



Kaspersky Security Center 10

Manuel de l'administrateur

Version de l'application: 10 Service Pack 2, Maintenance Release 1

Cher utilisateur,

Nous vous remercions de votre confiance. Nous espérons que ce document vous aidera dans votre travail et répondra à la plupart des problèmes émergents.

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

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

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

Ce document peut être modifié sans avertissement préalable.

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

Date de rédaction du document : 13/12/2016

© 2017 AO Kaspersky Lab. Tous droits réservés.

<http://www.kaspersky.fr>

<https://help.kaspersky.com/fr/>

<http://support.kaspersky.com/fr>

Table des matières

A propos de ce document	15
Dans ce document	15
Conventions	19
Sources d'informations sur l'application	21
Sources d'informations pour les recherches indépendantes	21
Forum sur les applications de Kaspersky Lab	23
Kaspersky Security Center	24
Nouveautés	25
Distribution	30
Configurations logicielle et matérielle	30
Interface de l'application	46
Fenêtre principale de l'application	47
Arborescence de la console	49
Zone de travail	54
Éléments de l'espace de travail	57
Ensemble de groupes d'informations	59
Groupe du filtrage de données	59
Menu contextuel.....	61
Configuration de l'interface.....	62
Licence de l'application	65
A propos du contrat de licence utilisateur final	65
A propos de la licence	66
A propos du certificat de licence	67
A propos de la clé	67
Options de licence de Kaspersky Security Center	68
A propos des restrictions de la fonctionnalité de base	71
A propos du code d'activation	73
A propos du fichier clé	73
A propos de l'abonnement.....	74

Assistant de configuration initiale du Serveur d'administration	75
Notions principales	77
Serveur d'administration	78
Hiérarchie des Serveurs d'administration	79
Serveur d'administration virtuel	80
Serveur des appareils mobiles	81
Serveur Internet	82
Agent d'administration. Groupe d'administration	83
Poste de travail de l'administrateur	84
Plug-in d'administration de l'application	85
Stratégies, paramètres de l'application et tâches	85
Corrélation de la stratégie et des paramètres locaux de l'application	88
Agent de mises à jour	90
Administration des Serveurs d'administration	94
Connexion au Serveur d'administration et permutation entre les Serveurs d'administration	95
Privilèges d'accès au Serveur d'administration et à ses objets	96
Conditions de connexion au Serveur d'administration via Internet	98
Connexion sécurisée au Serveur d'administration	99
Authentification du Serveur lors de la connexion de l'appareil	100
Authentification du Serveur lors de la connexion de la Console d'administration	100
Certificat du Serveur d'administration	101
Se déconnecter du Serveur d'administration	101
Ajout d'un Serveur d'administration à l'arborescence de la console.....	101
Suppression d'un Serveur d'administration de l'arborescence de la console	102
Changement du compte utilisateur du service du Serveur d'administration. Utilitaire klsrvswch	102
Affichage et modification des paramètres du Serveur d'administration.....	104
Configuration des paramètres généraux du Serveur d'administration	105
Traitement et stockage des événements sur le Serveur d'administration.....	105
Contrôle de l'émergence d'épidémies de virus	106
Restriction du trafic.....	107
Configuration des paramètres du Serveur Internet.....	107
Travail avec les utilisateurs internes	108

Administration des groupes d'administration	109
Création des groupes d'administration.....	110
Déplacement des groupes d'administration.....	112
Suppression des groupes d'administration	113
Création automatique de structure des groupes d'administration.....	114
Installation automatique des applications sur les appareils du groupe d'administration	116
Administration à distance des applications	118
Administration des stratégies	118
Création d'une stratégie	120
Affichage des stratégies héritées dans le groupe imbriqué.....	121
Activation d'une stratégie	122
Activation automatique d'une stratégie lors d'un événement "Attaque de virus" .	123
Application des stratégies pour les utilisateurs autonomes	123
Modification d'une stratégie. Restauration des modifications	124
Suppression d'une stratégie.....	125
Copie d'une stratégie	125
Exportation d'une stratégie	126
Importation d'une stratégie.....	126
Conversion des stratégies.....	127
Administration des profils de stratégie	127
A propos du profil de stratégie	128
Création d'un profil de stratégie	130
Modification du profil d'une stratégie	132
Suppression d'un profil de stratégie	133
Gérer les tâches.....	134
Création d'une tâche de groupe.....	135
Création d'une tâche du Serveur d'administration	136
Création d'une tâche pour un ensemble d'appareils	137
Création d'une tâche locale.....	138
Affichage d'une tâche de groupe héritée dans la zone de travail du groupe imbriqué	139
Activation automatique des appareils avec le lancement de la tâche	140
Arrêt automatique de l'appareil après l'exécution de la tâche	140
Limitation de la durée d'exécution de la tâche	141

Exportation d'une tâche.....	141
Importation d'une tâche.....	142
Conversion des tâches.....	143
Démarrage et arrêt manuels des tâches	143
Suspension et reprise manuelles d'une tâche.....	145
Suivi et affichage des comptes-rendus d'activité des tâches	145
Affichage de l'historique des tâches entreposé sur le Serveur d'administration ..	145
Configuration du filtre d'informations sur les résultats de la tâche	146
Modification d'une tâche. Restauration des modifications.....	146
Consultation et modification des paramètres locaux de l'application	147
Administration des appareils clients	149
Connexion des appareils clients au Serveur d'administration.....	150
Connexion manuelle de l'appareil client au Serveur d'administration. Utilitaire klmover	151
Connexion en tunnel de l'appareil client avec le Serveur d'administration.....	153
Connexion à distance au bureau de l'appareil client.....	154
Paramètres du redémarrage de l'appareil client.....	156
Audit des actions sur un appareil client distant	157
Vérification de la connexion de l'appareil client avec le Serveur d'administration ...	159
Vérification automatique de la connexion de l'appareil client avec le Serveur d'administration.....	159
Vérification manuelle de la connexion de l'appareil client avec le Serveur d'administration. Utilitaire klnagchk	160
Identification des appareils clients sur le Serveur d'administration	161
Ajout d'appareils à un groupe d'administration.....	162
Modification du Serveur d'administration pour les appareils clients	163
Démarrage, arrêt et redémarrage à distance des appareils clients.....	164
Envoi d'un message aux utilisateurs des appareils.....	165
Contrôle de modification de l'état des machines virtuelles	165
Attribution automatique de tags aux appareils	166
Diagnostic à distance des appareils clients. Utilitaire de diagnostic à distance Kaspersky Security Center	169
Connexion de l'utilitaire de diagnostic à distance à l'appareil client.....	170
Activation et désactivation du traçage, téléchargement du fichier de traçage.....	173
Téléchargement des paramètres des applications	174

Téléchargement des journaux des événements	174
Lancement du diagnostic et téléchargement des résultats	175
Lancement, arrêt ou relancement des applications	175
Administration des comptes utilisateur	177
Utilisation des comptes utilisateur	178
Ajout du compte utilisateur	179
Configuration du contrôle de l'originalité du nom de l'utilisateur interne.....	180
Ajout d'un groupe d'utilisateurs	181
Ajout d'un utilisateur dans le groupe	182
Configuration des autorisations. Rôles d'utilisateurs	183
Ajout d'un rôle utilisateur	183
Attribution d'un rôle à un utilisateur ou à un groupe d'utilisateurs	184
Désignation d'un utilisateur comme propriétaire de l'appareil.....	186
Diffusion des messages aux utilisateurs	187
Consultation de la liste des appareils mobiles de l'utilisateur	188
Installation du certificat pour l'utilisateur	188
Consultation de la liste des certificats octroyés à l'utilisateur	189
Utilisation des rapports, des statistiques et des notifications	190
Utilisation des rapports	191
Créer le nouveau rapport	192
Génération et affichage des rapports	192
Enregistrement du rapport	193
Création d'une tâche d'envoi du rapport.....	193
Travailler avec les données statistiques	194
Configuration des paramètres de notification sur les événements	196
Création d'un certificat pour le serveur SMTP	198
Sélections d'événements	199
Consultation d'une sélection d'événements	200
Configuration d'une sélection d'événements	200
Création d'une sélection d'événements.....	201
Exportation d'une sélection d'événements dans le fichier texte	201
Suppression des événements depuis la sélection	202
Exportation des événements dans le système SIEM	202
Sélections d'appareils	204

Affichage d'une sélection d'appareils	205
Configuration d'une sélection d'appareils	205
Création d'une sélection d'appareils	206
Exportation des paramètres de la sélection d'appareils dans un fichier	206
Création d'une sélection d'appareils selon les paramètres importés	207
Suppression des appareils depuis les groupes d'administration dans la sélection	207
Stratégies	208
Tâches	208
Appareils non définis	209
Sondage du réseau	209
Affichage et modification des paramètres de sondage du réseau Windows	211
Affichage et modification des paramètres de sondage des groupes Active Directory	211
Affichage et modification des paramètres de sondage des plages IP	212
Travail avec les domaines Windows. Affichage et modification des paramètres du domaine	213
Travail avec les plages IP	213
Création de la plage IP	214
Affichage et modification des paramètres de plage IP	214
Travail avec les groupes Active Directory. Affichage et modification des paramètres du groupe	215
Création des règles de déplacement automatique des appareils dans un groupe d'administration	215
Utilisation du mode dynamique VDI sur les appareils clients	216
Activation du mode dynamique VDI dans les propriétés du paquet d'installation de l'Agent d'administration	217
Recherche d'appareils qui font partie de VDI	218
Déplacement dans le groupe d'administration des appareils qui font partie de VDI	218
Administration des applications sur les appareils clients	219
Groupes des applications	220
Création des catégories d'applications	222
Configuration d'administration du lancement des applications sur les appareils clients	223
Consultation des résultats de l'analyse statique des règles de lancement des fichiers exécutables	225

Affichage du registre des applications	226
Création des groupes des applications sous licence	227
Gestion des clés pour les groupes des applications sous licence	228
Inventaire du logiciel Kaspersky Security Center	229
Inventaire des fichiers exécutables	230
Consultation des informations sur les fichiers exécutables	231
Vulnérabilités dans les applications	232
Consultation des informations relatives aux vulnérabilités dans les applications	233
Recherche de vulnérabilités dans les applications	234
Fermeture de vulnérabilités dans les applications	235
Mises à jour du logiciel	236
Consultation des informations sur les mises à jour disponibles	238
Synchronisation des mises à jour Windows Update avec le Serveur d'administration.....	238
Installation automatique des mises à jour pour Kaspersky Endpoint Security sur les appareils	239
Modèle hors ligne d'obtention des mises à jour	242
Activation et désactivation d'un modèle hors ligne d'obtention des mises à jour	245
Installation manuelle des mises à jour sur les appareils.....	246
Configuration des mises à jour Windows dans la stratégie de l'Agent d'administration.....	250
Installation à distance des systèmes d'exploitation et des applications.....	251
Création des images des systèmes d'exploitation	254
Ajout des pilotes pour l'environnement de préinstallation Windows (WinPE)	255
Ajout des pilotes dans le paquet d'installation avec l'image du système d'exploitation	256
Configuration des paramètres de l'utilitaire sysprep.exe.....	257
Déploiement des systèmes d'exploitation sur les nouveaux appareils dans le réseau	258
Déploiement des systèmes d'exploitation sur les appareils clients	259
Création des paquets d'installation des applications.....	260
Établissement d'un certificat pour les paquets d'installation des applications	261
Installation des applications sur les appareils clients	262
Administration des appareils mobiles	263
Administration des appareils mobiles à l'aide d'une stratégie MDM.....	263

Utilisation des commandes pour les appareils mobiles	266
Commandes d'administration de l'appareil mobile	266
Utilisation de Google Firebase Cloud Messaging	271
Envoi d'une commande	272
Consultation de l'état des commandes dans le journal des commandes	273
Utilisation des certificats	274
Installation d'un certificat	274
Configuration des règles d'octroi de certificats	275
Intégration à l'infrastructure de clés ouvertes	277
Activation de la prise en charge de Kerberos Constrained Delegation	278
Ajout d'un appareil mobile à la liste des appareils administrés	279
Gestion des appareils mobiles via les outils Exchange ActiveSync	284
Ajout d'un profil d'administration	286
Suppression d'un profil d'administration	288
Affichage des informations sur l'appareil EAS	289
Désactivation de l'administration d'un appareil EAS	289
Administration des appareils MDM iOS	290
Établissement d'un certificat de profil MDM iOS	291
Ajout du profil de configuration	292
Définition du profil de configuration sur l'appareil	293
Suppression du profil de configuration de l'appareil	295
Ajout du profil provisioning	296
Définition du profil provisioning sur l'appareil	297
Suppression du profil provisioning de l'appareil	298
Ajout d'une app administrée	300
Installation de l'app sur l'appareil mobile	301
Suppression de l'app de l'appareil	302
Installation de l'app Kaspersky Safe Browser sur l'appareil mobile	304
Affichage des informations sur l'appareil MDM iOS	305
Désactivation de l'administration de l'appareil MDM iOS	306
Administration des appareils KES	306
Création du paquet des apps mobiles pour les appareils KES	307
Activation de l'authentification à deux facteurs des appareils KES	308
Affichage des informations sur l'appareil KES	309

Désactivation d'un appareil KES de l'administration	310
Self Service Portal.....	311
Présentation du Self Service Portal	311
Ajout d'un appareil	314
Connexion de l'utilisateur au Self Service Portal	315
Chiffrement et protection des données	318
Consultation de la liste des appareils chiffrés	319
Consultation de la liste des événements du chiffrement.....	320
Exportation de la liste des événements du chiffrement dans le fichier texte.....	322
Formation et consultation des rapports sur le chiffrement	322
Inventaire du matériel détecté dans le réseau	326
Ajout d'informations sur les nouveaux appareils	327
Configuration des critères de définition des appareils d'entreprise	328
Mise à jour des bases de données et des modules d'application	329
Création d'une tâche de téléchargement des mises à jour dans le stockage	330
Création d'une tâche de téléchargement des mises à jour dans les stockages des agents de mises à jour.....	332
Configuration des paramètres de la tâche de téléchargement des mises à jour dans le stockage.....	333
Analyse des mises à jour récupérées	334
Configuration des stratégies de vérification et des tâches auxiliaires	336
Affichage des mises à jour récupérées	337
Déploiement de mises à jour automatique	338
Déploiement automatique des mises à jour sur les appareils clients.....	339
Redistribution automatique des mises à jour sur les Serveurs d'administration secondaires	340
Installation automatique des mises à jour des modules d'application des Agents d'administration.....	341
Désignation d'appareils comme agents de mises à jour	342
Suppression d'un appareil de la liste des agents de mises à jour.....	344
Récupération des mises à jour par les agents de mises à jour	345
Annulation des mises à jour installées	346
Travail avec les clés des applications	347
Consultation des informations sur les clés utilisées	348

Ajout de la clé dans le stockage du Serveur d'administration	349
Suppression de la clé du Serveur d'administration	349
Diffusion des clés sur les appareils clients	350
Diffusion automatique de la clé	350
Création et consultation du rapport d'utilisation des clés	352
Stockages des données.....	353
Exportation de la liste des objets en quarantaine dans le fichier texte	354
Paquets d'installation.....	354
Quarantaine et sauvegarde	355
Activation de la gestion à distance des fichiers dans les stockages	356
Consultation des propriétés du fichier placé dans le stockage	357
Suppression des fichiers depuis le stockage	357
Restauration des fichiers depuis le stockage.....	358
Enregistrement du fichier depuis le stockage sur le disque	358
Analyse des fichiers en quarantaine.....	359
Fichiers avec traitement différé	360
Désinfection du fichier avec traitement différé	360
Enregistrement du fichier avec traitement différé sur le disque	361
Suppression des fichiers du dossier "Fichiers avec traitement différé".....	362
Kaspersky Security Network (KSN).....	363
A propos de KSN	363
A propos des données.....	364
Configuration de l'accès à KSN.....	365
Activation et désactivation de KSN	367
Consulter les statistiques du serveur proxy KSN	368
Contacter le Support Technique.....	370
Moyens de bénéficier de l'assistance technique	370
Assistance technique par téléphone	371
Assistance technique via le Kaspersky CompanyAccount.....	371
Appendice.....	373
Possibilités complémentaires	373
Automatisation du fonctionnement de Kaspersky Security Center.	
Utilitaire klakaut	375
Utilisateurs autonomes	375

Événements dans le fonctionnement des applications	379
Définition du niveau d'importance de l'événement de dépassement de la restriction de licence.....	380
Notification relative aux événements via un fichier exécutable	380
Utilisation de l'application Kaspersky Security pour les environnements protégés	382
Suivi de l'état de la protection antivirus à l'aide d'informations du registre système.....	382
Clusters et matrices des serveurs	384
Algorithme d'installation du correctif pour l'application Kaspersky Lab dans le modèle de cluster	385
Recherche d'appareils.....	386
Connexion aux appareils à l'aide de Windows Desktop Sharing	388
A propos des comptes utilisateur utilisés	388
Fonctionnement avec les outils externes	389
Exportation des listes depuis les fenêtres de dialogue	390
Mode de clonage du disque de l'Agent d'administration.....	390
Préparation de l'appareil fonctionnant sous le système d'exploitation Linux à l'installation à distance de l'Agent d'administration	392
Copie de sauvegarde et restauration des données du Serveur d'administration	394
Sauvegarde et restauration des données en mode interactif	401
Installation de l'application à l'aide des stratégies de groupe Active Directory	402
Particularités d'utilisation de l'interface d'administration	405
Comment faire revenir la fenêtre des propriétés	405
Comment se déplacer dans l'arborescence de la console	406
Comment ouvrir la fenêtre des propriétés de l'objet dans l'espace de travail	406
Comment sélectionner le groupe des objets dans l'espace de travail	406
Comment modifier l'ensemble des colonnes dans l'espace de travail	407
Aide	408
Utilisation de l'agent de mises à jour en guise de passerelles	408
Utilisation des masques dans les variables chaînes.....	409
Commandes du menu contextuel	409
A propos du gestionnaire des connexions	416
Autorisations de l'utilisateur pour l'administration des appareils mobiles via Exchange ActiveSync.....	416
A propos de l'administrateur du Serveur virtuel	418
Liste des appareils administrés. Valeur des colonnes	419

Etats des appareils, des tâches et des stratégies.....	423
Icônes des états des fichiers dans la Console d'administration	426
Utilisation des expressions régulières dans la ligne de recherche.....	427
Glossaire	429
AO Kaspersky Lab	440
Protection complémentaire avec l'utilisation de Kaspersky Security Network.....	442
Avis de marques déposées	443
Index.....	445

A propos de ce document

Le manuel de l'administrateur de Kaspersky Security Center 10 (ci-après, "Kaspersky Security Center") est destiné aux experts chargés de l'installation et de l'administration du Kaspersky Security Center, et aux spécialistes du support technique au sein des organisations qui utilisent le Kaspersky Security Center.

