

KASPERSKY LAB

Kaspersky[®] Administration Kit
version 6.0

Introduction

KASPERSKY® ADMINISTRATION KIT
VERSION 6.0

Introduction

© Kaspersky Lab
<http://www.kaspersky.com/>

Date de révision : février 2007

Sommaire

CHAPITRE 1. INTRODUCTION	4
CHAPITRE 2. PREMIERS PAS	6
2.1. Installation de MSDE	7
2.2. Installation des composants Kaspersky Administration Kit	8
2.3. Assistant Démarrage rapide	8
2.4. Création d'un groupe d'administration	10
2.5. Installation distante de l'agent réseau	11
2.6. Déploiement de l'application Kaspersky Anti-Virus	12
2.7. Vérification de l'exécution de la tâche de mise à jour	13
2.8. Configuration des notifications	14
2.9. Mise à l'essai du système de notifications et de la tâche d'analyse à la demande	15
2.10. Génération de rapports	15
CHAPITRE 3. MISE A NIVEAU DES VERSIONS 5.X ET 6.0 A LA VERSION 6.0 (MAINTENANCE PACK 1)	17
CHAPITRE 4. CONCLUSION	19
ANNEXE A. KASPERSKY LAB	20
A.1. Autres produits antivirus	21
A.2. Coordonnées	33
ANNEXE B. CONTRAT DE LICENCE	34

CHAPITRE 1. INTRODUCTION

Ce document décrit à l'intention d'un administrateur de sécurité les principales étapes à suivre pour mettre en place rapidement et efficacement un système de protection antivirus contenant des applications Kaspersky Lab sur le réseau d'entreprise, en utilisant **Kaspersky Administration Kit**.

Ce document examine un scénario simplifié d'installation de la protection antivirus sur plusieurs ordinateurs disposant du système d'exploitation Microsoft Windows sans la hiérarchie du système d'administration. Pour réussir l'installation, les ordinateurs doivent être exploités sous : Microsoft Windows 98; Microsoft Windows ME; Microsoft Windows 2000 avec Maintenance Pack 1 et suivant; Microsoft Windows NT4 avec Maintenance Pack 6a et suivant; Microsoft Windows XP Professional avec Maintenance Pack 1 et suivant; Microsoft Windows XP Professional x64 et suivant; Microsoft Windows Server 2003 et suivant; Microsoft Windows Server 2003 x64 et suivant; Microsoft Windows Vista, Microsoft Windows Vista x64.

Ce document décrit également la mise à niveau de la version 5.x vers la version 6.x des applications Kaspersky Lab.

[Reportez-vous au manuel d'intégration, au manuel de l'administrateur et à l'aide de Kaspersky Administration Kit pour des informations détaillées sur l'application.](#)

Kaspersky Administration Kit est conçu pour administrer le système de protection antivirus à l'intérieur d'un réseau d'entreprise. Les possibilités offertes par l'application à l'administrateur sont les suivantes :

- Créer un réseau logique chargé de la protection antivirus de l'entreprise.
- Installer et désinstaller à distance les applications Kaspersky Lab sur le réseau.
- Gérer à distance le système de protection antivirus à partir d'un même poste.
- Recevoir des notifications sur des événements concernant la protection antivirus, à travers le réseau.
- Accumuler des statistiques et des rapports sur toutes les installations.
- Contrôler les licences de toutes les applications antivirus installées.
- Traiter de manière centralisée les objets mis en quarantaine ou copiés dans le dossier de sauvegarde par les applications antivirus.

Kaspersky Administration Kit 6.0 inclut les composants suivants :

- **Le serveur d'administration** permet le stockage centralisé d'informations sur les applications Kaspersky Lab installées sur le réseau corporatif et constitue un outil efficace de gestion de ces applications. Il conserve toutes les informations sur le système de protection antivirus de l'entreprise dans une base de données MSDE 2000 avec Maintenance Pack 3, Microsoft SQL Server 2000 avec Maintenance Pack 3 ou suivant, MySQL version 5.0.32, Microsoft SQL 2005 et suivant ou Microsoft SQL 2005 Express et suivant. Les bases de données doivent avoir été installées et configurées avant l'installation du serveur d'administration. Vous pouvez installer MSDE 2000 SP 3 à partir du paquet inclus dans le kit de distribution de Kaspersky Administration Kit 6.0. L'application Microsoft Data Access Component (MDAC) version 2.8 ou suivante doit être préalablement installée.
- **L'agent réseau (Réseau Agent)** coordonne les interactions entre le serveur d'administration et les applications Kaspersky Lab installées sur un poste spécifique du réseau (lui-même un poste de travail ou un serveur). Ce composant prend en charge toutes les applications présentes dans Kaspersky Lab Business Optimal et Kaspersky Corporate Suite. Il existe des versions de l'agent réseau spécifiques aux applications Kaspersky Lab tournant sur Novell ou Unix.
- **La console d'administration** fournit l'interface utilisateur nécessaire pour les services administratifs du serveur d'administration et de l'agent réseau. Elle se présente sous la forme d'une extension MMC (Microsoft Management Console).

CHAPITRE 2. PREMIERS PAS

Pour créer un périmètre de protection efficace autour de votre réseau d'entreprise, suivez ces étapes:

1. Installez Microsoft Data Access Component (MDAC) version 2.8 ou suivante. Cette étape n'est pas nécessaire si ce composant est déjà installé dans le réseau de l'entreprise.
2. Installez MSDE 2000 avec Maintenance Pack 3 (cf. 2.1, p. 7), Microsoft SQL Server 2000 avec Maintenance Pack 3 et suivant, MySQL version 5.0.32, Microsoft SQL 2005 et suivant ou Microsoft SQL 2005 Express et suivant.
3. Installez le serveur d'administration, et la console d'administration (voir section 2.2 à la page 8).
4. Faites une première configuration du système de protection antivirus à l'aide de l'Assistant Démarrage rapide (voir section 2.3 à la page 8).
5. Créez les groupes d'administration, au cas où cela n'aurait pas été fait à l'aide de l'assistant de configuration initiale, afin de contrôler des groupes de postes clients, par l'application de stratégies et des tâches de groupe.
6. Installez à distance l'agent réseau sur les postes clients pour que leurs applications antivirus puissent réagir au serveur d'administration (voir section 2.5 à la page 11).
7. Installez à distance sur les postes clients sélectionnés les applications de Kaspersky Lab chargées de la protection antivirus du réseau de l'entreprise et administrables via Kaspersky Administration Kit (cf. point 2.6, p. 12). C'est indispensable si cela n'a pas été fait précédemment.
8. Configurez le téléchargement des mises à jour des bases antivirus par Internet par le serveur d'administration, puis vérifiez que l'opération se réalise correctement. Vérifiez la mise à jour des bases de données sur les postes clients (voir section 2.7 à la page 13).
9. Configurez les notifications à l'administrateur sur les événements liés aux virus sur les postes clients (voir section 2.8 à la page 14).
10. Sur les postes clients, lancez une analyse à la demande et vérifiez que la tâche de notification est exécutée (voir section 2.9 à la page 14).

