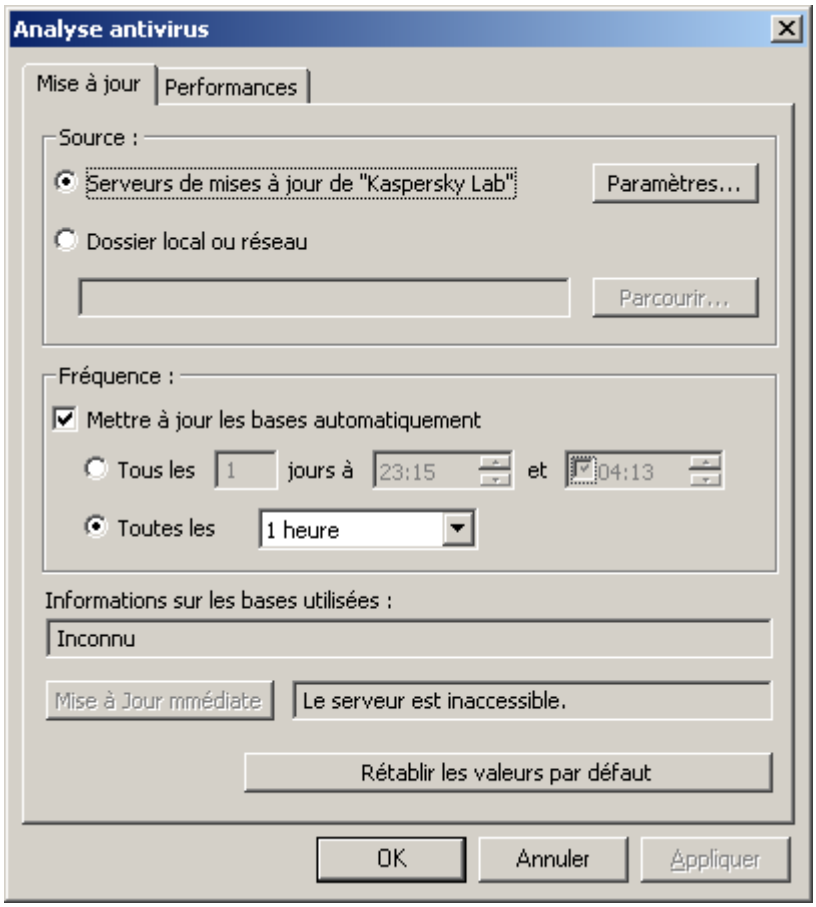

Illustration 6. Onglet "Mise à jour"

CONFIGURATION DES PARAMETRES DE MISE A JOUR DES BASES VIA INTERNET

Les paramètres sélectionnés seront appliqués à la mise à jour manuelle et à la mise à jour automatique des bases de l'antivirus.

Pour modifier les paramètres de la mise à jour via Internet, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console.
2. Cliquez sur **Analyse antivirus**. Ouvrez la fenêtre **Analyse antivirus** sous l'onglet **Mettre à jour**.
3. Cliquez sur le bouton **Paramètres** afin d'ouvrir la fenêtre **Paramètres de la mise à jour via Internet**.
4. Définissez les paramètres de sélection du serveur de mises à jour de Kaspersky Lab :
   - **Sélectionner le serveur de mise à jour automatiquement** : si vous choisissez cette option, le serveur adéquat pour la mise à jour sera sélectionné automatiquement ;
   - **Utiliser le serveur indiqué** : sélectionnez cette option s'il faut utiliser un serveur en particulier et indiquez l'adresse de ce serveur dans le champ correspondant.
5. Configurez les paramètres d'utilisation du serveur proxy :
   - Si la connexion à Internet s'opère via un serveur proxy, cochez la case **Utiliser le serveur proxy** et définissez les paramètres de connexion : adresse du serveur proxy et numéro du port pour la connexion ;
   - Si la connexion à Internet s'opère via un proxy du serveur Microsoft ISA Server / Forefront TMG sur lequel Kaspersky Anti-Virus est installé, cochez la case **Utiliser le proxy local** ;
   - Si l'accès au serveur proxy requiert un mot de passe, définissez les paramètres d'authentification. Pour ce faire, cochez la case **Utiliser l'authentification** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**. Si l'authentification NTLM est utilisée sur le serveur proxy, le **Nom d'utilisateur** doit contenir le domaine au format <Domaine>\<Nom d'utilisateur>. Si l'utilisateur est local pour le proxy, le format de saisie du **Nom d'utilisateur** est le suivant : <Nom de l'ordinateur>\<Nom de l'utilisateur> ou .\<nom de l'utilisateur>.
6. Cochez la case **Utiliser le FTP en mode passif** si la connexion au serveur FTP des mises à jour doit être réalisée en mode passif.
7. Cliquez sur **OK** pour enregistrer les modifications et fermer la fenêtre.

MISE A JOUR DES BASES DEPUIS UN REPERTOIRE RESEAU

Les moyens d'organiser l'accès partagé (définition des privilèges) au répertoire réseau pour permettre la mise à jour varient en fonction du mode de déploiement de l'application. Kaspersky Anti-Virus peut-être déployé à l'intérieur du domaine ou dans un groupe de travail.

DANS CETTE SECTION DE L'AIDE

MISE A JOUR DEPUIS UN REPERTOIRE RESEAU: KASPESKY ANTI-VIRUS DANS UN DOMAINE

Tout ordinateur à l'intérieur du domaine se caractérise par un compte unique dont le nom correspond au nom de l'utilisateur. Les processus lancés sur l'ordinateur au nom du compte **System** seront autorisés sous le compte utilisateur de l'ordinateur sur lequel ils ont été lancés lors de l'accès aux autres ordinateurs du domaine.

Pour organiser l'accès à la ressource réseau utilisée pour diffuser les mises à jour, procédez comme suit à l'intérieur du domaine :

1. Définissez les règles de réseau : attribuez les privilèges d'accès sur la lecture de cette ressource du compte de l'ordinateur du domaine où Kaspersky Anti-Virus est lancé.

2. Définissez les privilèges d'accès local de ce compte comme les privilèges de réseau.

Les privilèges d'accès local ne peuvent être inférieurs aux privilèges d'accès réseau.

MISE A JOUR DEPUIS UN REPERTOIRE RESEAU: KASPESKY ANTI-VIRUS DANS UN GROUPE DE TRAVAIL

Les données **System** des ordinateurs réunis au sein d'un groupe de travail ne sont pas différenciables dans le réseau. Il est impossible d'octroyer des privilèges individuels aux processus exécutés sous le compte **System** sur un autre ordinateur du groupe de travail. Par conséquent, en cas d'utilisation de la mise à jour centralisée au sein d'un groupe de travail, il faut procéder comme suit :

- Octroyez les privilèges d'accès à la ressource réseau à l'utilisateur anonyme (**ANONYMOUS LOGON**);

- Octroyez des privilèges spéciaux d'accès à la ressource réseau des utilisateurs anonymes.

Voici les règles d'octroi des privilèges d'accès.

Définition des privilèges de réseau

Il faut octroyer le privilège de lecture de la ressource réseau au compte **ANONYMOUS LOGON**.

Définition des privilèges d'accès local

Les privilèges d'accès local dovient être octroyés aux mêmes comptes utilisateur que les privilèges réseau et ils ne doivent pas être moins restreints que les privilèges d'accès réseau.

Pour octroyer les privilèges d'accès anonyme à une ressource réseau,dans l'éditeur de stratégies de sécurité du système exploitation Microsoft Windows Server 2003 / 2008, procédez comme suit :

1. Lancez l'éditeur de stratégies locales (**Démarrer** → **Panneau de configurationl** → **Outils d'administration** → **Stratégie de sécurité locale**).

2. Choisissez la rubrique **Paramètres de sécurité** → **Stratégies locales** → **Options de sécurité**.

3. Dans le volet des résultats, choisissez l'option **Accès réseau : les partages qui sont accessibles de manière anonyme** et ouvrez la fenêtre des propriétés à l'aide du menu contextuel. Sous l'onglet **Paramètre de stratégie locale**, saisissez le nom de la ressource réseau à laquelle l'accès doit être autorisé.

4. Pour que les modifications introduites entrent en vigueur, choisissez l'option **Recharger** dans le menu contextuel du noeud **Paramètres de sécurité**.

ANALYSE ANTIVIRUS

Vous pouvez configurer les paramètres de l'analyse antivirus pour obtenir la combinaison optimale de performance et de sécurité. Pour accéder aux fenêtres de configuration, sélectionnez le nœud correspondant au serveur dans la console d'administration et la zone des résultats présentera les boutons d'ouverture des fenêtres de configuration suivantes pour la configuration antivirus.

DANS CETTE SECTION DE L'AIDE

CONFIGURATION DES PARAMETRES DE PERFORMANCE DE L'ANALYSE ANTIVIRUS

Pour ouvrir la fenêtre des paramètres des performances de l'analyse antivirus, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console.
2. Cliquez sur le bouton **Analyse antivirus** situé dans le volet des résultats à droite.
3. Dans la fenêtre qui s'ouvre, choisissez l'onglet **Performances**.

Les valeurs suivantes sont attribuées par défaut aux paramètres :

- **Nombre d'instances du moteur antivirus**. En vue d'augmenter les performances de Kaspersky Anti-Virus lors du traitement de grands flux de données, il est possible de lancer simultanément plusieurs exemplaires du moteur antivirus. La valeur de ce paramètre est calculée par défaut comme 2n+1, où n est le nombre des processus logiques Microsoft ISA Server/Forefront TMG.
- **Parmi eux pour l'analyse uniquement des objets rapides** : 1. Le moteur antivirus peut fonctionner simultanément uniquement avec un objet. Pour éviter les situations où tous les moteurs antivirus sont occupés par l'analyse d'objets de grande taille tandis que les objets plus petits s'accumulent dans la file d'attente, il est conseillé de réserver au moins un moteur pour l'analyse des objets rapides. Les objets rapides sont les objets du trafic HTTP qui remplissent toutes les conditions suivantes :
  - Objet texte dont la taille ne dépasse pas 2 Mo ;
  - Objet graphique dont la taille ne dépasse pas 2 Mo ;
  - Tous les autres objets (à l'exception des fichiers exécutables) dont la taille ne dépasse pas 256 Ko.
- **Nombre maximum d'objets analysés en mémoire** – 128.
- **Taille maximum des objets analysés en mémoire** – 128 Ko.

Les filtres de Kaspersky Anti-Virus peuvent transmettre les objets pour analyse au moteur antivirus sans enregistrement sur le disque dur. Si la taille de l'objet est supérieure à la valeur du paramètre **Taille maximum des objets analysés en mémoire** ou si le nombre d'objets analysés en mémoire est égale à la valeur du paramètre **Nombre maximum d'objets analysés en mémoire**, l'objet est d'abord enregistré sur le disque.

- **Taille maximale de la file d'attente d'objets à analyser** – 1024. Si la file d'attente contient le nombre indiqué d'objets et qu'un nouvel objet apparaît, il sera transmis au client sans analyse. Le message relatif à l'objet ignoré sera consigné dans le journal des virus de l'application (cf. rubrique "Diagnostic" à la page 63).

- **Durée maximale d'analyse** – 1800 s. Si la durée d'analyse dépasse la valeur indiquée, alors l'objet sera transmis au client sans analyse. Le message relatif à l'objet ignoré sera consigné dans le journal des virus de l'application (cf. rubrique "Diagnostic" à la page 63).

- **Ne pas analyser les objets conteneurs dont le niveau d'imbrication est supérieur à** – 32 inclus. Le niveau d'imbrication maximum est 128.

Vous pouvez modifier les paramètres pour améliorer la productivité. Tous les paramètres décrits ci-dessus interviennent pour l'analyse de tous les protocoles pris en charge. Pour rétablir les paramètres par défaut, cliquez sur le bouton **Rétablir les valeurs par défaut**.

Dans le cas d'utilisation des gestionnaires des téléchargements (download managers) dans le mode du téléchargement multi-chaîne, l'augmentation du trafic de la connexion Internet est possible. Dans ce cas, la probabilité d'obtention d'un objet malveillant (non analysé) s'augmente. Cela est lié avec les particularités techniques des mécanismes du fonctionnement des gestionnaires des téléchargements et de Kaspersky Anti-Virus. Pour diminuer le risque, le est recommandé de ne pas utiliser le gestionnaire des téléchargements en mode du téléchargement multi-chaîne.

CONFIGURATION DES PARAMETRES DE L'ANALYSE DU TRAFIC HTTP

Pour ouvrir la fenêtre de configuration des paramètres, sélectionnez le nœud correspondant au serveur dans l'arborescence de la console,

cliquez sur le bouton **Paramètres d'analyse HTTP**, situé dans le volet des résultats à droite.

Les valeurs suivantes sont attribuées par défaut aux paramètres :

- **Temps maximal avant le transfert de données** – 30 sec. Si, après le début du téléchargement de l'objet, une durée supérieure à la valeur indiquée s'écoule et que l'objet n'a pas encore été entièrement téléchargé ou si l'analyse n'a pu être réalisée après le téléchargement, cet objet sera transmis au client sans analyse.

- **Volume de données non envoyées au client avant la fin de l'analyse** – 30%. Kaspersky Anti-Virus analyse uniquement un objet complètement téléchargé. Pour accélérer la récupération de l'objet par l'ordinateur client, le transfert de données débute avant la fin de l'analyse de l'objet, mais l'objet ne sera transmis en entier que lorsqu'il aura été analysé (s'il ne contient pas de menace). Ce paramètre régit le pourcentage de données qui sera retenu avant la fin de l'analyse.

- **Vitesse de transfert de l'objet non analysé au client**. Ce paramètre permet de configurer la vitesse de récupération des objets non analysés via le protocole HTTP. Seule l'expérience peut vous aider à trouver la valeur optimale pour ce paramètre car elle dépend de la vitesse de l'analyse antivirus et de la configuration de votre matériel.

Cette fenêtre permet de modifier les modèles de remplacement des fichiers bloqués.

Pour modifier un modèle de remplacement, procédez comme suit :

1. Ouvrez la fenêtre des **Paramètres d'analyse HTTP**.

2. Cliquez sur le bouton **Modèles de remplacement**.

3. Dans la fenêtre qui s'ouvre, choisissez le type de fichiers bloqués :
   - Objets infectés.
   - Objets suspects.
   - Objets protégés par un mot de passe.
4. En regard du type sélectionné, cliquez sur le bouton **Modèle de remplacement**.

Les modèles sont écrits au format HTML. Vous pouvez modifier le modèle à l'aide de balises HTML standard. Variables pouvant apparaître dans les modèles :

- **%URL%** – variable contenant le lien où a été découvert l'objet bloqué ;
- **%VIRUSNAME%** – variable contenant le nom du virus. Vous pouvez consulter toutes les variables disponibles en cliquant sur le bouton **Variables**.
- **%AV_SERVER%** - nom du serveur sur lequel Kaspersky Anti-Virus est installé.