Ce modèle permet de trouver des informations relatives à la configuration et à l'utilisation du Kaspersky Security Center.

Ce manuel renseigne également les sources d'informations sur l'application et les méthodes d'obtention de l'assistance technique.

Dans cette section

Dans ce document	15
Conventions	19

Dans ce document

Le Manuel de l'administrateur de Kaspersky Security Center contient l'introduction, les sections décrivant l'interface de l'application, ses paramètres et les services, les sections décrivant les résolutions des problèmes généraux, ainsi que les glossaires des termes.

Sources d'informations sur l'application (à la page [21](#))

Cette section décrit les sources d'informations sur 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.

Kaspersky Security Center (à la page [24](#))

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

Interface de l'application (à la page [46](#))

Cette section comprend des descriptions des éléments principaux de l'interface de Kaspersky Security Center, ainsi que de sa configuration.

Licence de l'application (à la page [65](#))

Cette section présente les notions principales relatives à la licence de l'application.

Assistant de configuration initiale (à la page [75](#))

Cette section reprend les informations sur le fonctionnement de l'Assistant de configuration initiale du Serveur d'administration.

Notions principales (à la page [77](#))

Cette section contient les définitions détaillées des notions principales, concernant Kaspersky Security Center.

Administration des Serveurs d'administration (à la page [94](#))

Cette section contient les informations sur l'utilisation des Serveurs d'administration et sur la configuration des paramètres du Serveur d'administration.

Administration des groupes d'administration (à la page [109](#))

Cette section contient les informations sur le travail avec les groupes d'administration.

Administration à distance des applications (à la page [118](#))

Cette section contient les informations sur l'administration à distance des applications Kaspersky Lab installées sur les appareils clients à l'aide de stratégies, de profils de stratégie, de tâches et de la configuration des paramètres locaux des applications.

Administration des appareils clients (à la page [149](#))

Cette section contient les informations sur le travail avec les appareils clients.

Manipulation avec les rapports, les statistiques et les notifications (à la page [190](#))

Cette section reprend les informations sur l'utilisation des rapports, les statistiques et les sélections d'événements et d'appareils dans Kaspersky Security Center, ainsi que sur la configuration des notifications du Serveur d'administration.

Ordinateurs non définis (à la page [209](#))

Cette section reprend les informations sur l'utilisation des appareils du réseau de l'entreprise, non inclus dans les groupes d'administration.

Administration des applications sur les postes clients (à la page [219](#))

Cette section décrit le travail avec les groupes des applications, ainsi que le processus de mise à jour du logiciel et le processus de fermeture des vulnérabilités que Kaspersky Security Center détecte sur les appareils clients.

Installation à distance des systèmes d'exploitation et des applications (à la page [251](#))

Cette section contient les informations sur la création des images des systèmes d'exploitation et sur leur déploiement sur les ordinateurs clients par le réseau, ainsi que sur l'installation à distance des applications de Kaspersky Lab et d'autres éditeurs du logiciel.

Administration des appareils mobiles (à la page [262](#))

Cette section décrit l'administration des appareils mobiles connectés au Serveur d'administration.

Self Service Portal (à la page [311](#))

Cette section contient des informations sur le Self Service Portal. Cette section contient des informations relatives à l'autorisation d'accès des utilisateurs au Self Service Portal, à la création de comptes utilisateur Self Service Portal et à l'ajout d'appareils mobiles sur le Self Service Portal.

Chiffrement et protection des données (à la page [318](#))

Cette section reprend les informations sur l'administration du chiffrement des données enregistrées sur les disques dur des appareils et sur les disques amovibles.

Inventaire du matériel détecté dans le réseau (à la page [326](#))

Cette section reprend les informations sur l'inventaire du matériel connecté au réseau de l'entreprise.

Mise à jour des bases et des modules d'application (à la page [329](#))

Cette section décrit le téléchargement et la diffusion des mises à jour des bases de données et des modules d'application à l'aide de Kaspersky Security Center.

Travail avec les clés des applications (à la page [347](#))

Cette section décrit les possibilités de Kaspersky Security Center sur l'utilisation des clés des applications administrées de Kaspersky Lab.

Stockages des données (à la page [353](#))

Cette section contient les informations sur les données enregistrées sur le Serveur d'administration et utilisées pour suivre les états des appareils clients et leur service.

Contacteur le Service du Support Technique (à la page [370](#))

Cette section contient des informations sur les moyens et les conditions d'accès à l'assistance technique.

Glossaire

La section reprend les termes utilisés dans ce document.

AO Kaspersky Lab (à la page [440](#))

Cette section reprend les informations sur Kaspersky Lab.

Informations sur le code tiers (à la page [442](#))

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

Avis de marques déposées (à la page [443](#))

Cette section reprend les notifications sur les marques de commerce déposées.

Index

Cette section vous aidera à trouver rapidement les informations nécessaires dans le document.

Conventions

Le présent document utilise les conventions suivantes (cf. tableau ci-dessous).

Tableau 1. Conventions

Exemple de texte	Description des conventions
N'oubliez pas que ...	Les avertissements apparaissent en rouge et sont encadrés. Ils contiennent des informations sur les actions pouvant avoir des conséquences indésirables.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Elles contiennent des informations complémentaires et de référence.
Exemple : ...	Les exemples sont présentés sur un fond bleu sous le titre "Exemple".
La <i>mise à jour</i> , c'est ... L'événement <i>Les bases sont dépassées</i> survient.	Les éléments de texte suivants apparaissent en italique : <ul style="list-style-type: none">• 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.

Exemple de texte	Description des conventions
<p>Cliquez sur le bouton Activer.</p>	<p>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.</p>
<p>► <i>Pour programmer une tâche, procédez comme suit :</i></p>	<p>Les phrases d'introduction des instructions sont en italique et présentent l'icône "flèche".</p>
<p>Dans la ligne de commande, saisissez le texte <code>help</code></p> <p>Les informations suivantes s'affichent :</p> <p>Indiquez la date au format <code>JJ:MM:AA</code>.</p>	<p>Les types suivants du texte apparaissent dans un style spécial :</p> <ul style="list-style-type: none"> • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir au clavier.
<p><Nom d'utilisateur></p>	<p>Les variables sont écrites entre chevrons. La valeur correspondant à la variable doit être remplacée par cette variable. Par ailleurs, les chevrons sont omis.</p>

Sources d'informations sur l'application

Cette section décrit les sources d'informations sur 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 indépendantes	21
Forum sur les applications de Kaspersky Lab.....	23

Sources d'informations pour les recherches indépendantes

Vous pouvez utiliser les sources suivantes pour une recherche indépendante d'informations sur le Kaspersky Security Center :

- page Kaspersky Security Center sur le site Internet de Kaspersky Lab ;
- page Kaspersky Security Center sur le site Internet du Service de 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 "Contacter le Support Technique" à la page [370](#)).

Une connexion Internet est requise pour utiliser les sources d'informations sur les sites Internet.

Page Kaspersky Security Center sur le site Internet de Kaspersky Lab

La page Kaspersky Security Center

(<https://www.kaspersky.fr/small-to-medium-business-security/security-center>) fournit des informations générales sur l'application, ses possibilités et ses particularités.

La page Kaspersky Security Center contient un lien vers la boutique en ligne. Ce lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

Page Kaspersky Security Center dans la Base de connaissances

La *base de connaissances* est une section du site Internet du Service de Support Technique.

La page Kaspersky Security Center dans la Base de connaissances

(<http://support.kaspersky.com/fr/ksc10>) comporte des articles contenant 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 de la Base de connaissances peuvent répondre à des questions en rapport non seulement avec le Kaspersky Security Center, mais également avec d'autres applications de Kaspersky Lab. Les articles de la Base de connaissances peuvent également comporter des actualités sur le Service de Support Technique.

Aide électronique

L'application contient des fichiers d'aide complète et contextuelle.

L'aide complète permet de trouver des informations relatives à la configuration et à l'utilisation du Kaspersky Security Center.

L'aide contextuelle permet de trouver des informations sur les fenêtres de Kaspersky Security Center : description des paramètres de Kaspersky Security Center et liens vers les descriptions de tâches au cours desquelles ces paramètres sont utilisés.

L'aide peut être incluse dans l'application ou affichée en ligne sur une ressource Web de Kaspersky Lab. Si l'aide est affichée en ligne, une fenêtre de navigateur s'ouvre lorsqu'elle est appelée. L'affichage de l'aide en ligne nécessite une connexion à Internet.

Documentation

La Documentation de l'application reprend tous les fichiers des manuels.

Le manuel de l'administrateur comporte des informations relatives à la configuration et à l'utilisation du Kaspersky Security Center.

Le manuel d'implantation comporte des informations relatives à l'exécution des tâches suivantes :

- planification de l'installation de l'application (en tenant compte des principes de fonctionnement de l'application, de la configuration requise, des schémas typiques de déploiement et des particularités de la compatibilité avec d'autres applications) ;
- préparation à l'installation, installation et activation du Kaspersky Security Center ;
- configuration de l'application après l'installation.

Le manuel de Prise en main comporte des informations pour une prise en main rapide de l'application (description de l'interface et des tâches principales qu'il est possible d'exécuter avec le Kaspersky Security Center).

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.

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'administrateur 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 élaborée à partir 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.

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.

Par *entreprises clientes*, il faut entendre les entreprises dont la protection antivirus est assurée par le prestataire de service.

- Former une hiérarchie des groupes d'administration pour administrer les appareils (les appareils 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 appareils clients par le réseau, ainsi qu'exécuter l'installation à distance des applications de Kaspersky Lab et d'autres éditeurs de logiciels.
- Gérer à distance les applications de Kaspersky Lab et d'autres éditeurs installées sur les périphériques clients : installer les mises à jour, rechercher et fermer les vulnérabilités.
- Diffuser de manière centralisée les clés des applications de Kaspersky Lab sur les ordinateurs 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.
- Administrer les appareils mobiles qui prennent en charge les protocoles Kaspersky Security pour Android™, Exchange ActiveSync® et iOS Mobile Device Management (MDM iOS).
- 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 la Sauvegarde par les applications de protection, ainsi qu'avec les fichiers dont le traitement est différé par les applications de protection.

Dans cette section

Nouveautés.....	25
Distribution.....	29
Configurations logicielle et matérielle	30

Nouveautés

Modifications apportées dans l'application Kaspersky Security Center par rapport à la version antérieure :

- Les modifications des paramètres des stratégies, tâches et du Serveur d'administration de Kaspersky Security Center sont enregistrées.

- Possibilité de restaurer les paramètres d'un objet pour la version sélectionnée de l'objet (cf. section "Modification d'une stratégie. Restauration des modifications" à la page [124](#)).
- Possibilité de filtrer l'historique des révisions par utilisateur et heure de modifications.
- Période réglée de conservation de la révision (par défaut 3 mois).
- Mécanisme de comparaison des révisions de la stratégie et des tâches.
- Exportation des révisions des stratégies et des tâches vers le fichier texte.
- Amélioration du diagnostic du processus d'installation automatique du correctif. Ajout d'avertissements supplémentaires à la création de la copie de sauvegarde des données du Serveur d'administration dans l'Assistant d'installation de Kaspersky Security Center :
 - Importance de la présence d'une nouvelle copie de sauvegarde des fichiers et des distributeurs de la version précédente de Kaspersky Security Center et de tous les correctifs installés.
 - Explication de la manière d'agir en cas de défaillance de la mise à jour.
 - Confirmation supplémentaire de l'utilisateur si l'utilisateur ne crée pas la copie de sauvegarde des données.
- Prise en charge de l'Agent d'administration Kaspersky Security Center (Windows 8 / 8.1, MS Surface) sur les tablettes fonctionnant sous le système d'exploitation Windows.
- Optimisation de l'Agent d'administration pour réduire le temps de chargement de Windows pour les appareils sur lesquels est installé Kaspersky Endpoint Security for Windows et l'Agent d'administration.
- Optimisation du fonctionnement de l'Agent d'administration pendant l'attente (mode veille, mode d'hibernation) du système Windows.
- L'Assistant d'installation de Kaspersky Security Center ajoute la possibilité de contrôler les dernières versions des plug-ins et des paquets d'installation de Kaspersky Lab ainsi que la possibilité d'appliquer les mises à jour disponibles. La fenêtre principale de l'application Kaspersky Security Center affiche aussi la présence de mises à jour pour les plug-ins/programmes et apps/composants de Kaspersky Security Center.

- La terminologie de l'application Kaspersky Security Center présenter un aspect plus général et indépendant par rapport aux autres applications. Par exemple, le terme "ordinateur" a été remplacé par le terme "appareil".
- Nouvel assistant d'installation des mises à jour du logiciel (cf. section "Installation manuelle des mises à jour sur les appareils" à la page [246](#)).
- Ajout des informations sur la barre de progression de l'exécution de la tâche. La liste des colonnes de la fenêtre **Résultats de la tâche** comporte les colonnes suivantes :
 - Compteurs des appareils sur lesquels la tâche est lancée, terminée ou s'est soldée par une erreur.
 - Etat (avec description de l'état de la tâche).
- Possibilité d'attribuer manuellement le nom du paquet d'installation.
- Demande de confirmation auprès de l'utilisateur si l'utilisateur crée une stratégie pour les applications Kaspersky Lab dans le groupe d'administration pour lequel la stratégie pour l'application en question existe déjà.
- Dans l'espace de travail du dossier **Appareils non définis**, le bouton **Configurer les règles** est ajouté pour déplacer automatiquement les appareils non définis (cf. section "Création des règles de déplacement automatique des appareils dans un groupe d'administration" à la page [215](#)).
- La case **Lancer l'Assistant de déploiement de la protection sur les postes de travail** est ajoutée dans l'Assistant de configuration initiale.
- Les pages de l'espace de travail sous l'onglet **Statistiques** du nœud du Serveur d'administration sont visuellement divisées.
- Amélioration de la navigation lors de l'utilisation des règles d'attribution automatique des tags.
- Mise au point de l'administration de l'accès sur la base des rôles définis dans les propriétés du Serveur d'administration.
- Ajout du filtre de description textuelle du champ **Événements**.

- Ajout de la possibilité de créer des tags dans les règles d'activation du profil de la stratégie.
- Accès rapide aux profils de stratégies depuis l'espace de travail du dossier **Stratégies** et depuis l'onglet **Stratégies** dans le nœud du Serveur d'administration.
- Possibilité de sélectionner la position des colonnes dans les listes.
- Indicateur de la barre de progression du processus de mise à jour des paquets d'installation.
- Modification de l'icône d'installation du Serveur d'administration dans la fenêtre principale d'installation de l'application Kaspersky Security Center.
- Mise au point des formulations dans l'Assistant de conversion des stratégies et des tâches.
- Ajout d'une description de la clé Server flags LP_ConsoleMustUsePort13291 et LP_InterUserUniqVsScope.
- Simplification de l'installation du Serveur MDM iOS. Création de l'Assistant d'installation du Serveur MDM iOS.
- Simplification de l'installation du Self Service Portal.
- Mise au point de l'Assistant de connexion du nouvel appareil mobile.
- L'appareil mobile ne se bloque pas suite à l'exécution des commandes **Définir l'emplacement** et **Emettre un signal sonore** (cf. section "**Commandes d'administration des appareils mobiles**" à la page [266](#)).
- Possibilité de définir manuellement l'état de l'appareil Android **Critique** ou **Avertissement** pour l'administrateur, si cet appareil où est installée l'app Kaspersky Endpoint Security for Android n'a pas activé l'accès aux services de fonctions spéciales puisque dans ce cas la Protection Internet ne fonctionne pas.
- Simplification de la configuration de Google Firebase Cloud Messaging. Ajout d'info-bulles et d'explications à l'interface de l'application.
- Création d'un utilitaire de copie de sauvegarde des fichiers depuis la ligne de commande pour le Serveur MDM iOS.

- Possibilité pour l'administrateur de Kaspersky Security Center d'indiquer manuellement la durée de validité du certificat Kaspersky Security for Mobile Devices lors de l'émission (ou la réémission) du certificat.
- Affichage du numéro de version de Self Service Portal dans l'interface Self Service Portal.
- Si pendant l'installation de Kaspersky Security Center, la case **Prise en charge des appareils mobiles** a été cochée, toutes les configurations nécessaires pour administrer les appareils mobiles et Kaspersky Security for Mobile Devices sont effectuées dans l'Assistant de configuration initiale de Kaspersky Security Center.
- Mise au point de la conception des fonctionnalités d'administration des correctifs et des mises à jour.
- Mise au point du composant Administration des vulnérabilités et des correctifs.
- Elargissement du suivi et de la recherche de vulnérabilités.
- Elargissement du contrôle des tâches exécutées.
- Transfert des événements au format Syslog (RFC 5424) aux systèmes SIEM (cf. section "Exportation des événements dans le système SIEM" à la page [202](#)).
- Unification des types d'équipement dans l'interface Kaspersky Security Center.
- Ajout d'informations sur les résultats de l'exécution des tâches **Installation des mises à jour requises et correction des vulnérabilités** et **Recherche de vulnérabilités et de mises à jour requises**.
- Analyse supplémentaire avant le lancement de la tâche **Création du paquet d'installation à partir de l'image du système d'exploitation de l'appareil de référence**. L'analyse contrôle la présence de droits dans le compte utilisateur indiqué par l'administrateur, dans le dossier partagé indiqué pour la conservation temporaire de l'image.
- Création automatique d'un incident si l'espace libre vient à manquer sur l'appareil jouant le rôle d'agent de mises à jour (cf. section "Agent de mises à jour" à la page [89](#)).