11. Affichez un compte-rendu de protection antivirus portant sur les postes clients, et sur le nombre de virus détectés par les applications Kaspersky Lab (voir section 2.10 à la page 15).

Si les étapes précédentes se sont déroulées avec succès, cela signifie que vous avez établi un système de protection antivirus fiable pour votre réseau.

Les sections suivantes décrivent ces étapes de manière plus détaillée.

2.1. Installation de MSDE

Vous pouvez passer cette étape si votre réseau d'entreprise est déjà doté de MSDE 2000 avec Maintenance Pack 3, Microsoft SQL 2000 avec Maintenance Pack 3 et suivant, MySQL version 5.0.32, Microsoft SQL 2005 et suivant ou Microsoft SQL 2005 Express et suivant.

Avant d'installer MSDE, il est indispensable d'installer Microsoft Data Access Components (MDAC) version 2.8 ou suivante (le fichier d'installation est accessible sur le site de Microsoft).

Pour installer MSDE 2000 depuis le paquet d'installation de Kaspersky Administration Kit,

1. Sélectionnez l'ordinateur où vous allez installer la base de données du serveur d'administration. Normalement, il s'agit du même ordinateur sur lequel est installé le serveur d'administration.
2. Exécutez localement le fichier **setup.exe** dans le répertoire **MSDE2KSP3** du CD d'installation de Kaspersky Administration Kit.
3. Suivez les instructions de l'Assistant d'installation.

Après avoir effectué toutes les étapes, l'application MSDE 2000 SP 3 sera installée sur le poste sélectionné. MSDE 2000 SP 3 n'exige aucune administration.

Le serveur d'administration conserve toutes les informations sur le système de protection antivirus de l'entreprise dans une base de données Microsoft Development Environment (MSDE) 2000 SP3 ou SQL Server 2000 SP3.

Pour sauvegarder les données du serveur d'administration, utiliser l'application **klbackup** présente dans le paquet de distribution de Kaspersky Administration Kit ou la tâche globale **Sauvegarde du serveur d'administration**. Pour de plus amples détails, reportez-vous au Guide de l'administrateur.

2.2. Installation des composants

Kaspersky Administration Kit

Pendant l'installation, Vous pouvez choisir les composants nécessaires : **Serveur d'administration, Posture Validation Server Kaspersky Lab pour Cisco NAC, Agent réseau et Console d'administration.** La console d'administration et l'agent réseau sont obligatoirement installés, il n'est pas possible de les décocher. Posture Validation Server Kaspersky Lab pour Cisco NAC est un composant standard permettant la collaboration avec Cisco Network Admission Control. Il ne sera pas traité dans le présent manuel. L'option par défaut installe tous les composants.

Si nécessaire, vous pouvez installer la console d'administration sur un autre ordinateur, et gérer le serveur d'administration depuis le réseau.

Pour installer le serveur d'administration et/ou la console d'administration,

1. Sélectionnez l'ordinateur où vous allez installer les composants. S'il votre réseau utilise une structure de domaine Windows, il est recommandé d'installer le serveur d'administration sur un membre du domaine.

Vous pouvez installer la version 6.0 (Maintenance Pack 1) du serveur d'administration sur le même ordinateur utilisé pour la version 5.x ou 6.0.

Il est conseillé de posséder des droits d'administrateur du domaine pour installer le produit. Ceci permet de créer automatiquement les groupes **KLAdmins** et **KLOperators**, et d'accorder les crédits nécessaires au compte utilisé par le serveur d'administration pour opérer.

2. Lancez le programme setup.exe à partir du CD d'installation de Kaspersky Administration Kit 6.0.
3. Suivez les instructions de l'Assistant.

Utilisez le compte de l'administrateur de domaine comme compte de service utilisé pour démarrer le serveur d'administration.


2.3. Assistant Démarrage rapide

Pour effectuer la configuration initiale de la protection antivirus ,

1. Lancez la console d'administration : cliquez sur **Démarrer** → **Programmes** → **Kaspersky Administration Kit** → **Kaspersky Administration Kit.**

2. Connectez-vous au serveur d'administration cible : cliquez sur l'entrée **Serveur d'administration** dans l'arborescence de console. Acceptez le certificat du serveur.
3. Dans le menu contextuel, cliquez sur **Assistant Démarrage rapide**.
4. Attendez jusqu'à ce que le serveur d'administration termine l'exploration du réseau et détecte tous les ordinateurs.
5. Créez des groupes d'administration par l'une des méthodes suivantes :
 - Puisque nous procédons uniquement avec quelques ordinateurs de test, cliquez sur **Manuellement** et ajoutez manuellement des postes clients à ce groupe.
 - Si vous êtes en train de déployer le système de protection antivirus à travers un réseau corporatif, il est possible de créer automatiquement les réseaux logiques. Pour ce faire, sélectionnez l'option **Ajouter des postes au groupe à partir du réseau de Windows**. Dans ce cas, le réseau logique utilisera une structure semblable à celle des domaines et des groupes d'utilisateurs du réseau Microsoft Windows (les groupes d'administration coïncideront avec les domaines Microsoft Windows et les groupes d'utilisateur).
6. Sélectionnez les options permettant d'envoyer par courrier électronique ou NET SEND les notifications générées par les applications Kaspersky Lab. Ces paramètres sont modifiables dans les propriétés du serveur d'administration. Pour plus d'informations, reportez-vous au Guide de l'administrateur.
7. Lancez le processus de création des stratégies pour les applications antivirus et définissez plusieurs tâches afin d'activer le système de protection antivirus. Kaspersky Administration Kit 6.0 fait appel à des stratégies de groupe pour appliquer uniformément la même configuration à tous les ordinateurs d'un groupe. Les tâches sont des actions effectuées par le logiciel antivirus sur tous les ordinateurs du groupe.

L'Assistant créera les stratégies et les tâches suivantes:

- Des stratégies de haut niveau pour Kaspersky Anti-Virus 5.0 ou 6.0 for Windows Workstations, avec une configuration par défaut. Par la suite, vous pourrez afficher et modifier les paramètres de stratégie. Pour appliquer les modifications de stratégie dans les postes clients, et pour éviter que l'utilisateur puisse les modifier à son tour, utilisez l'icône .
- Une tâche globale pour la mise à jour du serveur d'administration par Internet.

L'application téléchargera les mises à jour, à la fois des bases antivirus et des modules de programme, à partir d'un serveur de mises à jour de Kaspersky Lab et les enregistrera dans le dossier partagé spécifié lors de l'installation du serveur d'administration. Les postes clients récupéreront leurs mises à jour à travers ce dossier partagé. Par la suite, pour une configuration plus souple du téléchargement des mises à jour par les postes clients, il sera possible d'utiliser la diffusion des mises à jour sur les serveurs d'administration secondaires et les agents de mises à jour (pour de plus amples informations, consultez le guide de l'administrateur. Cliquez sur **Paramètres de mise à jour** pour configurer les options de mise à jour du serveur d'administration.