Pour revenir aux valeurs par défaut, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres d'analyse SMTP**.
2. Cliquez sur le bouton **Rétablir les valeurs par défaut**.

Quand vous aurez cliqué sur le bouton **Rétablir les valeurs par défaut**, les valeurs par défaut des paramètres et des modèles de remplacement seront rétablies.

CONFIGURATION DES PARAMETRES DE L'ANALYSE FTP

Pour ouvrir la fenêtre de configuration des paramètres, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud qui correspond au serveur.
2. cliquez sur le bouton **Paramètres d'analyse FTP** situé dans le volet des résultats à droite.

Les valeurs suivantes sont attribuées par défaut aux paramètres :

- **Durée maximale de l'analyse de la première partie des données** : 15 s. Si, après la réception de la première partie des données, une durée supérieure à la valeur indiquée s'écoule et que l'objet n'a pas encore été entièrement téléchargé ou si l'analyse n'a pu être réalisée après le téléchargement, cet objet sera transmis au client sans analyse.
- **Volume de données non envoyées au client avant la fin de l'analyse** – 10%. Kaspersky Anti-Virus analyse uniquement un objet complètement téléchargé. Pour accélérer la récupération de l'objet par le client, le transfert de données débute avant la fin de l'analyse de l'objet, mais l'objet ne sera transmis en entier que lorsqu'il aura été analysé (s'il ne contient pas de menace). Ce paramètre régit le pourcentage de données qui sera retenu avant la fin de l'analyse.

Pour revenir aux valeurs par défaut, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres d'analyse FTP**.
2. Cliquez sur le bouton **Rétablir les valeurs par défaut**.

CONFIGURATION DES PARAMETRES DE L'ANALYSE DU TRAFIC SMTP

Pour ouvrir la fenêtre de configuration des paramètres, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le nœud qui correspond au serveur.
2. Cliquez sur le bouton **Paramètres d'analyse SMTP** situé dans le volet des résultats à droite.

   Par défaut, le paramètre **Remplacer l'objet des messages infectés est** – activé.

Pour modifier le modèle de remplacement de l'objet du message,

Cliquez sur le bouton **Modèle de remplacement**.

Pour modifier les modèles de remplacement pour les fichiers bloqués dans cette même fenêtre, procédez comme suit :

1. Cliquez sur le bouton **Modèles de remplacement**.
2. Dans la fenêtre qui s'ouvre, choisissez le type de fichiers bloqués :
   - Objets infectés.
   - Objets suspects.
   - Objets protégés par un mot de passe.
3. Cliquez sur le bouton **Modèle de remplacement** pour le type sélectionné.

Les modèles sont écrits au format HTML. Vous pouvez modifier le modèle à l'aide de balises HTML standard. Variables pouvant apparaître dans les modèles :

- **%VIRUSNAME%** – variable contenant le nom du virus.

Vous pouvez consulter toutes les variables disponibles en cliquant sur le bouton **Variables**.

Pour revenir aux valeurs par défaut, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres d'analyse SMTP**.
2. Cliquez sur le bouton **Rétablir les valeurs par défaut**.

Quand vous aurez cliqué sur le bouton **Rétablir les valeurs par défaut**, les valeurs par défaut des paramètres et des modèles de remplacement seront rétablies.

CONFIGURATION DES PARAMETRES DE L'ANALYSE DU TRAFIC POP3

Pour ouvrir la fenêtre de configuration des paramètres, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud qui correspond au serveur.
2. Cliquez sur le bouton **Paramètres d'analyse POP3** situé dans le volet des résultats à droite.

Les paramètres d'analyse et les modèles de remplacement du trafic POP3 sont identiques aux paramètres d'analyse SMTP (cf. rubrique "Configuration des paramètres d'analyse du trafic SMTP" à la page 41).

DEFINITION DE LA STRATEGIE DE L'ANALYSE ANTIVIRUS

Les stratégies d'analyse antivirus permettent de définir diverses règles de traitement des protocoles, d'exclusion de l'analyse et d'actions à effectuer face aux menaces pour différentes entitées réseau et protocoles (cf. la rubrique "Entitées réseau" à la page 48). Par exemple, vous pouvez désigner des adresses de confiance pour les sources du trafic ou exclure certains types d'objet de l'analyse. Les stratégies permettent de configurer les paramètres de l'analyse de telle sorte que l'équilibre optimal entre le niveau de la protection et la productivité soit atteint.

Il existe trois types de stratégies :

- **Stratégie de traitement des protocoles** : paramètres de traitements du trafic FTP et du trafic HTTP.
- **Stratégie de l'exclusion de l'analyse** : paramètres d'exclusion de l'analyse des objets.
- **Stratégie de l'analyse antivirus** : paramètres de traitement des objets infectés et protégés par un mot de passe.

Une règle par défaut, qui ne peut être ni supprimée, ni modifiée, est définie pour chaque stratégie. Toute nouvelle règle aura une priorité supérieure à la règle définie par défaut.

L'application des règles des stratégies se déroule comme suit : la liste des règles classées par priorité est analysée selon les données sources (protocole, adresse du client et adresse du serveur) jusqu'à l'identification d'un protocole correspondant, de multiples clients contenant l'adresse du client et de nombreux serveurs contenant l'adresse du client. La règle trouvée sera utilisée. Le processus décrit est répété pour les règles de chaque type de stratégie.

Pour consulter la liste des stratégies et des règles, cliquez sur le nœud **Stratégies** (cf. illustration ci-dessous).

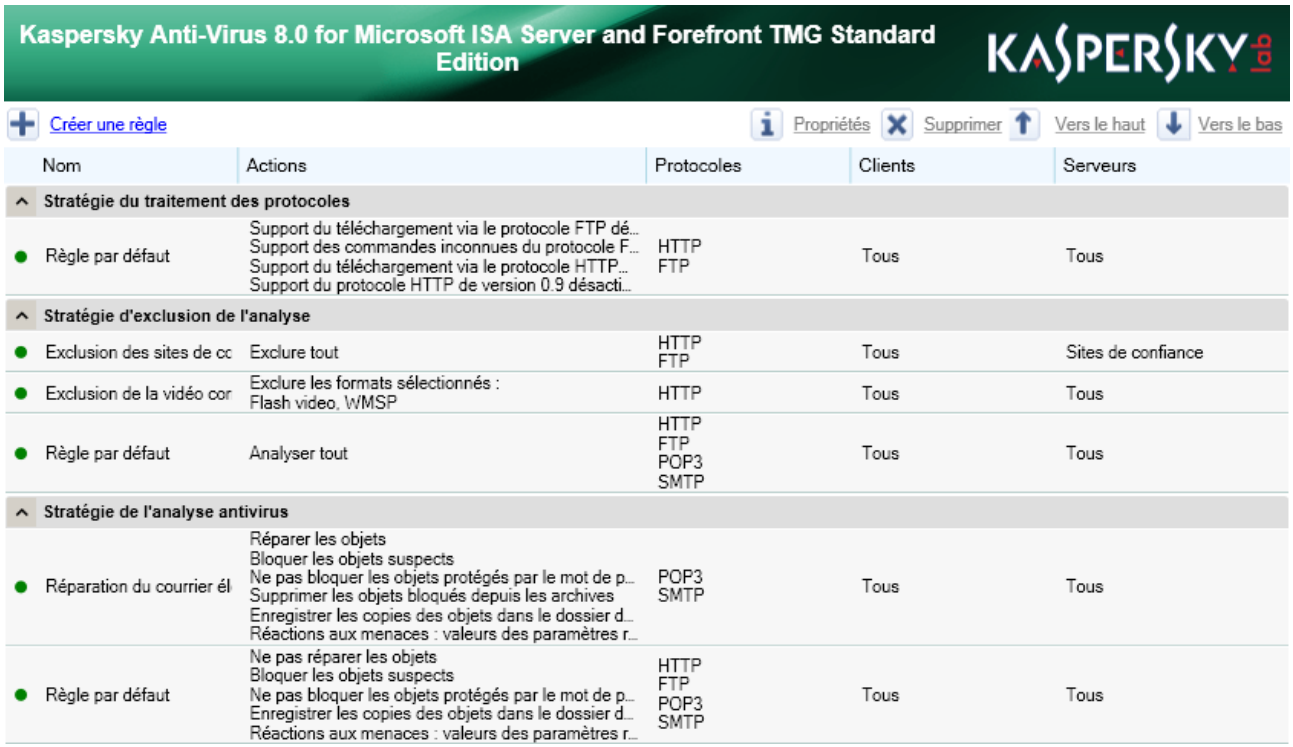

Illustration 7. Fenêtre "Stratégies"

DANS CETTE SECTION DE L'AIDE

STRATEGIE DE TRAITEMENT DES PROTOCOLES

La stratégie de traitement des protocoles est prévue pour définir les paramètres de traitement des trafics HTTP et FTP pour certaines entitées de réseau.

La **Règle par défaut**, active pour tous les ordinateurs, est définie par défaut.

Pour le protocole FTP, la règle possède les paramètres suivants :

- Le téléchargement des fichiers n'est pas pris en charge ;
- Les instructions inconnues du client FTP ne sont pas prises en charge.

Pour le protocole HTTP, la règle possède les paramètres suivants :

- Le téléchargement des fichiers n'est pas pris en charge ;
- HTTP version 0.9 n'est pas pris en charge.

STRATEGIE D'EXCLUSION DE L'ANALYSE

La stratégie d'exclusion de l'analyse permet de configurer l'exclusion d'objets de l'analyse pour les entitées réseaux et les protocoles définis.

Les règles suivantes sont définies par défaut et elles s'appliquent à tous les ordinateurs et à tous les protocoles :

- **Exclusion des sites de confiance**. La règle exclut de l'analyse les objets reçus de sites de confiance par défaut (par exemple, kaspersky.com, microsoft.com).
- **Exclusion de la video streaming**. La règle exclut de l'analyse les diffusions vidéo.
- **Règle par défaut**. La règle possède les paramètres suivants :
  - Analyser tous les types de fichier ;
  - Analyser le contenu des archives.

STRATEGIE D'ANALYSE ANTIVIRUS

La stratégie d'analyse antivirus permet de définir les paramètres de traitement des objets malveillants, des objets suspects et des archives protégées par un mot de passe pour les entitées réseau et les protocoles définis.

La **Règle par défaut**, active pour tous les ordinateurs et tous les protocoles, est définie par défaut. La règle possède les paramètres suivants :

- Tous les objets malveillants détectés sont bloqués ;
- Les objets protégés par un mot de passe sont acceptés ;
- La réparation des objets malveillants n'a pas lieu ;
- Les objets suspects sont bloqués ;
- Les parties infectées des objets composés ne sont pas supprimées.

AJOUT DE REGLES DE STRATEGIES

Vous pouvez ajouter des règles à n'importe quelle stratégie.

Pour créer une règle de traitement des protocoles, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Ensuite, sélectionnez le nœud **Stratégies**.
2. Cliquez sur **Créer un règle**.
3. Dans la fenêtre qui s'ouvre, choisissez l'option **Règle du traitement des protocoles**. L'Assistant de création de règles s'ouvre.
4. Dans la fenêtre qui s'ouvre, saisissez le **Nom de la règle** dans le champ prévu à cet effet. Le nom de la règle doit être unique. Après avoir saisi le nom, cliquez sur le bouton **Suivant**.
5. Dans la fenêtre suivante, configurez les paramètres de traitement du trafic pour chaque protocole :
   - **Prise en charge de la reprise du téléchargement des fichiers** : cochez cette case pour activer la reprise du téléchargement des fichiers.
   - **Prise en charge des commandes inconnues** : cochez la case pour activer la prise en charge des commandes inconnues du client FTP.
   - **Prise en charge de HTTP 0.9** : cochez la case pour activer la prise en charge de HTTP version 0.9.
6. Cliquez sur le bouton **Ensuite**.
7. Dans la fenêtre suivante, définissez les protocoles auxquels il faut appliquer la règle en cochant les cases. Cliquez sur le bouton **Ensuite**.
8. Dans la fenêtre suivante, désignez les entitées réseau dont le trafic de réseau sortant sera soumis à la règle. Pour ajouter une entitée réseau, cliquez sur le bouton **Ajouter**. Cliquez sur le bouton **Ensuite**. Dans la fenêtre suivante, désignez les entitées réseau dont le trafic de réseau entrant sera soumis à la règle. Pour ajouter une entitée réseau, cliquez sur le bouton **Ajouter**. La règle sera appliquée uniquement au trafic qui transite entre les ordinateurs clients et les serveurs mentionnés.
9. Cliquez sur le bouton **Terminer** pour créer la règle ou cliquez sur les boutons **Précédent** et **Suivant** pour naviguer entre les étapes de l'Assistant.

10. Pour que les modifications de la stratégie de l'analyse antivirus entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie inférieure de la fenêtre.

Pour créer une règle d'exclusion de l'analyse, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Ensuite, sélectionnez le nœud **Stratégies**.

2. Cliquez sur **Créer un règle**.

3. Dans le menu déroulant, choisissez l'option **Règle de l'exclusion de l'analyse**. L'Assistant de création de règles s'ouvre.

4. Dans la fenêtre qui s'ouvre, saisissez le **Nom de la règle** dans le champ prévu à cet effet. Le nom de la règle doit être unique. Après avoir saisi le nom, cliquez sur le bouton **Suivant**.

5. Dans la fenêtre suivante, sélectionnez une des valeurs de la liste déroulante :

   - **Exclure tous les objets** : tous les objets seront exclus de l'analyse.

   - **Exclure les types sélectionnés d'objet** : seuls les types de fichiers sélectionnés dans la liste seront exclus de l'analyse. Pour sélectionner le type de fichier requis, cochez la case en regard de son nom.

   - **Analyser tous les objets** : l'exclusion de l'analyse en fonction des types d'objets n'a pas lieu.

6. Cochez ou décochez la case **Analyser le contenu des archives** pour définir la règle de traitement des archives. Cliquez sur le bouton **Ensuite**.

7. Dans la fenêtre suivante, définissez les protocoles auxquels il faut appliquer la règle en cochant les cases. Cliquez sur le bouton **Ensuite**.

8. Dans la fenêtre suivante, désignez les entitées réseau dont le trafic de réseau sortant sera soumis à la règle. Pour ajouter une entitée réseau, cliquez sur le bouton **Ajouter**. Cliquez sur le bouton **Ensuite**. Dans la fenêtre suivante, désignez les entitées réseau dont le trafic de réseau entrant sera soumis à la règle. Pour ajouter une entitée réseau, cliquez sur le bouton **Ajouter**. La règle sera appliquée uniquement au trafic qui transite entre les ordinateurs clients et les serveurs mentionnés.

