Kaspersky Security Center 10.0

Guide de demarrage

VERSION DE L'APPLICATION : 10.0

Cher utilisateur,

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

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

Date d'édition : 12/12/2012

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

TABLE DES MATIERES

A PROPOS DU MANUEL

Ce document contient une description des actions qui vous permettent de commencer à utiliser rapidement l'application Kaspersky Security Center 10.0 (ci-après – Kaspersky Security Center) et de déployer le système de protection dans tout le réseau de l'entreprise cliente à partir des applications de Kaspersky Lab.

Le document s'adresse aux administrateurs des réseaux informatiques des entreprises et aux entreprises offrant des services SaaS (ci-après – prestataires de services).

Ici, le scénario simple de l'installation de Kaspersky Security Center est décrit en détail, quand la protection s'effectue sur quelques ordinateurs avec le système d'exploitation Microsoft® Windows® sans utilisation d'hiérarchie des Serveurs d'administration dans le réseau de l'entreprise.

Dans les cas, quand les étapes de configuration du fonctionnement de l'application pour le prestataire de services sont différentes des étapes de configuration du fonctionnement de l'application pour l'administrateur du réseau de l'entreprise, les actions du prestataire de services sont décrites à part.

La procédure de passage de la version 9.0 à la version 10.0 est aussi décrite dans ce document.

Les informations détaillées concernant Kaspersky Security Center se trouvent dans le *Manuel d'implantation* et le *Manuel de l'administrateur de Kaspersky Security Center*.

DANS CETTE SECTION

DANS CE DOCUMENT

Le *Guide de démarrage de Kaspersky Security Center* contient l'introduction, les sections décrivant les tâches typiques exécutées par Kaspersky Security Center et la conclusion.

Sources d'informations sur l'application (cf. page 8)

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

Kaspersky Security Center (à la page 10)

Cette section reprend les informations sur la désignation, les fonctions clés et la composition de l'application Kaspersky Security Center.

Licence de l'application (cf. page 11)

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

Interface de l'application (cf. page 17)

Cette section décrit les paramètres principaux de l'interface Kaspersky Security Center.

CONVENTIONS

Le texte du document est suivi des significations sur lesquelles nous attirons votre attention : avertissements, conseils, exemples.

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

Table 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DES CONVENTIONS
N'oubliez pas que ...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent les informations sur les actions indésirables potentielles qui peuvent amener à la perte d'informations ou à la perturbation du fonctionnement du matériel ou du système d'exploitation.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques fournissent des conseils et des informations d'aide. Il peut s'agir par exemple de conseils utiles, de recommandations, de valeurs importantes de paramètres ou de cas particuliers importants pour le fonctionnement de l'application.
Exemple : ...	Les exemples sont présentés dans les groupes sous le titre "Exemple".
La *mise à jour*, c'est ... L'événement *Bases dépassées* survient.	Les significations suivantes sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison des touches **ALT**+**F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il faut appuyer simultanément sur ces touches.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères gras.
Pour programmer une tâche, procédez comme suit :	Les phrases d'introduction des instructions sont en italique et présentent l'icône "flèche".
Dans la ligne de commande, saisissez le texte help Les informations suivantes s'affichent : Indiquez la date au format JJ:MM:AA.	La police spéciale (Courier) désigne les types de texte suivants : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir par l'utilisateur.
`<Nom d'utilisateur>`	Les variables sont écrites entre chevrons. La valeur correspondant à la variable doit être remplacée par cette variable à chaque fois. Par ailleurs, les chevrons sont omis.

SOURCES D'INFORMATIONS SUR L'APPLICATION

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

Vous pouvez ainsi choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

SOURCES D'INFORMATIONS POUR LES RECHERCHES INDEPENDANTES

Vous pouvez utiliser les sources suivantes pour une recherche indépendante des informations sur l'application :

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

Si vous ne parvenez pas à résoudre vous-même le problème, il est conseillé de contacter le Support technique de Kaspersky Lab (cf. section "Assistance technique par téléphone" à la page 39).

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

Page sur le site Web de Kaspersky Lab

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

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

La page http://www.kaspersky.com/fr/ contient le lien vers la boutique en ligne. Le lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

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

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

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

Les articles peuvent répondre à des questions en rapport non seulement avec Kaspersky Security Center, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur le Support Technique en général.

Aide électronique

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

L'aide contextuelle contient les informations sur chaque fenêtre de l'application : la liste et la description des paramètres et les liens vers les tâches dans lesquelles ces paramètres sont utilisés.

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

Documentation

La distribution de l'application contient les documents qui vous aideront à installer et activer l'application sur les ordinateurs du réseau de l'entreprise et à configurer les paramètres de fonctionnement ou à obtenir des informations sur les principes de fonctionnement de l'application.

FORUM SUR LES APPLICATIONS DE KASPERSKY LAB

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs de nos applications dans notre forum (http://forum.kaspersky.fr).

Sur le forum, vous pouvez consulter les sujets publiés, ajouter des commentaires, créer une nouvelle discussion ou lancer des recherches.

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

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

KASPERSKY SECURITY CENTER

Cette section reprend les informations sur la désignation, les fonctions clés et la composition de l'application Kaspersky Security Center.

L'application Kaspersky Security Center a été développée pour centraliser les principales tâches d'administration et assurer le système de protection du réseau de l'entreprise. L'application offre à l'utilisateur l'accès aux informations détaillées sur le niveau de sécurité du réseau de l'entreprise et permet de configurer tous les modules de la protection construite sur la base des applications de Kaspersky Lab.

L'application Kaspersky Security Center est un outil destiné aux administrateurs de réseaux d'entreprise et aux responsables de la sécurité.

La version SPE est un outil destiné aux entreprises offrant des services SaaS (ci-après – *prestataires de services*).

A l'aide de Kaspersky Security Center, vous pouvez :

- Former une hiérarchie des Serveurs d'administration pour administrer le réseau de votre propre entreprise, ainsi que les réseaux des postes distants ou des entreprises clientes.

  Les *entreprises-clientes* font référence aux entreprises dont la protection antivirus est assurée par le prestataire de services.

- Former une hiérarchie des groupes d'administration pour gérer les périphériques (les postes clients et les machines virtuelles) comme un ensemble.

- Administrer le système de protection antivirus formé à partir des applications de Kaspersky Lab.

- Créer de manière centralisée les images des systèmes d'exploitation et les déployer sur les postes clients par le réseau, ainsi qu'exécuter l'installation à distance des applications de Kaspersky Lab et d'autres éditeurs de logiciels.

- Administrer à distance les applications de Kaspersky Lab et d'autres éditeurs installées sur les postes clients : installer les mises à jour, rechercher et corriger les vulnérabilités.

- Diffuser de manière centralisée les clés des applications de Kaspersky Lab sur les postes clients, suivre l'utilisation des clés et prolonger la durée de validité des licences.

- Recevoir les statistiques et les rapports de fonctionnement des applications et des périphériques.

- Recevoir les notifications pour les événements critiques survenus pendant le fonctionnement des applications de Kaspersky Lab.

- Contrôler l'accès des périphériques dans le réseau de l'entreprise à l'aide des règles de restriction d'accès et à l'aide de la liste "blanche" des périphériques. Les agents NAC sont utilisés pour administrer l'accès des périphériques dans le réseau de l'entreprise.

- Administrer les périphériques mobiles qui prennent en charge les protocoles Exchange ActiveSync® et iOS Mobile Device Management (iOS MDM).

- Administrer le chiffrement des informations enregistrées sur les disques durs et les disques amovibles, et administrer l'accès des utilisateurs aux données chiffrées.

- Faire l'inventaire du matériel connecté au réseau de l'entreprise.

- Travailler de façon centralisée avec les objets, placés en quarantaine ou dans le dossier de sauvegarde par les applications antivirus, aussi qu'avec les fichiers dont le traitement est différé par les applications antivirus.

LICENCE DE L'APPLICATION

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

DANS CETTE SECTION

A PROPOS DU CONTRAT DE LICENCE

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

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

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

A PROPOS DE LA LICENCE

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

La licence vous donne droit aux types de service suivants :

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

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

- Contacter le Support Technique de Kaspersky Lab.

- Accès aux divers services offerts par Kaspersky Lab ou ses partenaires pendant la durée de validité de la licence.

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

Il existe les types de licence suivants :

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

  En général, la durée de validité d'une licence d'évaluation est brève. Une fois que la licence expirée, Kaspersky Security Center continue son fonctionnement en mode de fonctionnalité partiellement limitée.

- *Commerciale* : licence payante octroyée à l'achat de l'application. Plusieurs options de licence de Kaspersky Security Center sont prévues.

  A l'expiration de la durée de validité de la licence commerciale, l'application continue son fonctionnement en mode de fonctionnalité partiellement limitée (cf. section "A propos des restrictions de la fonctionnalité de base" à la page 14). Pour pouvoir continuer à utiliser toutes les fonctions de Kaspersky Security Center, il faut renouveler la licence commerciale.

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

OPTIONS DE LICENCE DE KASPERSKY SECURITY CENTER

Dans Kaspersky Security Center, la licence peut être diffusée sur des groupes différents de fonctionnalité.

Fonctionnalité de base de la Console d'administration

Les fonctions suivantes sont disponibles :

- création des Serveurs d'administration virtuels pour administrer le réseau des offices à distance et des entreprises clientes ;
- formation d'une hiérarchie des groupes d'administration pour administrer l'ensemble de périphériques comme un tout unique ;
- contrôle d'état de sécurité antivirus de l'entreprise ;
- installation à distance des applications ;
- consultation de la liste des images des systèmes d'exploitation accessibles à l'installation à distance ;
- configuration centralisée des paramètres des applications installées sur les postes clients ;
- consultation et modification des groupes existants des applications sous licence ;
- réception des statistiques et des rapports sur le fonctionnement des applications, ainsi que la réception des notifications sur les événements critiques ;
- administration du processus de chiffrement et de protection des données ;
- consultation et modification manuelle de la liste du matériel détecté suite au sondage du réseau ;
- travail centralisé avec les fichiers placés en quarantaine ou dans le dossier de sauvegarde, et avec les fichiers dont le traitement est différé.