- Une tâche de haut niveau pour la mise à jour des bases antivirus sur les postes clients sera créée sur les postes clients, avec des valeurs par défaut (Kaspersky Antivirus pour Windows Workstations 5.0 et 6.0). Les postes clients seront programmés pour récupérer les mises dans le dossier partagé.
 - Une tâche d'analyse à la demande des postes clients sera créée avec des valeurs par défaut (Kaspersky Antivirus pour Windows Workstations 5.0 et 6.0).
8. Indiquez s'il faut lancer un nom la mise à jour via le serveur d'administration immédiatement ou selon un horaire défini.
 9. Dans la dernière fenêtre, indiquez s'il faut lancer l'assistant d'installation à distance dès la fin de l'assistant de configuration initiale.

2.4. Création d'un groupe d'administration

Pour ajouter un nouveau groupe au réseau logique,

1. Dans l'arborescence de console ou dans le dossier **Groupes** du panneau de détails, sélectionnez un groupe auquel vous allez ajouter un nouveau groupe. Ouvrez le menu contextuel et cliquez sur **Nouveau → Groupe**. Introduisez le nom du nouveau groupe et cliquez sur le bouton **OK**.
2. Déplacez les postes sélectionnés du groupe **Réseau** vers le nouveau groupe : vous pouvez utiliser un copier-coller, un glisser-déplacer ou un assistant via la commande **Nouveau → Ordinateur** du menu contextuel.

Pour créer une sélection d'ordinateurs selon des critères quelconque afin de les déplacer dans le groupe d'administration, utilisez la commande **Rechercher un ordinateur** du menu contextuel (ou l'équivalent dans le menu **Action**). Pour obtenir de plus amples informations, consultez le guide de l'administrateur.

Pour la procédure détaillée de mise à jour de Kaspersky Administration Kit 5.x ou 6.0 vers la version 6.0 (Maintenance Pack 1), reportez-vous au Chapitre 3 à la page 17.

2.5. Installation distante de l'agent réseau

L'agent réseau peut être installé séparément ou avec d'autres applications. La présente section explique comment installer l'agent réseau séparément. Cela peut s'avérer utile lorsque, par exemple, la bonne version de l'application antivirus est déjà installée sur le poste client.

Pour installer Network Agent à partir d'un emplacement distant,

1. Dans la console d'administration, lancez l'Assistant de déploiement d'application dans le menu contextuel du serveur d'administration.
2. Sélectionnez le paquet d'installation de Network Agent créé par l'Assistant Démarrage rapide. Ce paquet est créé au cours de l'installation du serveur d'administration et contient les paramètres utilisés par l'agent réseau pour se connecter au serveur d'administration.
3. Définissez les ordinateurs ou le groupe d'administration créé qui feront office de clients cibles pour l'installation.
4. Configurez les paramètres de la tâche d'administration à distance.
5. Le cas échéant, indiquez le compte à utiliser pour accéder aux postes clients. Si le compte du serveur d'administration jouit des privilèges d'administrateur sur les postes clients, utilisez le compte par défaut.
6. La tâche d'installation à distance démarre alors. À la fin de la tâche, l'agent réseau aura été installé sur les ordinateurs clients spécifiés. Dans la boîte de dialogue suivante de l'Assistant, vous pouvez voir en temps réel la progression de la tâche d'installation à distance.
7. À la fin de la tâche, examinez les résultats et quittez l'Assistant de déploiement d'application.
8. Pour être sûr que le serveur d'administration peut se connecter à l'agent réseau à tout moment, il faut que le port numéro 15000 soit ouvert sur le poste client. Si le port UPD ne peut pas être ouvert, cochez la case **Maintenir la connexion** sur l'onglet **General** de la boîte de dialogue

Propriétés : <nom du poste> utilisé pour configurer les paramètres du poste client.

Pour vérifier que l'installation est réussie, cliquez sur **Propriétés** dans le menu contextuel de l'un des postes sur lequel vous venez d'installer l'agent réseau. Vérifiez que l'application Kaspersky Network Agent est signalée en **Exécution** dans l'onglet **Applications**.

Si le déploiement réussi mais l'agent réseau n'est pas en mesure de se connecter au serveur d'administration, utilisez l'outil kinagchik.exe. Cet outil est fourni avec le paquet de distribution de Network Agent et se trouve à la racine du dossier d'installation de l'agent réseau après son installation. Depuis la ligne de commande, cet outil réalise un diagnostic détaillé de la configuration de la connexion du serveur d'administration. Consultez l'aide pour une description plus détaillée de l'utilitaire.

2.6. Déploiement de l'application Kaspersky Anti-Virus

Cette section se concentre sur l'installation décentralisée de Kaspersky Anti-Virus for Windows Workstation. La procédure de déploiement à distance d'autres applications Kaspersky Lab est semblable à celle décrite ci-après.

Certaines applications de Kaspersky Lab dont l'administration via Kaspersky Administration Kit est possible, peuvent être installées sur les postes clients localement uniquement (pour de plus amples informations, consultez le guide spécifique de ces applications).

Pour déployer à distance Kaspersky Anti-Virus for Windows Workstation sur des postes réseau,

1. Créez un paquet d'installation pour Kaspersky Antivirus pour Stations de travail à l'aide d'un Assistant. L'Assistant peut être démarré à l'aide de la commande **Installation à distance** du menu contextuel.

Le fichier **.kpd** requis pour créer le paquet d'installation se trouve dans la racine du fichier de distribution de Kaspersky Antivirus 5 pour Stations de travail. Indiquez le fichier-clé de licence utilisé par Kaspersky Anti-Virus for Windows Workstations.

Si nécessaire, configurez le paquet d'installation. Il est recommandé, par exemple, d'autoriser le redémarrage automatique des postes clients.

2. Lancez l'Assistant de déploiement d'application, dans le menu contextuel du serveur d'administration.

3. Installez Kaspersky Antivirus 5 pour Stations de travail à partir du paquet, comme vous avez fait pour installer Network Agent (voir section 2.5 à la page 11). Vous pouvez également installer l'agent réseau en même temps que Kaspersky Anti-Virus for Windows Workstation.

Vous pouvez installer Kaspersky Anti-Virus 6.x sur des ordinateurs équipés d'applications de la version 5.x. Dans ce cas, les applications de la version 5.x seront automatiquement écrasées par ceux de la version 6.0.

Pour vérifier que l'installation s'est faite correctement, choisissez l'un des postes clients sur lequel vous venez d'installer l'application, et ouvrez sa fenêtre de propriétés. Ouvrez l'onglet **Applications** et vérifiez que l'application Kaspersky Anti-Virus pour stations de travail 5 application est signalée en **Exécution**. L'onglet **Tâches** doit afficher la tâche de protection en temps réel exécutée par Kaspersky Antivirus 5 pour Stations de travail.