9. Cliquez sur le bouton **Terminer** pour créer la règle ou cliquez sur les boutons **Précédent** et **Suivant** pour naviguer entre les étapes de l'Assistant.

10. Pour que les modifications de la stratégie de l'analyse antivirus entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie inférieure de la fenêtre.

Pour créer une règle d'analyse antivirus, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Ensuite, sélectionnez le nœud **Stratégies**.

2. Cliquez sur **Créer un règle**.

3. Dans le menu déroulant, choisissez l'option **Règle d'analyse antivirus**. L'Assistant de création de règles s'ouvre.

4. Dans la fenêtre qui s'ouvre, saisissez le **Nom de la règle** dans le champ prévu à cet effet. Le nom de la règle doit être unique. Après avoir saisi le nom, cliquez sur le bouton **Suivant**.

5. Dans la fenêtre suivante, cliquez sur **Modifier** pour sélectionner les types de menaces qui seront bloqués. Dans la fenêtre qui s'ouvre, cochez les cases des types des types de menace, puis cliquez sur **OK**. Vous pouvez également sélectionner des paramètres complémentaires de traitement des objets :

   - **Bloquer les objets suspects** : cochez la case pour bloquer les objets suspects.

- **Tenter de réparer les objets** : cochez la case pour que Kaspersky Anti-Virus répare les objets malveillants si cela est possible.

- **Tenter de supprimer les parties infectées des objets composés** : cochez la case pour que Kaspersky Anti-Virus supprime les parties infectées des objets composés, si cela est possible. La case sera accessible si la case **Tenter de réparer les objets** est cochée.

- **Enregistrer une copie des objets dans la sauvegarde** : cochez la case pour que les objets soient enregistrés sans la sauvegarde avant le blocage, la réparation ou la suppression.

6. Cliquez sur le bouton **Ensuite**.

7. Dans la fenêtre suivante, définissez les paramètres de traitement des objets protégés par un mot de passe :

   - **Ne pas accepter les objets protégés par un mot de passe** : cochez la case pour bloquer les objets protégés par un mot de passe.

   - **Enregistrer une copie des objets dans la sauvegarde** : cochez la case pour que les objets bloqués, protégés par un mot de passe, soient enregistrés dans la sauvegarde. La case sera accessible si la case **Ne pas accepter les objets protégés par un mot de passe** a été cochée.

8. Cliquez sur le bouton **Ensuite**.

9. Dans la fenêtre suivante, définissez les protocoles auxquels il faut appliquer la règle en cochant les cases. Cliquez sur le bouton **Ensuite**.

10. Dans la fenêtre suivante, désignez les entitées réseau dont le trafic de réseau sortant sera soumis à la règle. Pour ajouter une entitée réseau, cliquez sur le bouton **Ajouter**. Cliquez sur le bouton **Ensuite**. Dans la fenêtre suivante, désignez les entitées réseau dont le trafic de réseau entrant sera soumis à la règle. Pour ajouter une entitée réseau, cliquez sur le bouton **Ajouter**. La règle sera appliquée uniquement au trafic qui transite entre les ordinateurs clients et les serveurs mentionnés.

11. Cliquez sur le bouton **Terminer** pour créer la règle ou cliquez sur les boutons **Précédent** et **Suivant** pour naviguer entre les étapes de l'Assistant.

12. Pour que les modifications de la stratégie de l'analyse antivirus entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie inférieure de la fenêtre.

MODIFICATION DE LA PRIORITE D'UNE REGLE DE LA STRATEGIE

Pour modifier la priorité de la règle de la stratégie, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Ensuite, sélectionnez le nœud **Stratégies**.

2. Sélectionnez la règle dans le tableau et cliquez sur le bouton **Haut** pour augmenter la priorité de la règle ou sur **Bas** pour réduire la priorité.

3. Pour que les modifications de la stratégie de l'analyse antivirus entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie inférieure de la fenêtre.

MODIFICATION DES PARAMETRES D'UNE REGLE D'UNE STRATEGIE

Pour modifier les paramètres d'une règle d'une stratégie, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Ensuite, sélectionnez le nœud **Stratégies**.
2. Sélectionnez la règle dans le tableau et cliquez sur le bouton **Propriétés** pour ouvrir la fenêtre des propriétés de la règle. Vous pouvez également ouvrir cette fenêtre d'un double-clic.
3. Modifiez les paramètres de la règle.
4. Cliquez sur le bouton **OK**, pour enregistrer les modifications.
5. Pour que les modifications de la stratégie de l'analyse antivirus entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie inférieure de la fenêtre.

DESACTIVATION DE LA REGLE D'UNE STRATEGIE

Pour désactiver le fonctionnement de la règle de la stratégie, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Ensuite, sélectionnez le nœud **Stratégies**.
2. Sélectionnez la règle dans le tableau, puis cliquez sur le bouton **Propriétés**.
3. Dans la fenêtre qui s'ouvre, à l'onglet **Général**, désélectionnez la case **Activer**.
4. Cliquez sur le bouton **OK**, pour enregistrer les modifications.
5. Pour que les modifications de la stratégie de l'analyse antivirus entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie inférieure de la fenêtre.

Pour activer la règle de la stratégie, procédez comme suit :

SUPPRESSION D'UNE REGLE D'UNE STRATEGIE

Pour supprimer une règle de stratégie, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Ensuite, sélectionnez le nœud **Stratégies**.
2. Sélectionnez la règle dans le tableau, puis cliquez sur le bouton **Supprimer**.
3. Confirmez la suppression de la règle dans la boîte de dialogue qui s'ouvre.
4. Pour que les modifications de la stratégie de l'analyse antivirus entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie inférieure de la fenêtre.

ENTITEES RESEAU

Les entitées réseau doivent être utilisés dans les stratégies. Il existe quatre types d'entitées de réseau :

- **Ordinateur** – Adresse IP de l'ordinateur ;
- **Sous-réseau** : plusieurs ordinateurs dont les adresses se trouvent dans le sous-réseau indiqué ;
- **Plage d'adresses** : plusieurs ordinateurs dont les adresses appartiennent à la plage indiquée ;
- **Noms de domaine** : un ou plusieurs ordinateurs dont le nom de domaine correspond au nom indiqué.

Pour afficher le tableau avec la description des entitées réseau (cf. illustration ci-dessous), cliquez sur le nœud "Entitées réseau".

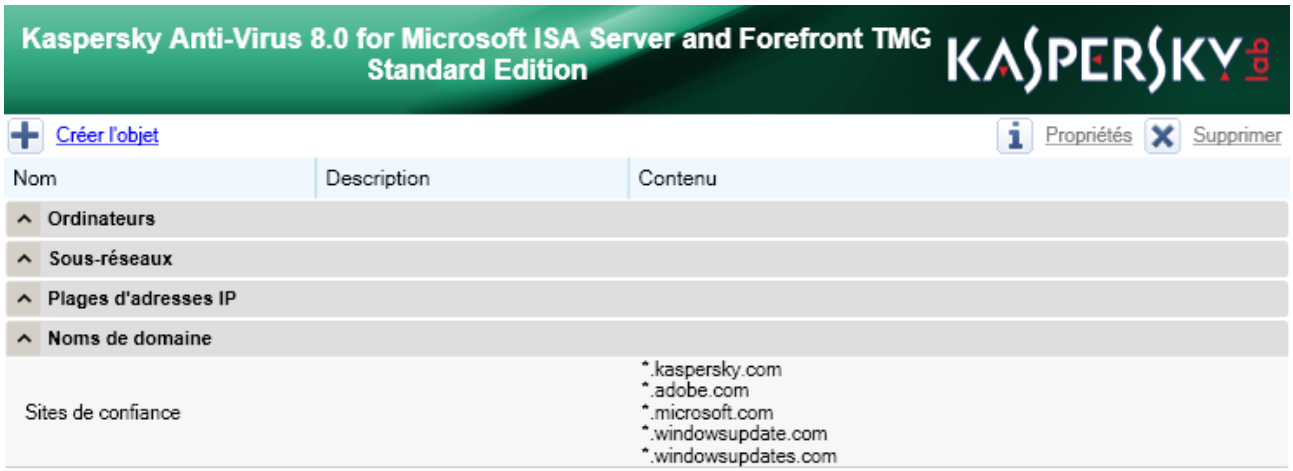

Illustration 8. Fenêtre "Entitées réseau"

DANS CETTE SECTION DE L'AIDE

CRÉATION D'ENTITÉES RÉSEAU

Pour créer une entitée réseau de type "Ordinateur", procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Sélectionnez ensuite le nœud **Stratégies**, puis **Entitées réseau**.
2. Cliquez sur **Créer une entitée**.
3. Dans le menu qui s'ouvre, choisissez l'option **Créer une entitée "Ordinateur"**.
4. Dans la fenêtre qui s'ouvre, définissez les paramètres de l'entitée réseau :

- **Nom** : nom unique de l'entitée réseau ;
- **IP** : adresse IP de l'entitée réseau ;
- **Description** : description détaillée de l'entitée réseau.

5. Cliquez sur **OK** pour enregistrer les modifications et fermer la fenêtre.
6. Pour que les modifications des entitées réseau entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie inférieure de la fenêtre.

Pour créer une entitée réseau de type "Sous-réseau", procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Sélectionnez ensuite le nœud **Stratégies**, puis **Entitées réseau**.
2. Cliquez sur **Créer une entitée**.
3. Dans le menu qui s'ouvre, choisissez l'option **Créer une entitée "Sous-réseau"**.
4. Dans la fenêtre qui s'ouvre, définissez les paramètres de l'entitée réseau :
   - **Nom** : nom unique de l'entitée réseau ;
   - **IP** : adresse IP de l'entitée réseau ;
   - **Masque** : masque de sous-réseau ;
   - **Description** : description détaillée de l'entitée réseau.
5. Cliquez sur **OK** pour enregistrer les modifications et fermer la fenêtre.
6. Pour que les modifications des entitées réseau entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie inférieure de la fenêtre.

Pour créer une entitée réseau de type "Plage d'adresses", procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Sélectionnez ensuite le nœud **Stratégies**, puis **Entitées réseau**.
2. Cliquez sur **Créer une entitée**.
3. Dans le menu qui s'ouvre, choisissez l'option **Créer une entitée "Plage d'adresses"**.
4. Dans la fenêtre qui s'ouvre, définissez les paramètres de l'entitée réseau :
   - **Nom** : nom unique de l'entitée réseau ;
   - **Début de la plage** : adresse IP du début de la plage ;
   - **Fin de la plage** : adresse IP de fin de la plage ;
   - **Description** : description détaillée de l'entitée réseau.
5. Cliquez sur **OK** pour enregistrer les modifications et fermer la fenêtre.
6. Pour que les modifications des entitées réseau entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie inférieure de la fenêtre.

Pour créer une entitée réseau de type "Noms de domaine", procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Sélectionnez ensuite le nœud **Stratégies**, puis **Entitées réseau**.

2. Cliquez sur **Créer une entitée**.

3. Dans le menu qui s'ouvre, choisissez l'option **Créer une entitée "Noms de domaine"**.

4. Dans la fenêtre qui s'ouvre, définissez les paramètres de l'entitée réseau :

   - **Nom** : nom unique de l'entitée réseau ;

   - **Description** : description détaillée de l'entitée réseau.

5. Cliquez sur le bouton **Ajouter** et saisissez le nom de domaine dans la fenêtre qui s'ouvre afin de l'ajouter à la liste **Domaines**. Le bouton **Supprimer** permet de supprimer une entitée de la liste. Le nom de domaine doit contenir le nom sous la forme standard, par exemple microsoft.com ou msdn.microsoft.com. Le nom de domaine peut également contenir le caractère générique ***** qui désigne n'importe quel nombre de domaines de niveau inférieur. Par exemple, le nom de domaine *****.microsoft.com désignera les domaines microsoft.com, www.microsoft.com, files.download.microsoft.com, etc. Le caractère ***** ne peut être utilisé qu'une seule fois dans le nom. Les préfixes du protocole (modèles du style http://*.microsoft.com, ://microsoft.com, etc.) ne peuvent figurer dans le nom de domaine. De tels modèles sont considérés comme erronés et sont ignorés par la stratégie.

6. Cliquez sur **OK** pour enregistrer les modifications et fermer la fenêtre.

7. Pour que les modifications des entitées réseau entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie inférieure de la fenêtre.

MODIFICATION DES PARAMETRES DES ENTITEES RESEAU

Pour modifier les paramètres d'une entitée de réseau de n'importe quel type, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Ensuite, sélectionnez le nœud **Stratégies**, puis **Entitées réseau**.

2. Sélectionnez l'entitée dans le tableau et cliquez sur le bouton **Propriétés** pour ouvrir la fenêtre des propriétés de l'entitée. Vous pouvez également ouvrir cette fenêtre d'un double-clic de la souris sur l'entitée.

3. Modifiez les paramètres de l'entitée réseau, puis cliquez sur **OK** pour enregistrer les modifications.

4. Pour que les modifications des entitées réseau entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie inférieure de la fenêtre.

SUPPRESSION DES ENTITÉES RÉSEAU

Pour supprimer une entitée réseau, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur souhaité dans l'arborescence de la console. Sélectionnez ensuite le nœud **Stratégies**, puis **Entitées réseau**.
2. Sélectionnez l'entitée dans le tableau, puis cliquez sur le bouton **Supprimer**.
3. Confirmez la suppression de l'entitée dans la boîte de dialogue qui s'ouvre.

   L'entitée sélectionné sera supprimé.

L'entitée réseau peut être supprimé uniquement s'il ne participe pas aux stratégies définies d'analyse antivirus.

RAPPORTS

Kaspersky Anti-Virus propose des rapports sur les résultats de la protection des ordinateurs clients contre les virus sur tous les protocoles protégés. Chaque rapport se présente sous la forme d'un tableau qui reprend les événements et les actions survenues pendant l'utilisation de l'application.

Les rapports sont créés automatiquement, conformément à la programmation ou à la demande, et sont enregistrés sur le disque. Le rapport enregistré est un fichier HTML stocké dans le dossier de conservation des données de l'application **Reports**. Les rapports peuvent être consultés à l'aide du navigateur Internet Explorer.

La fenêtre **Rapports** (cf. ill. ci-après) permet de créer, consulter ou supprimer des rapports et configurer leurs paramètres. Les paramètres de composition des rapports sont définis par la tâche de création de rapports.