L'application Kaspersky Security Center avec la prise en charge de la fonctionnalité de base de la Console d'administration est livrée dans la suite logicielle de Kaspersky Lab conçue pour la protection du réseau de l'entreprise. Il peut également être téléchargé depuis le site de Kaspersky Lab (http://www.kaspersky.com/fr).

Le Serveur d'administration virtuel est une unité d'administration pour la fonctionnalité de base de l'application. Il est possible de créer jusqu'à 10 Serveurs d'administration virtuels.

Avant l'activation de l'application ou à l'expiration de la durée de validité de la licence commerciale, Kaspersky Security Center fonctionne en mode de fonctionnalité de base de la Console d'administration (cf. section "A propos des restrictions de la fonctionnalité de base" à la page 14).

Fonctionnalité de Kaspersky Security Center, Service Provider Edition (ci-après – SPE)

La fonctionnalité de la version SPE de l'application double la fonctionnalité de base de la Console d'administration, mais il est possible de créer plus de 10 Serveur d'administration virtuels.

La version SPE de l'application est livrée sous les conditions particulières aux partenaires de Kaspersky Lab. Pour plus d'informations sur le programme de partenariat, visitez le site Internet de Kaspersky Lab, à la page http://www.kaspersky.com/fr/partners.

Fonctionnalité Administration système

Les fonctions suivantes sont disponibles :

- installation à distance des systèmes d'exploitation ;
- installation à distance des mises à jour du logiciel, recherche et fermeture des vulnérabilités ;
- administration d'accès des périphériques dans le réseau de l'entreprise (NAC) ;
- inventaire du matériel ;
- administration des groupes des applications sous licence ;
- connexion à distance aux postes clients.

Le poste client dans le groupe "Ordinateurs administrés" est une unité d'administration pour la fonctionnalité de l'Administration système.

Fonctionnalité Gestion des périphériques mobiles

La fonctionnalité de Gestion des périphériques mobiles est conçu pour administrer les périphériques mobiles Exchange ActiveSync et iOS MDM.

Pour les périphériques mobiles Exchange ActiveSync, les fonctions suivantes sont disponibles :

- création et modification des profils d'administration des périphériques mobiles, attribution des profils aux boîtes aux lettres des utilisateurs ;
- configuration des paramètres de fonctionnement du périphérique mobile (synchronisation du courrier, mot de passe de l'utilisateur, chiffrement des données, connexion des disques amovibles) ;
- installation des certificats sur les périphériques mobiles.

Pour les périphériques mobiles iOS MDM, les fonctions suivantes sont disponibles :

- création et modification des profils de configuration, installation des profils de configuration sur les périphériques mobiles ;
- installation des applications sur le périphérique mobile via App Store ou à l'aide des fichiers-manifestes(.plist) ;
- possibilité de bloquer le périphérique mobile, de remettre à zéro le mot de passe du périphérique et de supprimer toutes les données sur le périphérique mobile.

L'exécution des commandes prévues par les protocoles correspondants est aussi accessible dans le cadre de fonctionnalité Gestion des périphériques mobiles.

Le périphérique mobile est une unité d'administration de la fonctionnalité de Gestion des périphériques mobiles. Le périphérique mobile est considéré comme périphérique administré quand il est connecté au Serveur des périphériques mobiles.

A PROPOS DES RESTRICTIONS DE LA FONCTIONNALITE DE BASE

Avant l'activation de l'application ou à l'expiration de la durée de validité de la licence commerciale, Kaspersky Security Center fonctionne en mode de fonctionnalité de base de la Console d'administration. La description des restrictions imposées sur le fonctionnement de l'application dans ce mode est reprise ci-après.

Gestion des périphériques mobiles

Il est impossible de créer le nouveau profil et de le désigner au périphérique mobile (iOS MDM) ou à la boîte aux lettres (Exchange ActiveSync). La modification des profils existants et leur désignation aux boîtes aux lettres est toujours disponible.

Administration des applications

Il est impossible de lancer les tâches d'installation et de suppression des mises à jour. Toutes les tâches lancées avant l'expiration de la durée de validité de la licence sont exécutées jusqu'à la fin mais les dernières mises à jour ne s'installent pas. Par exemple, si avant l'expiration de la durée de validité de la licence, la tâche d'installation des mises à jour critiques a été lancée, les mises à jour critiques trouvées avant l'expiration de la durée de validité de la licence seront installées uniquement.

Le lancement et la modification des tâches de synchronisation, de recherche de vulnérabilités et de mise à jour de la base des vulnérabilités sont toujours disponibles. Les restrictions ne s'imposent pas aussi sur la consultation, la recherche et le classement des enregistrements dans la liste des vulnérabilités et des mises à jour.

Installation à distance des systèmes d'exploitation et des applications

Il est impossible de lancer les tâches de prise et d'installation de l'image du système d'exploitation. Les tâches lancées avant l'expiration de la durée de validité de la licence sont exécutées jusqu'à la fin.

Administration d'accès dans le réseau

L'agent NAC et NAC sont permutés en mode "Désactivé" sans la possibilité d'activation.

Inventaire du matériel

La collecte des informations sur les nouveaux périphériques n'est pas disponible à l'aide de NAC et du Serveur des périphériques mobiles. Avec cela, les informations sur les ordinateurs et les périphériques connectés s'actualisent.

Les notifications sur la modification de la configuration des périphériques ne fonctionnent pas.

La liste du matériel est disponible à la consultation et à la modification manuelle.

Administration des groupes des applications de licence

Il est impossible d'ajouter une nouvelle clé.

Les notifications sur les dépassements des restrictions sur l'utilisation des clés ne sont pas envoyées.

Connexion à distance aux postes clients

La connexion à distance aux postes clients n'est pas disponible.

Sécurité antivirus

L'Antivirus utilise les bases installées avant l'expiration de la durée de validité de la licence.

A PROPOS DU CODE D'ACTIVATION

Le *code d'activation* est un code que vous obtenez après avoir acheté une licence commerciale pour Kaspersky Security Center. Le code d'activation est une suite unique de 20 caractères alphanumériques au format XXXXX-XXXXX-XXXXX-XXXXX.

Pour activer l'application à l'aide du code d'activation, il faut se connecter au serveurs d'activation de Kaspersky Lab via Internet. Si la connexion aux serveurs d'activation et l'accès à Internet sont absents, l'activation de l'application est exécutée à l'aide du fichier clé (cf. section "A propos du fichier clé" à la page 15).

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

En cas de perte ou de suppression accidentelle du code d'activation après l'activation de l'application, contactez le Support Technique de Kaspersky Lab pour le récupérer.

A PROPOS DU FICHIER CLE

Le *fichier clé est un* fichier de type xxxxxxx.key.

Le fichier clé est utilisé pour activer l'application. Le fichier clé contient toutes les informations nécessaires pour l'activation. Lors du processus d'activation à l'aide du fichier clé, la connexion au serveurs d'activation et l'accès à Internet ne sont pas requis.

Pour obtenir le fichier clé ou pour le restaurer après une suppression accidentelle, vous pouvez envoyer une demande au Support Technique (cf. section "Contacter le Support Technique" à la page 39).

Le fichier clé contient les informations suivantes :

- La clé est une séquence unique de chiffres et de lettres. La clé peut être utilisée, par exemple, pour obtenir l'assistance technique de Kaspersky Lab.
- Les restrictions sur l'utilisation de l'application. Jusqu'à trois restrictions peuvent être indiquées dans le fichier clé de Kaspersky Security Center : nombre de Serveurs d'administration virtuels, nombre d'ordinateurs administrés et nombre de périphériques mobiles administrés. Le type de restriction est défini par la licence actuelle (cf. section "Options de licence de Kaspersky Security Center" à la page 12).
- La date de création du fichier clé est la date de création du fichier clé sur le serveur d'activation.
- La durée de validité de la licence est la durée prévue d'utilisation de l'application dans le Contrat de licence, calculée à partir de la date de la première activation de l'application à l'aide de ce fichier clé (par exemple, 1 an).

  La durée de validité de la licence expire pas au-delà du délai de validité du fichier clé à l'aide duquel l'application a été activée par cette licence.

- Le délai de validité du fichier clé est le délai défini à compter de la date de création du fichier clé. L'activation de l'application à l'aide de ce fichier de clé est possible uniquement avant l'expiration de ce délai.

  Le délai de validité du fichier clé est automatiquement considéré comme expiré dès le moment d'expiration de la durée de validité de la licence sur l'utilisation de l'application activée à l'aide de ce fichier clé.

A PROPOS DES DONNEES

En acceptant les conditions du Contrat de licence, vous acceptez de transmettre en mode automatique les informations sur les volumes de contrôle des fichiers traités (MD5), les informations pour définir la réputation de l'URL, ainsi que les données sur la protection contre le courrier indésirable. Vous acceptez aussi la collecte et la transfert des informations (depuis les postes clients sous Kaspersky Security Center) en provenance des moyens logiciels et des codes de retour obtenus après l'installation de ces moyens logiciels. Les informations transmises depuis les postes clients seront utilisées pour éliminer les problèmes dans le logiciel ou pour modifier sa fonctionnalité.

Toutes les informations obtenues ne contiennent aucunes données personnelles ou autres informations confidentielles. Les informations obtenues sont protégées par Kaspersky Lab conformément aux exigences établies par la loi. Pour plus d'informations sur la présentation des données, visitez notre site Internet http://support.kaspersky.com/fr et dans le Règlement sur Kaspersky Security Network livré avec l'application.

INTERFACE DE L'APPLICATION

Cette section décrit les paramètres principaux de l'interface Kaspersky Security Center.