Distribution

Kaspersky Endpoint Security peut être acheté dans la boutique en ligne de Kaspersky Lab (par exemple <http://www.kaspersky.fr>, section **Boutique en ligne**) ou du site d'un partenaire.

En achetant Kaspersky Security Center dans la boutique en ligne, vous copiez l'application depuis le site Internet de la boutique en ligne. Les informations indispensables à l'activation de l'application vous seront envoyées par email après le paiement.

Pour en savoir plus sur les modes d'achat et de distribution, contactez notre Service Ventes.

Configurations logicielle et matérielle

Serveur d'administration

Configuration matérielle :

- Processeur avec 1 GHz ou plus. La cadence minimale du processeur avec un système d'exploitation 64 bits est de 1,4 GHz.
- Mémoire vive : 4 GO.
- Espace disque disponible : 10 GO. Lors de l'utilisation de la fonctionnalité de l'Administration système, le volume d'espace libre sur le disque doit être au moins de 100 GO.

Configuration logicielle :

- Microsoft® Data Access Components (MDAC) version 2.8 ;
- Windows DAC 6.0 ;
- Microsoft Windows Installer 4.5.

Système d'exploitation :

- Microsoft Windows 10 Famille 32 bits/64 bits ;
- Microsoft Windows 10 Professionnel 32 bits/64 bits ;

- Microsoft Windows 10 Entreprise 32 bits/64 bits ;
- Microsoft Windows 10 Éducation 32 bits/64 bits ;
- Microsoft Windows 10 Pro RS1 32 bits/64 bits ;
- Microsoft Windows 10 Entreprise RS1 32 bits/64 bits ;
- Microsoft Windows 10 Education RS1 32 bits/64 bits ;
- Microsoft Windows 10 Pro RS2 32 bits/64 bits ;
- Microsoft Windows 10 Entreprise RS2 32 bits/64 bits ;
- Microsoft Windows 10 Education RS2 32 bits/64 bits ;
- Microsoft Windows 8.1 Professionnel 32 bits/64 bits ;
- Microsoft Windows 8.1 Entreprise 32 bits/64 bits ;
- Microsoft Windows 8 Professionnel 32 bits/64 bits ;
- Microsoft Windows 8 Entreprise 32 bits/64 bits ;
- Microsoft Windows 7 Professionnel SP1 32 bits/64 bits ;
- Microsoft Windows 7 Entreprise SP1 32 bits/64 bits ;
- Microsoft Windows 7 Édition Intégrale SP1 32 bits/64 bits ;
- Microsoft Small Business Server 2008 Standard 64 bits ;
- Microsoft Small Business Server 2008 Premium 64 bits ;
- Microsoft Small Business Server 2011 Essentials 64 bits ;
- Microsoft Small Business Server 2011 Premium Add-on 64 bits ;
- Microsoft Small Business Server 2011 Standard 64 bits ;
- Microsoft Windows Server® 2008 Datacenter SP1 32 bits/64 bits ;
- Microsoft Windows Server 2008 Entreprise SP1 32 bits/64 bits ;

- Microsoft Windows Server 2008 Foundation SP2 32 bits/64 bits ;
- Microsoft Windows Server 2008 SP1 32 bits/64 bits ;
- Microsoft Windows Server 2008 Standard SP1 32 bits/64 bits ;
- Microsoft Windows Server 2008 ;
- Windows Server 2008 SP1 ;
- Microsoft Windows Server 2008 R2 Server Core 64 bits ;
- Microsoft Windows Server 2008 R2 Datacenter 64 bits ;
- Microsoft Windows Server 2008 R2 Datacenter SP1 64 bits ;
- Microsoft Windows Server 2008 R2 Enterprise 64 bits ;
- Microsoft Windows Server 2008 R2 Enterprise SP1 64 bits ;
- Microsoft Windows Server 2008 R2 Foundation 64 bits ;
- Microsoft Windows Server 2008 R2 Foundation SP1 64 bits ;
- Microsoft Windows Server 2008 R2 SP1 Core Mode 64 bits ;
- Microsoft Windows Server 2008 R2 Standard 64 bits ;
- Microsoft Windows Server 2008 R2 Standard SP1 64 bits ;
- Microsoft Windows Server 2012 Server Core 64 bits ;
- Microsoft Windows Server 2012 Datacenter 64 bits ;
- Microsoft Windows Server 2012 Essentials 64 bits ;
- Microsoft Windows Server 2012 Foundation 64 bits ;
- Microsoft Windows Server 2012 Standard 64 bits ;
- Microsoft Windows Server 2012 R2 Server Core 64 bits ;
- Microsoft Windows Server 2012 R2 Datacenter 64 bits ;

- Microsoft Windows Server 2012 R2 Essentials 64 bits ;
- Microsoft Windows Server 2012 R2 Foundation 64 bits ;
- Microsoft Windows Server 2012 R2 Standard 64 bits ;
- Windows Storage Server 2008 R2 64 bits ;
- Windows Storage Server 2012 64 bits ;
- Windows Storage Server 2012 R2 64 bits ;
- Windows Server 2016 Datacenter Édition 64 bits ;
- Windows Server 2016 Standard Édition 64 bits ;

Serveur de bases de données (peut être installé sur une autre machine) :

- Microsoft SQL Server® 2008 Express 32 bits ;
- Microsoft SQL 2008 R2 Express 64 bits ;
- Microsoft SQL 2012 Express 64 bits ;
- Microsoft SQL 2014 Express 64 bits ;
- Microsoft SQL Server 2008 (toutes les versions) 32 bits/64 bits ;
- Microsoft SQL Server 2008 R2 (toutes les versions) 64 bits ;
- Microsoft SQL Server 2008 R2 Service Pack 2 64 bits ;
- Microsoft SQL Server 2012 (toutes les versions) 64 bits ;
- Microsoft SQL Server 2014 (toutes les versions) 64 bits ;
- Microsoft SQL Server 2016 (toutes les versions) 64 bits ;
- Microsoft Azure SQL Database ;
- MySQL 5.5 32 bits/64 bits ;
- MySQL Enterprise 5.5 32 bits/64 bits ;

- MySQL 5.6 32 bits/64 bits ;
- MySQL Enterprise 5.6 32 bits/64 bits ;
- MySQL 5.7 32 bits/64 bits ;
- MySQL Enterprise 5.7 32 bits/64 bits.

Plateformes virtuelles prises en charge :

- VMware vSphere™ 5.5 ;
- VMware vSphere 6 ;
- VMware™ Workstation 12.x Pro ;
- Microsoft Hyper-V® Server 2008 ;
- Microsoft Hyper-V Server 2008 R2 ;
- Microsoft Hyper-V Server 2008 R2 SP1 ;
- Microsoft Hyper-V Server 2012 ;
- Microsoft Hyper-V Server 2012 R2 ;
- Microsoft Virtual PC 2007 (6.0.156.0) ;
- Citrix® XenServer® 6.2 ;
- Citrix XenServer 6.5 ;
- Citrix XenServer 7 ;
- Parallels Desktop 11;
- Oracle® VM VirtualBox 4.0.4-70112 (prise en charge des systèmes d'exploitation invités Windows).

Pour installer le Serveur d'administration sur les appareils dotés du système d'exploitation Microsoft Windows Server 2008, il est nécessaire d'utiliser le paquet d'installation "lite". Avant d'installer le Serveur d'administration, il faut installer indépendamment la base de données, par exemple, Microsoft SQL Server 2014.

Kaspersky Security Center 10 Web Console

Configuration matérielle :

- Processeur avec 1 GHz ou plus. La cadence minimale du processeur avec un système d'exploitation 64 bits est de 1,4 GHz.
- Mémoire vive : 512 MO.
- Espace disque disponible : 1 GO.

Configuration logicielle :

- Pour fonctionner avec un système d'exploitation Microsoft Windows sur lequel est installé le serveur d'administration de Kaspersky Security Center version Service Pack 2 :
 - Microsoft Windows 10 Famille 32 bits/64 bits ;
 - Microsoft Windows 10 Professionnel 32 bits/64 bits ;
 - Microsoft Windows 10 Entreprise 32 bits/64 bits ;
 - Microsoft Windows 10 Éducation 32 bits/64 bits ;
 - Microsoft Windows 10 Pro RS1 32 bits/64 bits ;
 - Microsoft Windows 10 Entreprise RS1 32 bits/64 bits ;
 - Microsoft Windows 10 Education RS1 32 bits/64 bits ;
 - Microsoft Windows 10 Pro RS2 32 bits/64 bits ;
 - Microsoft Windows 10 Entreprise RS2 32 bits/64 bits ;
 - Microsoft Windows 10 Education RS2 32 bits/64 bits ;
 - Microsoft Windows 8.1 Professionnel 32 bits/64 bits ;
 - Microsoft Windows 8.1 Entreprise 32 bits/64 bits ;
 - Microsoft Windows 8 Professionnel 32 bits/64 bits ;
 - Microsoft Windows 8 Entreprise 32 bits/64 bits ;

- Microsoft Windows 7 Professionnel SP1 32 bits/64 bits ;
- Microsoft Windows 7 Entreprise SP1 32 bits/64 bits ;
- Microsoft Windows 7 Édition Intégrale SP1 32 bits/64 bits ;
- Microsoft Small Business Server 2008 Standard 64 bits ;
- Microsoft Small Business Server 2008 Premium 64 bits ;
- Microsoft Small Business Server 2011 Essentials 64 bits ;
- Microsoft Small Business Server 2011 Premium Add-on 64 bits ;
- Microsoft Small Business Server 2011 Standard 64 bits ;
- Microsoft Windows Server® 2008 Datacenter SP1 32 bits/64 bits ;
- Microsoft Windows Server 2008 Entreprise SP1 32 bits/64 bits ;
- Microsoft Windows Server 2008 Foundation SP2 32 bits/64 bits ;
- Microsoft Windows Server 2008 SP1 32 bits/64 bits ;
- Microsoft Windows Server 2008 Standard SP1 32 bits/64 bits ;
- Microsoft Windows Server 2008 ;
- Windows Server 2008 SP1 ;
- Microsoft Windows Server 2008 R2 Server Core 64 bits ;
- Microsoft Windows Server 2008 R2 Datacenter 64 bits ;
- Microsoft Windows Server 2008 R2 Datacenter SP1 64 bits ;
- Microsoft Windows Server 2008 R2 Entreprise 64 bits ;
- Microsoft Windows Server 2008 R2 Entreprise SP1 64 bits ;
- Microsoft Windows Server 2008 R2 Foundation 64 bits ;
- Microsoft Windows Server 2008 R2 Foundation SP1 64 bits ;

- Microsoft Windows Server 2008 R2 SP1 Core Mode 64 bits ;
- Microsoft Windows Server 2008 R2 Standard 64 bits ;
- Microsoft Windows Server 2008 R2 Standard SP1 64 bits ;
- Microsoft Windows Server 2012 Server Core 64 bits ;
- Microsoft Windows Server 2012 Datacenter 64 bits ;
- Microsoft Windows Server 2012 Essentials 64 bits ;
- Microsoft Windows Server 2012 Foundation 64 bits ;
- Microsoft Windows Server 2012 Standard 64 bits ;
- Microsoft Windows Server 2012 R2 Server Core 64 bits ;
- Microsoft Windows Server 2012 R2 Datacenter 64 bits ;
- Microsoft Windows Server 2012 R2 Essentials 64 bits ;
- Microsoft Windows Server 2012 R2 Foundation 64 bits ;
- Microsoft Windows Server 2012 R2 Standard 64 bits ;
- Windows Storage Server 2008 R2 64 bits ;
- Windows Storage Server 2012 64 bits ;
- Windows Storage Server 2012 R2 64 bits ;
- Windows Server 2016 Datacenter Édition 64 bits ;
- Windows Server 2016 Standard Édition 64 bits ;
- Debian GNU/Linux® 7.x 32 bits ;
- Debian GNU/Linux 7.x 64 bits ;
- Ubuntu Server 14.04 LTS 32 bits ;
- Ubuntu Server 14.04 LTS 64 bits ;
- CentOS 6.x (jusqu'à 6.6) 64 bits.

Kaspersky Security Center 10 Web Console ne prend pas en charge les versions des systèmes d'exploitation fonctionnant avec systemd, par exemple Fedora® 17.

Serveur Internet :

- Apache 2.4.25 (pour Windows) 32 bits ;
- Apache 2.4.25 (pour Linux) 32 bits/64 bits.

Pour utiliser Kaspersky Security Center 10 Web Console, vous pouvez ouvrir l'un des navigateurs suivants :

- Microsoft Internet Explorer® 9.0 et versions ultérieures ;
- Microsoft® Edge ;
- Chrome™ 53 et versions ultérieures ;
- Firefox™ 47 et versions ultérieures ;
- Safari® 8 sous Mac OS X 10.10 (Yosemite) ;
- Safari 9 sous Mac OS X 10.11 (El Capitan).

Serveur des appareils mobiles iOS Mobile Device Management (MDM iOS)

Configuration matérielle :

- Processeur avec 1 GHz ou plus. La cadence minimale du processeur avec un système d'exploitation 64 bits est de 1,4 GHz.
- Mémoire vive : 2 GO.
- Espace disque disponible : 2 GO.

Configuration logicielle : système d'exploitation Microsoft Windows (la version du système d'exploitation prise en charge est fixée par les exigences du Serveur d'administration).

Serveur des appareils mobiles Exchange ActiveSync

Les configurations logicielles et matérielles pour le Serveur des appareils mobiles Exchange ActiveSync sont entièrement incluses dans les exigences pour le serveur Microsoft Exchange Server.

L'utilisation de Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 et Microsoft Exchange Server 2013 est prise en charge.

Console d'administration Kaspersky

Configuration matérielle :

- Processeur avec 1 GHz ou plus. La cadence minimale du processeur avec un système d'exploitation 64 bits est de 1,4 GHz.
- Mémoire vive : 512 MO.
- Espace disque disponible : 1 GO.

Configuration logicielle :

- Système d'exploitation Microsoft Windows (la version du système d'exploitation prise en charge est fixée par les exigences du Serveur d'administration).
- Microsoft Management Console version 2.0 ;
- Microsoft Windows Installer 4.5 ;
- Microsoft Internet Explorer 7.0 et plus lors du fonctionnement avec Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 ou Microsoft Windows Vista® ;
- Microsoft Internet Explorer 8.0 et plus lors du fonctionnement avec Microsoft Windows 7 ;
- Microsoft Internet Explorer 10.0 et plus lors du fonctionnement avec Microsoft Windows 8 et 10 ;
- Microsoft Edge pour Microsoft Windows 10.

Agent d'administration

Configuration matérielle :

- Processeur avec 1 GHz ou plus. La cadence minimale du processeur avec un système d'exploitation 64 bits est de 1,4 GHz.
- Mémoire vive : 512 MO.
- Espace disque disponible : 1 GO.

Si l'appareil hôte de l'Agent d'administration joue également le rôle d'agent de mises à jour, il doit répondre aux prérequis matériels suivants :

- Processeur avec 1 GHz ou plus. La cadence minimale du processeur avec un système d'exploitation 64 bits est de 1,4 GHz.
- Mémoire vive : 1 GO.
- Espace disque disponible : 4 GO.

Configuration logicielle :

- Windows Embedded POSReady 7 32 bits/64 bits ;
- Windows Embedded Standard 7 SP1 32 bits/64 bits ;
- Windows Embedded 8 Standard 32 bits/64 bits ;
- Windows Embedded 8 Industry Pro 32 bits/64 bits ;
- Windows Embedded 8 Industry Enterprise 32 bits/64 bits ;
- Windows Embedded 8.1 Industry Pro 32 bits/64 bits ;
- Windows Embedded 8.1 Industry Enterprise 32 bits/64 bits ;
- Windows Embedded 8.1 Industry Update 32 bits/64 bits ;
- Windows 10 Famille 32 bits/64 bits ;
- Windows 10 Professionnel 32 bits/64 bits ;
- Windows 10 Entreprise 32 bits/64 bits ;
- Windows 10 Éducation 32 bits/64 bits ;
- Windows 10 Édition familiale RS1 32 bits/64 bits ;
- Windows 10 Pro RS1 32 bits/64 bits ;
- Windows 10 Entreprise RS1 32 bits/64 bits ;
- Windows 10 Éducation RS1 32 bits/64 bits ;
- Windows 10 Édition familiale RS2 32 bits/64 bits ;

- Windows 10 Pro RS2 32 bits/64 bits ;
- Windows 10 Entreprise RS2 32 bits/64 bits ;
- Windows 10 Éducation RS2 32 bits/64 bits ;
- Microsoft Windows 2000 Server ;
- Windows 8.1 Professionnel 32 bits/64 bits ;
- Windows 8.1 Entreprise 32 bits/64 bits ;
- Windows 8 Professionnel 32 bits/64 bits ;
- Windows 8 Entreprise 32 bits/64 bits ;
- Windows 7 Professionnel SP1 32 bits/64 bits ;
- Windows 7 Entreprise SP1 32 bits/64 bits ;
- Windows Édition Intégrale SP1 32 bits/64 bits ;
- Windows 7 Professionnel 32 bits/64 bits ;
- Windows 7 Entreprise 32 bits/64 bits ;
- Windows 7 Édition Intégrale 32 bits/64 bits ;
- Windows 7 Édition Familiale Basique 32 bits/64 bits ;
- Windows 7 Premium 32 bits/64 bits ;
- Windows Vista Business SP1 32 bits/64 bits ;
- Windows Vista Entreprise SP1 32 bits/64 bits ;
- Windows Vista Édition Intégrale SP1 32 bits/64 bits ;
- Windows Vista Business SP2 32 bits/64 bits ;
- Windows Vista Entreprise SP2 32 bits/64 bits ;
- Windows Vista Édition Intégrale SP2 32 bits/64 bits ;
- Windows XP Professionnel SP3 32 bits ;