Pour ouvrir la fenêtre **Rapports**, sélectionnez le nœud correspondant au serveur dans l'arborescence de la console (à gauche), puis le nœud **Rapports**. La fenêtre **Rapports** s'ouvre dans le volet des résultats de la partie droite de la fenêtre. La fenêtre **Rapports** reprend les tâches de création de rapports, les paramètres prévus pour celles-ci et permet de consulter ou de supprimer des rapports dans la liste. La liste contient les éléments suivants :

- **Nom de la tâche** : nom de la tâche de création du rapport.
- **État de la tâche** : état actuel de la tâche de création du rapport.
- **Résultat de l'exécution** : dernier résultat de l'exécution de la tâche de création du rapport.

Le cas échéant, il est possible d'ajouter d'autres tâches avec les paramètres sélectionnés de la période de rapport, le nom, la description et le niveau de détail du rapport.

Illustration 9. Fenêtre "Rapports"

DANS CETTE SECTION DE L'AIDE

CREATION D'UNE TACHE DE GENERATION DE RAPPORT

Pour créer une tâche de génération de rapport, procédez comme suit :

1. Sélectionnez, dans l'arborescence de la console, le nœud correspondant au serveur requis, puis choisissez le nœud Rapports. **Rapports**. La fenêtre **Rapports** s'ouvre dans le volet des résultats de la partie droite de la fenêtre.

2. Cliquez sur le bouton **Ajouter**. L'Assistant d'ajout de tâches de génération de rapport s'ouvre.

3. Dans la première fenêtre de l'Assistant de nouveau rapport **Informations relatives à la tâche**, indiquez le nom de la tâche dans le champ **Nom de la tâche** et la description dans le champ **Description**. Cliquez sur le bouton **Ensuite**.

4. Dans la fenêtre suivante **Paramètres du rapport**, indiquez le niveau de détail du rapport : **standard** ou **détaillé**. Sélectionnez la période qui sera couverte par le rapport. Cliquez sur le bouton **Ensuite**.

5. La fenêtre suivante **Paramètres du rapport** permet de sélectionner le mode automatique de génération du rapport. Pour ce faire, cochez la case **Créer un rapport automatiquement** et programmez la création du rapport. Si la case n'est pas cochée, vous devrez lancer la création du rapport manuellement. Cliquez sur le bouton **Terminer**.

   La nouvelle tâche de génération de rapport est créée et elle apparaît dans la liste avec les paramètres définis. Si vous avez choisi la génération automatique de rapport, la création du rapport aura lieu à l'heure indiquée. En cas de sélection de la création manuelle du rapport, celui-ci est créé après que vous ayez cliqué sur le bouton **Créer un rapport**.

L'état d'exécution de la tâche de génération d'un rapport apparaît dans la colonne **État de la tâche** du tableau général des rapports.

Le rapport ne reprendra pas les données remises à zéro si la date de remise à zéro des statistiques tombe dans l'intervalle de temps couvert par le rapport. Les données statistiques du rapport peuvent être supprimées manuellement. Elles sont également supprimées automatiquement à l'échéance de la durée de conservation prévue (par défaut, un an).

CONSULTATION DU RAPPORT

Pour consulter le rapport, procédez comme suit :

1. Sélectionnez, dans l'arborescence de la console, le nœud correspondant au serveur, puis choisissez le nœud **Rapports**. La fenêtre **Rapports** s'ouvre dans le volet des résultats de la partie droite de la fenêtre.

2. Choisissez dans la liste la tâche de génération de rapport à utiliser pour obtenir le rapport souhaité.

3. Cliquez sur le bouton **Consulter le rapport**. Le dernier rapport créé en date s'ouvre. La liste de tous les rapports est accessible dans les propriétés de la tâche de génération du rapport sous l'onglet **Rapports**.

4. Dans la fenêtre qui s'ouvre, sélectionnez le rapport requis, puis cliquez sur le bouton **Consulter**. Le contenu du rapport sélectionné apparaîtra dans la nouvelle fenêtre.

SUPPRESSION DU RAPPORT

Pour supprimer le rapport créé, procédez comme suit :

1. Sélectionnez, dans l'arborescence de la console, le nœud correspondant au serveur, puis choisissez le nœud **Rapports**. La fenêtre **Rapports** s'ouvre dans le volet des résultats de la partie droite de la fenêtre.

2. Dans le menu contextuel de la tâche de génération de rapport dont il faut supprimer un rapport, choisissez l'option **Propriétés**. La fenêtre des propriétés de la tâche s'ouvre.

3. Dans la fenêtre qui s'ouvre, choisissez l'onglet **Rapports**.

4. Sélectionnez le rapport, puis cliquez sur **Supprimer**.

SUPPRESSION D'UNE TACHE DE GENERATION DE RAPPORT

Pour supprimer une tâche de génération de rapport, procédez comme suit :

1. Sélectionnez, dans l'arborescence de la console, le nœud correspondant au serveur, puis choisissez le nœud **Rapports**. La fenêtre **Rapports** s'ouvre dans le volet des résultats de la partie droite de la fenêtre.

2. Dans le menu contextuel de la tâche de génération de rapports, choisissez l'option **Supprimer**.

MODIFICATION DES PARAMETRES DE LA GENERATION DU RAPPORT

Pour modifier les propriétés de la tâche de génération du rapport, procédez comme suit :

1. Sélectionnez, dans l'arborescence de la console, le nœud correspondant au serveur, puis choisissez le nœud **Rapports**. La fenêtre **Rapports** s'ouvre dans le volet des résultats de la partie droite de la fenêtre.

2. Dans le menu contextuel de la tâche de génération de rapports, choisissez l'option **Propriétés**. La fenêtre des propriétés de la tâche s'ouvre.

3. Modifiez les propriétés de la tâche (cf. rubrique "Création d'une tâche de génération de rapport" à la page 52).

MODIFICATION DES PROPRIETES GENERALES DES RAPPORTS

Pour modifier les propriétés générales des rapports, procédez comme suit :

1. Sélectionnez, dans l'arborescence de la console, le nœud correspondant au serveur, puis choisissez le nœud **Rapports**. Ouvrez le menu contextuel et sélectionnez l'option **Propriétés**. La fenêtre des propriétés générales des rapports s'ouvre.

2. Dans la fenêtre qui s'ouvre, vous pouvez activer/désactiver la création de rapports en cochant ou en décochant la case **Activer la consignation des statistiques**.

3. Pour configurer la durée de conservation des données statistiques, choisissez la période souhaitée dans le champ **Durée de conservation**.

4. Pour restaurer les paramètres par défaut, cliquez sur **Rétablir les valeurs par défaut**.

SUPPRESSION DES STATISTIQUES DES RAPPORTS

Les données statistiques qui servent à générer les rapports sont conservés dans une base de données spécifique. Les données sont supprimées automatiquement à l'issue de la période de conservation définie dans les propriétés générales des rapports (par défaut, un an). En cas d'accumulation d'un nombre important de données dans la base, la vitesse de traitement de celles-ci peut ralentir. Le cas échéant, vous pouvez supprimer manuellement les données statistiques.

Pour supprimer les données statistiques, procédez comme suit :

1. Ouvrez la fenêtre des propriétés générales des applications (cf. rubrique "Modification des paramètres généraux des rapports" à la page 54).

2. Cliquez sur le bouton **Supprimer les données statistiques**.

CONTROLE DU FONCTIONNEMENT DE L'APPLICATION

La fenêtre **Contrôle** (cf. illustration ci-dessous) est prévue pour contrôler le fonctionnement de Kaspersky Anti-Virus. Elle reprend les informations relatives aux paramètres de fonctionnement de l'application et les statistiques sur les objets analysés. Ces données permettent de contrôler rapidement le fonctionnement de Kaspersky Anti-Virus en vérifiant le fonctionnement des filtres, l'état des mises à jour des bases de l'Antivirus et la licence.

Pour ouvrir la fenêtre **Contrôle**, sélectionnez dans l'arborescence de la console le nœud correspondant au serveur, puis choisissez le nœud **Contrôle**. La fenêtre **Contrôle** s'ouvre dans le panneau des résultats de la partie droite de la fenêtre.

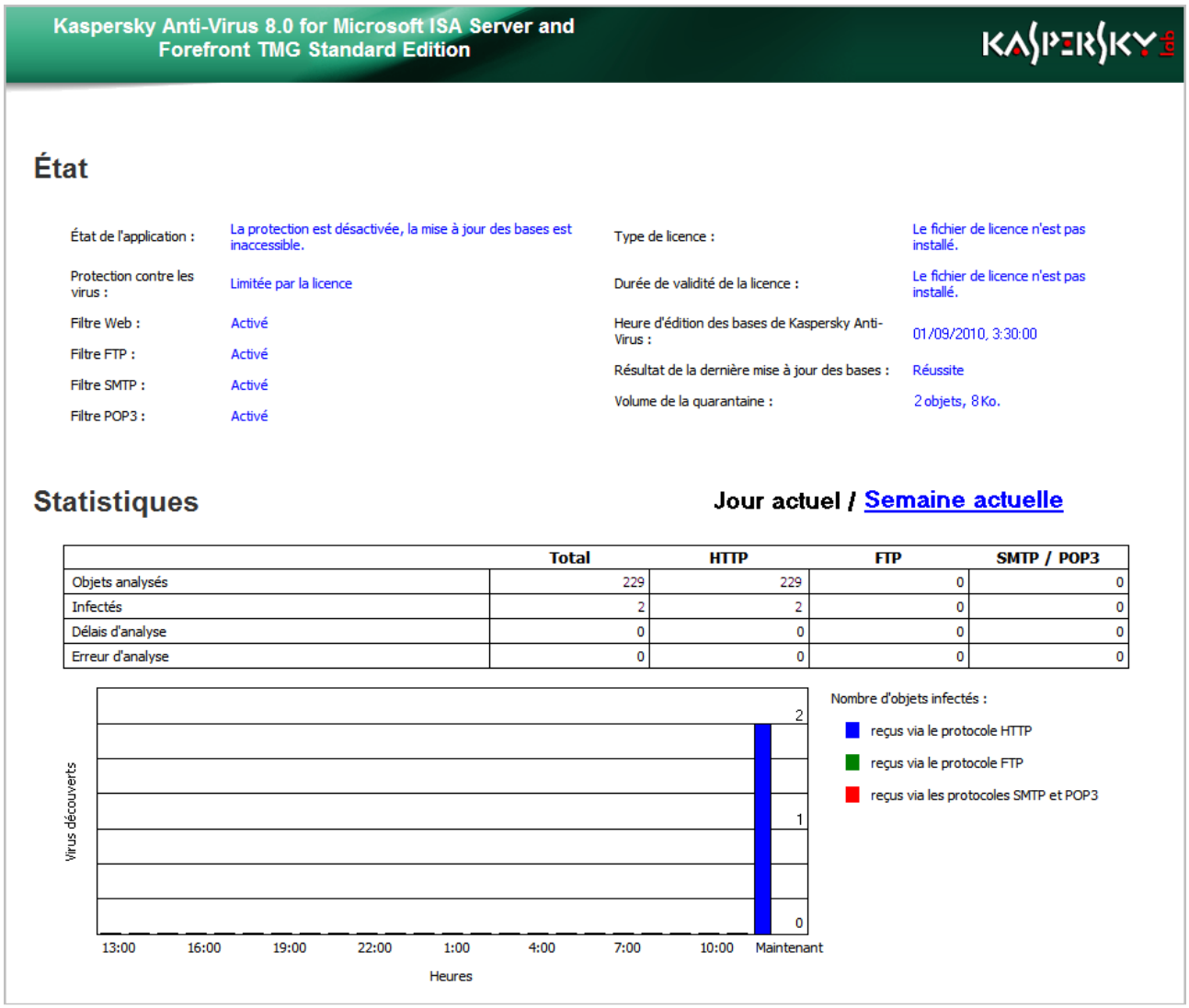

Illustration 10. Fenêtre "Contrôle"

DANS CETTE SECTION DE L'AIDE

ÉTAT DU FONCTIONNEMENT DE KASPERSKY ANTI-VIRUS

Le volet **État** reprend les informations suivantes sur les paramètres de fonctionnement de Kaspersky Anti-Virus :

- **État de l'application** : description de la fonctionnalité de l'application. Les options suivantes sont proposées :
  - Protection désactivée, mise à jour des bases inaccessible ;
  - Seule la mise à jour des bases est accessible ;
  - Fonctionnement sans mise à jour des bases ;
  - Fonctionnalité complète.
- **Protection contre les virus** : état du fonctionnement de la protection contre les virus. Si la protection est désactivée, le trafic des postes clients n'est pas analysé. Les options suivantes sont proposées :
  - Inactive ;
  - Active ;
  - Erreur interne. Protection inaccessible ;
  - Limitée par la licence.
- **Filtres Web, FTP, SMTP, POP3** : état du fonctionnement des filtres (activé/désactivé). La protection du trafic en fonction du protocole est assurée uniquement si le filtre correspondant est activé.
- **Type de licence**– type de licence. Les licences suivantes existent :
  - La licence commerciale, prévue pour l'activation des logiciels de Kaspersky Lab acquis légitimement. La licence commerciale permet d'utiliser ces logiciels pendant la période définie lors de l'achat.
  - La licence d'évaluation permet de découvrir les fonctions des logiciels de Kaspersky Lab pendant une période définie. Les licences d'évaluation sont proposées gratuitement par Kaspersky Lab.

Si aucune licence n'est installée, le champ affichera une erreur avec la cause.

- **Durée de validité de la licence** : date jusqu'à laquelle la licence actuelle sera valide.
- **Heure d'édition des bases de l'Antivirus** : date et heure d'édition des bases utilisées par Kaspersky Anti-Virus.
- **Résultat de la dernière mise à jour des bases** : résultat de la dernière mise à jour des bases de l'Antivirus.
- **Volume de la sauvegarde** : total des objets placés dans la sauvegarde et espace occupé sur le disque (en Ko).

STATISTIQUES DU FONCTIONNEMENT DE KASPERSKY ANTI-VIRUS

Le volet **Statistiques** reprend les données statistiques relatives aux objets analysés. Le tableau reprend les informations relatives au nombre d'objets analysés, aux objets infectés, aux délais d'attente dépassés lors de l'analyse d'un objet, ainsi que les erreurs d'analyse. Toutes les données sont fournies globalement et pour les protocoles HTTP, FTP, SMTP / POP3. Les informations peuvent porter sur les **dernières 24 heures** ou **la dernière semaine**. Pour permuter l'affichage, utilisez les liens correspondants.

Sous le tableau se trouve un graphique du nombre d'objets infectés découverts selon une ligne du temps (par heure, pour le graphique des dernières 24 heures ou, par jour pour le graphique par semaine). Les objets bleus sont les objets reçus via le protocole HTTP, les objets verts sont reçus par le protocole FTP, les objets rouges sont reçus par les protocoles SMTP et POP3.