La consultation, la création, la modification et la configuration des groupes d'administration, l'administration centralisée du fonctionnement des applications de Kaspersky Lab installées sur les postes clients sont exécutées depuis le poste administrateur. La Console d'administration correspond à l'interface d'administration. Elle représente un outil autonome centralisé intégré à Microsoft Management Console (MMC), c'est pourquoi l'interface de Kaspersky Security Center est standard pour MMC. Pour plus d'informations, cf. le *Manuel de l'administrateur de Kaspersky Security Center*.

La fenêtre principale de l'application (cf. ill. ci-dessous) contient le menu, la barre d'outils, la barre de consultation et la zone de travail.

Le menu permet de gérer les fenêtres et d'accéder à l'aide. L'option du menu **Action** reprend les commandes du menu contextuel pour l'objet de l'arborescence de la console.

La barre de consultation affiche l'étendue des noms de **Kaspersky Security Center** dans l'arborescence de la console.

Les boutons dans la barre d'outils assure un accès direct à certaines options du menu principal. Les boutons dans la barre d'outils changent selon l'entrée ou le dossier de l'arborescence de la console sélectionné.

Le type de zone de travail de la fenêtre principale dépend de l'entrée (du dossier) de l'arborescence de la console à laquelle il/elle appartient et les fonctions qu'il/elle assure.

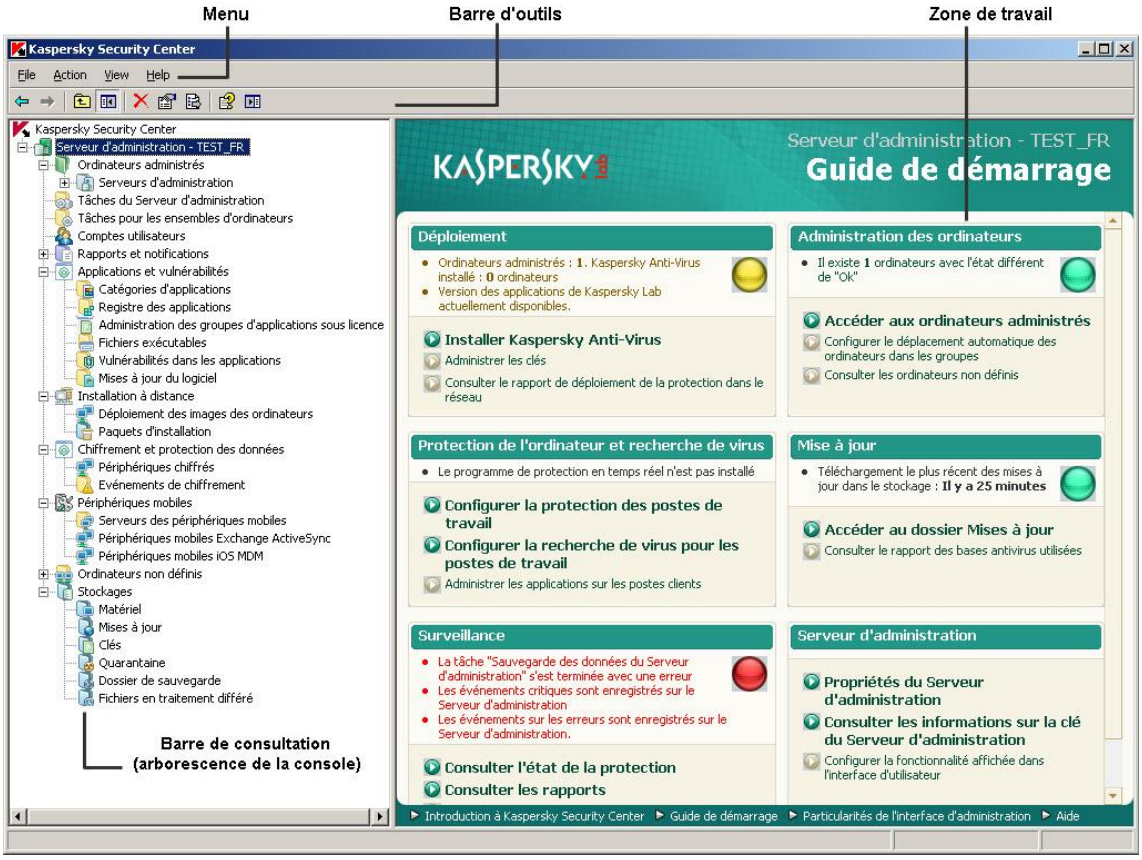

Illustration 1. Fenêtre principale de Kaspersky Security Center

LANCEMENT DE L'APPLICATION

Cette section décrit le lancement de l'application Kaspersky Security Center.

Kaspersky Security Center est lancé automatiquement lors du lancement du Serveur d'administration.

- *Pour lancer la Console d'administration de l'application,*

  sélectionnez l'option **Kaspersky Security Center** du groupe de programme **Kaspersky Security Center** du menu standard **Démarrer** → **Applications**.

Ce groupe d'applications **Kaspersky Security Center** est créé sur les postes administrateurs pendant l'installation de la Console d'administration.

DEPLOIEMENT DU SYSTEME DE PROTECTION

Cette section décrit deux scénarios possibles de déploiement du système de protection du réseau de l'entreprise :

- le déploiement du système de protection à l'intérieur de l'entreprise ;
- le déploiement du système de protection du réseau de l'entreprise-cliente (lors de l'utilisation des versions SPE de l'application).

Si vous devez déployer le système de protection à l'intérieur de l'entreprise qui inclut les bureaux distants ne faisant pas partie du réseau de l'entreprise, vous pouvez utiliser le scénario de déploiement de la protection antivirus pour les prestataires de services.

Les actions qui font partie des scénarios cités de déploiement de la protection sont décrites en détails dans la section "Résolution des tâches types".

DANS CETTE SECTION

DEPLOIEMENT DE LA PROTECTION ANTIVIRUS A L'INTERIEUR DE L'ENTREPRISE

Afin de déployer le système de protection dans le réseau de l'entreprise, procédez comme suit :

1. Installez et configurez le Serveur d'administration et la Console d'administration (cf. section "Installation des modules de l'application Kaspersky Administration Kit" à la page 22).
2. Créez les groupes d'administration et y ajoutez les postes clients (cf. section "Création du groupe d'administration" à la page 22).
3. Installez à distance l'Agent d'administration et les applications nécessaires de Kaspersky Lab sur les postes clients sélectionnés (cf. section "Installation à distance de l'application" à la page 28).
4. Si besoin, mettez à jour les bases des applications de Kaspersky Lab sur les postes clients (cf. *Manuel de l'administrateur de Kaspersky Security Center*).
5. S'il faut, exécutez une configuration complémentaire des applications installées à l'aide des stratégies (cf. section "Configuration de la stratégie pour l'application" à la page 31) et à l'aide des paramètres locaux des applications (cf. section "Consultation et modifications des paramètres locaux de l'application" à la page 32).
6. Configurez les paramètres des notifications de l'administrateur sur les événements sur les périphériques clients (cf. section "Configuration des paramètres des notifications" à la page 32).
7. Vérifiez le fonctionnement des notifications sur les événements dans le fonctionnement du système de protection (cf. section "Analyse des mises à jour récupérées" à la page 30).

8. Consultez les rapports (cf. section "Création et consultation du rapport" à la page 33) et configurez l'envoi automatique des rapports nécessaires par courrier électronique (cf. section "Création d'une tâche de diffusion du rapport" à la page 34).

9. Configurez l'installation automatique des applications sur les nouveaux ordinateurs dans le réseau (cf. section "Configuration de l'installation automatique des applications" à la page 28).

Suite à ces actions, le système de protection sera déployé dans le réseau informatique de l'entreprise.

DEPLOIEMENT DE SYSTEME DE PROTECTION DU RESEAU DE L'ENTREPRISE-CLIENT

Afin de déployer le système de protection antivirus dans le réseau de l'entreprise cliente, procédez comme suit :

1. Installez le Serveur d'administration et la Console d'administration sur le poste de travail de l'administrateur (cf. section "Installation des modules de l'application Kaspersky Security Center" à la page 22).

2. Installez Kaspersky Security Center Web-Console sur le poste de travail de l'administrateur (cf. section "Installation de Kaspersky Security Center Web-Console" à la page 23).

3. Configurez le Serveur d'administration pour le fonctionnement avec Kaspersky Security Center Web-Console (cf. *Manuel d'implantation de Kaspersky Security Center*).

4. Créez et configurez le Serveur d'administration virtuel sous l'administration duquel le réseau de l'entreprise-client se trouve (cf. section "Création du Serveur d'administration virtuel" à la page 24).

5. Désignez et configurez l'agent de mises à jour dans le réseau de l'entreprise-client (cf. section "Désignation de l'agent de mises à jour. Configuration des paramètres de l'agent de mises à jour" à la page 24).

6. Configurez les paramètres du paquet d'installation de l'Agent d'administration que vous allez utiliser pour installer l'Agent d'administration sur les ordinateurs de l'entreprise-client (cf. section "Configuration du paquet d'installation de l'Agent d'administration" à la page 25).

7. Installez à distance l'Agent d'administration et les applications nécessaires de Kaspersky Lab sur les postes clients sélectionnés (cf. section "Installation à distance de l'application" à la page 28).

8. S'il faut, exécutez une configuration complémentaire des applications installées à l'aide des stratégies (cf. section "Configuration de la stratégie pour l'application" à la page 31) et à l'aide des paramètres locaux des applications (cf. section "Consultation et modifications des paramètres locaux de l'application" à la page 32).

Une fois actions exécutée, le système de protection sera déployé dans le réseau de l'entreprise cliente.

RESOLUTION DES PROBLEMES TYPES

La section décrit les opérations principales que vous pouvez exécuter à l'aide de Kaspersky Security Center.

DANS CETTE SECTION

INSTALLATION DES MODULES DE L'APPLICATION KASPERSKY SECURITY CENTER

Pour installer le Serveur d'administration et la Console d'administration, procédez comme suit :

1. Sélectionnez l'ordinateur sur lequel seront installés le Serveur et la Console d'administration. Il est recommandé d'installer ces modules sur l'ordinateur, qui fait partie du domaine.