- Windows XP Professionnel SP2 32 bits/64 bits ;
- Windows XP Édition familiale SP3 32 bits ;
- Essential Business Server 2008 64 bits ;
- Small Business Server 2003 Standard SP1 32 bits ;
- Small Business Server 2003 Premium SP1 32 bits ;
- Small Business Server 2008 Standard 64 bits ;
- Small Business Server 2008 Premium 64 bits ;
- Small Business Server 2011 Essentials 64 bits ;
- Small Business Server 2011 Premium Add-on 64 bits ;
- Small Business Server 2011 Standard 64 bits ;
- Windows Home Server 2011 64 bits ;
- Windows MultiPoint™ Server 2011 64 bits ;
- Windows Server 2003 Entreprise SP2 32 bits/64 bits ;
- Windows Server 2003 Standard SP2 32 bits/64 bits ;
- Windows Server 2003 R2 Entreprise SP2 32 bits/64 bits ;
- Windows Server 2003 R2 Standard SP2 32 bits/64 bits ;
- Windows Server 2008 Datacenter SP1 32 bits/64 bits ;
- Windows Server 2008 Entreprise SP1 32 bits/64 bits ;
- Windows Server 2008 Foundation SP2 32 bits/64 bits ;
- Windows Server 2008 SP1 Server Core 32 bits/64 bits ;
- Windows Server 2008 Standard SP1 32 bits/64 bits ;
- Windows Server 2008 32 bits/64 bits ;
- Windows Server 2008 R2 Server Core 64 bits ;

- Windows Server 2008 R2 Datacenter 64 bits ;
- Windows Server 2008 R2 Datacenter SP1 64 bits ;
- Windows Server 2008 R2 Enterprise 64 bits ;
- Windows Server 2008 R2 Enterprise SP1 64 bits ;
- Windows Server 2008 R2 Foundation 64 bits ;
- Windows Server 2008 R2 Foundation SP1 64 bits ;
- Windows Server 2008 R2 SP1 Core Mode 64 bits ;
- Windows Server 2008 R2 Standard 64 bits ;
- Windows Server 2008 R2 Standard SP1 64 bits ;
- Windows Server 2012 Server Core 64 bits ;
- Windows Server 2012 Datacenter 64 bits ;
- Windows Server 2012 Essentials 64 bits ;
- Windows Server 2012 Foundation 64 bits ;
- Windows Server 2012 Standard 64 bits ;
- Windows Server 2012 R2 Server Core 64 bits ;
- Windows Server 2012 R2 Datacenter 64 bits ;
- Windows Server 2012 R2 Essentials 64 bits ;
- Windows Server 2012 R2 Foundation 64 bits ;
- Windows Server 2012 R2 Standard 64 bits ;
- Windows Server 2016 Datacenter Édition ;
- Windows Server 2016 Standard Édition ;
- Windows Nano Server 2016 ;
- Windows Storage Server 2008 R2 64 bits ;

- Windows Storage Server 2012 64 bits ;
- Windows Storage Server 2012 R2 64 bits ;
- Debian GNU/Linux 8.x 32 bits ;
- Debian GNU/Linux 8.x 64 bits ;
- Debian GNU/Linux 7.x (jusqu'à 7.8) 32 bits ;
- Debian GNU/Linux 7.x (jusqu'à 7.8) 64 bits ;
- Ubuntu Server 16.04 LTS x32 32 bits ;
- Ubuntu Server 16.04 LTS x64 64 bits ;
- Ubuntu Server 14.04 LTS x32 32 bits ;
- Ubuntu Server 14.04 LTS x64 64 bits ;
- Ubuntu Desktop 16.04 LTS x32 32 bits ;
- Ubuntu Desktop 16.04 LTS x64 64 bits ;
- Ubuntu Desktop 14.04 LTS x32 32 bits ;
- Ubuntu Desktop 14.04 LTS x64 64 bits ;
- CentOS 6.x (jusqu'à 6.6) 64 bits ;
- CentOS 7.0 64 bits ;
- Red Hat Enterprise Linux Server 7.0 64 bits ;
- SUSE Linux Enterprise Server 12 64 bits ;
- SUSE Linux Enterprise Desktop 12 64 bits ;
- Mac OS X® 10.4 (Tiger®) ;
- Mac OS X 10.5 (Leopard®) ;
- Mac OS X 10.6 (Snow Leopard®) ;
- OS X 10.7 (Lion) ;

- OS X 10.8 (Mountain Lion) ;
- OS X 10.9 (Mavericks) ;
- OS X 10.10 (Yosemite) ;
- OS X 10.11 (El Capitan) ;
- macOS® Sierra (10.12) ;
- VMware vSphere™ 5.5 ;
- VMware vSphere 6 ;
- VMware Workstation 9.x ;
- VMware Workstation 10.x ;
- VMware Workstation 11.x ;
- VMware Workstation 12.x Pro ;
- Microsoft Hyper-V Server 2008 ;
- Microsoft Hyper-V Server 2008 R2 ;
- Microsoft Hyper-V Server 2008 R2 SP1 ;
- Microsoft Hyper-V Server 2012 ;
- Microsoft Hyper-V Server 2012 R2 ;
- Citrix XenServer 6.2 ;
- Citrix XenServer 6.5 ;
- Citrix XenServer 7.

Vous pouvez obtenir les informations sur la dernière version des configurations logicielles et matérielles sur le site Internet du Support Technique, sur la page de Kaspersky Security Center, dans la section Configuration requise.

<http://support.kaspersky.com/fr/ksc10#requirements>).

Interface de l'application

Cette section comprend des descriptions des éléments principaux de l'interface de Kaspersky Security Center, ainsi que de sa configuration.

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 appareils clients sont exécutées depuis le poste de travail de l'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.

La Console d'administration permet de se connecter au Serveur d'administration distant par Internet.

Pour travailler localement avec les appareils clients, l'application prévoit la possibilité d'installer une connexion à distance avec l'appareil par la Console d'administration à l'aide de l'application standard Microsoft Windows "Connexion en cours au poste de travail distant".

Afin d'utiliser cette possibilité, il est nécessaire d'autoriser la connexion à distance au poste de travail sur l'appareil client.

Dans cette section

Fenêtre principale de l'application	47
Arborescence de la console	49
Zone de travail	54
Groupe du filtrage de données	59
Menu contextuel	61
Configuration de l'interface	61

Fenêtre principale de l'application

La fenêtre principale de l'application (cf. ill. ci-dessous) contient le menu, la barre d'outils, l'arborescence de la console 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.

L'ensemble des boutons dans la barre d'outils assure un accès direct à certains points du menu principal. Les boutons 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 du noeud (du dossier) de l'arborescence de la console auquel appartient la zone de travail et des fonctions qu'elle assure.

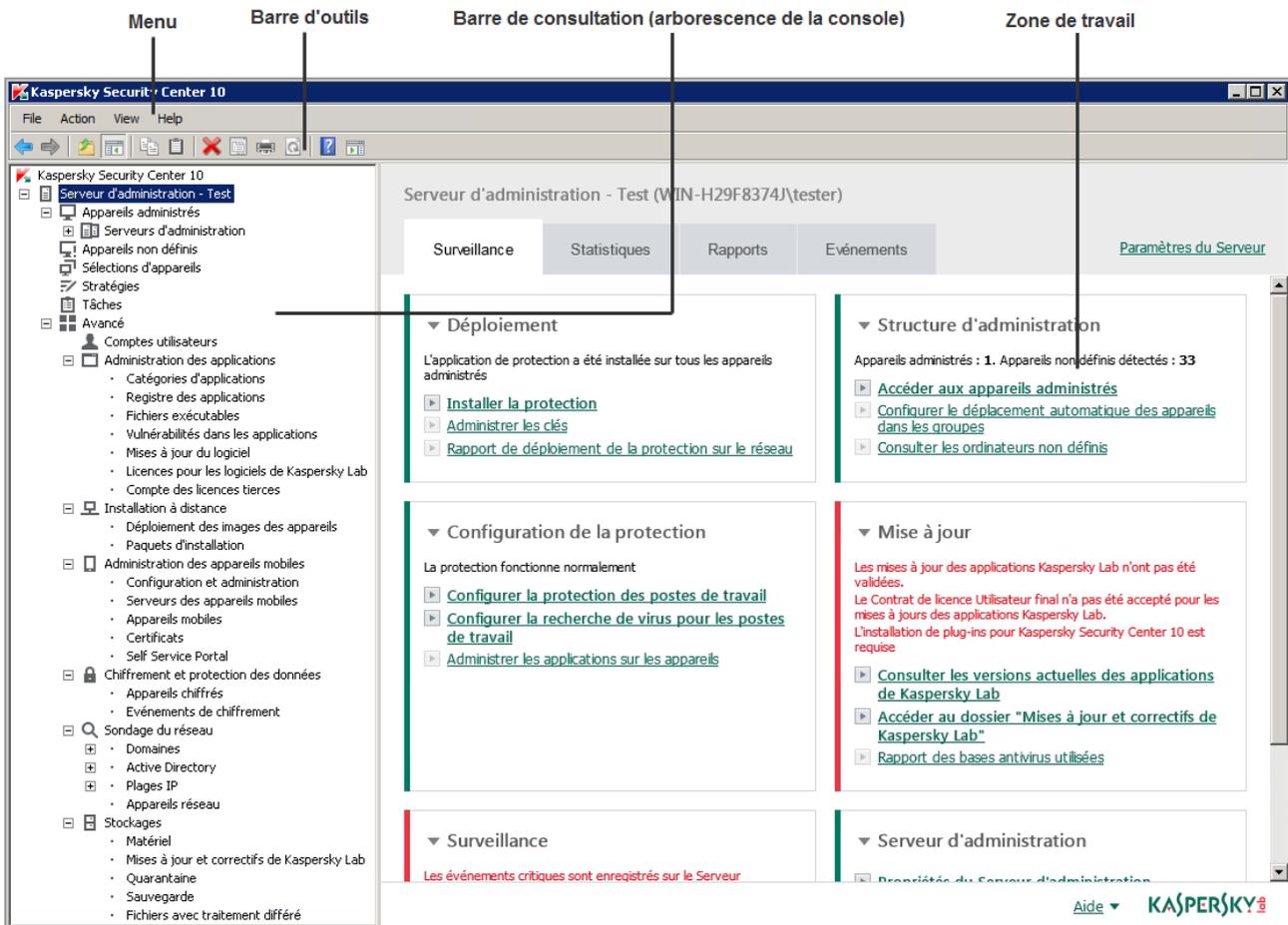


Illustration 1 Fenêtre principale de l'application Kaspersky Security Center

Arborescence de la console

L'arborescence de la console (cf. ill. ci-dessous) est conçue pour refléter la hiérarchie (formée dans le réseau) des Serveurs d'administration, de la structure de leurs groupes d'administration, ainsi que d'autres objets de l'application, tels que **Stockages** et **Administration des applications**. L'étendue des noms de Kaspersky Security Center peut inclure plusieurs sections avec les noms des serveurs qui correspondent aux Serveurs d'administration installés et inclus dans la structure du réseau.

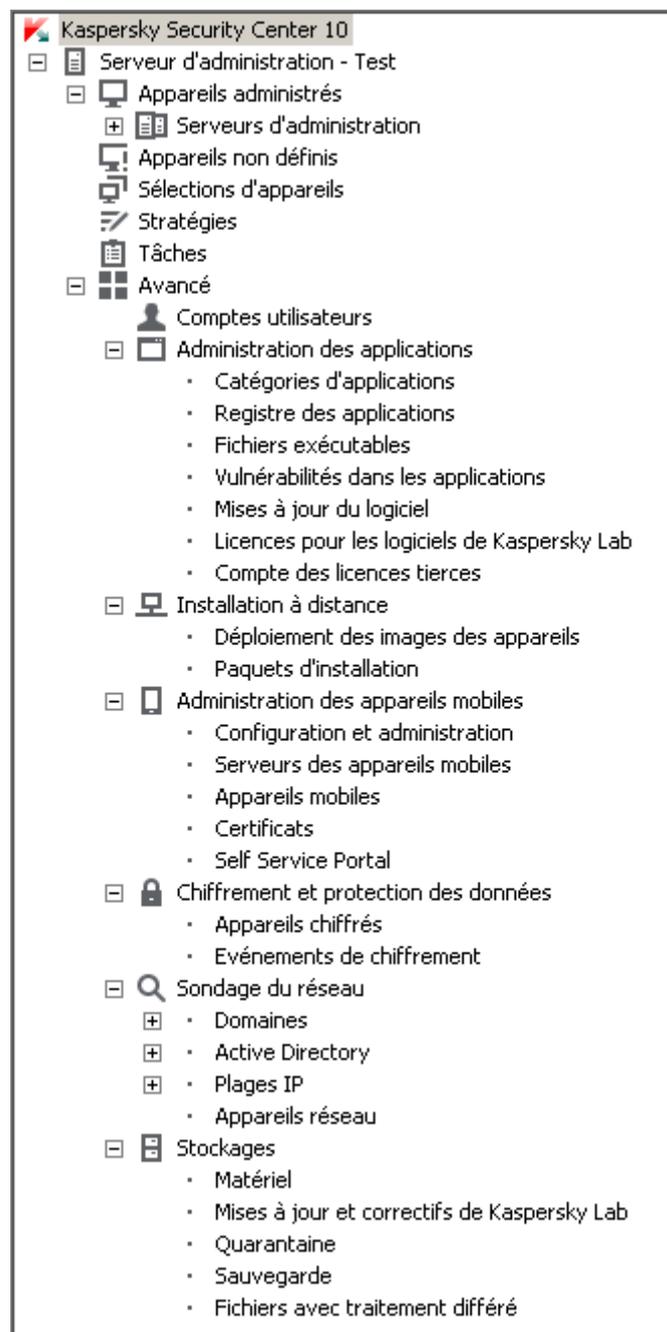


Illustration 2 Arborescence de la console

Entrée Serveur d'administration

La section **Serveur d'administration** : <Nom de l'appareil> est un conteneur et reflète la structure du Serveur d'administration indiqué.

Le nœud **Serveur d'administration** contient des informations récapitulatives sur l'état actuel de l'application et des appareils administrés par le Serveur d'administration. Les informations sur la zone de travail se trouvent dans les onglets suivants :

- **Surveillance.** L'onglet **Surveillance** affiche en temps réel des informations sur le fonctionnement de l'application et sur l'état actuel des appareils clients. Les messages importants destinés à l'administrateur (par exemple sur des vulnérabilités, sur des erreurs ou sur la détection de virus) sont mis en couleur. Les liens de l'onglet **Surveillance** permettent d'effectuer des tâches typiques d'administrateur (par exemple, installer et configurer l'application de protection sur les appareils clients), ainsi que d'accéder à d'autres dossiers de l'arborescence de la console.
- **Statistiques.** Contient un ensemble de diagrammes regroupés par thèmes (état de la protection, statistique anti-virus, mises à jour, etc.). Des diagrammes visuels présentent des informations à jour sur le fonctionnement de l'application et l'état des appareils clients.
- **Rapports.** Contient des modèles de rapports constitués par l'application. Dans l'onglet, vous pouvez constituer des rapports à partir des modèles prévus et créer vos propres modèles de rapports.
- **Événements.** Contient des écritures d'événements enregistrés pendant le fonctionnement de l'application. Pour faciliter la lecture et le tri, les enregistrements sont répartis selon des sélections thématiques. Dans l'onglet, vous pouvez examiner les sélections des événements créées automatiquement et créer vos propres sélections.

Dossiers du nœud Serveur d'administration

Le nœud **Serveur d'administration** – <Nom de l'appareil> inclut les dossiers suivants :

- **Appareils administrés.** Le dossier est conçu pour conserver, refléter, configurer et modifier la structure des groupes d'administration, les stratégies de groupe et les tâches de groupe.
- **Sélections d'appareils.** Le dossier est conçu pour une sélection rapide d'appareils correspondant à des critères définis (sélections d'appareils), parmi tous les appareils

administrés. Par exemple, vous pouvez sélectionner rapidement les appareils sur lesquels l'application de protection n'est pas installée et accéder à ces appareils (voir leurs listes). Avec les appareils sélectionnés, vous pouvez effectuer des actions, par exemple, leur affecter des tâches. Vous pouvez utiliser les sélections fournies et créer vos propres sélections (d'utilisateur).

- **Appareils non définis.** Ce dossier contient une liste d'appareils qui ne font partie d'aucun groupe d'administration. Vous pouvez effectuer des annonces avec des appareils non définis : les extraire du groupe d'administration et installer des applications sur ces appareils.
- **Stratégies.** Ce dossier est conçu pour la consultation et la création de stratégies.
- **Tâches.** Ce dossier est conçu pour la consultation et la création de tâches.
- **Avancé.** Ce dossier contient un ensemble de dossiers joints correspondant à différents groupes de fonctionnalités de l'application.

Dossier Avancé. Déplacement des dossiers dans l'arborescence de la console

Le dossier **Avancé** contient les dossiers suivants :

- **Comptes utilisateurs.** Ce dossier contient une liste de comptes utilisateurs du réseau.
- **Administration des applications.** Le dossier est conçu pour administrer les applications installées sur les appareils du réseau. Le dossier **Administration des applications** contient aussi les dossiers joints suivants :
 - **Catégories d'applications.** Conçu pour travailler avec les catégories d'utilisateurs des applications.
 - **Registre des applications.** Contient la liste des applications sur les appareils avec l'Agent d'administration installé.
 - **Fichiers exécutables.** Contient la liste des fichiers exécutables enregistrés sur les appareils clients avec l'Agent d'administration installé.
 - **Vulnérabilités dans les applications.** Contient la liste des vulnérabilités dans les applications sur les appareils avec l'Agent d'administration installé.