SAUVEGARDE

Le dossier de sauvegarde est une banque où se trouvent les copies inchangées des objets dangereux ou protégés par un mot de passe et réalisées avant le traitement des objets en question. Cette copie pourra être restaurée ultérieurement ou supprimée. La possibilité de restauration est utile, par exemple, si des données ont été perdues lors de la réparation de l'objet. Les objets sont conservés sous un format spécial et ne présentent aucun danger pour l'ordinateur de l'utilisateur.

La fenêtre (cf. illustration ci-dessous) contient la liste des objets qui se trouvent dans le dossier de sauvegarde. Vous pouvez exécuter les opérations suivantes sur les objets :

- Consulter les informations sur les objets du dossier de sauvegarde ;
- Enregistrer les informations sur le disque ;
- Supprimer les objets ;
- Enregistrer la liste des objets sur le disque.

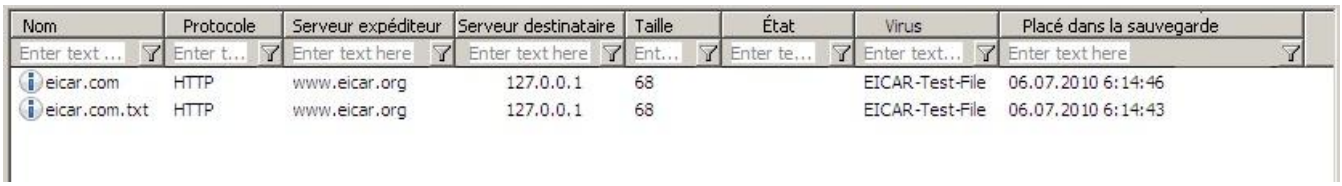

Illustration 11. Fenêtre "Dossier de sauvegarde"

Pour faciliter la recherche d'objets, vous pouvez utiliser les filtres : dynamiques (cf. rubrique "Filtrage dynamique de la liste d'objets" à la page 60) et statiques (cf. rubrique "Création d'un filtre statique dans le dossier de sauvegarde" à la page 61).

DANS CETTE SECTION DE L'AIDE

PARAMETRES DE FONCTIONNEMENT DE LA SAUVEGARDE

Pour ouvrir la fenêtre de configuration des paramètres de la sauvegarde, sélectionnez le nœud du serveur correspondant dans l'arborescence de la console, puis choisissez **Dossier de sauvegarde**. Cliquez avec le bouton droit de la souris dans le volet des résultats à droite pour ouvrir le menu contextuel et sélectionnez l'option **Propriétés**.

Les valeurs suivantes sont attribuées par défaut aux paramètres :

- **Taille maximale de la sauvegarde** : 1 024 Mo. Si la taille de l'objet mis dans la sauvegarde fait passer la taille du dossier au-delà de la valeur indiquée, l'objet le plus ancien sera supprimé.
- **Durée maximale de conservation de l'objet** : 30 jours. À l'issue de la période indiquée, l'objet sera supprimé automatiquement.
- **Nombre maximum d'objets dans la banque** : 1 million. Quand cette valeur est dépassée, l'objet le plus ancien est supprimé.

Pour rétablir les paramètres par défaut, cliquez sur le bouton **Rétablir les valeurs par défaut**.

CONSULTATION DES INFORMATIONS SUR LES OBJETS DU DOSSIER DE SAUVEGARDE

Pour consulter les informations sur l'objet dans la sauvegarde, procédez comme suit :

1. Sélectionnez, dans l'arborescence de la console, le nœud correspondant au serveur, puis choisissez le nœud **Dossier de sauvegarde**. La fenêtre **Dossier de sauvegarde** s'ouvre dans le panneau des résultats à droite sous la forme d'un tableau contenant tous les objets de la banque.
2. Localisez l'objet dans le tableau et consultez ses propriétés. Le cas échéant, vous pouvez utiliser un filtre (cf. rubrique "Filtrage dynamique de la liste des objets" à la page 60).

Vous pouvez obtenir des informations plus détaillées sur chaque objet en choisissant l'option **Propriétés** du menu contextuel. Les données suivantes seront reprises dans la fenêtre qui s'ouvre :

- **Nom** : nom du fichier.
- **Description** : lien vers la description de l'objet.
- **Virus** : nom du virus.
- **Protocole** : protocole dont le trafic contenait l'objet découvert.
- **Serveur expéditeur** : serveur d'où provient le fichier.
- **Serveur destinataire** : serveur ayant reçu le fichier.
- **Etat** – état de l'objet.
- **Placé dans la sauvegarde** : date et heure du placement de l'objet dans la sauvegarde.
- **Taille** – taille de l'objet.
- **Date d'édition des bases** : date et heure d'édition des bases de Kaspersky Anti-Virus qui ont permis de découvrir l'objet.

CONFIGURATION DE L'AFFICHAGE EXTERIEUR DU DOSSIER DE SAUVEGARDE

Vous pouvez configurer l'affichage de la sauvegarde en ajoutant ou en supprimant certaines colonnes du tableau.

Pour ajouter ou supprimer des colonnes au tableau de la sauvegarde, procédez comme suit :

1. Sélectionnez, dans l'arborescence de la console, le nœud correspondant au serveur, puis choisissez le nœud **Dossier de sauvegarde**. La fenêtre **Dossier de sauvegarde** s'ouvre dans le panneau des résultats à droite.

2. Dans le menu contextuel de la fenêtre, choisissez l'option **Affichage**, puis les options **Ajouter / Supprimer des colonnes**.

3. Dans la boîte de dialogue **Ajouter / Supprimer des colonnes** qui s'ouvre, cliquez sur le bouton **Ajouter** ou **Supprimer** pour déplacer des colonnes de la liste des colonnes disponibles dans la liste des colonnes affichées dans le panneau des résultats ou vice-versa.

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

Appuyez sur la combinaison de touches **Ctrl+NumPlus** pour adapter automatiquement la largeur de la colonne à son contenu.

FILTRAGE DYNAMIQUE DE LA LISTE DES OBJETS

L'utilisation de filtres dynamiques permet de rechercher et de structurer les informations présentées dans la sauvegarde car après l'application du filtre, les seuls informations disponibles seront celles qui répondent aux critères du filtre. Le filtrage dynamique peut être réalisé dans n'importe quelle colonne de la liste.

Pour filtrer les objets selon une condition définie à l'aide d'un filtre dynamique, procédez comme suit :

1. Sélectionnez, dans l'arborescence de la console, le nœud correspondant au serveur, puis choisissez le nœud **Dossier de sauvegarde**. La fenêtre **Dossier de sauvegarde** s'ouvre dans le panneau des résultats à droite sous la forme d'un tableau contenant tous les objets de la banque.

2. Vous trouverez dans la partie supérieure du tableau les champs de saisie des conditions du filtre dynamique. Définissez la condition de filtrage, en indiquant dans chaque colonne la valeur requise (vous pouvez filtrer les objets selon les valeurs d'une ou de plusieurs colonnes).

3. Le filtre est appliqué automatiquement quelques secondes après avoir saisi la valeur ou après avoir appuyé sur la touche **ENTRÉE** dans le champ de saisie. Le filtre est également appliqué directement après la sélection de l'option dans le menu déroulant ou après avoir cliqué sur le bouton **OK** dans la boîte de dialogue, lorsque celle-ci est proposée. Pour appliquer le filtre, il est également possible de cliquer sur le bouton en regard du champ de saisie de la condition (pour filtre selon une seule condition) ou sur le bouton **Mettre à jour** dans la barre d'outils de Kaspersky Anti-Virus.

Vous pouvez forcer l'actualisation de l'affichage du tableau avec les informations sur les objets de la sauvegarde en appuyant sur la touche **F5**. Vous pouvez ainsi suivre en temps réel la mise à jour des informations sur les objets placés dans la sauvegarde.

Pour annuler le filtre dynamique et afficher à nouveau toutes les entrées du tableau, supprimez tous les caractères du champ et appliquez le filtre ou choisissez l'option **Tous** dans le menu de la colonne requise du tableau.

CREATION D'UN FILTRE STATIQUE DANS LA SAUVEGARDE

Pour utiliser à plusieurs reprises les paramètres du filtre, vous pouvez créer un filtre statique dans le nœud **Dossier de sauvegarde** de l'arborescence de la Console d'administration.

Pour créer un filtre statique, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le nœud **Dossier de sauvegarde**.
2. Ouvrez le menu contextuel et sélectionnez l'option **Nouveau filtre**. La fenêtre de l'Assistant de création d'un filtre s'ouvre.
3. Réalisez les actions indiquées à chaque étape de l'Assistant.

Pour appliquer le filtre créé, cliquez sur le bouton à côté du champ dans le tableau du filtre et sélectionnez l'option portant le nom du filtre dans le menu contextuel.

ENREGISTREMENT SUR LE DISQUE D'UN OBJET DE LA SAUVEGARDE

Pour enregistrer n'importe quel objet de la sauvegarde sur le disque, procédez comme suit :

1. Dans l'arborescence de la console sélectionnez l'entrée **Dossier de sauvegarde**.
2. Sélectionnez l'objet à restaurer dans le tableau qui montre le contenu de la banque. Pour chercher l'objet, vous pouvez utiliser un filtre (cf. rubrique "Filtrage dynamique de la liste des objets" à la page 60).
3. Ouvrez le menu contextuel et cliquez sur l'option **Enregistrer sur le disque** ou choisissez l'option équivalente dans le menu **Action**.
4. Dans le message d'avertissement qui apparaît, confirmez la restauration de l'objet en cliquant sur **Oui**.
5. Dans la fenêtre qui s'ouvre, indiquez le dossier dans lequel l'objet restauré sera enregistré et, le cas échéant, saisissez un nom pour l'objet ou modifiez le nom existant.
6. Cliquez sur le bouton **Enregistrer**.

L'objet est décrypté, sa copie est placée dans le dossier indiqué et enregistrée sous le nom défini. L'objet restauré retrouvera son format d'origine. Un message de circonstance apparaît à l'écran pour confirmer la réussite de la restauration de l'objet.

ENREGISTREMENT DE LA LISTE DES OBJETS DE LA SAUVEGARDE

Vous pouvez enregistrer la liste des objets de la sauvegarde dans un fichier texte. Les informations relatives aux objets seront présentées sous la forme d'un tableau.

Pour enregistrer la liste des objets de la sauvegarde dans un fichier texte, procédez comme suit :

1. Sélectionnez, dans l'arborescence de la console, le nœud correspondant au serveur, puis choisissez le nœud **Dossier de sauvegarde**.
2. Dans le menu contextuel du nœud **Dossier de sauvegarde**, choisissez l'option **Export List**.

3. Dans la boîte de dialogue qui s'ouvre, indiquez le dossier et le nom du fichier dans lequel la liste des objets sera exportée.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer le fichier.

SUPPRESSION D'UN OBJET DE LA SAUVEGARDE

Les objets suivants sont supprimés automatiquement de la sauvegarde :

- L'objet le plus ancien, si l'ajout d'un nouvel objet fait passer le nombre d'objets de la banque à plus d'un million.
- Les objets les plus anciens quand une restriction sur la taille de la sauvegarde a été définie et que l'ajout d'un nouvel objet entraîne le dépassement de cette limite.
- Les objets dont la durée de conservation a expiré, pour autant qu'une telle limite ait été définie.

Il est possible également de supprimer manuellement les objets de la sauvegarde. Cette option peut se révéler utile afin de supprimer les objets qui ont bien été restaurés où envoyés pour examen ou pour gagner de la place dans la sauvegarde lorsque le mode de suppression automatique des objets n'est pas approprié.

Pour supprimer manuellement les objets de la sauvegarde, procédez comme suit :

1. Sélectionnez, dans l'arborescence de la console, le nœud **Dossier de sauvegarde**.

2. Sélectionnez les objets à supprimer dans le tableau qui montre le contenu de la banque. Pour chercher les objets, vous pouvez utiliser un filtre (cf. rubrique "Filtrage dynamique de la liste des objets" à la page 60). Vous pouvez supprimer quelques fichiers ou tous les fichiers. Pour ce faire, sélectionnez tous les fichiers que vous souhaitez supprimer.

3. Ouvrez le menu contextuel et cliquez sur l'option **Supprimer** ou choisissez l'option équivalente dans le menu **Action**.

4. Confirmez la suppression dans la boîte de dialogue qui s'ouvre.

Les objets seront ensuite supprimés de la sauvegarde.

DIAGNOSTIC

Vous pouvez configurer la tenue des journaux des événements de Kaspersky Anti-Virus pour pouvoir diagnostiquer son fonctionnement à n'importe quelle étape du filtrage antivirus des flux de données.

Pour ouvrir la fenêtre de configuration des paramètres de diagnostic, procédez comme suit :

1. Sélectionnez, dans l'arborescence de la console, le nœud correspondant au serveur.
2. Cliquez sur le bouton **Paramètres généraux** situé dans le volet des résultats à droite.
3. Choisissez l'onglet **Diagnostic** (cf. illustration ci-dessous).

Voici les différents types de journaux :

- **Texte** : le journal contient des informations sur le fonctionnement de l'application pour le volume défini à la date donnée. Format du nom du journal : kavisaAAAAMMJJ.log, où JJ est le jour d'aujourd'hui, MM, le mois et AAAA l'année.
- **Texte** : le journal contient des informations sur le fonctionnement des filtres pour le volume défini à la date donnée. Format du nom du journal : kavfltAAAAMMJJ.log, où JJ est le jour d'aujourd'hui, MM, le mois et AAAA l'année.
- **Virus** : le journal contient des informations sur les objets malveillants découverts dans le volume défini à la date donnée. Format du nom du journal : viruslogAAAAMMJJ.log, où JJ est le jour d'aujourd'hui, MM, le mois et AAAA l'année.

Les journaux sont sauvegardés dans le dossier, chemin indiqué dans le champ **Dossier de journaux sur le serveur**. Vous pouvez modifier les paramètres de journalisation suivants :

- **Niveau de diagnostic**. Pour tous les journaux, vous pouvez choisir le niveau de détail suivant :
  - **Autre** – niveau de détail des journaux configurable. Seul le journal texte est accessible. Pour configurer une entrée, cliquez sur Configuration précise et sélectionnez le niveau de détail pour chaque composant du programme.
  - **Ne pas enregistrer** : aucune information n'est enregistrée dans les journaux.
  - **Minimal** : consigner dans le journal uniquement les événements principaux. Cette valeur est sélectionnée par défaut.
  - **Moyenne** : consigner, en plus des événements principaux, toute une série d'événements complémentaires qui définissent plus en détails le fonctionnement de Kaspersky Anti-Virus.
  - **Maximum** : consigne dans le journal l'information la plus complète sur le fonctionnement de l'application, à l'exception des messages de débogage.
  - **Debug** – toutes les informations seront sauvegardées dans le journal, y compris celles concernant le débogage. A ce niveau de diagnostic, un grand nombre de messages peut s'afficher, ce qui peut provoquer une chute de performance et un manque d'espace libre sur le disque dur. Il est recommandé d'activer ce mode uniquement pour diagnostiquer des erreurs dans le fonctionnement du programme.
- **Enregistrer l'heure à laquelle l'événement s'est produit**. Format de l'heure : **temps universel coordonnée (TUC)** ou **heure locale du serveur**. La valeur par défaut est **TUC**.
- **Ne pas conserver plus de N fichiers de chaque journal**. Nombre de journaux sauvegardés sur le disque. Le paramètre N peut prendre une valeur comprise entre 1 et 365. La valeur par défaut est 5.