   Le Serveur d'administration et la Console Kaspersky Security Center 10.0 peuvent être installés sur le même ordinateur sur lequel fonctionnent le Serveur d'administration et la Console version 9.0.

   Il est recommandé d'effectuer l'installation avec les droits d'administrateur du domaine. Cela permettra de créer automatiquement les groupes des utilisateurs **KLAdmins** et **KLOperators** et d'accorder les privilèges nécessaires du compte sous lequel le Serveur d'administration fonctionnera.

2. Lancez le fichier exécutable setup.exe et suivez les consignes de l'Assistant d'installation.

3. Sélectionnez le type d'installation standard. Dans ce cas, la plupart des paramètres sont définis automatiquement.

   L'installation personnalisée est décrite en détail dans le *Manuel d'implantation de Kaspersky Security Center*.

   Ensuite, les applications nécessaires seront installées sur l'ordinateur si elles n'étaient pas installées auparavant :

   - Microsoft Windows Installer version 3.1 ;
   - Microsoft Data Access Components (MDAC) version 2.8 ;
   - Microsoft .NET Framework 2.0 ;
   - Microsoft SQL Server® 2008 R2 Express Edition.

   Les applications installées ne demandent aucun service ni aucune administration.

A l'étape suivante de l'Assistant, la copie des fichiers d'installation est commencée, et la base de données créée, où le Serveur d'administration sauvegarde de façon centralisée les informations sur la protection antivirus du réseau.

A la fin de l'Assistant d'installation, vous pouvez lancer immédiatement la Console d'administration et exécuter la configuration initiale des paramètres de l'application à l'aide de l'Assistant de configuration initiale.

CREATION DES GROUPES D'ADMINISTRATION

La hiérarchie des groupes d'administration se forme dans la fenêtre principale de l'application Kaspersky Security Center dans le dossier **Ordinateurs administrés**. Les groupes d'administration s'affichent sous forme de dossiers dans l'arborescence de la console (cf. ill. ci-après).

Juste après l'installation de Kaspersky Security Center, le groupe **Ordinateurs administrés** contient uniquement le dossier vide **Serveurs d'administration**.

La présence ou l'absence du dossier **Serveurs d'administration** dans l'arborescence de la console est définie par les paramètres de l'interface utilisateur. Pour inclure l'affichage de ce dossier, il faut passer dans le menu **Vue** → **Configuration de l'interface** et dans la fenêtre ouverte **Configuration de l'interface**, cocher la case **Afficher les serveurs d'administration secondaires**.

Lors de la création d'une hiérarchie de groupes d'administration, des postes clients, des machines virtuelles et des sous-groupes peuvent être ajoutés au dossier **Ordinateurs administrés**. Le dossier **Serveurs d'administration** permet d'ajouter des Serveurs d'administration secondaires.

Chaque groupe créé, tel que le groupe **Ordinateurs administrés**, contient d'abord uniquement le dossier vide **Serveurs d'administration** pour le fonctionnement avec les Serveurs d'administration secondaires de ce groupe. Les informations sur les stratégies, les tâches de ce groupe, ainsi que les périphériques compris dans ce groupe s'affichent sur les onglets correspondants dans la zone de travail de ce groupe.

Illustration 2. Consultation des hiérarchies des groupes d'administration

Pour créer un groupe d'administration, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Ordinateurs administrés**.
2. Si vous voulez créer un sous-groupe du groupe d'administration existant, dans le dossier **Ordinateurs administrés**, sélectionnez le sous-dossier correspondant au groupe auquel le nouveau groupe d'administration doit appartenir.

   Si vous créez un nouveau groupe d'administration de niveau supérieur de la hiérarchie, vous pouvez ignorer cette étape.
3. Lancez le processus de création du groupe d'administration par l'un des moyens suivants :
   - à l'aide de la commande du menu contextuel **Créer** → **Groupe** ;
   - à l'aide du lien **Créer un sous-groupe** situé dans la zone de travail de la fenêtre principale de l'application sous l'onglet **Groupes**.
4. Dans la fenêtre **Nom de groupe** qui s'ouvre, saisissez le nom du groupe et cliquez sur le bouton **OK**.

L'arborescence de la console affichera un nouveau dossier de groupe d'administration avec le nom saisi.

INSTALLATION DE KASPERSKY SECURITY CENTER WEB-CONSOLE

Pour Installer Kaspersky Security Center Web-Console sur le poste de travail de l'administrateur,

lancez le fichier exécutable setup.exe qui fait partie du distributif de Kaspersky Security Center Web-Console.

L'Assistant d'installation de Kaspersky Security Center Web-Console se lance. Cet Assistant vous proposera de configurer les paramètres d'installation. Suivez les instructions de l'Assistant.

CREATION D'UN SERVEUR D'ADMINISTRATION VIRTUEL

Pour ajouter un Serveur d'administration virtuel dans le groupe d'administration sélectionné, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier du groupe d'administration, sélectionnez l'entrée **Serveurs d'administration**.

2. Lancez le processus de création du Serveur d'administration virtuel par l'un des moyens suivants :

   - dans le menu contextuel de l'entrée **Serveurs d'administration**, sélectionnez l'option **Créer** → **Serveur d'administration virtuel**.

   - à l'aide du lien **Ajouter un Serveur d'administration virtuel** dans la zone de travail.

L'Assistant de création du Serveur d'administration virtuel s'ouvre. Suivez les instructions de l'Assistant.

DESIGNATION DE L'AGENT DE MISE A JOUR. CONFIGURATION DES PARAMETRES DE L'AGENT DE MISE A JOUR

Pour désigner un ordinateur en tant qu'agent de mise à jour de l'entreprise cliente, procédez comme suit :

1. Créez le paquet autonome d'installation de l'Agent d'administration. Procédez comme suit :

   a. Dans l'arborescence de la console, sélectionnez le Serveur d'administration virtuel sous l'administration duquel se trouve le réseau de l'entreprise-cliente.

   b. Dans le dossier **Installation à distance** du Serveur d'administration virtuel, sélectionnez le sous-dossier **Paquets d'installation**.

   c. Dans la zone de travail du dossier, sélectionnez ou créez le paquet d'installation de l'Agent d'administration.

   d. Ouvrez la fenêtre des propriétés du paquet d'installation de l'Agent d'administration.

   e. Dans la section **Connexion** dans la ligne **Adresse du serveur**, vérifiez l'adresse du Serveur d'administration virtuel. L'adresse doit être indiquée au format suivant : <Adresse du Serveur d'administration principal>/<Nom du Serveur d'administration virtuel>.

   f. Lancez le processus de création du paquet d'installation autonome pour ce paquet d'installation à l'aide d'un des moyens suivants :

      - dans le menu contextuel du paquet d'installation, sélectionnez l'option **Créer un paquet d'installation autonome** ;

      - à l'aide du lien **Créer un paquet d'installation autonome** dans le groupe de travail avec le paquet d'installation sélectionné.

   g. Ouvrez la liste des paquets d'installation autonomes créés du paquet d'installation de l'Agent d'administration à l'aide d'un des moyens suivants :

      - dans la dernière fenêtre de l'Assistant de création du paquet autonome, cochez la case **Ouvrir la liste des paquets autonomes** ;

      - dans le menu contextuel du paquet d'installation, sélectionnez l'option **Afficher la liste des paquets autonomes**.

h. Dans la liste des paquets autonomes qui s'ouvre, sélectionnez le paquet autonome créé et indiquez le mode de livraison du paquet autonome à l'administrateur de l'entreprise-cliente.

2. Contactez l'administrateur de l'entreprise-cliente pour une installation locale de l'Agent d'administration sur le poste client sélectionné par l'agent de mise à jour.

   Après l'installation de l'Agent d'administration sur le poste client sélectionné par l'agent de mise à jour, cet ordinateur s'affiche dans le dossier **Ordinateurs administrés** du Serveur d'administration virtuel.

   Kaspersky Security Center désigne automatiquement cet ordinateur en tant qu'agent de mise à jour et le configure en tant que passerelle des connexions lors de la première connexion au Serveur d'administration.

   Si vous devez désigner un ordinateur en tant qu'agent de mise à jour manuellement, procédez comme suit :

   a. Ouvrez la fenêtre des propriétés du dossier **Ordinateurs administrés** du Serveur d'administration virtuel.

   b. Dans la section **Agents de mise à jour**, sélectionnez le poste client qui exécutera le rôle de l'agent de mise à jour, en cliquant sur le bouton **Ajouter**.

   c. Ouvrez la fenêtre des propriétés de l'agent de mise à jour et procédez comme suit :

      - Configurez les paramètres de sondage du réseau par l'agent de mise à jour dans la section **Sondage du réseau**.

      - Sélectionnez la section **Avancé** et cochez la case **Passerelle des connexions** pour utiliser l'agent de mise à jour en tant que passerelle des connexions dans le réseau de l'entreprise-cliente.

Finalement, le poste client sélectionné devient l'agent de mise à jour de l'entreprise-cliente et il est utilisé dans l'entreprise en tant que passerelle des connexions au Serveur d'administration virtuel.

Vous pouvez manuellement désigner l'ordinateur en tant qu'agent de mise à jour uniquement si la désignation automatique est désactivée (section **Paramètres** de la fenêtre des propriétés du Serveur d'administration virtuel).

CONFIGURATION DU PAQUET D'INSTALLATION DE L'AGENT D'ADMINISTRATION

Avant l'installation de l'Agent d'administration sur les ordinateurs de l'entreprise-cliente, il faut configurer les paramètres du paquet d'installation de l'Agent d'administration qui sera utilisé pour une installation à distance.

Pour configurer le paquet d'installation de l'Agent d'administration pour une installation sur les ordinateurs de l'entreprise-cliente, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration virtuel sous l'administration duquel se trouve le réseau de l'entreprise-cliente.