2.7. Vérification de l'exécution de la tâche de mise à jour

Pour vérifier que les postes clients récupèrent correctement les mises à jour,

1. Exécutez la tâche de mise à jour sur le serveur d'administration, dans le niveau supérieur de l'entrée **Tâche** de l'arborescence de console. L'Assistant Démarrage rapide crée automatiquement cette tâche. L'application téléchargera les mises à jour à partir d'un serveur de mises à jour de Kaspersky Lab et les enregistrera dans le dossier partagé spécifié lors de l'installation du serveur d'administration. Patientez jusqu'à ce que la tâche soit terminée.

Cliquez sur **Historique** pour voir la réponse en sortie de la tâche.

Pour voir la liste de mises à jour téléchargées, cliquez sur l'entrée **Mises à jour** dans l'arborescence de console.

Des détails sur la procédure de mise à jour sont disponibles sur le site Web de Kaspersky Lab (<http://www.kaspersky.com/fr/avupdates>).

2. Lancez la tâche de mise à jour de groupe sur les postes clients. Cette tâche est créée par l'Assistant Démarrage rapide, et conservée dans le dossier **Tâches de groupe** de l'entrée **Groupe**. Patientez jusqu'à ce que la tâche soit terminée.

Cliquez sur **Historique** pour voir la réponse en sortie de la tâche.




La tâche créée par l'Assistant Démarrage rapide met à jour les postes clients à travers la connexion entre l'agent d'administration et le serveur d'administration. Les méthodes suivantes de mise à jour des postes clients sont prises en charge :

- Dans le dossier partagé du serveur d'administration ;
- Dans le dossier partagé du serveur d'administration principal (en cas d'utilisation d'une hiérarchie de serveur).
- Depuis les serveurs de mise à jour de Kaspersky Lab.
- Par un serveur HTTP ou FTP;


Pour pouvoir copier les dernières mises à jour depuis le dossier partagé, les postes clients doivent posséder des privilèges de lecture sur ce dossier. Si, pour une raison ou une autre, ceci est impossible, utilisez un serveur FTP ou HTTP pour déployer les mises à jour sur les postes clients. Créez un répertoire FTP ou HTTP associé au sous-dossier **Mises à jour**, du dossier partagé, dans lequel le serveur d'administration enregistrera les mises à jour téléchargées par Internet (par exemple, ftp://admserver/updates). Spécifiez ce dossier (ftp://admserver/updates) en tant que source des tâches de mise à jour exécutées sur les postes clients.

2.8. Configuration des notifications

Pour recevoir des notifications d'événements liés à la protection antivirus,

1. Ouvrez l'onglet **Traitement des événements** dans les Propriétés de la stratégie de haut niveau d'une application antivirus (par exemple, Kaspersky Anti-Virus pour stations de travail).
2. Sur cet onglet, spécifiez les événements sur lesquels vous souhaitez être informé et précisez comment les notifications vous seront envoyées. Pour ce faire, cocher la case dans la colonne correspondante ( - courrier électronique,  - NET SEND,  - lancement d'un fichier exécutable) et complétez les paramètres dans l'onglet **Notification** de la fenêtre des propriétés de l'événement.

Pour tester le système de notifications (voir section 2.9 à la page 15), il suffit de configurer une notification d'événement **Virus détecté** ou **Détection de virus, vers, chevaux de Troie et programmes nuisibles**.

3. L'icône  pour tous les paramètres configurés, afin de les étendre à tous les postes clients. Pour appliquer les modifications, allez dans

l'onglet **Contrôle**, cliquez sur le lien **Avancé** et, dans la boîte de dialogue, enfoncez le bouton **Modifier maintenant**.

4. Vous pouvez vérifier votre configuration par l'envoi manuel d'un message. Pour ce faire, cliquez sur le bouton **Test** dans l'onglet **Notification** de la fenêtre des propriétés de l'événement. Cette action ouvre le fenêtre d'envoi du message d'essai. En cas d'erreur, un message détaillé apparaîtra.

2.9. Mise à l'essai du système de notifications et de la tâche d'analyse à la demande

Pour tester le système de notifications et la tâche d'analyse à la demande,

1. Essayez de copier le virus de test **Eicar** vers l'ordinateur protégé. L'opération de copie échouera si la tâche de protection en temps réel est en cours d'exécution. Vous devez recevoir une notification sur la détection d'un virus, et cet événement doit être enregistré sous l'entrée **Événements** dans l'arborescence de console.

Le « virus d'essai » EICAR n'est pas un vrai virus et il ne contient aucun code qui puisse nuire à votre ordinateur. Néanmoins, la majorité des logiciels antivirus identifient ce fichier comme un virus. Vous pouvez télécharger le « virus d'essai » sur le site officiel de l'organisation **EICAR** à l'adresse http://www.eicar.org/anti_virus_test_file.htm.

2. Arrêtez la tâche de protection en temps réel sur le poste client. Copiez le virus d'essai **Eicar** sur le poste client et activez à nouveau la tâche de protection en temps réel.
3. Lancez la tâche de groupe d'analyse à la demande sur un groupe de postes clients. Comme résultat, l'application doit détecter le fichier eicar.com et vous envoyer une notification à son sujet. Un enregistrement sur cet événement doit apparaître sous l'entrée **Événements** de l'arborescence de console.

2.10. Génération de rapports

Le programme peut générer des rapports sur l'état actuel du système de protection antivirus à partir du journal d'événements de Kaspersky Administration Kit, conservé sur le serveur d'administration. Les modèles de rapport sont conservés et sont disponibles dans l'entrée **Rapports** de l'arborescence de console.

Il existe 13 modèles standard qui correspondent à autant de types de rapports :

- **Rapport de version des bases antivirus**
- **Rapport d'erreurs**
- **Rapport sur les licences**
- **Rapport sur les postes les plus infectés**
- **Rapport de protection**
- **Rapport de version du logiciel**
- **Rapport d'activité antivirus**
- **Rapport sur les applications d'autres fabricants**
- **Rapport sur les attaques de réseau**
- **Rapport sur les types d'application**
- **Rapport sur les applications protégeant les stations de travail et les serveurs de fichiers**
- **Rapport sur les applications protégeant le périmètre informatique**
- **Rapport sur les applications protégeant les systèmes de messagerie**

Par exemple, un rapport d'activité antivirus créé à l'aide du modèle correspondant contiendra des informations sur toutes les apparitions de virus enregistrées par Kaspersky Administration Kit.

Si vous ajoutez au groupe d'administration un ordinateur non équipé de l'agent réseau, le rapport de protection indiquera que ce poste n'est pas protégé.