- **Créer un fichier de journal une fois par T**. T est la périodicité de journalisation. Les nouveaux fichiers peuvent être créés tous les jours, toutes les semaines ou tous les mois. La valeur par défaut est mois.

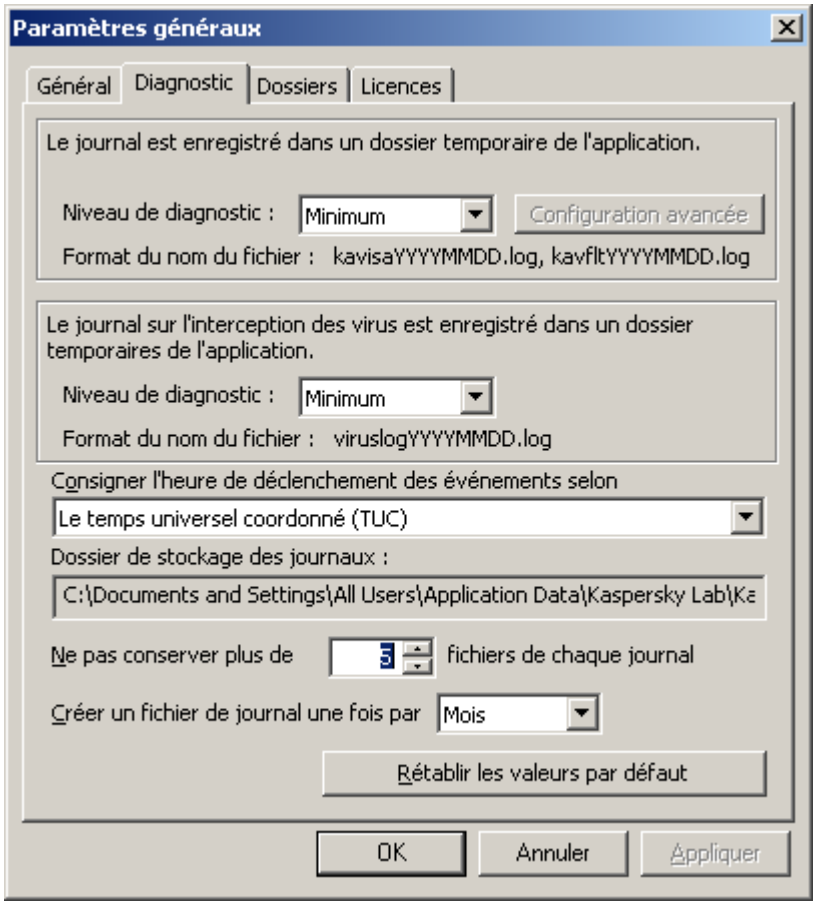

Illustration 12. Onglet "Diagnostic"

MODIFICATION DE L'EMPLACEMENT DU DOSSIER DES DONNEES DE L'APPLICATION

Pour modifier l'emplacement du dossier de conservation des données de l'application avec toutes les données qu'il contient, utilisez l'utilitaire de migration **DataMigrationTool.exe**.

Pour modifier l'emplacement du dossier des données de l'application, procédez comme suit :

1. Ouvrez la fenêtre de la console Microsoft Windows. Vous pouvez ouvrir cette fenêtre d'une des manières suivantes :

   - Utilisez la combinaison de touches **WINDOWS + R**.

   - Dans la boîte de dialogue **Exécuter** qui s'ouvre, saisissez `cmd`, puis appuyez sur la touche **ENTRÉE**.

2. Passez du dossier de travail de la console Microsoft Windows au dossier d'installation de Kaspersky Anti-Virus à l'aide de l'instruction `cd [chemin d'accès au dossier d'installation de l'application]`. Par exemple, `cd C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG Standard Edition\`. Le chemin d'accès au dossier d'installation de Kaspersky Anti-Virus figure dans la fenêtre **Paramètres généraux**, sous l'onglet **Dossiers** de la console d'administration dans le champ **Dossier d'installation de l'application**.

3. Dans la console Microsoft Windows, exécutez l'instruction `DataMigrationTool.exe [chemin d'accès au nouveau dossier de données de l'application]`. Par exemple, `DataMigrationTool.exe c:\data\KAV4ISA`. Si le nouveau dossier de conservation des données de Kaspersky Anti-Virus existe déjà, alors il doit être vide.

4. Appuyez sur la barre **D'ESPACE** pour confirmer la migration du dossier des données.

5. Par la suite, l'utilitaire arrêtera les services de Microsoft Firewall et Kaspersky Anti-Virus, analysera toutes les conditions requises pour une migration réussie et commencera à copier les fichiers. Une fois les fichiers copiés et les modifications enregistrées dans la configuration, l'utilitaire lancera automatiquement les services suspendus.

6. Une fois que l'utilitaire aura terminé ses tâches, le message suivant sera affiché : les données ont été migrées dans le dossier [chemin d'accès au nouveau dossier des données de l'application].

Le chemin d'accès au dossier des données de l'application figure dans la fenêtre **Paramètres généraux**, sous l'onglet **Dossiers** de la console d'administration dans le champ **Dossier d'enregistrement des données de l'application**.

ACTIVATION DE L'INSPECTION DU TRAFIC HTTPS

S'agissant de Forefront TMG, il est possible également d'analyser le trafic entrant via le protocole HTTPS. Il n'y a pas de configuration spéciale pour l'analyse du trafic HTTPS. Les paramètres d'analyse du protocole HTTP sont appliqués. Pour que Kaspersky Anti-Virus puisse analyser le trafic HTTPS, il faut activer l'inspection du trafic dans la console d'administration de Forefront TMG.

Pour activer l'inspection du trafic HTTPS, procédez comme suit :

1. Ouvrez la console d'administration de Forefront TMG.
2. Dans l'arborescence de la console d'administration, sélectionnez le nœud du serveur, puis le nœud **Web Access Policy**.
3. Sous l'onglet **Tasks**, cliquez sur le bouton **Configure HTTPS Inspection**.
4. Dans la fenêtre **HTTPS Outbound Inspection** qui s'ouvre, sous l'onglet **General**, cochez la case **Enable HTTPS Inspection**.
5. Cliquez sur **OK**, pour fermer la fenêtre.
6. Cliquez sur **Apply** pour enregistrer les modifications apportées et actualiser la configuration.

ANNEXE 1. MODIFICATIONS DANS LA BASE DE REGISTRES MICROSOFT WINDOWS

Lors de l'installation de Kaspersky Anti-Virus sur une plateforme 32 bits, les entrées suivantes de la base de registres Microsoft Windows sont ajoutées/modifiées :

HKEY_CLASSES_ROOT\AppID\{9F99C160-A3C7-438d-9BF8-76BE4D65370B}
HKEY_CLASSES_ROOT\AppID\{BE11C033-F253-400D-A7DC-931F193CDC9F}

HKEY_CLASSES_ROOT\AppID\kavisasrv.exe
HKEY_CLASSES_ROOT\AppID\KavHost.exe

HKEY_CLASSES_ROOT\CLSID\{162D6D1C-BEE9-4ae0-9E63-AA5E451A9985}
HKEY_CLASSES_ROOT\CLSID\{372C6E94-BA70-4493-893E-44A86EFA5FBA}
HKEY_CLASSES_ROOT\CLSID\{583F03A3-E02B-46D7-839D-4CBC63F82D59}
HKEY_CLASSES_ROOT\CLSID\{5CCFC1A2-A174-4A6C-9F84-B33C5FE14BF1}
HKEY_CLASSES_ROOT\CLSID\{620FF8BD-4798-4807-A2AB-F625B0EB3B44}
HKEY_CLASSES_ROOT\CLSID\{7A78B705-8CA4-4301-AADF-55F54E6A01AE}
HKEY_CLASSES_ROOT\CLSID\{84C221B0-73E9-4885-A044-30192B4DBC36}
HKEY_CLASSES_ROOT\CLSID\{92C67CDB-A762-43a7-A96D-E1A9D15686A5}
HKEY_CLASSES_ROOT\CLSID\{948600BB-5D4E-4808-B338-312257496A69}
HKEY_CLASSES_ROOT\CLSID\{9F3FD649-0012-4245-A443-CC23CFF9F713}
HKEY_CLASSES_ROOT\CLSID\{CFC47218-E213-405a-859E-2CEE0367ED6F}
HKEY_CLASSES_ROOT\CLSID\{D6E53EF2-B6B2-4A1A-ACF4-0F7B5C656D98}
HKEY_CLASSES_ROOT\CLSID\{D8CF93DF-788A-4699-9071-F3A854E5957C}
HKEY_CLASSES_ROOT\CLSID\{D8EE0CCE-F573-47cb-856B-37540B0DB34F}
HKEY_CLASSES_ROOT\CLSID\{DACDDD16-3454-49cc-B758-693FA413BB64}
HKEY_CLASSES_ROOT\CLSID\{E1F068E0-0FC0-4B8B-BE9A-6BDE3F496080}
HKEY_CLASSES_ROOT\CLSID\{F7CA6538-BCB6-44b0-A266-54C7C921F7C5}

HKEY_CLASSES_ROOT\Interface\{448D32AF-54D0-4BBD-8A81-C368E2C6E533}
HKEY_CLASSES_ROOT\Interface\{B620A5D5-8551-4887-B304-9800387A24CA}

HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmAbout
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmAbout.1
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmComponentData
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmComponentData.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.FtpFilter
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.FtpFilter.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavpop3,Pop3Filter
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavpop3,Pop3Filter.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavsmtp.SmtpFilter
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavsmtp.SmtpFilter.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.Watchdog3
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.Watchdog3.1
HKEY_CLASSES_ROOT\KavHost.KavHost
HKEY_CLASSES_ROOT\KavHost.KavHost.1

HKEY_CLASSES_ROOT\TypeLib\{7FCD1648-8A7B-41AF-B76C-0699922B8770}

HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\FX:{AA517B36-9B43-4246-9122-1AB672E4A6E1}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\NodeTypes\{2F8FE3D1-9A16-4ED3-B6C6-F912D99E99FD}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{162D6D1C-BEE9-4ae0-9E63-AA5E451A9985}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{372C6E94-BA70-4493-893E-44A86EFA5FBA}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{620FF8BD-4798-4807-A2AB-F625B0EB3B44}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{92C67CDB-A762-43a7-A96D-E1A9D15686A5}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{948600BB-5D4E-4808-B338-312257496A69}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{CFC47218-E213-405a-859E-2CEE0367ED6F}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{D8CF93DF-788A-4699-9071-F3A854E5957C}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{D8EE0CCE-F573-47cb-856B-37540B0DB34F}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{F7CA6538-BCB6-44b0-A266-54C7C921F7C5}

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0D40E22B-2FB4-4237-AB63-3FFA9A4CE2EA}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG Standard Edition
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ISAV
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\KAV
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kavisasrv

Lors de l'installation de Kaspersky Anti-Virus sur une plateforme 64 bits, les entrées suivantes de la base de registres Microsoft Windows sont ajoutées/modifiées :

HKEY_CLASSES_ROOT\AppID\{9F99C160-A3C7-438d-9BF8-76BE4D65370B}
HKEY_CLASSES_ROOT\AppID\{BE11C033-F253-400D-A7DC-931F193CDC9F}

HKEY_CLASSES_ROOT\AppID\kavisasrv.exe
HKEY_CLASSES_ROOT\AppID\KavHost.exe

HKEY_CLASSES_ROOT\CLSID\{583F03A3-E02B-46D7-839D-4CBC63F82D59}
HKEY_CLASSES_ROOT\CLSID\{5CCFC1A2-A174-4A6C-9F84-B33C5FE14BF1}
HKEY_CLASSES_ROOT\CLSID\{7A78B705-8CA4-4301-AADF-55F54E6A01AE}
HKEY_CLASSES_ROOT\CLSID\{7CBB6809-47B8-48D5-8ACD-8085935CCF6E}
HKEY_CLASSES_ROOT\CLSID\{84C221B0-73E9-4885-A044-30192B4DBC36}
HKEY_CLASSES_ROOT\CLSID\{9F3FD649-0012-4245-A443-CC23CFF9F713}
HKEY_CLASSES_ROOT\CLSID\{D6E53EF2-B6B2-4A1A-ACF4-0F7B5C656D98}

HKEY_CLASSES_ROOT\Interface\{448D32AF-54D0-4BBD-8A81-C368E2C6E533}
HKEY_CLASSES_ROOT\Interface\{B620A5D5-8551-4887-B304-9800387A24CA}
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmAbout
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmAbout.1
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmComponentData
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmComponentData.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.FtpFilter
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.FtpFilter.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavpop3,Pop3Filter
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavpop3,Pop3Filter.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavsmtp.SmtpFilter
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavsmtp.SmtpFilter.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.Watchdog3
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.Watchdog3.1
HKEY_CLASSES_ROOT\KavHost.KavHost
HKEY_CLASSES_ROOT\KavHost.KavHost.1

HKEY_CLASSES_ROOT\TypeLib\{7FCD1648-8A7B-41AF-B76C-0699922B8770}

HKEY_CLASSES_ROOT\Wow6432Node\AppID\{9F99C160-A3C7-438d-9BF8-76BE4D65370B}
HKEY_CLASSES_ROOT\Wow6432Node\AppID\{BE11C033-F253-400D-A7DC-931F193CDC9F}

HKEY_CLASSES_ROOT\Wow6432Node\AppID\KavHost.exe
HKEY_CLASSES_ROOT\Wow6432Node\AppID\kavisasrv.exe

HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{162D6D1C-BEE9-4ae0-9E63-AA5E451A9985}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{372C6E94-BA70-4493-893E-44A86EFA5FBA}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{5CCFC1A2-A174-4A6C-9F84-B33C5FE14BF1}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{620FF8BD-4798-4807-A2AB-F625B0EB3B44}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{7A78B705-8CA4-4301-AADF-55F54E6A01AE}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{7CBB6809-47B8-48D5-8ACD-8085935CCF6E}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{92C67CDB-A762-43a7-A96D-E1A9D15686A5}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{948600BB-5D4E-4808-B338-312257496A69}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{9F3FD649-0012-4245-A443-CC23CFF9F713}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{CFC47218-E213-405a-859E-2CEE0367ED6F}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{D8CF93DF-788A-4699-9071-F3A854E5957C}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{D8EE0CCE-F573-47cb-856B-37540B0DB34F}

HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{DACDDD16-3454-49cc-B758-693FA413BB64}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{E1F068E0-0FC0-4B8B-BE9A-6BDE3F496080}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{F7CA6538-BCB6-44b0-A266-54C7C921F7C5}

HKEY_CLASSES_ROOT\Wow6432Node\Interface\{448D32AF-54D0-4BBD-8A81-C368E2C6E533}
HKEY_CLASSES_ROOT\Wow6432Node\Interface\{B620A5D5-8551-4887-B304-9800387A24CA}

HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.IsaMmc.IsaAdmAbout
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.IsaMmc.IsaAdmAbout.1
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.IsaMmc.IsaAdmComponentData
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.IsaMmc.IsaAdmComponentData.1
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.FtpFilter
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.FtpFilter.1
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.isavpop3,Pop3Filter
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.isavpop3,Pop3Filter.1
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.isavsmtp.SmtpFilter
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.isavsmtp.SmtpFilter.1
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.Watchdog3
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.Watchdog3.1
HKEY_CLASSES_ROOT\Wow6432Node\KavHost.KavHost
HKEY_CLASSES_ROOT\Wow6432Node\KavHost.KavHost.1

HKEY_CLASSES_ROOT\Wow6432Node\TypeLib\{7FCD1648-8A7B-41AF-B76C-0699922B8770}

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\FX:{AA517B36-9B43-4246-9122-1AB672E4A6E1}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\NodeTypes\{2F8FE3D1-9A16-4ED3-B6C6-F912D99E99FD}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{162D6D1C-BEE9-4ae0-9E63-AA5E451A9985}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{372C6E94-BA70-4493-893E-44A86EFA5FBA}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{620FF8BD-4798-4807-A2AB-F625B0EB3B44}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{92C67CDB-A762-43a7-A96D-E1A9D15686A5}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{948600BB-5D4E-4808-B338-312257496A69}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{CFC47218-E213-405a-859E-2CEE0367ED6F}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{D8CF93DF-788A-4699-9071-F3A854E5957C}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{D8EE0CCE-F573-47cb-856B-37540B0DB34F}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{F7CA6538-BCB6-44b0-A266-54C7C921F7C5}

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SharedDLLs
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{0D40E22B-2FB4-4237-AB63-3FFA9A4CE2EA}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG Standard Edition
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\ISAV
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\KAV
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kavisasrv

INFORMATIONS SUR LE CODE TIERS

DANS CETTE SECTION DE L'AIDE

CODE DE L'APPLICATION

Informations relatives au code logiciel d'éditeurs tiers utilisé dans le développement de l'application.

DANS CETTE SECTION DE L'AIDE

A C# IP ADDRESS CONTROL

BOOST 1.36.0, 1.39.0

EXPAT 1.2

LOKI 0.1.3

LZMALIB 4.43

MICROSOFT CABINET SOFTWARE DEVELOPMENT KIT

SQLITE 3.6.18

WIX 3.0

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

ZLIB 1.0.8, 1.2, 1.2.3

Copyright (C) 1995-1998, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

AUTRES INFORMATIONS

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.

La bibliothèque du programme "Agava-C", développée par OOO "R-Alpha", est utilisée pour vérifier une signature numérique.

CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB

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

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

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

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

1. Définitions

1.1. On entend par **Logiciel** le logiciel et toute mise à jour, ainsi que tous les documents associés.

1.2. On entend par **Titulaire des droits** (propriétaire de tous les droits exclusifs ou autres sur le Logiciel) Kaspersky Lab ZAO, une société de droit russe.

1.3. On entend par **Ordinateur(s)** le matériel, en particulier les ordinateurs personnels, les ordinateurs portables, les stations de travail, les assistants numériques personnels, les " téléphones intelligents ", les appareils portables, ou autres dispositifs électroniques pour lesquels le Logiciel a été conçu où le Logiciel sera installé et/ou utilisé.

1.4. On entend par **Utilisateur final (vous/votre)** la ou les personnes qui installent ou utilisent le Logiciel en son ou en leur nom ou qui utilisent légalement le Logiciel ; ou, si le Logiciel est téléchargé ou installé au nom d'une entité telle qu'un employeur, *" Vous "* signifie également l'entité pour laquelle le Logiciel est téléchargé ou installé, et il est déclaré par la présente que ladite entité a autorisé la personne acceptant ce contrat à cet effet en son nom. Aux fins des présentes, le terme *" entité ",* sans limitation, se rapporte, en particulier, à toute société en nom collectif, toute société à responsabilité limitée, toute société, toute association, toute société par actions, toute fiducie, toute société en coparticipation, toute organisation syndicale, toute organisation non constituée en personne morale, ou tout organisme public.

1.5. On entend par **Partenaire(s)** les entités, la ou les personnes qui distribuent le Logiciel conformément à un contrat et une licence concédée par le Titulaire des droits.

1.6. On entend par **Mise(s) à jour** toutes les mises à jour, les révisions, les programmes de correction, les améliorations, les patchs, les modifications, les copies, les ajouts ou les packs de maintenance, etc.

1.7. On entend par **Manuel de l'utilisateur** le manuel d'utilisation, le guide de l'administrateur, le livre de référence et les documents explicatifs ou autres.

2. Concession de la Licence

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

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

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

2.2. Si le Logiciel a été acquis sur un support physique, Vous avez le droit d'utiliser le Logiciel pour la protection du nombre d'ordinateurs stipulé sur l'emballage du Logiciel.

2.3. Si le Logiciel a été acquis sur Internet, Vous pouvez utiliser le Logiciel pour la protection du nombre d'Ordinateurs stipulé lors de l'acquisition de la Licence du Logiciel.

2.4. Vous ne pouvez faire une copie du Logiciel qu'à des fins de sauvegarde, et seulement pour remplacer l'exemplaire que vous avez acquis de manière légale si cette copie était perdue, détruite ou devenait inutilisable. Cette copie de sauvegarde ne peut pas être utilisée à d'autres fins et devra être détruite si vous perdez le droit d'utilisation du Logiciel ou à l'échéance de Votre licence ou à la résiliation de celle-ci pour quelque raison que ce soit, conformément à la législation en vigueur dans votre pays de résidence principale, ou dans le pays où Vous utilisez le Logiciel.

2.5. À compter du moment de l'activation du Logiciel ou de l'installation du fichier clé de licence (à l'exception de la version de démonstration du Logiciel), Vous pouvez bénéficier des services suivants pour la période définie stipulée sur l'emballage du Logiciel (si le Logiciel a été acquis sur un support physique) ou stipulée pendant l'acquisition (si le Logiciel a été acquis sur Internet) :

- Mises à jour du Logiciel par Internet lorsque le Titulaire des droits les publie sur son site Internet ou par le biais d'autres services en ligne. Toutes les Mises à jour que vous êtes susceptible de recevoir font partie intégrante du Logiciel et les conditions générales de ce Contrat leur sont applicables ;
- Assistance technique en ligne et assistance technique par téléphone.

3. Activation et durée de validité

3.1. Si vous modifiez Votre Ordinateur ou procédez à des modifications sur des logiciels provenant d'autres vendeurs et installés sur celui-ci, il est possible que le Titulaire des droits exige que Vous procédiez une nouvelle fois à l'activation du Logiciel ou à l'installation du fichier clé de licence. Le Titulaire des droits se réserve le droit d'utiliser tous les moyens et toutes les procédures de vérification de la validité de la Licence ou de la légalité du Logiciel installé ou utilisé sur Votre ordinateur.

3.2. Si le Logiciel a été acquis sur un support physique, le Logiciel peut être utilisé dès l'acceptation de ce Contrat pendant la période stipulée sur l'emballage et commençant à l'acceptation de ce Contrat.

3.3. Si le Logiciel a été acquis sur Internet, le Logiciel peut être utilisé à votre acceptation de ce Contrat, pendant la période stipulée lors de l'acquisition.

3.4. Vous avez le droit d'utiliser gratuitement une version de démonstration du Logiciel conformément aux dispositions de la Clause 2.1 pendant la seule période d'évaluation correspondante (30 jours) à compter de l'activation du Logiciel conformément à ce Contrat, *sachant que* la version de démonstration ne Vous donne aucun droit aux mises à jour et à l'assistance technique par Internet et par téléphone.

3.5. Votre Licence d'utilisation du Logiciel est limitée à la période stipulée dans les Clauses 3.2 ou 3.3 (selon le cas) et la période restante peut être visualisée par les moyens décrits dans le Manuel de l'utilisateur.

3.6. Si vous avez acquis le Logiciel dans le but de l'utiliser sur plus d'un Ordinateur, Votre Licence d'utilisation du Logiciel est limitée à la période commençant à la date d'activation du Logiciel ou de l'installation du fichier clé de licence sur le premier Ordinateur.

3.7. Sans préjudice des autres recours en droit ou équité à la disposition du Titulaire des droits, dans l'éventualité d'une rupture de votre part de toute clause de ce Contrat, le Titulaire des droits sera en droit, à sa convenance et sans préavis, de révoquer cette Licence sans rembourser le prix d'achat en tout ou en partie.

3.8. Vous vous engagez, dans le cadre de votre utilisation du Logiciel et de l'obtention de tout rapport ou de toute information dans le cadre de l'utilisation de ce Logiciel, à respecter toutes les lois et réglementations internationales, nationales, étatiques, régionales et locales en vigueur, ce qui comprend, sans toutefois s'y limiter, les lois relatives à la protection de la vie privée, des droits d'auteur, au contrôle des exportations et à la lutte contre les outrages à la pudeur.

3.9. Sauf disposition contraire spécifiquement énoncée dans ce Contrat, vous ne pouvez transférer ni céder aucun des droits qui vous sont accordés dans le cadre de ce Contrat ou aucune de vos obligations de par les présentes.

4. Assistance technique

4.1. L'assistance technique décrite dans la Clause 2.5 de ce Contrat Vous est offerte lorsque la dernière mise à jour du Logiciel est installée (sauf pour la version de démonstration du Logiciel).
Service d'assistance technique : http://support.kaspersky.com

4.2. Les données de l'utilisateur, spécifiées dans Personal Cabinet/My Kaspersky Account, ne peuvent être utilisées par les spécialistes de l'assistance technique que lors du traitement d'une requête de l'utilisateur.

5. Limitations

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

5.2. Vous ne devrez transférer les droits d'utilisation du Logiciel à aucune tierce partie.

5.3. Vous vous engagez à ne communiquer le code d'activation et/ou le fichier clé de licence à aucune tierce partie, et à ne permettre l'accès par aucune tierce partie au code d'activation et au fichier clé de licence qui sont considérés comme des informations confidentielles du Titulaire des droits.

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

5.5. Vous vous engagez à ne pas vous servir du Logiciel pour la création de données ou de logiciels utilisés dans le cadre de la détection, du blocage ou du traitement des menaces décrites dans le Manuel de l'utilisateur.

5.6. Votre fichier clé peut être bloqué en cas de non-respect de Votre part des conditions générales de ce Contrat.

5.7. Si vous utilisez la version de démonstration du Logiciel, Vous n'avez pas le droit de bénéficier de l'assistance technique stipulée dans la Clause 4 de ce Contrat, et Vous n'avez pas le droit de transférer la licence ou les droits d'utilisation du Logiciel à une tierce partie.

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

6.1. Le Titulaire des droits garantit que le Logiciel donnera des résultats substantiellement conformes aux spécifications et aux descriptions énoncées dans le Manuel de l'utilisateur, *étant toutefois entendu* que cette garantie limitée ne s'applique pas dans les conditions suivantes : (w) des défauts de fonctionnement de Votre Ordinateur et autres non-respects des clauses du Contrat, auquel cas le Titulaire des droits est expressément dégagé de toute responsabilité en matière de garantie ; (x) les dysfonctionnements, les défauts ou les pannes résultant d'une utilisation abusive, d'un accident, de la négligence, d'une installation inappropriée, d'une utilisation ou d'une maintenance inappropriée ; des vols ; des actes de vandalisme ; des catastrophes naturelles ; des actes de terrorisme ; des pannes d'électricité ou des surtensions ; des sinistres ; de l'altération, des modifications non autorisées ou des réparations par toute partie autre que le Titulaire des droits ; ou des actions d'autres tierces parties ou Vos actions ou des causes échappant au contrôle raisonnable du Titulaire des droits ; (y) tout défaut non signalé par Vous au Titulaire dès que possible après sa constatation ; et (z) toute incompatibilité causée par les composants du matériel et/ou du logiciel installés sur Votre Ordinateur.

6.2. Vous reconnaissez, acceptez et convenez qu'aucun logiciel n'est exempt d'erreurs, et nous Vous recommandons de faire une copie de sauvegarde des informations de Votre Ordinateur, à la fréquence et avec le niveau de fiabilité adapté à Votre cas.

6.3. Le Titulaire des droits n'offre aucune garantie de fonctionnement correct du Logiciel en cas de non-respect des conditions décrites dans le Manuel de l'utilisateur ou dans ce Contrat.

6.4. Le Titulaire des droits ne garantit pas que le Logiciel fonctionnera correctement si Vous ne téléchargez pas régulièrement les Mises à jour spécifiées dans la Clause 2.5 de ce Contrat.

6.5. Le Titulaire des droits ne garantit aucune protection contre les menaces décrites dans le Manuel de l'utilisateur à l'issue de l'échéance de la période indiquée dans les Clauses 3.2 ou 3.3 de ce Contrat, ou à la suite de la résiliation pour une raison quelconque de la Licence d'utilisation du Logiciel.