- **Mises à jour du logiciel.** Contient la liste des mises à jour des applications, mises à jour reçues par le Serveur d'administration qui peuvent être déployées sur les appareils.
- **Licence pour une application Kaspersky Lab.** Contient la liste des clés accessibles pour les applications Kaspersky Lab. Dans l'espace de travail du dossier, vous pouvez ajouter de nouvelles clés dans le stockage de clés, répartir des clés sur les appareils administrés et consulter un rapport sur l'utilisation des clés.
- **Utilisation des licences tierces.** Comporte une liste des groupes des applications sous licence. À l'aide des groupes d'applications sous licence, vous pouvez suivre l'utilisation des licences sur les applications tierces (et non Kaspersky Lab) et la violation des restrictions sur les licences.
- **Installation à distance.** Le dossier est conçu pour administrer l'installation à distance des systèmes d'exploitation et des applications. Le dossier **Installation à distance** contient aussi les dossiers joints suivants :
 - **Déploiement des images des appareils** Conçu pour déployer les images des systèmes d'exploitation sur les appareils.
 - **Paquets d'installation.** Contient la liste des paquets d'installation qui peuvent être utilisés pour l'installation à distance des applications sur les appareils.
- **Gestion des appareils mobiles.** Ce dossier est conçu pour la gestion des appareils mobiles. Le dossier **Gestion des appareils mobiles** contient aussi les dossiers joints suivants :
 - **Appareils mobiles.** Conçu pour la gestion des appareils mobiles KES, Exchange ActiveSync et MDM iOS.
 - **Certificats.** Conçu pour la gestion des certificats des appareils mobiles.
- **Chiffrement et protection des données.** Le dossier est conçu pour administrer le processus de chiffrement des données sur les disques durs et les disques amovibles.

- **Sondage du réseau.** Le dossier est conçu pour afficher le réseau où le Serveur d'administration est installé. Le Serveur d'administration obtient les informations relatives à la structure du réseau et aux appareils qu'elle héberge lors des sondages réguliers du réseau Windows, des plages IP ou d'Active Directory® ayant lieu dans le réseau de l'entreprise. Les résultats des sondages s'affichent dans les espaces de travail des dossiers suivants : **Domaines**, **Plages IP** et **Active Directory**.
- **Stockages.** Le dossier permet de manipuler les objets utilisés pour la surveillance de l'état des appareils et les entretenir. Le dossier **Stockages** contient aussi les dossiers joints suivants :
 - **Mises à jour et correctifs de Kaspersky Lab.** Contient la liste des mises à jour reçues par le Serveur d'administration qui peuvent être déployées sur les appareils.
 - **Matériel.** Contient la liste du matériel connecté au réseau de l'entreprise.
 - **Quarantaine.** Contient la liste des objets placés par les applications antivirus dans les dossiers de quarantaine des appareils.
 - **Sauvegarde.** Ce dossier contient la liste des copies de sauvegarde des fichiers supprimés et modifiés au cours de la désinfection sur les appareils.
 - **Fichiers avec traitement différé.** Contient la liste des fichiers pour lesquels les applications antivirus ont décidé le traitement ultérieur.

Vous pouvez modifier l'ensemble de dossiers placés dans le dossier **Avancé**. Ces dossiers utilisés activement peuvent être déplacés du dossier **Avancé** vers un niveau supérieur. Les dossiers utilisés rarement peuvent être placés dans le dossier **Avancé**.

► *Pour extraire un dossier imbriqué du dossier **Avancé**, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier imbriqué à déplacer du dossier **Avancé**.
2. Dans le menu contextuel du dossier imbriqué, sélectionnez le point **Affichage** → **Déplacer depuis le dossier Avancés**.

Vous pouvez également extraire le dossier imbriqué du dossier **Avancé** dans l'espace de travail de ce même dossier **Avancé**, par le lien **Déplacer depuis le dossier Avancés** dans le groupe avec le nom du dossier imbriqué.

► *Pour déplacer un dossier vers le dossier **Avancé**, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier imbriqué à déplacer vers le dossier **Avancé**.
2. Dans le menu contextuel, sélectionnez le point **Affichage** → **Déplacer vers le dossier Avancés**.

Zone de travail

L'espace de travail (cf. illustration ci-dessous) contient les éléments suivants :

- listes d'objets gérés par l'administrateur à l'aide de l'application (appareils, groupes d'administration, comptes utilisateurs, stratégies, tâches, enregistrements d'événements, autres applications, etc.) (cf. section "Éléments de l'espace de travail" p. [56](#)) ;
- éléments de gestion (boutons affichant des listes de commandes, liens pour l'exécution de commandes et accès à d'autres dossiers de l'arborescence de la console) ;
- informations en format texte et graphique (messages de l'application, diagrammes dans les panneaux d'informations, informations statistiques et d'aide) (cf. section "Ensemble de groupes d'informations" p. [59](#)).

Le contenu de l'espace de travail correspond au noeud ou au dossier sélectionné dans l'arborescence de la console.

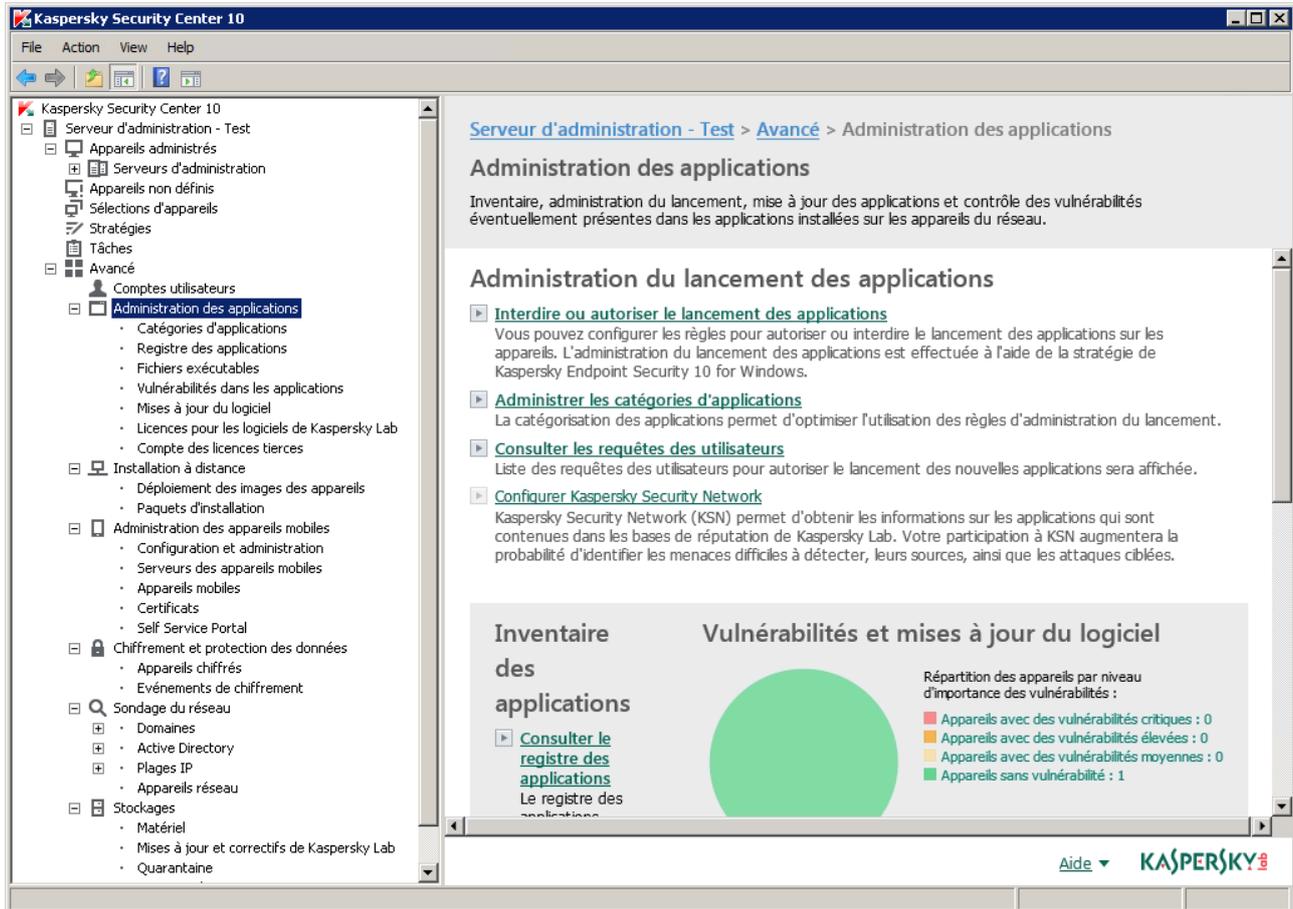


Illustration 3 Zone de travail

L'espace de travail du noeud ou du dossier peut contenir certains onglets (cf. illustration ci-dessous). Chaque onglet correspond à un groupe défini (type) d'objet ou de fonctions de l'application.

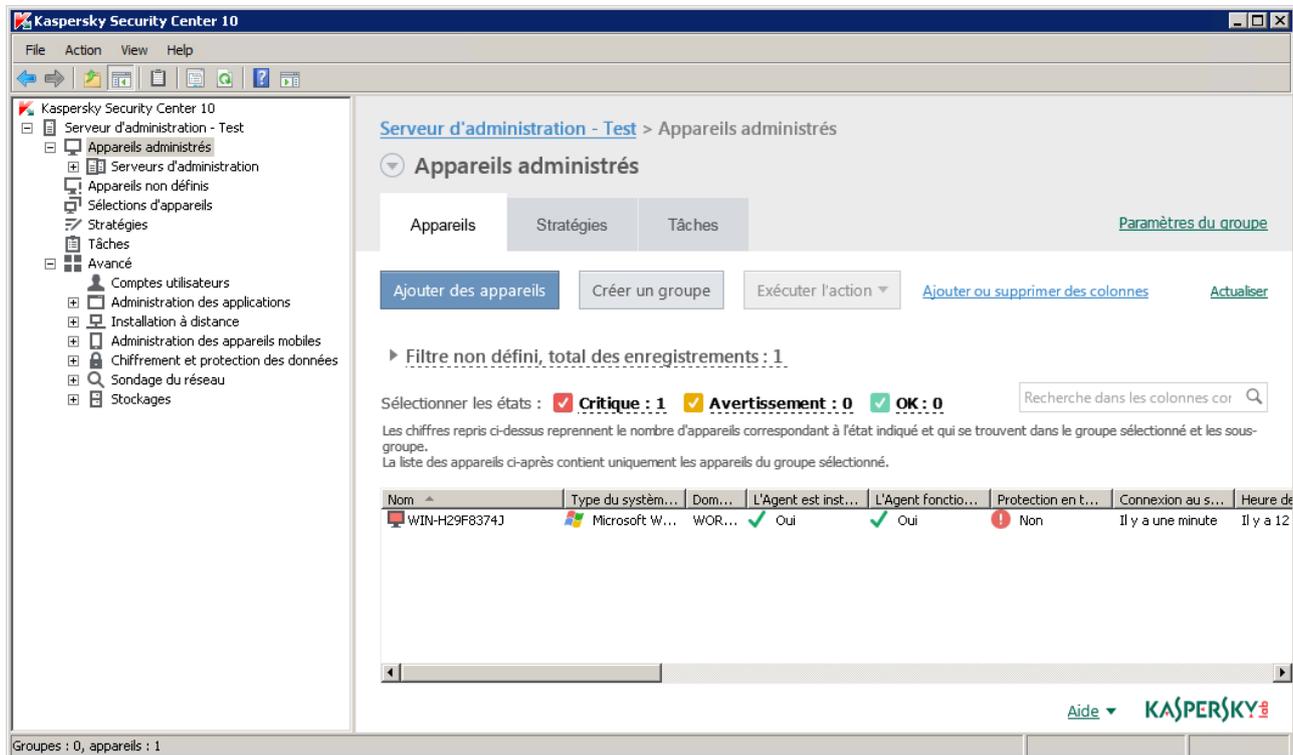


Illustration 4 Zone de travail partagée sur onglets

Dans cette section

Éléments de l'espace de travail	56
Ensemble de groupes d'informations	59

Éléments de l'espace de travail

L'espace de travail du dossier ou du noeud peut contenir les éléments suivants (cf. illustration ci-dessous).

- Groupe d'administration de la liste. Contient des boutons qui affichent des listes de commandes et des liens. Conçu pour les actions avec les objets sélectionnés dans la liste.
- Liste des objets. Contient les objets d'administration (par exemple des appareils, des comptes utilisateurs, des stratégies, des tâches). Vous pouvez trier et filtrer des objets de la liste, effectuer des actions avec ces objets à l'aide du groupe de gestion et de commandes du menu contextuel de l'objet). Vous pouvez aussi configurer un ensemble de graphiques affichés dans la liste.
- Groupe de travail avec l'objet sélectionné. Contient des informations récapitulatives sur l'objet sélectionné. Le groupe peut également contenir des liens pour des actions rapides avec l'objet sélectionné. Par exemple, le groupe de travail avec la stratégie sélectionnée contient un lien vers la fenêtre de configuration de la stratégie.

- Groupe du filtrage de données. À l'aide du groupe de filtrage, vous pouvez configurer l'affichage des objets dans la liste. Par exemple, le groupe du filtrage de données permet de configurer une liste d'appareils de manière à y afficher uniquement ceux à l'état "critique".

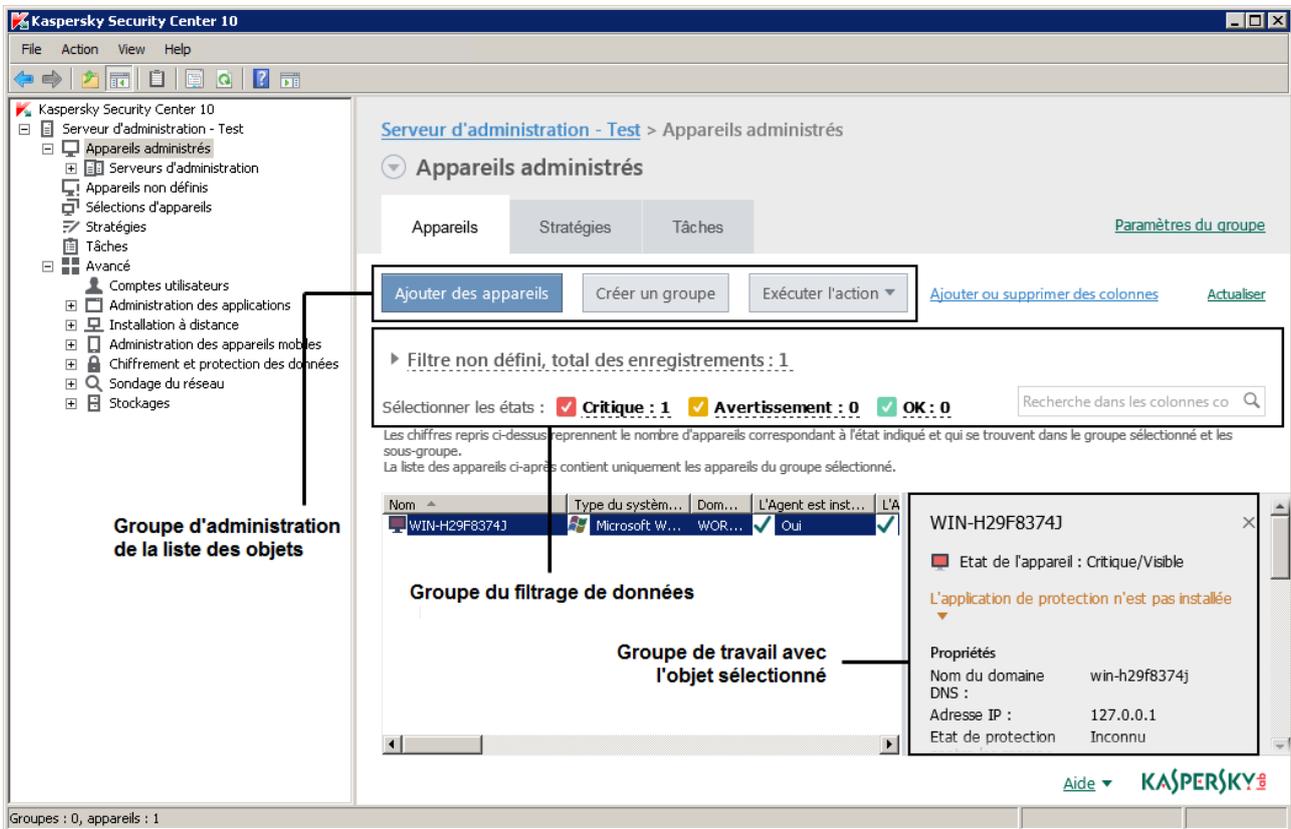


Illustration 5 Zone d'informations présentée par la liste des objets d'administration

Ensemble de groupes d'informations

Dans l'espace de travail du noeud **Serveur d'administration**, l'onglet **Statistiques** affiche des données statistiques sur des panneaux d'informations. Ces panneaux sont répartis sur quelques pages thématiques (cf. illustration ci-dessous). Vous pouvez configurer la présentation des données sur les panneaux d'informations : modifier les types de diagrammes et l'ensemble de données les concernant, modifier et ajouter des panneaux d'informations, ainsi que des pages entières dans l'onglet **Statistiques** (cf. section "**Utilisation des données statistiques**" p. [194](#)).