2. Dans le dossier **Installation à distance** du Serveur d'administration virtuel, sélectionnez le sous-dossier **Paquets d'installation**.

3. Dans la zone de travail, sélectionnez ou créer le paquet d'installation de l'Agent d'administration qui sera utilisé pour installer l'Agent d'administration sur les ordinateurs de l'entreprise-cliente.

4. Dans le menu contextuel du paquet d'installation, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du paquet d'installation de l'Agent d'administration s'ouvre.

5. Dans la fenêtre des propriétés, configurez les paramètres suivants du paquet d'installation :

   - Dans la section **Connexion**, dans la ligne **Adresse du serveur**, indiquez la même adresse du Serveur d'administration virtuel que lors d'une installation locale de l'Agent d'administration sur l'agent de mises à jour (cf. section "Désignation des agents de mises à jour. Configuration des paramètres de l'agent de mises à jour" à la page 24).

   - Dans la section **Avancé**, cochez la case **Se connecter au Serveur d'administration via la passerelle des connexions**. Dans la ligne **Adresse de la passerelle des connexions**, indiquez l'adresse de l'agent de mise à jour. Pour l'adresse de l'ordinateur, vous pouvez utiliser l'adresse IP ou le nom de l'ordinateur sur le réseau Windows.

6. Cliquez sur le bouton **OK**.

GESTION DES PERIPHERIQUES MOBILES

Kaspersky Security Center permet d'administrer les périphériques mobiles qui prennent en charge les protocoles Exchange ActiveSync et iOS Mobile Device Management (iOS MDM).

La collecte d'informations sur les périphériques mobiles et l'enregistrement de leurs profils est exécutée par les Serveurs des périphériques mobiles. Le *Serveur des périphériques mobiles* est un module de Kaspersky Security Center qui offre à l'administrateur l'accès aux périphériques mobiles et qui permet de les administrer via Console d'administration.

Il existe deux types des Serveurs des périphériques mobiles :

- Le Serveur des périphériques mobiles Exchange ActiveSync. Il est installer sur le poste client avec le serveur déjà installé Microsoft Exchange et permet de recevoir les données depuis le serveur Microsoft Exchange et de les transmettre sur le Serveur d'administration. Ce Serveur des périphériques mobiles est utilisé pour administrer les périphériques mobiles qui prennent en charge le protocole Exchange ActiveSync.

- Le Serveur des périphériques mobiles iOS MDM. S'installe sur le poste client et permet de connecter les périphériques mobiles iOS au Serveur d'administration et de les administrer à l'aide du service Apple Push Notifications (APNs).

Pour les périphériques mobiles Exchange ActiveSync, les fonctions suivantes sont disponibles :

- création et modification des profils d'administration des périphériques mobiles, attribution des profils aux boîtes aux lettres des utilisateurs ;

- configuration des paramètres de fonctionnement du périphérique mobile (synchronisation du courrier, mot de passe de l'utilisateur, chiffrement des données, connexion des disques amovibles) ;

- installation des certificats sur les périphériques mobiles.

Pour les périphériques mobiles iOS MDM, les fonctions suivantes sont disponibles :

- création et modification des profils de configuration, installation des profils de configuration sur les périphériques mobiles ;

- installation des applications sur le périphérique mobile via App Store ou à l'aide des fichiers-manifestes(.plist) ;

- possibilité de bloquer le périphérique mobile, de remettre à zéro le mot de passe du périphérique et de supprimer toutes les données sur le périphérique mobile.

Les informations détaillées sur la gestion des périphériques mobiles sont présentées dans le *Manuel de l'administrateur de Kaspersky Security Center*.

Ensuite, une brève description des actions à exécuter pour se connecter au Serveur d'administration des périphériques mobiles qui prennent en charge les protocoles Exchange ActiveSync et iOS Mobile Device Management (iOS MDM) est reprise.

CONNEXION DES PERIPHERIQUES MOBILES EXCHANGE ACTIVESYNC

- *Pour connecter les périphériques mobiles Exchange ActiveSync au Serveur d'administration, procédez comme suit :*

1. Installez le Serveur des périphériques mobiles Exchange ActiveSync sur le poste client avec le serveur installé Microsoft Exchange.

2. Créez le profil d'administration des périphériques mobiles Exchange ActiveSync.

3. Désignez les profils d'administration des périphériques mobiles Exchange ActiveSync aux boîtes aux lettres des utilisateurs.

   L'utilisateur du périphérique mobile connecte le périphérique mobile au serveur Microsoft Exchange et il reçoit une notification que sa boîte aux lettres se trouve sous l'administration d'un profil qui impose les restrictions sur le périphérique mobile connecté. Pour plus d'informations sur les actions de l'utilisateur du périphérique mobile Exchange ActiveSync, cf. *Manuel d'implantation de Kaspersky Endpoint Security 10 pour les périphériques mobiles*.

   Le périphérique mobile de l'utilisateur connecté au serveur Microsoft Exchange s'affiche dans le dossier **Périphériques mobiles Exchange ActiveSync** joint dans le dossier **Périphériques mobiles** de l'arborescence de la console.

Les informations détaillées sur la connexion des périphériques mobiles Exchange ActiveSync au Serveur d'administration sont décrites dans le *Manuel d'implantation de Kaspersky Security Center*.

L'administrateur peut gérer les périphériques mobiles Exchange ActiveSync connectés au Serveur d'administration. Les informations sur l'administration des périphériques mobiles Exchange ActiveSync sont présentées dans le *Manuel de l'administrateur de Kaspersky Security Center*.

CONNEXION DES PERIPHERIQUES MOBILES IOS MDM

- *Pour connecter les périphériques mobiles iOS MDM au Serveur d'administration, procédez comme suit :*

1. Installez sur le poste client sélectionné le Serveur des périphériques mobiles iOS MDM qui fait partie des paquets d'installation du Serveur d'administration par défaut.

2. Installez le certificat Apple Push Notification Service (APNs) sur le Serveur d'administration.

3. Configurez la connexion des périphériques mobiles au Serveur des périphériques mobiles iOS MDM.

4. Envoyez aux utilisateurs des périphériques mobiles iOS le lien pour télécharger le profil iOS MDM.

   Les utilisateurs des périphériques mobiles reçoivent une notification avec le lien pour télécharger le profil iOS MDM du portail Internet et exécutent d'une façon indépendante l'installation du profil iOS MDM sur le périphérique mobile.

Le périphérique mobile se connecte au Serveur des périphériques mobiles iOS MDM. Les périphériques mobiles connectés iOS MDM s'affichent dans le dossier **Périphériques mobiles iOS MDM** joint dans le dossier **Périphériques mobiles** de l'arborescence de la console.

Les informations détaillées sur la connexion des périphériques mobiles iOS MDM au Serveur d'administration sont décrites dans le *Manuel d'implantation de Kaspersky Security Center*.

Après la connexion du périphérique mobile iOS MDM au Serveur d'administration, il est possible d'installer le profil de configuration et le profil provisioning sur le périphérique mobile iOS MDM. Les informations détaillées sur l'installation du profil de configuration et du profil provisioning sont décrites dans le *Manuel d'implantation de Kaspersky Security Center.*

L'administrateur peut gérer les périphériques mobiles iOS MDM connectés au Serveur d'administration. Les informations sur l'administration des périphériques mobiles iOS MDM sont présentées dans le *Manuel de l'administrateur Kaspersky Security Center*.

INSTALLATION A DISTANCE DE L'APPLICATION

Certaines applications de Kaspersky Lab dont l'administration est accessible via Kaspersky Security Center, ne peuvent être installées sur les postes clients que localement (cf. Manuels des applications de Kaspersky Lab).

Pour effectuer l'installation à distance de l'application sur les postes clients, procédez comme suit :

1. Dans l'arborescence de la console, accédez à l'entrée du Serveur d'administration sous l'administration duquel se trouvent les postes clients se trouvent.

2. Dans l'arborescence de la console dans le dossier **Installation à distance** à l'aide du lien **Exécuter l'Assistant d'installation à distance**, lancez l'Assistant d'installation à distance.

3. Dans la fenêtre de l'Assistant **Sélection du paquet d'installation**, indiquez le paquet d'installation de l'application que vous voulez installer.

4. Suivez les instructions de l'Assistant.

Une fois l'Assistant terminé, la tâche d'installation à distance de l'application sur les postes clients est créée. L'Assistant d'installation à distance crée et lance la tâche d'installation à distance de l'application sélectionnée. Selon l'ensemble de périphériques ou du groupe d'administration sélectionné, la tâche créée est placée dans le dossier **Tâches pour les ensembles d'ordinateurs** ou dans la zone de travail du groupe d'administration sélectionné, sous l'onglet **Tâches**.

Une fois la tâche créée, l'application sera installée sur les postes clients sélectionnés.

Vous pouvez utiliser le mode indiqué ci-dessus pour installer l'application antivirus sur les postes clients. Les informations sur l'installation de l'application antivirus sur les postes clients du groupe d'administration sont à consulter sous l'onglet **Ordinateurs** dans la zone de travail du groupe. Les informations sur l'installation de l'application sur l'ensemble des postes clients peuvent être consultées dans la zone de travail du dossier **Ordinateurs non définis**. Dans la liste des ordinateurs sous l'onglet **Ordinateurs** et dans la zone de travail du dossier **Ordinateurs non définis** dans la colonne **Agent/Antivirus**, les informations sur l'installation des ordinateurs de l'Agent d'administration et de l'application antivirus s'affichent. Si la colonne possède le signe plus (+) après une barre oblique inverse, l'application antivirus a été installée avec succès.

CONFIGURATION DE L'INSTALLATION AUTOMATIQUE DES APPLICATIONS

Afin de configurer l'installation automatique des applications sur les nouveaux périphériques dans le groupe d'administration, procédez comme suit :

1. Sélectionnez le groupe d'administration nécessaire dans l'arborescence de la console.

2. Ouvrez la fenêtre des propriétés de ce groupe d'administration.

3. Dans la section **Installation automatique**, sélectionnez les paquets d'installation qui doivent être installés sur des nouveaux périphériques en cochant les cases à côté des noms de paquets d'installation des applications nécessaires. Cliquez sur le bouton **OK**.