CHAPITRE 3. MISE A NIVEAU DES VERSIONS 5.X ET 6.0 A LA VERSION 6.0 (MAINTENANCE PACK 1)

Cette section décrit la mise à niveau de Kaspersky Administration Kit 5.x ou 6.0 vers la version 6.0 (Maintenance Pack 1). La structure du réseau logique pour Kaspersky Antivirus pour Windows Workstations et Kaspersky Antivirus pour Windows Servers 5.x et 6.x est créée lors de cette mise à niveau. Certaines de ces étapes ont été décrites précédemment. Les instructions suivantes vous permettront de réaliser pas à pas une transition sans difficultés.

Voici un scénario de transition typique :

1. Créez une sauvegarde de données de l'ancienne version du serveur d'administration à l'aide de l'utilitaire **klbackup.exe**. Ce dernier fait partie du paquet d'installation de Kaspersky Administration Kit et, une fois le serveur d'administration installé, se trouve dans la racine du répertoire d'installation. Garder à l'esprit que la restauration des données du serveur d'administration exige la sauvegarde du certificat du serveur. Il s'agit d'un paramètre obligatoire de l'utilitaire **klbackup.exe**.
2. Installez la version 6.0 (Maintenance Pack 1) du serveur d'administration dans le réseau logique de l'entreprise. Elle peut être installée sur le même ordinateur utilisé pour la version 5.x ou 6.0. Lors de la mise à niveau de la version 5.x ou 6.0 vers la version 6.0 (Maintenance Pack 1), les données et paramètres de l'ancienne version du serveur et/ou de la console d'administration sont sauvegardés pour être utilisés dans la nouvelle version.
3. Créez une structure de réseau logique (groupes d'administration) pour les applications des versions 5.x et 6.x.
4. Créez des stratégies et des tâches de groupe pour les applications de la version 5.x et 6.x sur le réseau logique. Configurez les paramètres nécessaires et définissez des règles de traitement des événements, liés à la protection antivirus.
5. Spécifiez quels postes vont basculer de la version 5.x à la version 6.x.
6. Créez un paquet d'installation pour les applications de la version 5.x et 6.x, puis installez les applications de la version 5.x et 6.x sur les

ordinateurs choisis. Pendant l'installation, les anciennes versions des applications sont automatiquement écrasées par les nouvelles versions.

7. Les postes équipés du logiciel antivirus de la version 5.x et 6.x sont ajoutés au réseau logique de la version 6.0 (Maintenance Pack 1) du serveur d'administration.

De cette manière, l'environnement système de protection antivirus de votre entreprise, encore basé sur les versions 5.x et 6.x, fera graduellement la transition vers la version 6.0 (Maintenance Pack 1).

CHAPITRE 4. CONCLUSION

Kaspersky Administration Kit 6.0 dispose d'une panoplie de composants administratifs, qui vont bien plus loin que ceux décrits dans ce document. Ce document décrit les principes de base nécessaires pour bien démarrer avec Kaspersky Administration Kit 6.0 et pour déployer le système de protection antivirus sur plusieurs ordinateurs connectés au réseau. Ce scénario simplifié montre comment résoudre les problèmes de base liés à l'établissement d'un système de protection fiable, permettant à l'administrateur de :

- Déployer et configurer l'administration du système de protection antivirus
- Déployer des applications antivirus sur plusieurs postes clients à partir d'un même poste centralisé.
- Définir la stratégie de protection antivirus
- Créer et examiner le fonctionnement de la tâche de mise à jour sur les postes clients
- Tester le fonctionnement de la tâche de protection en temps réel.
- Créer et examiner la tâche d'analyse à la demande sur les postes clients
- Définir des règles pour l'envoi de notifications an cas d'événements critiques.
- Produire et afficher des rapports sur le système de protection antivirus

ANNEXE A. KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, 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 250 spécialistes, tous spécialistes des technologies antivirus : 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. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications 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. Le produit vitrine de la société est Kaspersky Antivirus : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Ses outils de gestion intuitifs et faciles à utiliser se prêtent à une automation avancée, en vue d'une protection antivirus rapide à l'échelle de l'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Antivirus : Nokia ICG (États-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde), BorderWare (Canada), etc.

Les clients de Kaspersky Lab profitent d'un large éventail de services supplémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

A.1. Autres produits antivirus

Kaspersky Lab News Agent

Le programme News Agent a été développé pour communiquer les informations relatives à Kaspersky Lab, la "météo" des virus et les dernières infos. Le programme se connecte selon une fréquence déterminée au serveur d'informations de Kaspersky Lab afin de relever les infos des différents canaux.

News Agent permet également de :

- Visualiser la « météo » des virus dans la barre des tâches;
- S'abonner et se désabonner aux canaux d'information de Kaspersky Lab;
- Recevoir selon une fréquence définie les informations des canaux auxquels on est abonné et de recevoir une notification en cas d'informations non lues;
- Lire les informations dans les canaux auxquels on est abonné;
- Consulter la liste des canaux et leur contenu;
- Ouvrir dans le navigateur une page contenant la version complète de l'information.

News Agent tourne sous Microsoft Windows et peut être utilisé comme produit autonome ou être intégré à diverses solutions de Kaspersky Lab.

Kaspersky® OnLine Scanner

Il s'agit d'un service gratuit offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace en ligne de l'ordinateur. Kaspersky OnLine Scanner est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html.

Kaspersky® OnLine Scanner Pro

Il s'agit d'un service payant offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace de l'ordinateur et de réparer les fichiers infectés en ligne. Kaspersky OnLine Scanner Pro est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html;

Kaspersky® Anti-Virus 7.0

Kaspersky Anti-Virus 7.0 a été développé pour protéger les ordinateurs personnels contre les programmes malveillants. Il présente une combinaison optimale de méthodes traditionnelles de lutte contre les virus et de technologies proactives.

Le programme assure une analyse antivirus sophistiquée, notamment :

- Analyse antivirus du trafic de messagerie au niveau du protocole de transfert des données (POP3, IMAP ou NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé et analyse et réparation des bases antivirus.
- Analyse en temps réel du trafic Internet transmis via le protocole HTTP.
- Analyse antivirus de n'importe quel fichier, répertoire ou disque. De plus, au départ de la tâche proposée, il est possible de lancer la recherche d'éventuels virus uniquement dans les secteurs critiques du système d'exploitation ou dans les objets chargés au démarrage du système d'exploitation de Microsoft Windows.

La défense proactive permet de :

- **Contrôler les modifications du système de fichiers.** Le programme autorise la création de listes d'applications dont la composition sera contrôlée. Les programmes malveillants ne pourront pas ainsi violer l'intégrité de l'application.
- **Observer les processus dans la mémoire vive.** Kaspersky Anti-Virus 7.0 avertit en temps utiles l'utilisateur en cas de détection de processus dangereux, suspects ou dissimulés ou en cas de modification non autorisée des processus actifs.
- **Surveiller les modifications de la base de registres système** grâce au contrôle de l'état de la base de registres.