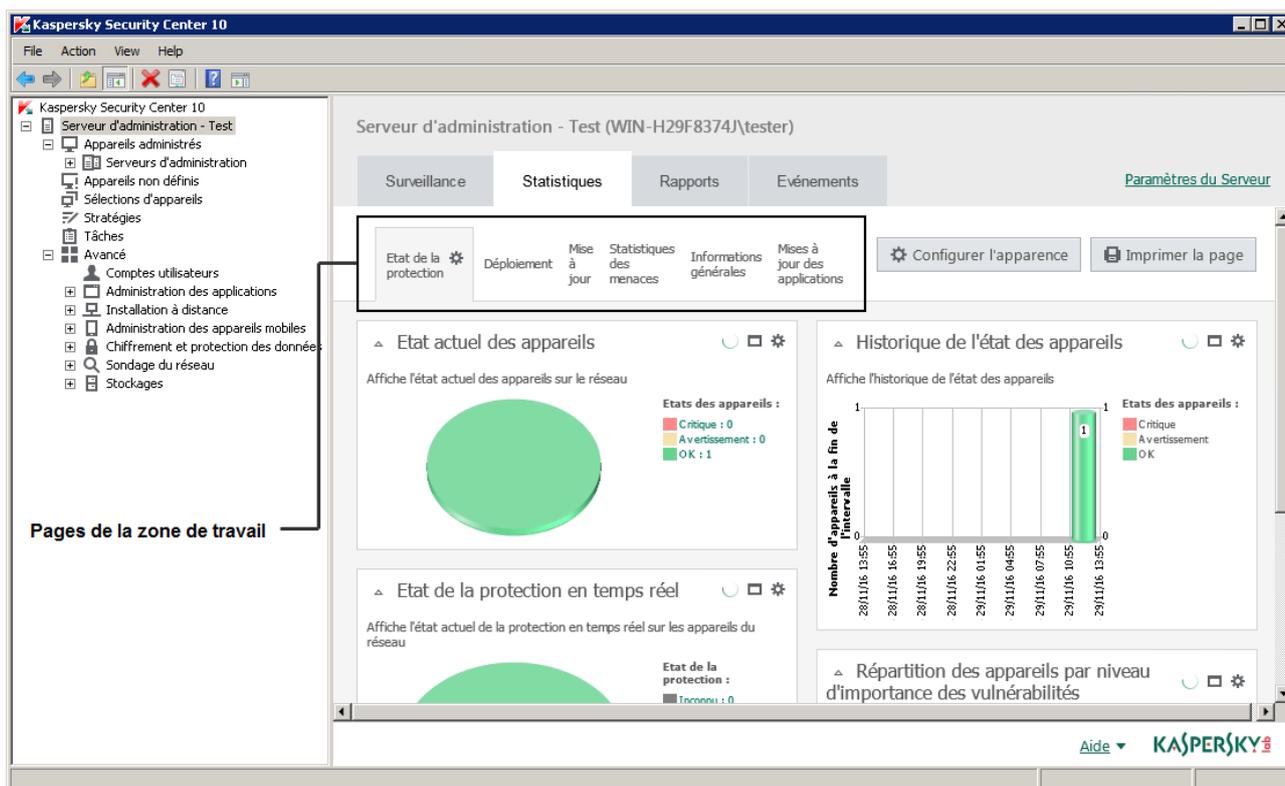


Illustration 6 Zone de travail partagée sur pages

Groupe du filtrage de données

Le *Groupe de filtrage de données* (ci -après *groupe de filtrage*) est utilisé dans les espaces de travail et dans les sections des boîtes de dialogue qui contiennent les listes des objets (par exemple, appareils, applications, vulnérabilités, utilisateurs).

Le groupe de filtrage peut contenir une ligne de recherche, un filtre et des boutons (cf. ill. ci-dessus).

The screenshot shows the 'Appareils administrés' section of an application. At the top, there's a breadcrumb 'Serveur d'administration - Test > Appareils administrés'. Below it, the title 'Appareils administrés' is followed by tabs for 'Appareils', 'Stratégies', and 'Tâches'. A 'Paramètres du groupe' link is on the right. A row of buttons includes 'Ajouter des appareils', 'Créer un groupe', 'Exécuter l'action', 'Ajouter ou supprimer des colonnes', and 'Actualiser'. A filter status line reads 'Filtre non défini, total des enregistrements : 1'. Below this, the 'Sélectionner les états' section shows three options: 'Critique : 1' (with a red checkmark), 'Avertissement : 0' (with a yellow checkmark), and 'OK : 0' (with a green checkmark). A search box on the right contains the text 'Recherche dans les colonnes contenant du texte'. Two vertical lines with labels 'Boutons' and 'Ligne de recherche' point to the filter buttons and the search box respectively.

Bloc de filtrage élargi. Configuration du filtre

Pour filtrer ces données, vous pouvez utiliser le groupe de filtrage standard ou élargi (cf. illustration ci-dessous). Dans le groupe de filtrage standard, vous pouvez filtrer les données à l'aide de la ligne de recherche et des boutons du groupe **Sélectionner les états**. Dans le groupe de filtrage élargi, vous pouvez utiliser d'autres critères de filtrage. Ces autres critères de filtrage sont accessibles en cliquant sur le lien **Configurer le filtre**.

► *Pour configurer le filtrage, procédez comme suit :*

1. Appuyez sur la zone **Filtre non défini**.

À droite de la fenêtre, le lien **Configurer le filtre** s'affiche.

2. Dans la section **Configurer le filtre**, sélectionnez les critères de filtrage.

Les critères sélectionnés apparaissent sur fond gris dans le champ **Filtre**.

3. Indiquez une valeur pour chaque critère (par exemple "*L'agent est installé*").

4. Dans le groupe **Sélectionner les états**, configurez un filtrage supplémentaire des appareils en fonction de leur état (*Critique, Avertissement, OK*).

Les appareils correspondant au filtre s'affichent dans la liste. Vous pouvez également rechercher des appareils par mots-clés et par expressions régulières (cf. section "Nouveautés" à la page [25](#)) dans le champ **Recherche**.

The image displays two screenshots of a filtering interface. The top screenshot, labeled "Groupe du filtrage de type standard", shows a search bar with the text "Recherche dans les colonnes contenant du texte" and a magnifying glass icon. Below the search bar is a button "Configurer le filtre". The bottom screenshot, labeled "Groupe du filtrage de type élargi", shows a search bar with the text "Recherche dans les colonnes contenant du texte" and a magnifying glass icon. Below the search bar are four dropdown menus: "Type:", "Protocole:", "Utilisateur:", and "Etat:". Each dropdown menu has a small square icon to its left. Above the search bars are buttons for "Ajouter ou supprimer des colonnes" and "Actualiser".

Menu contextuel

Dans l'arborescence de la console Kaspersky Security Center, chaque objet possède le menu contextuel. En plus des commandes standard du menu contextuel de Microsoft Management Console, on y retrouve des commandes complémentaires qui permettent d'exécuter des travaux avec l'objet en question. La liste des commandes complémentaires du menu contextuel qui correspondent à différents objets de l'arborescence de la console se trouve dans Applications (cf. section "Commandes du menu contextuel" p. [409](#)).

Certains objets de l'espace de travail (par exemple des appareils de la liste des appareils administrés, d'autres objets de listes) comportent également un menu contextuel avec des commandes complémentaires.

Configuration de l'interface

Vous pouvez configurer l'interface de Kaspersky Security Center :

- afficher et masquer des objets dans l'arborescence de la console, de l'espace de travail, dans les fenêtres de propriétés des objets (dossiers, sections) selon de la fonctionnalité utilisée ;
- afficher et masquer des parties de la fenêtre principale (par exemple, l'arborescence de la console, les menus standard **Actions** et **Affichage**).

► *Pour configurer l'interface de Kaspersky Security Center selon la fonctionnalité utilisée, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
2. Dans le menu de la fenêtre de l'application, sélectionnez le point **Affichage** → **Configuration de l'interface**.
3. Dans la fenêtre ouverte **Configuration de l'interface**, configurez l'affichage des éléments de l'interface à l'aide des cases suivantes :

- **Afficher l'Administration système.**

Si la case est cochée, le dossier **Installation à distance** affiche le dossier joint **Déploiement des images des appareils** et le dossier **Stockages** affiche le dossier joint **Matériel**.

Celle-ci est décochée par défaut.

- **Afficher le chiffrement et la protection des données.**

Si la case est cochée, l'administration du chiffrement des données stockées sur les appareils connectés au réseau est accessible. Quand l'application a été relancée, le dossier **Chiffrement et protection des données** apparaît dans l'arborescence de la console.

Celle-ci est décochée par défaut.

- **Afficher les paramètres Endpoint Control.**

Si la case est cochée, la section **Contrôle du bureau** de la fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security 10 for Windows affiche les sous-sections suivantes :

- **Contrôle du lancement des applications;**

- **Surveillance des vulnérabilités;**
- **Contrôle des appareils ;**
- **Contrôle Internet.**

Si la case n'est pas cochée, les sous-sections indiquées ci-dessus n'apparaissent pas dans la section **Contrôle du bureau**.

Celle-ci est décochée par défaut.

- **Afficher l'Administration des appareils mobiles.**

Si la case est cochée, la fonction **Gestion des appareils mobiles** est accessible. Quand l'application a été relancée, le dossier **Appareils mobiles** apparaît dans l'arborescence de la console.

Celle-ci est décochée par défaut.

- **Afficher les Serveurs d'administration secondaires.**

Si la case est cochée, l'arborescence de la console affiche les entrées des Serveurs d'administration secondaires et virtuels dans les groupes d'administration. Avec cela, la fonction liée avec les Serveurs d'administration secondaires et virtuels (par exemple, la création de la tâche d'installation à distance des applications sur les Serveurs d'administration secondaires) est accessible.

Par défaut, la case est cochée.

- **Afficher les sections avec les paramètres de sécurité.**

Si la case est cochée, la section **Sécurité** s'affichera dans les fenêtres des propriétés du Serveur d'administration, des groupes d'administration et d'autres objets. Ceci permettra de fournir aux utilisateurs et aux groupes d'utilisateurs les droits de travail avec les objets, autres que les valeurs par défaut.

Par défaut, la case est cochée.

4. Cliquez sur le bouton **OK**.

L'application de certaines modifications nécessite la fermeture et la réouverture de la fenêtre principale de l'application.

- ▶ *Pour configurer l'affichage d'éléments de la fenêtre principale de l'application, procédez comme suit :*
 1. Dans le menu de la fenêtre de l'application, sélectionnez le point **Affichage** → **Personnaliser**.
 2. Dans la fenêtre **Configuration de l'affichage** qui s'ouvre, configurez l'affichage à l'aide des cases à cocher.
 3. Cliquez sur le bouton **OK**.

Licence de l'application

Cette section présente les notions principales relatives à la licence de l'application.

Dans cette section

A propos du contrat de licence	65
A propos de la licence	66
A propos du certificat de licence	67
A propos de la clé	67
Options de licence de Kaspersky Security Center.....	68
A propos des restrictions de la fonctionnalité de base.....	71
A propos du code d'activation	73
A propos du fichier clé.....	73
A propos de l'abonnement.....	74

A propos du contrat de licence utilisateur final

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

Lisez attentivement les conditions du Contrat de licence avant de commencer à utiliser l'application.

Vous pouvez prendre connaissance des conditions du Contrat de licence de l'une des manières suivantes :

- Pendant l'installation du Kaspersky Security Center.
- En lisant le document license.txt. Ce document est fourni dans la distribution de l'application.

Vous acceptez les conditions du contrat de licence, en confirmant votre accord avec le texte du contrat de licence lors de l'installation de l'application. Si vous n'êtes pas d'accord avec les termes du Contrat de licence, vous devez interrompre l'installation de l'application et ne pas l'utiliser.

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 vous donne droit aux types de service suivants :

- utilisation de l'application conformément aux conditions du Contrat de licence ;
- accès au Support Technique.

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

Les types suivants de licences sont prévus :

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

La licence d'évaluation présente une courte durée de validité. Une fois que la licence expirée, Kaspersky Security Center cesse de remplir toutes ces fonctions. Pour continuer à utiliser l'application, vous devez acheter une licence commerciale.

Vous pouvez activer l'application à l'aide d'une licence d'évaluation une seule fois uniquement.

- *Commerciale* : licence payante octroyée à l'achat de l'application.

A l'expiration de la licence commerciale, l'application continue à fonctionner, mais ses fonctionnalités sont limitées (par exemple, la mise à jour des bases du Kaspersky Security Center n'est pas disponible). Pour pouvoir continuer à bénéficier de toutes les fonctionnalités du Kaspersky Security Center, vous devez renouveler la licence commerciale.

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

A propos du certificat de licence

Le *certificat de licence* est un document qui vous est transmis avec le fichier clé ou le code d'activation.

Il comporte les informations suivantes à propos de la licence :

- numéro de la commande ;
- informations relatives à l'utilisateur qui reçoit la licence ;
- informations relatives à l'application qui peut être activée à l'aide de la licence ;
- restrictions associées au nombre d'unités concernées par la licence (par exemple, le nombre d'appareils sur lesquels l'application peut être utilisée avec la licence) ;
- début de validité de la licence ;
- date de fin de la durée de validité de la licence ou durée de validité de la licence ;
- type de licence.

A propos de la clé

Une *clé* est une séquence de caractères qui vous permet d'activer puis d'utiliser une application conformément aux conditions du Contrat de licence. Elle est créée par les experts de Kaspersky Lab.

Vous pouvez ajouter la clé à l'application d'une des manières suivantes : utiliser le *fichier clé* ou saisir le *code d'activation*. Une fois ajoutée, elle s'affiche dans l'interface de l'application sous la forme d'une séquence alphanumérique unique.

Une clé peut être bloquée par Kaspersky Lab en cas de non-respect des conditions du Contrat de licence. Dans ce cas, vous devrez ajouter une autre clé pour utiliser l'application.

Une clé peut être active ou complémentaire.

La *clé active* est la clé actuellement utilisée pour faire fonctionner l'application. Une licence d'essai ou une licence commerciale peuvent être ajoutées au titre de clé active. Il ne peut pas y avoir plus d'une clé active par application.

La *clé additionnelle* est une clé qui confirme le droit d'utilisation de l'application, mais qui n'est pas utilisée pour le moment. La clé additionnelle devient automatiquement active lorsque la durée de validité de la licence associée à la clé active expire. On ne peut ajouter une clé additionnelle que s'il existe une clé active.

La clé d'une licence d'évaluation ne peut être ajoutée qu'en tant que clé active. Elle ne sera pas acceptée en tant que clé additionnelle.

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 d'appareils 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 appareils clients ;
- consultation et modification des groupes des applications sous licence existants ;
- 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 la 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>).

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 [71](#)).

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 ;
- inventaire du matériel ;

- administration des groupes des applications sous licence ;
- autorisation à distance de la connexion au poste client via le composant "Connexion Bureau à distance" de Microsoft® Windows® ;
- connexion à distance aux appareils clients à l'aide de Windows Desktop Sharing ;
- administration des rôles des utilisateurs.

L'appareil client dans le groupe "Appareils administrés" est une unité d'administration pour la fonctionnalité de l'Administration système.

La fonctionnalité Administration système comprend lors de l'inventaire des informations détaillées sur le matériel des appareils.

Lors de l'utilisation juste de la fonctionnalité de l'Administration système, le volume d'espace libre sur le disque dur doit être au moins 100 GO.

Fonctionnalité Gestion des appareils mobiles

La fonctionnalité Gestion des appareils mobiles est conçue pour administrer les appareils mobiles Exchange ActiveSync et MDM iOS.

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

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

Pour les appareils MDM iOS, les fonctions suivantes sont disponibles :

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

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

L'appareil mobile est une unité d'administration de la fonctionnalité Gestion des appareils mobiles. L'appareil mobile est considéré comme appareil administré quand il est connecté au Serveur des appareils mobiles.

A propos des restrictions de la fonctionnalité 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.

Administration des appareils mobiles

Il est impossible de créer le nouveau profil et de le désigner à l'appareil mobile (MDM iOS) 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.

Inventaire du matériel

La réception d'informations sur les nouveaux appareils n'est pas disponible à l'aide du Serveur des appareils mobiles. Avec cela, les informations sur les ordinateurs et les appareils connectés s'actualisent.

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

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

Administration des groupes des applications sous 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 appareils clients

La connexion à distance aux appareils 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 une suite unique de 20 caractères alphanumériques. Vous le saisissez pour ajouter la clé activant le Kaspersky Security Center. Vous recevez le code d'activation à l'adresse électronique que vous avez indiquée après l'achat de Kaspersky Security Center ou après la commande d'une version d'évaluation de Kaspersky Security Center.

Pour activer l'application à l'aide de ce code, vous avez besoin d'un accès à Internet pour vous connecter aux serveurs d'activation de Kaspersky Lab.

Si l'application a été activée à l'aide d'un code d'activation, dans certains cas après l'activation, l'application envoie des requêtes régulières au serveur d'activation de Kaspersky Lab pour vérifier le statut de la clé. Pour envoyer ces requêtes, un accès Internet est nécessaire.

En cas de perte du code d'activation après l'activation de l'application, vous pouvez le restaurer. Le code d'activation peut vous être utile pour vous inscrire sur Kaspersky CompanyAccount, par exemple. Pour restaurer le code d'activation, vous devez vous adresser au support technique de Kaspersky Lab (cf. section "Moyens de bénéficier du support technique" p. [370](#)).

A propos du fichier clé

Le *fichier clé* est un fichier doté d'une extension key qui vous est fourni par Kaspersky Lab. Il permet d'ajouter la clé activant l'application.

Vous recevez le fichier clé à l'adresse électronique que vous avez indiquée après l'achat de Kaspersky Security Center ou après la commande d'une version d'évaluation de Kaspersky Security Center.

Pour activer l'application à l'aide du fichier clé, il n'est pas nécessaire de se connecter aux serveurs d'activation de Kaspersky Lab.

Si le fichier clé a été accidentellement supprimé, vous pouvez le restaurer. Le fichier clé peut vous être utile pour vous inscrire sur Kaspersky CompanyAccount, par exemple.

Pour restaurer le fichier clé, vous devez effectuer l'une des opérations suivantes :

- Contacter le support technique (<http://support.kaspersky.com/fr>).
- Obtenir le fichier clé sur le site Internet de Kaspersky Lab (<https://activation.kaspersky.com/fr/>) à partir du code d'activation que vous possédez.

A propos de l'abonnement

Abonnement à Kaspersky Security Center est une commande d'utilisation de l'application avec les paramètres sélectionnés (date de fin de l'abonnement, nombre de appareils protégés).

L'abonnement à Kaspersky Security Center peut être enregistré auprès du fournisseur de services (par exemple, auprès du fournisseur d'accès à Internet). Il est possible de prolonger l'abonnement en mode manuel et automatique, ainsi que de le refuser.

L'abonnement peut être limité (par exemple pour un an) ou illimité (sans date de fin). Pour continuer à utiliser Kaspersky Security Center après la fin de l'abonnement limité, celui-ci doit être prolongé. L'abonnement illimité se prolonge automatiquement à condition d'avoir été payé en temps voulu au fournisseur de services.