Les tâches de groupe sont créées. Elles seront lancées sur les postes clients juste après avoir été ajoutées au groupe d'administration.

Si plusieurs paquets d'installation d'une seule application sont indiqués pour une installation automatique, la tâche d'installation sera uniquement créée pour la dernière version de l'application.

CREATION D'UNE TACHE DE TELECHARGEMENT DES MISES A JOUR DANS LE STOCKAGE

La tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration est créée automatiquement lors du fonctionnement de l'Assistant de configuration initiale de Kaspersky Security Center. La tâche de téléchargement des mises à jour dans le stockage peut être créée dans un exemplaire unique. Par conséquent, vous pouvez créer une tâche de téléchargement des mises à jour dans le stockage uniquement dans le cas si elle a été supprimée de la liste des tâches du Serveur d'administration.

Pour créer une tâche de téléchargement des mises à jour dans le stockage, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches du Serveur d'administration**.

2. Lancez le processus de création de la tâche par un des moyens suivants :

   - Dans le menu contextuel du dossier de l'arborescence de la console **Tâches du Serveur d'administration**, sélectionnez l'option **Créer** → **Tâche**.

   - A l'aide du lien **Création d'une tâche** dans la zone de travail.

   Ceci permet de lancer l'assistant de création de tâche. Suivez les instructions de l'Assistant. Dans la fenêtre de l'Assistant **Type de tâche**, sélectionnez le type de tâche **Téléchargement des mises à jour dans le stockage**.

Après la fin de fonctionnement de l'Assistant, la tâche créée **Téléchargement des mises à jour dans le stockage** apparaît dans la liste des tâches du Serveur d'administration.

Suite à l'exécution de la tâche **Téléchargement des mises à jour dans le référentiel**, les mises à jour des bases et des modules des applications sont copiées depuis la source définie vers le dossier partagé.

Les mises à jour du dossier partagé sont diffusées sur les postes clients et les Serveurs d'administration secondaires.

Les ressources suivantes peuvent faire office de source des mises à jour pour le Serveur d'administration :

- Les Serveurs de mises à jour Kaspersky Lab sont les serveurs Kaspersky Lab où sont déposés les mises à jour de la base antivirus et des modules de programmes.

- Serveur d'administration principal.

- Le serveur FTP/HTTP ou le dossier de réseau des mises à jour – le serveur FTP, HTTP, le dossier local ou de réseau ajouté par l'utilisateur et contenant les mises à jour actuelles. Lors de la sélection du dossier local, il faut indiquer le dossier sur l'ordinateur avec le Serveur d'administration installé.

  Pour actualiser le Serveur d'administration à partir du serveur FTP/HTTP ou à partir du dossier local, il faut copier sur ces ressources la structure valide des dossiers avec les mises à jour, qui coïncide avec la structure formée lors de l'utilisation des serveurs de mise à jour de Kaspersky Lab.

La sélection de la ressource dépend des paramètres de la tâche. L'option par défaut télécharge les mises à jour depuis les serveurs de mise à jour Kaspersky Lab par Internet.

ANALYSE DES MISES A JOUR RECUPEREES

Pour que Kaspersky Security Center analyse les mises à jour reçues avant des les diffuser sur les postes clients, procédez comme suit :

1. Dans la zone de travail du dossier **Tâches du Serveur d'administration** de l'arborescence de la console, sélectionnez la tâche **Téléchargement des mises à jour dans le stockage** dans la liste des tâches.

2. Ouvrez la fenêtre des propriétés de la tâche à l'aide d'un des moyens suivants :

   - Dans le menu contextuel de la tâche, sélectionnez l'option **Propriétés**.

   - A l'aide du lien **Modifier les paramètres de la tâche** dans la zone de travail de la tâche sélectionnée.

3. Dans la fenêtre des propriétés de la tâche qui s'ouvre, dans la section **Vérification des mises à jour**, cochez la case **Vérifier les mises à jour avant de les déployer** et sélectionnez la tâche de vérification des mises à jour à l'aide d'un des moyens suivants :

   - Cliquez sur le bouton **Sélectionner** pour sélectionner une tâche de vérification des mises à jour déjà créée.

   - Cliquez sur le bouton **Créer** pour créer une tâche de vérification des mises à jour.

     L'Assistant de création d'une tâche de vérification des mises à jour s'ouvre. Suivez les instructions de l'Assistant.

     Durant le processus de création de la tâche de vérification des mises à jour, il faut sélectionner un groupe d'administration dont la tâche sera exécutée sur les ordinateurs. Les ordinateurs de ce groupe sont appelés les *ordinateurs d'essai*.

     Pour les ordinateurs d'essai, il est recommandé d'utiliser des ordinateurs bien protégés avec la configuration logicielle la plus répandue dans le réseau de l'entreprise. La qualité de la vérification sera ainsi accrue, le risque de faux-positifs ainsi que la probabilité d'identifier des virus lors de la vérification seront réduits (en cas de détection de virus sur les ordinateurs d'essai, la tâche de vérification des mises à jour est considérée comme manquée).

4. Fermez la fenêtre des propriétés de la tâche de téléchargement des mises à jour dans le stockage, en cliquant sur le bouton **OK**.

Dans le cadre de l'exécution de la tâche de téléchargement des mises à jour dans le stockage, la tâche de vérification des mises à jour reçues sera exécutée. Le Serveur d'administration va copier les mises à jour depuis la source, va les placer dans un dossier temporaire et va lancer la tâche de vérification des mises à jour. Si l'exécution de cette tâche réussit, les mises à jour seront copiées depuis le dossier temporaire vers le dossier partagé du Serveur d'administration (<Dossier d'installation Kaspersky Security Center>\Share\Updates), puis seront diffusées vers les postes clients pour lesquels le Serveur d'administration est une source de mise à jour.

Si, à la fin de la tâche de vérification des mises à jour placées dans le dossier temporaire, les mises à jour sont considérées comme incorrectes ou si la tâche se solde sur une erreur, la copie des mises à jour dans le dossier partagé n'a pas lieu et la version précédente des mises à jour est conservée sur le Serveur d'administration. Les tâches dont la programmation est **Lors du téléchargement des mises à jour dans le stockage** ne sont pas lancées. Ces opérations sont réalisées à l'exécution suivante de la tâche de téléchargement des mises à jour dans le stockage si la vérification du nouvel ensemble des mises à jour réussit.

L'ensemble de mises à jour est considéré comme incorrect si sur au moins un ordinateur d'essai une des conditions suivantes est remplie :

- une erreur s'est produite pendant l'exécution de la tâche de mise à jour ;

- après l'application des mises à jour, l'état de la protection en temps réel de l'application antivirus est modifié ;

- un objet infecté a été identifié durant l'analyse à la demande ;

- une erreur de l'application de Kaspersky Lab s'est produite.

Si aucune des conditions citées n'est remplie sur aucun des ordinateurs d'essai, alors les mises à jour sont considérées comme correctes et la tâche de vérification des mises à jour a réussi.

DEPLOIEMENT AUTOMATIQUE DES MISES A JOUR SUR LES POSTES CLIENTS

- *Pour que les mises à jour de l'application sélectionnée se diffusent automatiquement sur les postes clients tout de suite après le téléchargement des mises à jour dans le stockage du Serveur d'administration, procédez comme suit :*

1. Connectez-vous au Serveur d'administration, qui gère les postes clients.

2. Créez une tâche de diffusion des mises à jour de cette application pour les postes clients sélectionnées par un des moyens suivants :

   - S'il faut diffuser les mises à jour sur les postes clients qui font partie du groupe d'administration sélectionné, créer une tâche pour le groupe sélectionné.

   - S'il faut diffuser les mises à jour sur les postes clients qui font partie des différents groupes d'administration ou non, créez une tâche pour l'ensemble d'ordinateurs.

   Ceci permet de lancer l'Assistant de création de tâche. Suivez ses instructions, exécutant les conditions suivantes :

   a. Dans la fenêtre de l'Assistant **Type de tâche** dans l'entrée de l'application nécessaire, sélectionnez la tâche de diffusion des mises à jour.

   > Le nom de la tâche de diffusion des mises à jour, qui s'affiche dans la fenêtre **Type de tâche**, dépende de l'application pour lequel la tâche a été créée. Pour plus d'informations sur les noms des tâches de mise à jour pour les applications sélectionnées de Kaspersky Lab, cf. Manuels pour ces applications.

   b. Dans la fenêtre de l'Assistant **Planification** dans le champ **Planification**, sélectionnez l'option de lancement **Lors du téléchargement des mises à jour dans le stockage**.

Finalement, la tâche créée de diffusion des mises à jour sera lancée pour les ordinateurs sélectionnés chaque fois lors du téléchargement des mises à jour dans le stockage du Serveur d'administration.

Si la tâche de diffusion des mises à jour de l'application nécessaire a déjà été créée pour les ordinateurs sélectionnés, pour une diffusion automatique des mises à jour sur les postes clients dans la fenêtre des propriétés de la tâche dans la section **Planification**, il faut sélectionner l'option de lancement **Lors du téléchargement des mises à jour dans le stockage** dans le champ **Planification pour**.

CONFIGURATION DE LA STRATEGIE POUR L'APPLICATION

- *Afin de configurer la stratégie pour l'application, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut configurer une stratégie.

2. Dans la zone de travail du groupe sous l'onglet **Stratégies**, sélectionnez la stratégie de l'application nécessaire.

3. Ouvrez la fenêtre des propriétés de la stratégie et configurez la stratégie.

Une fois les modifications apportées enregistrées, la stratégie sera appliquée sur les ordinateurs du groupe d'administration avec les paramètres modifiés.