- **Le contrôle des processus cachés** permet de lutter contre les outils de dissimulation d'activité qui cachent le code malveillant dans le système d'exploitation.
- **Analyseur heuristique.** Lors de l'analyse d'un programme quelconque, l'analyseur émule son exécution et enregistre dans un rapport toutes les actions suspectes telles que l'ouverture ou l'enregistrement d'un fichier, l'interception de vecteurs d'interruptions, etc. Sur la base de ce rapport, l'application décide de l'éventuelle infection du programme par un virus. L'émulation a lieu dans un milieu artificiel isolé, ce qui permet d'éviter l'infection de l'ordinateur.
- **Restaurer le système** après les actions malveillantes des logiciels espions grâce à la correction des modifications de la base de registres et du système de fichiers de l'ordinateur et leur remise à l'état antérieur sur décision de l'utilisateur.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 est une solution sophistiquée de protection des ordinateurs personnels contre les principales menaces informatiques que sont les virus, les pirates, le courrier indésirable et les logiciels espions. L'interface utilisateur unique permet de configurer et d'administrer tous les composants de la solution.

Les fonctions antivirus proposées sont les suivantes :

- **Analyse antivirus du flux de messagerie** au niveau du protocole de transfert des données (POP3, IMAP et NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé. La réparation des messages infectés dans les bases de messagerie et des plug in sont prévus pour les clients de messagerie les plus utilisés comme Microsoft Office Outlook, Microsoft Outlook Express et The Bat!
- **Analyse en temps réel du trafic Internet** transmis via le protocole HTTP.
- **Protection du système de fichiers** : n'importe quel fichier, répertoire ou disque peut être soumis à l'analyse antivirus. Il est possible également d'analyser uniquement les secteurs critiques du système d'exploitation et les objets lancés au démarrage de Microsoft Windows.
- **Protection proactive** : le programme surveille en permanence l'activité des applications et des processus exécutés dans la mémoire vive de l'ordinateur, empêche les modifications dangereuses du système de fichiers et rétablit le système après une action malveillante.

La **protection contre les escroqueries en ligne** est assurée grâce à l'identification des attaques de phishing. La fuite d'informations confidentielles

est ainsi évitée (il s'agit avant tout des mots de passe, des numéros de compte et de carte bancaires, blocage de l'exécution de scripts dangereux, des fenêtres pop up et des bannières). La **fonction de blocage des appels téléphoniques automatiques payants** permet d'identifier les programmes qui tentent d'établir une connexion cachée via votre modem à des services téléphoniques payant et de les bloquer. Le module **Protection des données confidentielles** vous protège contre l'accès non-autorisé aux données personnelles et contre le transfert de celles-ci. Le composant **Contrôle parental** garantit le contrôle de l'accès de l'utilisateur aux sites Internet.

Kaspersky Internet Security 7.0 **identifie les tentatives de balayage des ports de votre ordinateur**, signe précurseur des attaques de réseau et bloque avec succès les attaques de pirates informatiques les plus répandues. **Sur la base des règles définies**, le programme surveille toutes les interactions au niveau du réseau et contrôle tous **les paquets entrants et sortants**. **Le mode furtif empêche la découverte de votre ordinateur de l'extérieur du réseau**. Lorsque ce mode est activé, toutes les activités de réseau sont bloquées, à l'exception de celles autorisées par les règles d'exception définies par l'utilisateur.

Le programme adopte une démarche complexe pour le filtrage du courrier entrant afin d'identifier les messages non sollicités :

- Vérification selon des listes « blanche » ou « noire » d'adresses (y compris les adresses de sites de phishing) ;
- Analyse des expressions dans le corps des messages ;
- Analyse du corps des messages à l'aide d'un algorithme d'auto-apprentissage ;
- Identification du spam sous forme graphique.

Kaspersky® Anti-Virus Mobile

Kaspersky Anti-Virus Mobile garantit la protection antivirus des appareils nomades tournant sous Symbian OS et Microsoft Windows Mobile. Le logiciel est capable de réaliser des analyses antivirus sophistiquées dont :

- **L'analyse à la demande** de la mémoire de l'appareil nomade, de la carte mémoire, d'un répertoire particulier ou d'un fichier distinct. En cas de découverte d'un objet infecté, celui-ci est placé dans le répertoire de quarantaine ou il sera supprimé ;
- **L'analyse en temps réel** : tous les objets entrants ou modifiés sont automatiquement analysés, de même que les fichiers auxquels des requêtes sont adressées ;
- **L'analyse programmée** des informations conservées dans la mémoire de l'appareil nomade ;

- **Protection contre les sms et mms indésirables .**

Kaspersky Anti-Virus for File servers

Ce logiciel offre une protection fiable pour les systèmes de fichiers des serveurs tournant sous Microsoft Windows, Novell NetWare, Linux et Samba contre tous les types de programmes malveillants. Le logiciel contient les applications suivantes de Kaspersky Lab :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-virus for Samba Server.

Avantages et fonctions :

- *Protection des systèmes de fichiers des serveurs en temps réel* : tous les fichiers du serveur sont analysés à chaque tentative d'ouverture ou d'enregistrement sur le serveur.
- *Prévention des épidémies de virus* ;
- *Analyse à la demande* de tout le système de fichiers ou de répertoires ou de fichiers distincts ;
- *Application de technologies d'optimisation* lors de l'analyse des objets du système de fichiers du serveur ;
- *Restauration du système après une infection* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Respect de l'équilibre de la charge du système* ;
- *Constitution d'une liste de processus de confiance* dont l'activité sur le serveur n'est pas contrôlée par le logiciel ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Enregistrement des copies de sauvegarde des objets infectés ou supprimés* au cas où il faudra les restaurer ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Notifications des événements* survenus dans l'utilisation du logiciel par l'administrateur du système ;

- *Génération de rapports détaillés ;*
- *Mise à jour automatique des bases de l'application.*

Kaspersky Open Space Security

Kaspersky Open Space Security est un logiciel qui adopte une nouvelle conception de la sécurité des réseaux des entreprises de n'importe quelle taille dans le but d'offrir une protection centralisée des systèmes d'informations tout en prenant en charge les utilisateurs nomades et les télétravailleurs.

Cette application est composée de quatre logiciels :

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Voici une description détaillée de chacun d'entre eux.