Si l'abonnement est limité, une période de renouvellement à tarif préférentiel peut être instituée à la fin de la validité pour le prolonger. Au cours de cette période, la fonctionnalité de l'application est conservée. Le fournisseur de services détermine l'existence et la durée de la période de renouvellement à tarif préférentiel.

L'utilisation de Kaspersky Security Center sur abonnement nécessite l'application d'un code d'activation communiqué par le fournisseur de services.

Vous pouvez appliquer un autre code d'activation pour l'utilisation de Kaspersky Security Center uniquement après la fin de l'abonnement ou le refus de celui-ci.

Les ensembles d'actions possibles pour gérer l'abonnement peuvent varier en fonction du fournisseur de services. Celui-ci peut ne pas offrir de période de renouvellement à tarif préférentiel pour le prolongement de l'abonnement au cours de laquelle la fonctionnalité de l'application est conservée.

Les codes d'activation reçus lors de l'abonnement ne peuvent pas être utilisés pour l'activation de versions précédentes de Kaspersky Security Center.

Lors de l'utilisation de l'application sur abonnement, Kaspersky Security Center s'adresse automatiquement au serveur d'activation dans un laps de temps déterminé jusqu'à la date de fin de l'abonnement. Vous pouvez prolonger l'abonnement sur le site Internet du fournisseur de services.

Assistant de configuration initiale du Serveur d'administration

Cette section reprend les informations sur le fonctionnement de l'Assistant de configuration initiale du Serveur d'administration.

L'application Kaspersky Security Center permet de configurer un ensemble minimum de paramètres indispensables à l'établissement d'un système d'administration centralisée de la protection à l'aide de l'Assistant de configuration initiale. Pendant le fonctionnement de l'Assistant, les modifications suivantes dans l'application sont :

- Ajout des clés ou des codes à diffuser automatiquement sur les appareils dans les groupes d'administration.
- Configuration de l'interaction avec Kaspersky Security Network (KSN). KSN permet de recevoir les informations sur les applications installées sur les appareils administrés qui se trouvent dans la base de réputation de Kaspersky Lab. Si vous avez autorisé l'utilisation de KSN, l'Assistant active le service du serveur proxy KSN qui assure l'interaction entre KSN et les appareils.
- Configuration de l'envoi de notifications par email des événements survenus pendant l'utilisation du Serveur d'administration et des applications administrées (afin qu'une notification passe avec succès, sur le Serveur d'administration et sur tous les appareils, le service Windows Messenger doit être lancé).
- Configuration des paramètres des mises à jour et de fermeture des vulnérabilités des applications installées sur les appareils.
- Pour le niveau supérieur de la hiérarchie des appareils administrés, la stratégie de protection des postes de travail et des serveurs, ainsi que les tâches d'analyse antivirus, de récupération des mises à jour et de sauvegarde des données se composent.

L'Assistant de configuration initiale crée les stratégies de protection uniquement pour les applications pour lesquelles ces stratégies ne sont pas encore présentées dans le dossier **Appareils administrés**. L'Assistant de configuration initiale ne crée pas les tâches si les tâches avec de tels noms ont déjà été formées pour le niveau supérieur de la hiérarchie des appareils administrés.

L'application invite à lancer l'Assistant de configuration initiale est affichée lors de la première connexion au Serveur d'administration après son raccordement. L'Assistant de configuration initiale peut être lancé à la main à l'aide du menu contextuel du nœud **Serveur d'administration**.

Notions principales

Cette section contient les définitions détaillées des notions principales, concernant Kaspersky Security Center.

Dans cette section

Serveur d'administration.....	77
Hiérarchie des Serveurs d'administration	78
Serveur d'administration virtuel.....	80
Serveur des périphériques mobiles.....	81
Serveur Internet.....	82
Agent d'administration. Groupe d'administration	83
Poste de travail de l'administrateur	84
Plug-in d'administration de l'application	84
Stratégies, paramètres de l'application et tâches.....	85
Corrélation de la stratégie et des paramètres locaux de l'application	88
Agent de mises à jour.....	89

Serveur d'administration

Les modules de Kaspersky Security Center permettent d'effectuer l'administration centralisée des applications de Kaspersky Lab installées sur les appareils clients.

Les appareils, sur lesquels le module Serveur d'administration est installé, s'appellent les *Serveurs d'administration* (ci-après aussi *Serveurs*).

Le Serveur d'administration s'installe sur l'appareil en qualité de service avec la sélection d'attributs suivante :

- sous le nom "Serveur d'administration de Kaspersky Security Center" ;
- avec lancement automatique lors du démarrage du système d'exploitation ;
- avec le compte utilisateur **Système local** ou le compte utilisateur selon la sélection effectuée lors de l'installation du Serveur d'administration.

Le Serveur d'administration exécute les fonctions suivantes :

- sauvegarde de la structure des groupes d'administration ;
- sauvegarde des informations sur la configuration des appareils clients ;
- gestion des stockages des distributeurs des applications ;
- installation à distance des applications sur les appareils clients et suppression des applications ;
- mise à jour des bases de données et des modules des applications de Kaspersky Lab ;
- administration des stratégies et des tâches sur les appareils clients ;
- sauvegarde des informations sur les événements survenus sur les appareils clients ;
- formation des rapports sur le fonctionnement des applications de Kaspersky Lab ;
- extension des clés sur les appareils clients, sauvegarde des informations sur les licences ;
- envoi des notifications sur l'exécution en cours de la tâche (par exemple, des virus détectés sur l'appareil client).

Hiérarchie des Serveurs d'administration

Les Serveurs d'administration peuvent développer une hiérarchie du type "serveur principal – serveur secondaire". Chaque Serveur d'administration peut avoir plusieurs Serveurs d'administration secondaires (ci-après *Serveurs secondaires*) aux différents niveaux hiérarchiques. Le niveau d'intégration des Serveurs secondaires n'est pas limité. De plus, les appareils clients de tous les Serveurs secondaires feront partie des groupes d'administration du Serveur principal. De cette façon, les participants du réseau informatiques indépendants peuvent être administrés par différents Serveurs d'administration qui, à leur tour, sont administrés par le Serveur principal.

Le cas particulier des Serveurs d'administration secondaires : les *Serveurs d'administration virtuels* (cf. section "Serveur d'administration virtuel" à la page [80](#)).

La hiérarchie des Serveurs d'administration peut être utilisée pour remplir les objectifs suivants :

- Limiter la charge sur le Serveur d'administration (par rapport à un Serveur installé sur le réseau).
- Diminuer le trafic sur le réseau et simplifier le travail sur les bureaux distants. Il n'est pas nécessaire d'établir de connexion entre le Serveur principal et tous les appareils du réseau qui peuvent se trouver par exemple dans d'autres régions. Il suffit d'installer dans chaque segment du réseau un Serveur d'administration secondaire, de répartir les appareils dans les groupes d'administration des Serveurs secondaires et fournir aux Serveurs secondaires une connexion avec le Serveur principal par des canaux de liaisons rapides.
- La répartition des responsabilités entre les administrateurs de la sécurité antivirus. En outre, toutes les possibilités d'administration centralisée et de surveillance de la sécurité antivirus du réseau de l'entreprise seront maintenues.
- L'utilisation de Kaspersky Security Center par les prestataires de services. Il suffit au prestataire de services d'installer Kaspersky Security Center et Kaspersky Security Center 10 Web Console. Pour gérer un grand nombre d'appareils clients des entreprises différentes, le prestataire de services peut inclure dans une hiérarchie des Serveurs d'administration les Serveurs d'administration virtuels.

Chaque appareil inclus dans la hiérarchie du groupe d'administration peut être connecté à un seul Serveur d'administration. Il vous faut vérifier la connexion des appareils aux Serveurs d'administration. Pour ce faire, vous pouvez utiliser la fonction de recherche d'appareils selon les attributs de réseau dans les groupes d'administration des Serveurs différents.

Serveur d'administration virtuel

Serveur d'administration virtuel (ci-après *Serveur virtuel*) – le module de l'application Kaspersky Security Center conçu pour l'administration du système de protection antivirus du réseau de l'entreprise cliente.

Le Serveur d'administration virtuel est un cas particulier du Serveur d'administration secondaire et, par rapport au Serveur d'administration physique, possède des restrictions suivantes :

- Le Serveur d'administration virtuel peut fonctionner uniquement s'il fait partie du Serveur d'administration principal.
- Le Serveur d'administration virtuel utilise pour son fonctionnement la base de données du Serveur d'administration principal : les tâches de sauvegarde et de restauration des données, les analyses et les réceptions des mises à jour ne sont pas prises en charge sur le serveur virtuel. Ces tâches se résolvent dans le cadre du Serveur d'administration principal.
- La création des Serveurs d'administration secondaires (y compris les Serveurs virtuels) n'est pas prise en charge pour le Serveur virtuel.

Outre cela, le Serveur d'administration virtuel possède des restrictions suivantes :

- Dans la fenêtre des propriétés du Serveur virtuel, l'ensemble de sections est limité.
- Pour une installation à distance des applications de Kaspersky Lab sur les appareils clients fonctionnant sous l'administration du Serveur virtuel, il faut que l'Agent d'administration soit installé sur un des appareils clients pour la connexion au Serveur virtuel. Lors de la première connexion au Serveur virtuel, cet appareil est automatiquement désigné en tant qu'agent de mises à jour et exécute le rôle de la passerelle des connexions des appareils clients avec le Serveur virtuel.

- Le Serveur virtuel peut sonder le réseau uniquement par les agents de mises à jour.
- Pour relancer le Serveur virtuel dont la productivité a été perturbée, Kaspersky Security Center relance le Serveur d'administration principal et tous les Serveurs virtuels.

L'administrateur du Serveur virtuel possède tous les privilèges dans le cadre de ce Serveur virtuel.

Serveur des appareils mobiles

Le *Serveur des appareils mobiles* est un module de Kaspersky Security Center qui offre l'accès aux appareils mobiles et permet de les administrer via Console d'administration. Le Serveur des appareils mobiles obtient les informations sur les appareils mobiles et enregistre leurs profils.

Il existe deux types des Serveurs des appareils mobiles :

- Le Serveur des appareils mobiles Exchange ActiveSync. Il est installé sur l'appareil 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 appareils mobiles est utilisé pour administrer les appareils mobiles qui prennent en charge le protocole Exchange ActiveSync.
- Serveur MDM iOS. Ce Serveur des appareils mobiles est utilisé pour administrer les appareils mobiles qui prennent en charge le service Apple Push Notifications (APNs).

Les Serveurs des appareils mobiles de Kaspersky Security Center permettent d'administrer les objets suivants :

- appareil mobile distinct ;
- plusieurs appareils mobiles ;
- plusieurs appareils mobiles connectés au cluster de serveurs simultanément. Lors de la connexion au cluster des serveurs, le Serveur des appareils mobiles installé sur ce cluster s'affiche dans la Console d'administration comme un serveur.

Serveur Internet

Serveur Internet de Kaspersky Security Center (ci-après *Serveur Internet*) est un module de Kaspersky Security Center qui s'installe avec le Serveur d'administration. Le Serveur Internet est conçu pour transférer via réseau des paquets d'installation autonomes, des profils MDM iOS, ainsi que des fichiers du dossier partagé.

Lors de la création, le paquet d'installation autonome est automatiquement publié sur le Serveur Internet. Le lien pour télécharger la paquet autonome s'affiche dans la liste des paquets d'installation autonomes créés. En cas de nécessité, vous pouvez annuler la publication du paquet autonome ou le publier de nouveau sur le Serveur Internet.

Lors de la création, le profil MDM iOS pour l'appareil mobile de l'utilisateur est aussi automatiquement publié sur le Serveur Internet. Le profil publié est automatiquement supprimé depuis le Serveur Internet après une installation réussie sur l'appareil mobile de l'utilisateur (pour plus d'informations sur la création et sur l'installation du profil MDM iOS, consulter *Manuel d'implantation de Kaspersky Security Center*).

Le dossier partagé est utilisé pour placer les informations accessibles à tous les utilisateurs dont les appareils fonctionnent sous le Serveur d'administration. Si l'utilisateur n'a pas d'accès direct au dossier partagé, il est possible de lui transférer les informations depuis ce dossier à l'aide du Serveur Internet.

Pour transférer aux utilisateurs les informations depuis le dossier partagé à l'aide du Serveur Internet, l'administrateur doit créer le dossier public imbriqué dans le dossier partagé et y placer les informations.

La syntaxe du lien de transfert des informations à l'utilisateur ressemble à ceci :

```
https://<nom du Serveur Internet>:<port HTTPS>/public/<objet>
```

où

- `<nom du Serveur Internet>` est un nom du Serveur Internet de Kaspersky Security Center.
- `<port HTTPS>` est un port HTTPS du Serveur Internet défini par l'administrateur. Le port HTTPS peut être défini dans la section **Serveur Internet** de la fenêtre des propriétés du Serveur d'administration. Le numéro de port par défaut est 8061.
- `<objet>` est un dossier imbriqué ou le fichier dont l'accès doit être ouvert à l'utilisateur.

L'administrateur peut transférer à l'utilisateur le lien formé à l'aide d'un moyen commode quelconque, par exemple, via email.

A l'aide du lien reçu, l'utilisateur peut télécharger les informations sur l'appareil local.

Agent d'administration. Groupe d'administration

L'interaction entre le Serveur d'administration et les appareils s'opère via le module *Agent d'administration* de l'application Kaspersky Security Center. L'Agent d'administration doit être installé sur tous les appareils où l'administration des applications de Kaspersky Lab se réalise à l'aide de Kaspersky Security Center.

L'Agent d'administration s'installe sur l'appareil en tant que service avec une sélection d'attributs suivante :

- sous le nom "Agent d'administration Kaspersky Security Center" ;
- avec lancement automatique lors du démarrage du système d'exploitation ;
- avec le compte utilisateur **Systeme local**.

L'appareil, le serveur ou le poste de travail sur lequel l'Agent d'administration est installé, ainsi que les applications administrées de Kaspersky Lab sont appelés *client du serveur d'administration* (ci-après *appareil client* ou *appareil*).

La multitude des appareils du réseau de l'entreprise peut être divisée en groupes, qui créent une hiérarchie de la structure. De tels groupes s'appellent les *groupes d'administration*. La hiérarchie des groupes d'administration est affichée dans l'arborescence de la console dans la section du Serveur d'administration.

Groupe d'administration (ci-après *groupe*) : c'est l'ensemble des appareils clients, réunis selon un critère dans le but d'administrer les appareils en tant que groupe unique. Pour tous les appareils clients dans le groupe, les éléments suivants sont installés :

- les paramètres uniques de fonctionnement des applications, à l'aide *des stratégies de groupe* ;
- mode unique de fonctionnement des applications, grâce à la création de *tâches de groupe* avec l'ensemble établi des paramètres (par exemple : création et installation du *paquet*

d'installation unique, mise à jour des bases de données et des modules d'applications, analyse de l'appareil à la demande et protection en temps réel).

L'appareil client peut être inclus dans un seul groupe d'administration.

Vous pouvez créer une hiérarchie des Serveurs et des groupes de n'importe quel degré de complexité. Les Serveurs d'administration secondaires et virtuels, les groupes et les appareils clients peuvent se trouver à un niveau de la hiérarchie.

Poste de travail de l'administrateur

Les appareils, sur lesquels le module *Console d'administration* est installé, s'appellent les *postes de travail de l'administrateur*. A partir de ces appareils, les administrateurs peuvent administrer à distance de manière centralisée les applications de Kaspersky Lab installées sur les appareils clients.

Après avoir installé la Console d'administration sur l'appareil, dans le menu

Démarrer → **Applications** → **Kaspersky Security Center**, l'icône de son lancement s'affiche.

Aucune restriction n'est imposée sur le nombre de postes de travail de l'administrateur. Depuis chaque poste de travail de l'administrateur, il est possible d'administrer les groupes d'administration de plusieurs Serveurs d'administration dans le réseau. Le poste de travail de l'administrateur peut être connecté au Serveur d'administration (physique et virtuel) de n'importe quel niveau de la hiérarchie.

Le poste de travail de l'administrateur peut être inclus dans le groupe d'administration en tant qu'appareil client.

Dans le cadre des groupes d'administration de n'importe quel Serveur d'administration, le même appareil peut être simultanément client du Serveur d'administration, Serveur d'administration et poste de travail de l'administrateur.

Plug-in d'administration de l'application

L'administration des applications de Kaspersky Lab via la Console d'administration s'exécute à l'aide du module spécial : le *plug-in d'administration de l'application*. Il est repris dans toutes les applications de Kaspersky Lab qui peuvent être administrées à l'aide de Kaspersky Security Center.

Le plug-in d'administration de l'application s'installe sur le poste de travail de l'administrateur. A l'aide du plug-in d'administration de l'application, il est possible d'exécuter les actions suivantes dans la Console d'administration :

- créer et modifier les stratégies et les paramètres de l'application, ainsi que les paramètres des tâches de cette application ;
- obtenir les informations sur les tâches de l'application, sur les événements dans son fonctionnement, et sur les statistiques de fonctionnement de l'application obtenues depuis les appareils clients.

Stratégies, paramètres de l'application et tâches

L'action concrète, exécutée par l'application de Kaspersky Lab, porte le nom *la tâche*. Selon les fonctions exécutées, les tâches sont divisées par *types*.

L'ensemble des paramètres de fonctionnement de l'application lors de son exécution correspond à une tâche. L'ensemble des paramètres de fonctionnement de l'application, unique pour tous les types de ses tâches, compose les paramètres de l'application. Les paramètres de fonctionnement de l'application, spécifiques à chaque type de tâches, constituent les paramètres de la tâche.

La description détaillée des types de tâches pour chaque application de Kaspersky Lab est présentée dans les manuels.

Nous appellerons *paramètres locaux de l'application* les paramètres de l'application qui sont définis pour l'appareil client particulier par l'interface locale, ou à distance par la Console d'administration.

La configuration centralisée des paramètres de fonctionnement des applications installées sur les appareils clients s'opère à l'aide de la définition de stratégies.

Stratégie est un ensemble de paramètres de fonctionnement de l'application. Cet ensemble est défini pour le groupe d'administration. La stratégie ne définit pas tous les paramètres de l'application.