6.6. LE LOGICIEL EST FOURNI " TEL QUEL " ET LE TITULAIRE DES DROITS N'OFFRE AUCUNE GARANTIE QUANT À SON UTILISATION OU SES PERFORMANCES. SAUF DANS LE CAS DE TOUTE GARANTIE, CONDITION, DÉCLARATION OU TOUT TERME DONT LA PORTÉE NE PEUT ÊTRE EXCLUE OU LIMITÉE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS ET SES PARTENAIRES N'OFFRENT AUCUNE GARANTIE, CONDITION OU DÉCLARATION (EXPLICITE OU IMPLICITE, QUE CE SOIT DE PARLA LÉGISLATION EN VIGUEUR, LA " COMMON LAW ", LA COUTUME, LES USAGES OU AUTRES) QUANT À TOUTE QUESTION DONT, SANS LIMITATION, L'ABSENCE D'ATTEINTE AUX DROITS DE TIERCES PARTIES, LE CARACTÈRE COMMERCIALISABLE, LA QUALITÉ SATISFAISANTE, L'INTÉGRATION OU L'ADÉQUATION À UNE FIN PARTICULIÈRE. VOUS ASSUMEZ TOUS LES DÉFAUTS, ET L'INTÉGRALITÉ DES RISQUES LIÉS À LA PERFORMANCE ET AU CHOIX DU LOGICIEL POUR ABOUTIR AUX RÉSULTATS QUE VOUS RECHERCHEZ, ET À L'INSTALLATION DU LOGICIEL, SON UTILISATION ET LES RÉSULTATS OBTENUS AU MOYEN DU LOGICIEL. SANS LIMITER LES DISPOSITIONS PRÉCÉDENTES, LE TITULAIRE DES DROITS NE FAIT AUCUNE DÉCLARATION ET N'OFFRE AUCUNE GARANTIE QUANT À L'ABSENCE D'ERREURS DU LOGICIEL, OU L'ABSENCE D'INTERRUPTIONS OU D'AUTRES PANNES, OU LA SATISFACTION DE TOUTES VOS EXIGENCES PAR LE LOGICIEL, QU'ELLES SOIENT OU NON DIVULGUÉES AU TITULAIRE DES DROITS.

7. Exclusion et Limitation de responsabilité

7.1. DANS LA MESURE MAXIMALE PERMISE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS OU SES PARTENAIRES NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES DE TOUT DOMMAGE SPÉCIAL, ACCESSOIRE, PUNITIF, INDIRECT OU CONSÉCUTIF QUEL QU'IL SOIT (Y COMPRIS, SANS TOUTEFOIS S'Y LIMITER, LES DOMMAGES POUR PERTES DE PROFITS OU D'INFORMATIONS CONFIDENTIELLES OU AUTRES, EN CAS D'INTERRUPTION DES ACTIVITÉS, DE PERTE D'INFORMATIONS PERSONNELLES, DE CORRUPTION, DE DOMMAGE À DES DONNÉES OU À DES PROGRAMMES OU DE PERTES DE CEUX-CI, DE MANQUEMENT À L'EXERCICE DE TOUT DEVOIR, Y COMPRIS TOUTE OBLIGATION STATUTAIRE, DEVOIR DE BONNE FOI OU DE DILIGENCE RAISONNABLE, EN CAS DE NÉGLIGENCE, DE PERTE ÉCONOMIQUE, ET DE TOUTE AUTRE PERTE PÉCUNIAIRE OU AUTRE PERTE QUELLE QU'ELLE SOIT) DÉCOULANT DE OU LIÉ D'UNE MANIÈRE QUELCONQUE À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISATION DU LOGICIEL, À L'OFFRE D'ASSISTANCE OU D'AUTRES SERVICES OU À L'ABSENCE D'UNE TELLE OFFRE, LE LOGICIEL, ET LE CONTENU TRANSMIS PAR L'INTERMÉDIAIRE DU LOGICIEL OU AUTREMENT DÉCOULANT DE L'UTILISATION DU LOGICIEL, OU AUTREMENT DE PAR OU EN RELATION AVEC TOUTE DISPOSITION DE CE CONTRAT, OU DÉCOULANT DE TOUTE RUPTURE DE CE CONTRAT OU DE TOUT ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE, LA FAUSSE DÉCLARATION, OU TOUTE OBLIGATION OU DEVOIR EN RESPONSABILITÉ STRICTE), OU DE TOUT MANQUEMENT À UNE OBLIGATION STATUTAIRE, OU DE TOUTE RUPTURE DE GARANTIE DU TITULAIRE DES DROITS ET/OU DE TOUT PARTENAIRE DE CELUI-CI, MÊME SI LE TITULAIRE DES DROITS ET/OU TOUT PARTENAIRE A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

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

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

8. Licence GNU et autres licences de tierces parties

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

9. Droits de propriété intellectuelle

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

le Logiciel, sauf dans les conditions expressément décrites dans le cadre de ce Contrat. Toutes les reproductions du Logiciel effectuées dans le cadre de ce Contrat doivent faire mention des mêmes avis d'exclusivité que ceux qui figurent sur le Logiciel. Sauf dans les conditions énoncées par les présentes, ce Contrat ne vous accorde aucun droit de propriété intellectuelle sur le Logiciel et vous convenez que la Licence telle que définie dans ce document et accordée dans le cadre de ce Contrat ne vous donne qu'un droit limité d'utilisation en vertu des conditions générales de ce Contrat. Le Titulaire des droits se réserve tout droit qui ne vous est pas expressément accordé dans ce Contrat.

9.2. Vous convenez de ne modifier ou altérer le Logiciel en aucune façon. Il vous est interdit d'éliminer ou d'altérer les avis de droits d'auteur ou autres avis d'exclusivité sur tous les exemplaires du Logiciel.

10. Droit applicable ; arbitrage

10.1. Ce Contrat sera régi et interprété conformément aux lois de la Fédération de Russie sans référence aux règlements et aux principes en matière de conflits de droit. Ce Contrat ne sera pas régi par la Conférence des Nations-Unies sur les contrats de vente internationale de marchandises, dont l'application est strictement exclue. Tout litige auquel est susceptible de donner lieu l'interprétation ou l'application des clauses de ce Contrat ou toute rupture de celui-ci sera soumis à l'appréciation du Tribunal d'arbitrage commercial international de la Chambre de commerce et d'industrie de la Fédération de Russie à Moscou (Fédération de Russie), à moins qu'il ne soit réglé par négociation directe. Tout jugement rendu par l'arbitre sera définitif et engagera les parties, et tout tribunal compétent pourra faire valoir ce jugement d'arbitrage. Aucune disposition de ce Paragraphe 10 ne saurait s'opposer à ce qu'une Partie oppose un recours en redressement équitable ou l'obtienne auprès d'un tribunal compétent, avant, pendant ou après la procédure d'arbitrage.

11. Délai de recours.

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

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

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

13. Informations de contact du Titulaire des droits

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

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

GLOSSAIRE

A

Activation de l'application

L'application devient entièrement fonctionnelle. L'utilisateur doit avoir une licence pour activer l'application.

B

Bases

Bases de données créées par les experts de Kaspersky Lab et qui contiennent une description détaillée de toutes les menaces informatiques qui existent à l'heure actuelle ainsi que les moyens de les identifier et de les neutraliser. Les bases sont actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouvelles menaces sont découvertes.

Blocage d'un objet

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

C

Console d'administration

Composant de l'application Kaspersky Anti-Virus qui offre l'interface utilisateur pour les services d'administration du Serveur d'administration et de l'Agent d'administration.

E

Exclusion

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

Fichier de licence

Fichier portant l'extension *.key et qui est votre "clé" personnelle, indispensable au fonctionnement de l'application de Kaspersky Lab. Ce fichier sera inclus dans la boîte si vous avez achetez le logiciel chez un distributeur Kaspersky Lab. En revanche, il vous sera envoyé par email si le produit provient d'une boutique Internet.

G

Groupe d'administration

Sélection d'ordinateurs regroupés selon les fonctions exécutées et les applications de Kaspersky Lab installées. Les ordinateurs sont regroupés pour en faciliter la gestion dans son ensemble. Le groupe peut se trouver à l'intérieur d'autres groupes. Il est possible de créer dans le groupe les stratégies de groupe pour chacune des applications installées et chacune des tâches de groupe créées.

H

HOTE

Ordinateur sur lequel l'application serveur fonctionne. Un hôte peut exécuter une multitude d'applications serveur, à savoir le serveur FTP, le serveur de messagerie et le serveur Web peut fonctionner sur un hôte. L'utilisateur utilise un logiciel client, par exemple un navigateur, pour accéder à l'hôte. Le terme serveur désigne également souvent un ordinateur sur lequel fonctionne une application serveur, ce qui supprime la différence entre serveur et hôte.

Dans le secteur des télécommunications, l'hôte est un ordinateur d'où proviennent des informations (telles que des fichiers FTP, des informations ou des pages Web). Sur Internet, les hôtes sont également appelés nœuds.

L

LA STRATEGIE DE GROUPE

cf. Stratégie

LICENCE ACTIVE

Licence utilisée dans la période de temps définie par l'application de Kaspersky Lab. Elle définit la durée de validité de l'ensemble des fonctions, ainsi que la politique de licence vis-à-vis de l'application. L'application ne peut pas compter plus d'une licence dont l'état est "actif".

LISTE NOIRE DES LICENCES

Base de données contenant des informations relatives aux fichiers de licence Kaspersky Lab bloquées. Le contenu du fichier de la liste noire est mis à jour en même temps que les bases.

M

MASQUE DE FICHIER

Représentation du nom et de l'extension d'un fichier par des caractères génériques. Les deux caractères principaux utilisés à cette fin sont * et ? (où * – représente n'importe quel nombre de caractères et ? – représente un caractère unique). À l'aide de ces caractères, il est possible de représenter n'importe quel fichier. Attention ! Le nom et l'extension d'un fichier sont toujours séparés par un point.

MASQUE DE SOUS-RESEAU

Le masque de sous-réseau et l'adresse réseau permettent d'identifier un ordinateur au sein d'un réseau informatique.

MISE A JOUR

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

MISE A JOUR DES BASES

Une des fonctions de l'application de Kaspersky Lab qui permet de garantir l'actualité de la protection. Dans ce scénario, les bases sont copiées depuis les serveurs de mise à jour de Kaspersky Lab sur l'ordinateur et elles sont installées automatiquement.

MISE A JOUR DISPONIBLE

Paquet des mises à jour des modules de l'application Kaspersky Lab qui contient les mises à jour urgentes recueillies au cours d'un intervalle de temps et les modifications dans l'architecture de l'application.

MODELE DE RAPPORT

Modèle de création des rapports sur les résultats du fonctionnement de l'application. Il contient toute une série de paramètres qui définissent la période couverte par le rapport, l'horaire de création du rapport et son format.

MODELE DE REMPLACEMENT.

Modèle du message d'information qui remplace le corps du message en cas de découverte dans le message ou dans ses pièces jointes d'objets infectés ou suspects.

O

OBJET CONTENEUR

Objet contenant plusieurs objets, par exemple, une archive un message avec un message joint. Cf. également "objet simple".

OBJET DANGEREUX

Objet contenant un virus. Nous vous déconseillons de manipuler de tels objets car ils pourraient infecter votre ordinateur. Suite à la découverte d'un objet infecté, il est conseillé de le réparer à l'aide d'une application de Kaspersky Lab ou de le supprimer si la réparation est impossible.

OBJET INFECTE

Objet contenant un code malveillant : l'analyse de l'objet a mis en évidence une équivalence parfaite entre une partie du code de l'objet et le code d'une menace connue. Les experts de Kaspersky Lab vous déconseillent de manipuler de tels objets car ils pourraient infecter votre ordinateur.

P

PARAMETRES DE LA TACHE

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

PARE-FEU

Outils matériels et/ou logiciels qui contrôle et filtre les paquets de réseau en transit, conformément aux règles définies. La tâche principale de l'écran est de protéger les réseaux informatiques ou certains nœuds contre les accès non autorisés. Les pare-feu sont souvent appelés filtres car leur tâche principale est de bloquer (filtrer) les paquets qui ne correspondent pas aux critères de la configuration.

PROCESSUS DE CONFIANCE

Processus d'une application dont les opérations sur les fichiers ne sont pas contrôlées par l'application de Kaspersky Lab dans le cadre de la protection en temps réel. Les objets lancés, ouverts ou conservés par un processus de confiance ne sont pas analysés.

PROTECTION

Mode de fonctionnement pendant lequel l'application recherche en temps réel la présence éventuelle de code malveillant.

L'application intercepte toutes les tentatives d'ouverture d'un objet en lecture, écriture et exécution et recherche la présence éventuelle de menaces. Les objets sains sont ignorés alors que les objets (potentiellement) malveillants sont traités conformément aux paramètres de la tâche (réparation, suppression, mise en quarantaine).

PROTECTION MAXIMUM

Niveau de protection de l'ordinateur qui correspond à la protection maximum que peut offrir l'application. Dans ce mode, tous les fichiers de l'ordinateur, les disques amovibles et les unités de réseau (si elles sont raccordées à l'ordinateur) sont soumis à l'analyse antivirus.

R

RESTAURATION

Transfert de l'objet original depuis la quarantaine ou du dossier de sauvegarde vers le dossier où se trouvait l'objet avant qu'il ne soit placé en quarantaine, supprimé ou réparé, ou vers tout autre emplacement désigné 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. Lorsque la réparation est la première action prévue pour un objet (autrement dit, la première action exercée sur cet objet directement après sa découverte), une copie de sauvegarde de l'objet sera créée avant de procéder à la réparation. Une partie des données peut être endommagée pendant la réparation. La copie vous donne la possibilité de restaurer l'objet à l'état antérieur à la réparation.

S

STOCKAGE DES COPIES DE SAUVEGARDE

Dossier spécial pour la conservation des copies des données du Serveur d'administration, créées à l'aide de l'utilitaire de copie de sauvegarde.

T

TACHE

Fonctions exécutées par l'application de Kaspersky Lab qui se présente sous la forme d'une tâche, par exemple : Protection en temps réel des fichiers, Analyse complète de l'ordinateur, Mise à jour des bases.

TACHE DE GROUPE

Tâche définie pour un groupe et exécutée sur tous les postes clients de ce groupe d'administration.

TACHE POUR UNE SELECTION D'ORDINATEURS

Tâche définie pour une sélection des postes clients parmi des groupes d'administration aléatoires et exécutée sur ceux-ci.

V

VITESSE MAXIMALE

Niveau de protection auquel seuls les objets potentiellement infectés sont analysés. C'est ce qui permet d'accélérer la vitesse de l'analyse.

É

ÉTAT DE LA PROTECTION

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

KASPERSKY LAB

Kaspersky Lab a été fondé en 1997. Il s'agit à l'heure actuelle de l'éditeur russe de logiciels de sécurité polyvalents le plus connu : protection contre les virus, le courrier indésirable et les hackers.

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, aux États-Unis (Canada), dans les pays du Benelux, en Chine et en Pologne. 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. 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts 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. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. En qualité de produit phare de la société, Kaspersky Anti-Virus offre une protection efficace pour tous les éléments qui pourraient être la cible d'un virus : postes de travail, serveurs de fichiers, systèmes de messagerie, pare-feu, passerelles Internet et ordinateurs de poches. 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 oeuvre 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 vous adresser à nos distributeurs ou directement à Kaspersky Lab Ltd. Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Site Web de Kaspersky Lab :	http://www.kaspersky.fr
Encyclopédie des virus	http://www.securelist.com/fr/
Laboratoire d'étude des virus	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)

INDEX

M

N

Q

R

S

T

V