Kaspersky WorkSpace Security est un logiciel conçu pour la protection centralisée des postes de travail dans le réseau d'entreprise et en dehors de celui-ci contre tous les types de menaces modernes présentes sur Internet : Virus, logiciels espions, pirates informatiques et courrier indésirable.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable. ;*
- *Défense proactive* contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Annulation des modifications malveillantes dans le système ;*
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable ;*
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;

- *Compatibilité avec Cisco® NAC (Network Admission Control) ;*
- *Analyse du courrier électronique et du trafic Internet en temps réel ;*
- *Blocage des fenêtres pop up et des bannières publicitaires pendant la navigation sur Internet ;*
- *Travail en toute sécurité dans les réseaux de n'importe quel type, y compris les réseaux Wi-Fi ;*
- *Outils de création d'un disque de démarrage capable de restaurer le système après une attaque de virus ;*
- *Système développé de rapports sur l'état de la protection ;*
- *Mise à jour automatique des bases ;*
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits ;*
- *Optimisation du fonctionnement de l'application sur les ordinateurs portables (technologie Intel® Centrino® Duo pour ordinateurs portables) ;*
- *Possibilité de réparation à distance (technologie Intel® Active Management, composant Intel® vPro™).*

Kaspersky Business Space Security offre une protection optimale des ressources informatiques de l'entreprise contre les menaces Internet modernes. Kaspersky Business Space Security protège les postes de travail et les serveurs de fichiers contre tous les types de virus, de chevaux de Troie et de vers, prévient les épidémies de virus et garantit l'intégrité des informations ainsi que l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Administration à distance de l'application, y compris l'installation, la configuration et l'administration ;*
- *Compatibilité avec Cisco® NAC (Network Admission Control) ;*
- *Protection des postes de travail et des serveurs de fichiers contre tous les types de menaces Internet ;*
- *Utilisation de la technologie iSwift pour éviter les analyses répétées dans le cadre du réseau ;*
- *Répartition de la charge entre les processeurs du serveur ;*

- *Isolement des objets suspects* du poste de travail dans un répertoire spécial ;
- *Annulation des modifications malveillantes dans le système* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Analyse du courrier électronique et du trafic Internet* en temps réel ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Protection lors de l'utilisation des réseaux sans fil* Wi-Fi ;
- *Technologie d'autodéfense de l'antivirus* contre les programmes malveillants ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Mise à jour automatique des bases.*

Kaspersky Enterprise Space Security

Ce logiciel propose des composants pour la protection des postes de travail et des serveurs contre tous les types de menaces Internet modernes, supprime les virus du flux de messagerie, assure l'intégrité des informations et l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Protection des postes de travail et des serveurs* contre les virus, les chevaux de Troie et les vers ;
- *Protection des serveurs de messagerie* Sendmail, Qmail, Postfix et Exim ;
- *Analyse de tous les messages sur le serveur Microsoft Exchange* y compris les dossiers partagés ;
- *Traitement des messages, des bases de données et d'autres objets des serveurs Lotus Domino* ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;

- *Prévention des épidémies de virus et des diffusions massives ;*
- *Montée en capacité de l'application dans le cadre des ressources disponibles dans le système ;*
- *Administration à distance de l'application, y compris l'installation, la configuration et l'administration ;*
- *Compatibilité avec Cisco® NAC (Network Admission Control) ;*
- *Défense proactive des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;*
- *Pare-feu personnel avec système d'identification des intrusions et de prévention des attaques de réseau ;*
- *Utilisation sécurisée des réseaux sans fil Wi-Fi ;*
- *Analyse du trafic Internet en temps réel ;*
- *Annulation des modifications malveillantes dans le système ;*
- *Redistribution dynamique des ressources lors de l'analyse complète du système ;*
- *Isolement des objets suspects dans un répertoire spécial ;*
- *Système de rapports sur l'état de la protection ;*
- *Mise à jour automatique des bases.*

Kaspersky Total Space Security

Le logiciel contrôle tous les flux de données entrant et sortant : courrier électronique, trafic Internet et interaction dans le réseau. Le logiciel prévoit des composants pour la protection des postes de travail et des périphériques nomades, garantit l'accès instantané et sécurisé des utilisateurs aux ressources informatiques de l'entreprise et à Internet et garantit également une communication sûre via courrier électronique.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable à tous les niveaux du réseau de l'entreprise : depuis les postes de travail jusqu'aux passerelles d'accès Internet ;*
- *Défense proactive des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;*

- *Protection des serveurs de messagerie et des serveurs de coopération ;*
- *Analyse du trafic Internet (HTTP/FTP) qui arrive sur le réseau local en temps réel ;*
- *Montée en capacité de l'application dans le cadre des ressources disponibles dans le système ;*
- *Blocage de l'accès depuis un poste de travail infecté ;*
- *Prévention des épidémies de virus ;*
- *Rapports centralisés sur l'état de la protection ;*
- *Administration à distance de l'application, y compris l'installation, la configuration et l'administration ;*
- *Compatibilité avec Cisco® NAC (Network Admission Control) ;*
- *Compatibilité avec les serveurs proxy matériels ;*
- *Filtrage du trafic Internet selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;*
- *Utilisation de la technologie iSwift pour éviter les analyses répétées dans le cadre du réseau ;*
- *Redistribution dynamique des ressources lors de l'analyse complète du système ;*
- *Pare-feu personnel avec système d'identification des intrusions et de prévention des attaques de réseau ;*
- *Travail en toute sécurité dans les réseaux de n'importe quel type, y compris les réseaux Wi-Fi ;*
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable ;*
- *Possibilité de réparation à distance (technologie Intel® Active Management, composant Intel® vPro™) ;*
- *Annulation des modifications malveillantes dans le système ;*
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants ;*
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits ;*
- *Mise à jour automatique des bases.*

Kaspersky Security for Mail Servers

Ce logiciel a été développé pour la protection des serveurs de messagerie et des serveurs de coopération contre les programmes malveillants et le courrier indésirable. Le logiciel contient des applications pour la protection de tous les serveurs de messagerie populaires : Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix et Exim et il permet également d'organiser la répartition des passerelles de messagerie. La solution contient :

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel ;*
- *Filtrage des messages non sollicités ;*
- *Analyse des messages et des pièces jointes du courrier entrant et sortant ;*
- *Analyse antivirus de tous les messages sur le serveur Microsoft Exchange y compris les dossiers partagés ;*
- *Analyse des messages, des bases de données et d'autres objets des serveurs Lotus Domino ;*
- *Filtrage des messages en fonction du type de pièce jointe ;*
- *Isolement des objets suspects dans un répertoire spécial ;*
- *Système convivial d'administration du logiciel ;*
- *Prévention des épidémies de virus ;*
- *Surveillance de l'état du système de protection à l'aide de notifications ;*
- *Système de rapports sur l'activité de l'application ;*
- *Montée en capacité de l'application dans le cadre des ressources disponibles dans le système ;*
- *Mise à jour automatique des bases.*

Kaspersky Security for Internet Gateway

Ce logiciel garantit un accès sécurisé au réseau Internet pour tous les membres de l'organisation. Il supprime automatiquement les programmes malveillants et

les programmes présentant un risque potentiel de tous les flux de données qui arrivent dans le réseau via le protocole HTTP/FTP. La solution contient :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel ;*
- *Analyse du trafic Internet (HTTP/FTP) en temps réel ;*
- *Filtrage du trafic Internet selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;*
- *Isolement des objets suspects dans un répertoire spécial ;*
- *Système convivial d'administration ;*
- *Système de rapports sur le fonctionnement de l'application ;*
- *Compatibilité avec les serveurs proxy matériels ;*
- *Montée en capacité de l'application dans le cadre des ressources disponibles dans le système ;*
- *Mise à jour automatique des bases.*

Kaspersky® Anti-Spam

Kaspersky Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages, avec l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

Kaspersky® Anti-Spam se comporte comme un filtre, placé à l'entrée du réseau, qui analyse les flux entrants de courrier électronique à la recherche d'objets identifiés en tant que courrier indésirable. Le logiciel est compatible avec tous les systèmes de messagerie existants sur votre réseau et il peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes des bases de données utilisées par les filtres, à partir des échantillons fournis par les spécialistes linguistiques du laboratoire.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper offre une analyse antivirus rapide du trafic sur les serveurs qui utilisent Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

Le programme se présente sous la forme d'un module externe et il analyse et traite en temps réel les messages entrants et sortants.