CONSULTATION ET MODIFICATION DES PARAMETRES LOCAUX DE L'APPLICATION

Le système d'administration Kaspersky Security Center permet d'administrer à distance les paramètres locaux des applications sur les postes clients via la Console d'administration.

Les *Paramètres locaux des applications* sont les paramètres de l'application individuels pour chaque poste client. A l'aide de Kaspersky Security Center, vous pouvez installer les paramètres locaux des applications pour les postes clients inclus dans le groupe d'administration.

Les descriptions détaillées des paramètres des applications Kaspersky Lab sont présentées dans les documentations respectives.

Pour consulter ou modifier les paramètres locaux de l'application, procédez comme suit :

1. Dans la zone de travail du groupe dans lequel se trouve le poste client nécessaire, sélectionnez l'onglet **Ordinateurs**.
2. Dans la fenêtre des propriétés du poste client dans la section **Applications**, sélectionnez l'application nécessaire.
3. Ouvrez la fenêtre des propriétés de l'application en double cliquant sur le nom de l'application ou à l'aide du bouton **Propriétés**.

La fenêtre des paramètres locaux de l'application sélectionnée s'ouvre. Il est possible de consulter et de modifier ces paramètres.

Vous pouvez modifier les valeurs des paramètres dont la modification n'est pas interdite par la stratégie de groupe (le paramètre n'est pas verrouillé dans la stratégie).

CONFIGURATION DES PARAMETRES DE NOTIFICATIONS

Kaspersky Security Center offre la possibilité de configurer les paramètres de notification de l'administrateur pour les événements survenus sur les postes clients et de sélectionner le mode de notification :

- courrier électronique ;
- SMS ;
- fichier exécutable.

Pour configurer les paramètres de notifications sur les événements survenus sur les postes clients, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez la fenêtre des propriétés du dossier **Rapports et notifications** à l'aide d'un des moyens suivants :
   - Dans le menu contextuel du dossier de l'arborescence de la console **Rapports et notifications**, sélectionnez l'option **Propriétés**.
   - Dans la zone de travail du dossier **Rapports et notifications** sous l'onglet **Notifications**, ouvrez la fenêtre à l'aide du lien **Modifier les paramètres d'envoi des notifications**.
2. Dans la section **Notification** de la fenêtre des propriétés du dossier **Rapports et notifications**, configurez les paramètres de notifications pour les événements.

Les paramètres configurés de notification sont diffusés sur tous les événements survenus sur les postes clients.

Vous pouvez configurer les paramètres de notification pour l'événement dans la fenêtre des propriétés de cet événement. L'accès rapide aux paramètres d'événements s'effectue à l'aide des liens **Modifier les paramètres des événements de Kaspersky Endpoint Security** et **Modifier les paramètres des événements du Serveur d'administration**.

VERIFICATION DE DEPLOIEMENT DES NOTIFICATIONS

Pour vérifier le déploiement des notifications sur les événements, la notification sur la détection du virus d'essai Eicar sur les postes clients est utilisée.

Pour vérifier le déploiement des notifications sur les événements, procédez comme suit :

1. Arrêter la tâche de PTR du système de fichier sur le poste client et copier le "virus" d'essai Eicar sur le poste client. Activer de nouveau la tâche de PTR du système de fichier.

2. Lancez la tâche d'analyse des postes clients pour le groupe d'administration ou pour l'ensemble d'ordinateurs incluant le poste client avec le "virus" Eicar.

   Si la tâche d'analyse est configurée correctement, le "virus" d'essai sera détecté lors de l'exécution de l'analyse. Si les paramètres de notifications sont configurés correctement, vous recevrez la notification sur le virus détecté.

   Dans le dossier de l'arborescence de la console **Rapports et notifications** dans le sous-dossier **Evénements** dans la sélection **Derniers événements**, l'enregistrement relative à la détection d'un "virus" s'affichera.

Le "virus" d'essai Eicar N'EST PAS UN VIRUS et ne contient pas du code pouvant nuire à votre ordinateur. Avec cela la plupart des applications des compagnies-fabricants d'antivirus l'identifie comme un virus. Vous pouvez télécharger le "virus" d'essai sur le site Web officiel de la société EICAR.

GENERATION ET AFFICHAGE DES RAPPORTS

Pour former et consulter le rapport, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Rapports et notifications** qui reprend la liste des modèles de rapports.

2. Sélectionnez le modèle du rapport, qui vous intéresse, dans l'arborescence de la console ou dans la zone de travail sous l'onglet **Rapports**.

   Finalement, la zone de travail affiche le rapport formé selon le modèle sélectionné.

Le rapport affiche les données suivantes :

- le type et le nom du rapport, une brève description et la période couverte, ainsi que les informations sur la création d'un rapport créée pour un groupe de périphériques ;
- diagramme illustrant les données générales du rapport ;
- tableau récapitulatif avec les données illustrant les indices calculés ;
- tableau avec les données détaillées.

ENREGISTREMENT DU RAPPORT

Afin de sauvegarder un rapport formé, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Rapports et notifications** qui reprend la liste des modèles de rapports.
2. Sélectionnez le modèle du rapport, qui vous intéresse, dans l'arborescence de la console ou dans la zone de travail sous l'onglet **Rapports**.
3. Dans le menu contextuel du modèle sélectionné du rapport, sélectionnez l'option **Enregistrer**.

L'Assistant d'enregistrement du rapport se lance. Suivez les instructions de l'Assistant.

Après la fin de fonctionnement de l'Assistant, le dossier avec le fichier du rapport enregistré s'ouvre.

CREATION D'UNE TACHE D'ENVOI DU RAPPORT

La diffusion des rapports dans l'application Kaspersky Security Center s'effectue à l'aide de la tâche de diffusion du rapport. Les rapports peuvent être diffusés par courrier électronique ou enregistrés dans le dossier sélectionné, par exemple, dans le dossier partagé sur le Serveur d'administration ou sur l'ordinateur local.

Pour créer une tâche de diffusion d'un rapport, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Rapports et notifications** qui reprend la liste des modèles de rapports.
2. Sélectionnez le modèle du rapport, qui vous intéresse, dans l'arborescence de la console ou dans la zone de travail sous l'onglet **Rapports**.
3. Dans le menu contextuel du modèle du rapport, sélectionnez l'option **Envoi des rapports**.

Finalement, l'Assistant de création de la tâche de diffusion du rapport sélectionné se lance. Suivez les instructions de l'Assistant.

Pour créer une tâche de diffusion de plusieurs rapports, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches du Serveur d'administration**.
2. Lancez le processus de création de la tâche par un des moyens suivants :
   - Dans le menu contextuel du dossier de l'arborescence de la console **Tâches du Serveur d'administration**, sélectionnez l'option **Créer** → **Tâche**.
   - A l'aide du lien **Création d'une tâche** dans la zone de travail.

Finalement, l'Assistant de création d'une tâche du Serveur d'administration se lance. Suivez les instructions de l'Assistant. Dans la fenêtre de l'Assistant **Type de tâche**, sélectionnez le type de tâche **Envoi du rapport**.

La tâche créée de diffusion du rapport s'affiche dans le dossier de l'arborescence de la console **Tâches du Serveur d'administration**.

La tâche de diffusion du rapport est créée automatiquement dans le cas, si les paramètres du courrier électronique ont été spécifiés lors de l'installation de Kaspersky Security Center.

AFFICHAGE DU RAPPORT SUR LES VIRUS DETECTES

Pour consulter le rapport sur les virus détectés, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Rapports et notifications**.
2. Dans la zone de travail du dossier sous l'onglet **Statistiques**, sélectionnez la page **Statistiques antivirus**.

Les barres d'informations de cette page affichent par défaut les données suivantes pour les dernières vingt-quatre heures :

- historique de l'activité virale ;
- virus les plus répandus dans le réseau ;
- ordinateurs les plus infectés ;
- utilisateurs les plus infectés.

Dans le dossier de l'arborescence de la console **Rapports et notifications**, vous pouvez aussi consulter le rapport détaillé sur les virus, détectés dans le réseau, sous l'onglet **Rapports**. Cet onglet du groupe **Statistiques antivirus** vous permet d'accéder aux rapports détaillés à l'aide des liens suivants :

- **Rapport de virus**.
- **Rapport sur les ordinateurs les plus infectés**.
- **Rapport sur les utilisateurs des ordinateurs infectés**.

Une fois le rapport nécessaire sélectionné, la zone de travail affiche les informations détaillées sur les virus détectés. Ces informations sont récoltées dès l'installation du Serveur d'administration.

Vous pouvez modifier les paramètres de n'importe quel rapport : par exemple, la période couverte par le rapport ou l'ensemble de champs affichés dans le rapport (cf. *Manuel de l'administrateur de Kaspersky Security Center*).

AFFICHAGE DES INFORMATIONS SUR LES EVENEMENTS

Pour afficher les informations sur les événements survenus pendant le fonctionnement de l'application, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Evénements**.
2. Ouvrez une sélection d'événements par l'un des moyens suivants :
   - Dans l'arborescence de la console, ouvrez le dossier **Evénements** et sélectionnez le dossier avec la sélection d'événements nécessaire.
   - Dans la zone de travail du dossier **Evénements**, dans le groupe **Sélections prédéfinies**, à l'aide du lien correspondant au nom de la sélection d'événements nécessaires.

   La zone de travail reprend la liste des événements du type sélectionné enregistrés sur le Serveur d'administration.

Vous pouvez former votre propre sélection d'événements (cf. *Manuel de l'administrateur de Kaspersky Security Center*).

AFFICHAGE DE L'ETAT EN COURS DE LA PROTECTION ANTIVIRUS

Vous pouvez surveiller l'état du système de protection des postes clients et des périphériques sous l'administration du Serveur d'administration **<Nom du serveur>** dans la zone de travail de l'entrée **<Nom du serveur>**. Les groupes d'administration de la zone de travail affichent les informations générales sur l'état des zones suivantes du fonctionnement de l'application :

- déploiement de la protection dans le réseau (groupe **Déploiement**) ;
- formation de la structure des groupes d'administration contenant les ordinateurs administrés (groupe **Administration des ordinateurs**) ;
- fonctionnement de la protection sur les postes clients (groupe **Protection de l'ordinateur et recherche des virus**) ;
- mise à jour des bases et des modules des applications (groupe **Mise à jour**) ;
- surveillance et fonctionnement des mises à jour (groupe **Surveillance**).

Vous pouvez évaluer l'état du système de protection antivirus à l'aide des icônes des signaux lumineux situés dans les groupes d'administration. Si l'icône est verte, les tâches nécessaires dans cette zone sont accomplies. Si l'icône est jaune ou rouge, vous devez faire attention à cette zone et exécuter les actions requises le cas échéant.

En dehors de l'indicateur coloré, chaque groupe contient une brève description de l'état du système de protection ou du problème survenu ainsi que des liens vous permettant d'exécuter les tâches principales du groupe.

Pour de plus amples informations sur l'état du système de protection, consultez le dossier **Rapports et notifications**.

CREATION D'UNE COPIE DE SAUVEGARDE DES DONNEES DU SERVEUR D'ADMINISTRATION

L'Assistant de configuration initiale de Kaspersky Security Center forme la tâche de création d'une copie de sauvegarde des données du Serveur d'administration. Par défaut, la copie de sauvegarde est créée quotidiennement sur l'ordinateur avec le Serveur d'administration dans le dossier d'installation de l'application dans le sous-dossier Backup.

Pour lancer manuellement la formation d'une sauvegarde des données du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches du Serveur d'administration**.
2. La zone de travail du dossier permet de sélectionner la tâche de création d'une sauvegarde des données du Serveur d'administration (par défaut, la tâche est **Sauvegarde des données du Serveur d'administration**).
3. Lancez la tâche sélectionnée.

Puisque les serveurs d'administration virtuels utilisent la base de données du Serveur d'administration principal, la copie de sauvegarde et la restauration des données du Serveur d'administration virtuel sont effectuées uniquement dans le cadre de la copie de sauvegarde et de la restauration des données du Serveur principal.

PASSAGE DE LA VERSION KASPERSKY SECURITY CENTER 9.0 A LA VERSION KASPERSKY SECURITY CENTER 10.0

Cette section décrit la procédure de passage de la version Kaspersky Security Center 9.0 à la version Kaspersky Security Center 10.0, ainsi que les actions principales relatives à la configuration initiale de l'application dans la nouvelle version.

Pour passer de version Kaspersky Security Center 9.0 à la version Kaspersky Security Center 10.0, procédez comme suit :

1. Pour Kaspersky Security Center 9.0, créez une copie de sauvegarde des données du Serveur d'administration à l'aide de l'utilitaire *klbackup*. Cet utilitaire fait partie du distributif de l'application et se trouve dans la racine du dossier d'installation Kaspersky Security Center.

2. Installez le Serveur d'administration et la Console d'administration version 10.0.

   Vous pouvez installer le Serveur d'administration sur l'ordinateur où la version précédente du Serveur d'administration est installée. Lors de la mise à jour jusqu'à la version 10.0, les données et les paramètres de la version précédente du Serveur d'administration sont enregistrés.

   Si vous installez le Serveur d'administration sur un autre ordinateur, vous pouvez restaurer les paramètres de la version précédente du Serveur d'administration à l'aide de l'utilitaire de sauvegarde et de restauration des données (*klbackup*).

3. Effectuez la configuration initiale du Serveur d'administration si les paramètres n'ont pas été transférés depuis la version précédente du Serveur d'administration.

4. Formez la structure des groupes d'administration.

5. Sélectionnez les postes clients sur lesquels seront installées la nouvelle version de l'Agent d'administration et les nouvelles versions des applications de Kaspersky Lab.

6. Pour les ordinateurs sélectionnés, créez la tâche d'installation à distance de la nouvelle version de l'Agent d'administration et des nouvelles versions des applications de Kaspersky Lab. Pour une installation à distance des applications, vous pouvez utiliser les paquets d'installation formés automatiquement lors de l'installation de Kaspersky Security Center 10.0.

7. Lancez la tâche créée.

   Les nouvelles versions de l'Agent d'administration et des applications de Kaspersky Lab seront installées sur les postes clients sélectionnés.

8. Ajoutez les postes clients sur lesquels est effectuée l'installation des nouvelles versions des applications dans la structure des groupes d'administration.

Le système de protection des versions précédentes des applications sous l'administration de Kaspersky Security Center 10.0.

Vous pouvez convertir les stratégies et les tâches (créées pour les versions précédentes des applications de Kaspersky Lab) pour la nouvelle version des stratégies et des tâches de ces applications à l'aide de l'Assistant de conversion des stratégies et des tâches. Pour plus d'informations, cf. *Manuel de l'administrateur de Kaspersky Security Center*.

CONCLUSION

Cette section synthétise les informations présentées dans le document.

Ce document décrit le scénario simple de déploiement de la protection dans le réseau de l'entreprise, ainsi que les actions nécessaires pour déployer rapidement la protection et pour commencer à travailler avec l'application Kaspersky Security Center. Pour plus d'informations sur les possibilités de Kaspersky Security Center et sur les scénarios de déploiement de la protection, cf. *Manuel d'implantation de Kaspersky Security Center* et *Manuel de l'administrateur de Kaspersky Security Center*.

CONTACTER LE SUPPORT TECHNIQUE

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

DANS CETTE SECTION

MODES D'OBTENTION DE L'ASSISTANCE TECHNIQUE

Si vous n'avez pas trouvé comment résoudre votre problème dans la documentation de l'application ou dans une des sources d'informations sur l'application (cf. section "Sources d'informations sur l'application" à la page 8), veuillez contacter le Support technique de Kaspersky Lab. Les experts du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application.

Avant de contacter le service du Support Technique, veuillez lire les règles d'octroi du Support Technique (http://support.kaspersky.com/support/rules).

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

- Par téléphone. Vous pouvez contacter les experts du Support Technique en France.
- Envoyer une demande via système Kaspersky CompanyAccount sur le site Internet du Support Technique. Cette méthode permet de contacter les experts du Support Technique via un formulaire.

ASSISTANCE TECHNIQUE PAR TELEPHONE

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

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

OBTENTION DU SUPPORT TECHNIQUE VIA KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount est un service Internet (https://companyaccount.kaspersky.com) prévu à l'envoi et à la surveillance des demandes dans Kaspersky Lab.

Pour accéder à Kaspersky CompanyAccount, il faut s'enregistrer sur la page d'enregistrement (https://support.kaspersky.com/companyaccount/registration) et recevoir l'identifiant et le mot de passe. Pour ce faire, il faudra indiquer le code d'activation ou le fichier clé (cf. section "A propos du fichier clé" à la page 15).

Kaspersky CompanyAccount permet de réaliser les actions suivantes :

- Envoyer des demandes au Support Technique et au Laboratoire d'étude des virus ;
- Communiquer avec le Support Technique sans devoir envoyer des messages électroniques ;
- Suivre le statut de vos demandes en temps réel.
- Consulter l'historique complet de votre interaction avec le Support Technique.
- Obtenir une copie du fichier clé en cas de perte ou de suppression de celui-ci.

Formulaire de soumission de demande du Support Technique

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

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

- type de demande ;
- Nom et numéro de version de l'application ;
- texte de la demande.

S'il faut, vous pouvez aussi attacher les fichiers à la forme électronique de la demande.

L'expert du Support Technique répond via Kaspersky CompanyAccount, en envoyant un message électronique à l'adresse indiquée lors de l'enregistrement.

Demande électronique adressée au Laboratoire d'étude des virus

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

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

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

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

- *Faux positif du logiciel antivirus* : Kaspersky Security Center considère un certain fichier comme infecté mais vous êtes convaincu que ce n'est pas le cas.

Vous pouvez également envoyer une demande au laboratoire d'étude des virus depuis le formulaire de demande (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr), sans vous enregistrer dans Kaspersky CompanyAccount. Dans ce cas, vous ne devez pas indiquer le code d'activation de l'application. La priorité des demandes créés via formulaire de demande est inférieure aux demandes créées via Kaspersky CompanyAccount.

KASPERSKY LAB ZAO

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement « IDC Worldwide Endpoint Security Revenue by Vendor »). Selon les résultats d'une étude réalisée par KomKon TGI-Russia 2009, Kaspersky Lab est l'éditeur de système de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est basé à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

Produits. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers reprend des logiciels antivirus pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des ordinateurs de poche, des smartphones et d'autres appareils nomades.

La société offre également des services pour la protection des postes de travail, des serveurs de fichiers, des serveurs Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont mises à jour toutes les heures*, tandis que *Les bases antispam sont mises à jour toutes les 5 minutes*.

Technologies. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (É-U), Alt-N Technologies (É-U), Blue Coat Systems (É-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (É-U), Critical Path (Irlande), D-Link (Taïwan), M86 Security (É-U), GFI (Malte), IBM (É-U), Juniper Networks (É-U), LANDesk (É-U), Microsoft (É-U), NETASQ (France), NETGEAR (É-U), Parallels (Russie), SonicWALL (USA), WatchGuard Technologies (É-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

Réalisations. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

Site officiel de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.securelist.com/fr/
Laboratoire Anti-Virus :	newvirus@kaspersky.com (uniquement pour l'envoi d'objets suspects sous forme d'archive)
	http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr
	(pour les demandes auprès des experts en virus)
Forum de Kaspersky Lab :	http://forum.kaspersky.fr

INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

NOTIFICATIONS SUR LES MARQUES DE COMMERCE

Les noms et les marques déposés appartiennent à leurs propriétaires respectifs.

ActiveSync, Microsoft, Windows, SQL Server – les marques Microsoft Corporation déposées aux Etats-Unis et aux autres pays.

Apple – la marque déposée Apple Inc.