A.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab (en anglais). 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.

Support technique	Pour une assistance technique, adressez-vous à : http://case.kaspersky.fr/
Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://support.kaspersky.fr E-mail : info@fr.kaspersky.com

ANNEXE B. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") CONÇU PAR KASPERSKY LAB ("KASPERSKY LAB").

SI VOUS AVEZ ACHETE CE LOGICIEL VIA INTERNET EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN UTILISANT LE CD VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'UTILISEZ PAS LE CD, NE TELECHARGEZ PAS, N'INSTALLEZ PAS ET N'UTILISEZ PAS CE LOGICIEL.

EN ACCORD AVEC LA LEGISLATION FRANCAISE, SI VOUS ETES UN PARTICULIER ET QUE VOUS AVEZ ACHETE VOTRE LOGICIEL EN FRANCE, VIA INTERNET, SUR UNE BOUTIQUE EN LIGNE, VOUS BENEFICIEZ D'UNE POSSIBILITE DE RETOUR ET DE REMBOURSEMENT DURANT UN DELAI DE 7 JOURS. L'EVENTUEL DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL. CONTACTEZ LA BOUTIQUE EN LIGNE SUR LAQUELLE VOUS AVEZ EFFECTUE VOTRE ACHAT POUR PLUS DE RENSEIGNEMENTS. KASPERSKY N'EST NI TENU D'APPLIQUER, NI RESPONSABLE DU CONTENU ET DES CLAUSES CONTRACTUELLES DE SES PARTENAIRES.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la clé d'activation du logiciel qui vous sera fournie par Kaspersky Lab comme faisant partie du Logiciel.

1. *Octroi de la Licence.* Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Lab vous offre le droit non-exclusif et non-transférable d'utiliser cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer ce Logiciel sur un ordinateur.

1.1 Utilisation. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un ordinateur, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation" sur un ordinateur lorsqu'il est chargé dans la mémoire tampon (i.e., random-access memory ou RAM) ou installé dans la mémoire permanente (e.g., disque dur, CD-ROM, ou autre périphérique de stockage) de cet ordinateur. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

1.1.2 Si vous cédez l'ordinateur sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire l'ingénierie amont, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, et de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Lab contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Lab vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez l'ingénierie amont ou ne décompiliez pas hors les limites autorisées par la loi.

1.1.4 Il est interdit de copier, d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

1.1.5 Il est interdit de louer ou prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.1.6 Ce logiciel ne peut-être utilisé dans des outils automatiques, semi-automatiques ou manuels conçus pour la création de définitions de virus, de routines de détection de virus ou de n'importe quel autre type de données ou de codes servant à détecter des données ou des codes malicieux.

2. Assistance technique.

Kaspersky peut vous fournir une assistance technique ("Assistance Technique") comme décrit sur le site www.kaspersky.fr.

3. *Droits de Propriété.* Le Logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les copyrights, brevets, marques déposées et autres droits de propriété intellectuelle concernés. Votre possession, installation ou utilisation du Logiciel ne vous transmet pas le droit de propriété intellectuelle sur le Logiciel, et ne vous donne aucun droit sur le Logiciel sauf si décrit expressément ci-après dans ce Contrat.

4. *Confidentialité.* Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez, fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.

5. *Limites de Garantie.*

- (i) Kaspersky Lab garantit que pour une durée de 6 mois suivant le premier téléchargement ou la première installation d'un logiciel kaspersky en version sur CD-ROM, le logiciel fonctionnera, en substance, comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.
- (ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le Logiciel et/ou la Documentation répondent à ces besoins et que leur utilisation soit exempte d'interruptions et d'erreurs.
- (iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaisse tous les virus connus ou qu'il n'affichera pas de message de détection erroné.
- (iv) L'entière responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un ayant-droit au cours de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel.
- (v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Lab, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat.
- (vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce paragraphe (vi) ont effet entre Kaspersky Lab et vous ou sont implicites ou intégrés dans ce Contrat ou autre contrat collatéral, soit par statut, loi commune ou tout ce qui est exclu ici (incluant sans limitation les conditions, garanties ou autres termes relatifs à la qualité de

satisfaction, justesse d'utilisation ou pour le respect de compétences et du bon sens).

6. *Limites de Responsabilité.*

- (i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Lab en cas (a) de non-satisfaction de l'utilisateur, (b) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, ou (c) d'autre responsabilité qui ne peut être exclue par la loi.
- (ii) Selon les termes du paragraphe (i) au-dessus, Kaspersky Lab ne pourra être tenu pour responsable (si dans le contrat, acte dommageable, compensation ou autres) pour les dommages et pertes suivants (si de tels dommages ou pertes étaient prévus, prévisibles, connus ou autres):
 - (a) Perte de revenus;
 - (b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats);
 - (c) Perte de moyens de paiement;
 - (d) Perte d'économies prévues;
 - (e) Perte de marché;
 - (f) Perte d'occasions commerciales;
 - (g) Perte de clientèle;
 - (h) Atteinte à l'image;
 - (i) Perte, endommagement ou corruption des données; ou
 - (j) Tout dommage ou toute perte qu'ils soient directs ou indirects, ou causés de quelque façon que ce soit (incluant, pour éviter le doute, ces dommages ou pertes spécifiés dans les paragraphes (ii), (a) jusque (ii), (i).
- (iii) Selon les termes du paragraphe (i), la responsabilité de Kaspersky Lab (si dans le contrat, acte dommageable, compensation ou autres) survenant lors de la fourniture du Logiciel n'excèdera en aucun cas un montant égal à celui du prix d'achat du Logiciel.

7. Ce Contrat constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous

et Kaspersky Lab, et qui ont été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'Effet.

Le support technique, tel que présenté en clause 2 de cet EULA ne vous concerne pas si vous utilisez ce programme en mode de démonstration ou d'essai. De même vous n'avez pas le droit de vendre les éléments de ce programme, ensembles ou séparément.

Vous pouvez utiliser le logiciel pour des raisons de démonstration ou d'essai pour la période spécifiée dans la licence. La période d'essai ou de démonstration commence à l'activation de la licence ou dès son installation. La période est visible dans l'interface graphique windows du logiciel.