Plusieurs stratégies avec les valeurs différentes des paramètres peuvent être définies pour une application, mais une seule stratégie pour l'application peut être active.

Les paramètres de fonctionnement de l'application peuvent varier en fonction des groupes. Une stratégie propre pour l'application peut être créée dans chaque groupe.

Les paramètres de l'application sont définis par les paramètres des stratégies et des tâches.

Les sous-groupes et les Serveurs d'administration secondaires héritent des tâches de groupe des niveaux plus élevés de la hiérarchie. La tâche, définie pour le groupe, sera exécutée non seulement sur les appareils clients inclus dans ce groupe, mais aussi sur les appareils clients inclus dans les sous-groupes et dans les Serveurs d'administration secondaires aux niveaux suivants de la hiérarchie.

Chaque paramètre, présenté dans la stratégie, a pour attribut le "cadenas" : . Le "cadenas" affiche, s'il est interdit de modifier le paramètre dans les stratégies du niveau intégré de la hiérarchie (pour les groupes intégrés et pour les Serveurs d'administration secondaires). Il en est de même pour les paramètres des tâches et les paramètres locaux de l'application. Si dans la stratégie, le "cadenas" est placé pour le paramètre, il sera impossible de prédéfinir sa valeur (cf. section "Corrélation de stratégie et des paramètres locaux de l'application" à la page [88](#)).

Si dans la fenêtre des propriétés de la stratégie héritée vous décochez la case **Hériter des paramètres de la stratégie de niveau supérieur** située dans le groupe **Héritage des paramètres** de la section **Général**, l'action du "cadenas" pour cette stratégie sera annulée.

Il y a la possibilité d'activer la stratégie qui n'est pas active, selon l'événement. Cela permet, par exemple, d'installer des paramètres plus stricts de la protection antivirus dans les périodes de l'épidémie de virus.

Vous pouvez aussi former la stratégie pour les utilisateurs autonomes.

La création et la configuration des tâches pour les objets administrées par un Serveur d'administration s'effectuent de manière centralisée. Les tâches des types suivants peuvent être définies :

- *la tâche de groupe* : tâche qui définit les paramètres de fonctionnement de l'application installés sur les appareils et inclus dans le groupe d'administration ;
- *la tâche locale* : tâche pour un appareil individuel ;
- *la tâche pour un ensemble d'appareils* : tâche pour la sélection aléatoire d'appareils, qu'ils soient ou non compris dans le groupe d'administration ;
- *la tâche du Serveur d'administration* : la tâche, qui est définie directement pour le Serveur d'administration.

Une tâche de groupe peut être définie pour un groupe, même si l'application de Kaspersky Lab n'est pas installée sur tous les appareils clients du groupe. Dans ce cas, la tâche de groupe s'exécute uniquement pour les appareils sur lesquels l'application indiquée est installée.

Les tâches créées pour l'appareil client d'une manière locale sont exécutées uniquement pour cet appareil. Lors de la synchronisation de l'appareil client avec le Serveur d'administration, les tâches locales seront ajoutées à la liste des tâches formées pour l'appareil client.

Puisque les paramètres de fonctionnement de l'application sont définis par la stratégie, les paramètres qui ne sont pas interdits peuvent être redéfinis, ainsi que les paramètres qui peuvent être installés uniquement pour l'exemplaire concret de la tâche. Par exemple, pour la tâche d'analyse du disque, il s'agit du nom du disque et des masques des fichiers analysés.

La tâche peut être lancée automatiquement (selon la planification) ou manuellement. Les résultats de l'exécution de la tâche sont enregistrés sur le Serveur d'administration et de manière locale. L'administrateur peut recevoir des notifications sur l'exécution de telle ou telle tâche, ainsi que parcourir les rapports détaillés.

Les informations sur les stratégies, les paramètres de l'application, les paramètres des tâches pour des ensembles d'appareils et les tâches de groupe sont enregistrées sur le Serveur et diffusées sur les appareils clients lors de la synchronisation. Avec cela, le Serveur d'administration enregistre les informations sur les modifications locales autorisées par la stratégie et réalisées sur les appareils clients. En outre, la liste des applications qui fonctionnent sur l'appareil client est actualisée, ainsi que leur état et la liste des tâches formées.

Corrélation de la stratégie et des paramètres locaux de l'application

A l'aide des stratégies, les mêmes valeurs des paramètres de fonctionnement de l'application peuvent être installées pour tous les appareils inclus dans le groupe.

Vous pouvez redéfinir les valeurs des paramètres définies par la stratégie pour les appareils individuels dans le groupe à l'aide des paramètres locaux de l'application. Avec cela, vous pouvez établir les valeurs des paramètres, dont la modification n'est pas interdite par la stratégie (le paramètre n'est pas fermé par le "cadenas").

La valeur du paramètre, utilisée par l'application sur l'appareil client (cf. ill. ci-dessous), est définie par la présence du "cadenas" dans le paramètre de la stratégie :

- Si la modification du paramètre est interdite, la même valeur est utilisée sur tous les appareils clients : définie par la stratégie.

- Si ce n'est pas interdit, l'application n'utilise alors pas la valeur qui est indiquée dans la stratégie sur chaque appareil client, mais la valeur locale du paramètre. Cela dit, la valeur du paramètre peut être modifiée par les paramètres locaux de l'application.



Illustration 7 Stratégie et paramètres locaux de l'application

De cette façon, lorsque la tâche est en exécution sur un appareil client, l'application utilise les paramètres définis selon deux manières différentes :

- par les paramètres de la tâche et les paramètres locaux de l'application, si l'interdiction de modifier le paramètre n'était pas établie dans la stratégie ;
- par la stratégie du groupe, si l'interdiction de modifier le paramètre était établie dans la stratégie.

Les paramètres locaux de l'application sont modifiés après la première utilisation de la stratégie conformément aux paramètres de la stratégie.

Agent de mises à jour

L'Agent de mises à jour est un appareil avec un Agent d'administration installé qui sert à déployer les mises à jour, à installer les applications à distance et à recevoir des informations sur les appareils du réseau. L'Agent de mises à jour peut remplir les fonctions suivantes :

- Diffusion des mises à jour et des paquets d'installation récupérés sur le Serveur d'administration vers les appareils clients du groupe (notamment à l'aide d'une diffusion multicast via le protocole UDP). Les mises à jour peuvent être obtenues à partir du Serveur d'administration comme à partir des serveurs de mise à jour de Kaspersky Lab. Dans ce dernier cas, une tâche de mise à jour doit être créée pour l'appareil qui est l'agent de mises à jour (cf. section "Installation automatique de mises à jour pour Kaspersky Endpoint Security sur les appareils" à la page [239](#)).

Les agents de mises à jour accélèrent la diffusion des mises à jour et permettent d'économiser les ressources du serveur d'administration.

- Diffuser les stratégies et les tâches de groupe à l'aide d'une diffusion multicast via le protocole UDP.
- Passerelle de connexions au Serveur d'administration pour les appareils du groupe d'administration (cf. section "Utilisation de l'agent de mises à jour en guise de passerelles" à la page [408](#)).

Lorsqu'il est impossible d'établir une connexion directe entre les appareils administrés du groupe et le serveur d'administration, l'Agent de mises à jour peut être désigné comme passerelle de connexion de ce groupe au Serveur d'administration. Dans ce cas, les appareils administrés se connectent à la passerelle qui se connecte à son tour au Serveur d'administration.

La présence d'un agent de mises à jour qui fonctionne en mode passerelle de connexions n'empêche pas la connexion directe des appareils administrés au Serveur d'administration. Si la passerelle de connexion n'est pas disponible et qu'une connexion directe au Serveur d'administration est possible sur le plan technique, les appareils administrés se connectent directement au Serveur.

- Sonder le réseau dans le but de détecter de nouveaux appareils et de mettre à jour les informations sur les appareils détectés. L'agent de mises à jour peut exécuter les mêmes types de sondage de réseau que le Serveur d'administration.
- Installer à distance les applications tierces comme les applications Kaspersky Lab à l'aide de Microsoft Windows, y compris sur les appareils clients sans Agent d'administration installé.

Cette fonction permet de transmettre à distance les paquets d'installation de l'Agent d'administration sur les appareils clients du réseau auxquels le Serveur d'administration n'a pas d'accès direct.

La transmission des fichiers à l'agent de mises à jour par le Serveur d'administration s'effectue via le protocole HTTP ou, si une connexion SSL est configurée, via le protocole HTTPS. L'utilisation du protocole HTTP ou HTTPS assure une performance plus élevée par rapport au protocole SOAP grâce à la réduction du trafic.

Les appareils sur lesquels l'Agent d'administration est installé peuvent être désignés comme agents de mises à jour manuellement par l'administrateur ou automatiquement par le Serveur d'administration (cf. section "Désignation d'appareils comme agents de mises à jour" à la page [342](#)). Pour obtenir la liste complète des Agents des mises à jour pour les groupes d'administration indiqués, il faut créer un rapport sur la liste des agents des mises à jour.

L'Agent de mises à jour est opérationnel dans le groupe d'administration pour lequel il a été désigné comme administrateur et dans les sous-groupes de celui-ci, quel que soit le niveau d'imbrication. Si la hiérarchie des groupes d'administration compte plusieurs agents de mises à jour, l'Agent d'administration de l'appareil administré se connecte à l'agent de mises à jour le plus proche dans la hiérarchie.

Le sous-réseau NLA peut aussi être une zone d'action des agents de mises à jour. Le sous-réseau NLA s'utilise pour la création en mode manuel d'un ensemble d'appareils sur lesquels l'agent de mises à jour déploiera les mises à jour.

Si les agents de mises à jour sont désignés automatiquement comme Serveurs d'administration, le serveur désigne ces agents de mises à jour par domaines multicast, et non par groupes d'administration. Cela se produit dès que les domaines multicast sont connus. L'Agent d'administration communique avec les autres Agents d'administration de son réseau par messages et envoie au Serveur d'administration des informations sur lui-même et de brèves informations sur

les autres Agents d'administration. Sur la base de ces informations, le Serveur d'administration peut regrouper des Agents d'administration par domaines multicast. Les domaines multicast deviennent connus du Serveur d'administration dès que plus de 70 % des Agents d'administration ont été sondés dans les groupes d'administration. Le Serveur d'administration sonde les domaines multicast toutes les deux heures.

Dès que les agents de mises à jour sont désignés par domaines multicast, ils ne doivent pas être de nouveau désignés par groupes d'administration.

Les Agents d'administration avec un profil actif de connexion ne participent pas à la définition d'un domaine multicast.

Quand, sur une seule parcelle de réseau ou dans un groupe d'administration, au moins deux agents de mises à jour sont désignés, l'un d'entre eux devient l'agent de mises à jour actif et les autres sont nommés agents de réserve. L'agent de mises à jour actif télécharge les mises à jour et les paquets d'installation directement à partir du Serveur d'administration et les agents de mises à jour de réserve s'adressent uniquement à l'agent de mises à jour actif pour obtenir des mises à jour. Dans ce cas, les fichiers sont téléchargés une seule fois à partir du Serveur d'administration, puis répartis entre les agents de mises à jour. Si l'agent de mises à jour actif devient inaccessible pour une raison ou pour une autre, l'un des agents de mises à jour de réserve est désigné comme l'agent actif. Le Serveur d'administration désigne automatiquement l'agent de mises à jour comme agent de réserve.

L'état de l'agent de mises à jour (*Actif / De réserve*) est indiqué par une case à cocher dans le rapport de l'utilitaire klnagchk (cf. section "Vérification manuelle de la connexion de l'appareil client avec le Serveur d'administration. Utilitaire klnagchk" à la page [160](#)).

Le fonctionnement de l'agent de mises à jour nécessite au moins 4 Go d'espace libre sur le disque dur. Si l'espace libre disponible sur le disque de l'agent de mises à jour est inférieur à 2 Go, Kaspersky Security Center crée un incident avec le niveau d'importance *Avertissement*. L'incident sera publié dans les propriétés de l'appareil dans la section **Incidents**.

En présence, sur le Serveur d'administration, de tâches d'installation à distance, l'appareil avec l'agent de mises à jour demande en plus une quantité d'espace sur le disque égale à la taille totale des paquets d'installation installés.

En présence sur le Serveur d'administration d'un ou plusieurs exemplaires de tâches d'installation des mises à jour (correctifs) et de correction des vulnérabilités, l'appareil avec l'agent de mises à jour demande en plus une quantité d'espace sur le disque égale à la taille totale de tous les correctifs installés.

Administration des Serveurs d'administration

Cette section contient les informations sur l'utilisation des Serveurs d'administration et sur la configuration des paramètres du Serveur d'administration.

Dans cette section

Connexion au Serveur d'administration et permutation entre les Serveurs d'administration	95
Privilèges d'accès au Serveur d'administration et à ses objets	96
Conditions de connexion au Serveur d'administration via Internet	98
Connexion sécurisée au Serveur d'administration	99
Se déconnecter du Serveur d'administration	101
Ajout d'un Serveur d'administration à l'arborescence de la console	101
Suppression d'un Serveur d'administration de l'arborescence de console	102
Changement du compte utilisateur du service du Serveur d'administration. Utilitaire klsrvswch.....	102
Affichage et modification des paramètres du Serveur d'administration.....	104

Connexion au Serveur d'administration et permutation entre les Serveurs d'administration

Lors du lancement, l'application Kaspersky Security Center tente de se connecter au Serveur d'administration. S'il existe plusieurs Serveurs d'administration sur votre réseau, l'application se connectera au Serveur utilisé lors d'une session précédente de Kaspersky Security Center.

Lors du premier démarrage de l'application après l'installation, une tentative de connexion au Serveur d'administration, indiqué lors de l'installation de Kaspersky Security Center, s'exécute.

Après la connexion au Serveur d'administration, la structure des dossiers de ce Serveur s'affiche dans l'arborescence de la console.

Si plusieurs Serveurs d'administration ont été ajoutés dans l'arborescence de la console, vous pouvez vous déplacer entre eux.

► *Pour se connecter à un autre Serveur d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans le menu contextuel de l'entrée, sélectionnez l'option **Se connecter au Serveur d'administration**.
3. Dans la fenêtre ouverte **Paramètres de connexion** dans le champ **Adresse du serveur**, indiquez le nom du Serveur d'administration auquel vous voulez vous connecter. En tant que le nom du Serveur d'administration, vous pouvez indiquer l'adresse IP ou le nom de l'appareil dans le réseau Windows. En cliquant sur le bouton **Avancé** dans la partie inférieure de la fenêtre, vous pouvez configurer les paramètres de connexion au Serveur d'administration (cf. ill. ci-après).

Pour vous connecter au Serveur d'administration à travers un port différent du port par défaut, indiquez, dans le champ **Adresse du serveur** la valeur au format <Nom du Serveur

d'administration>:<Port>.Les utilisateurs qui ne jouissent pas des privilèges de **Lecture** ne pourront pas accéder au Serveur d'administration.

Paramètres de connexion

KASPERSKY

Adresse du serveur :
localhost

Utiliser une connexion SSL

Nom d'utilisateur : WIN-H29F8374J\tester

Mot de passe : ●●●●●●●●

Mémoriser les identifiants

Utiliser la compression de données

Utiliser un serveur proxy

Adresse :
Nom d'utilisateur :
Mot de passe :

OK Annuler Avancé <<

Illustration 8 Etablissement de la connexion au Serveur d'administration

4. Cliquez sur le bouton **OK** pour terminer la permutation entre les Serveurs.

Après la connexion au Serveur d'administration, la structure des dossiers de l'entrée correspondante est actualisée dans l'arborescence de la console.

Privilèges d'accès au Serveur d'administration et à ses objets

Lors de l'installation de Kaspersky Security Center, les groupes d'utilisateurs **KLAdmins** et **KLOperators** sont automatiquement formés. Ces groupes possèdent des privilèges de connexion au Serveur d'administration et de fonctionnement avec ses objets.

Selon le compte utilisateur sous lequel l'installation de Kaspersky Security Center se passe, les groupes **KLAdmins** et **KLOperators** sont créés de la manière suivante :

- Si l'installation se passe sous le compte utilisateur, appartenant au domaine, alors les groupes sont créés dans le domaine, incluant le Serveur d'administration, et sur le Serveur d'administration.
- Si l'installation se passe sous le compte utilisateur du système, les groupes sont créés uniquement sur le Serveur d'administration.

La consultation des groupes **KLAdmins** et **KLOperators** et l'insertion des modifications nécessaires dans les privilèges d'utilisateurs des groupes **KLAdmins** et **KLOperators** peut être réalisée à l'aide des outils standards d'administration du système d'exploitation.

Tous les privilèges sont accordés au groupe **KLAdmins** et les privilèges de lecture au groupe **KLOperators**. L'ensemble des droits présentés dans le groupe **KLAdmins** n'est pas disponible à la modification.

Les utilisateurs du groupe **KLAdmins** portent le nom : les *administrateurs de Kaspersky Security Center*, les utilisateurs du groupe **KLOperators** – les *opérateurs de Kaspersky Security Center*.

Outre les utilisateurs du groupe **KLAdmins**, les privilèges d'administrateur de Kaspersky Security Center sont accordés aux administrateurs locaux des appareils sur lesquels le Serveur d'administration est installé.

Il est possible d'exclure les administrateurs locaux de la liste des utilisateurs qui possèdent les privilèges d'administrateur de Kaspersky Security Center.

Toutes les opérations lancées par les administrateurs de Kaspersky Security Center sont exécutées avec les privilèges du compte utilisateur du Serveur d'administration.

Pour chaque Serveur d'administration dans le réseau, un propre groupe **KLAdmins** peut être formé. Ce groupe possédera des privilèges uniquement dans le cadre du travail avec ce Serveur.

Si les appareils appartiennent au même domaine et font partie des groupes d'administration de Serveurs différents, l'administrateur est l'administrateur de Kaspersky Security Center dans le cadre de tous ces groupes d'administration. Le groupe **KLAdmins** est unique pour ces groupes d'administration et est créé lors de l'installation du premier Serveur d'administration. Les opérations

lancées par l'administrateur Kaspersky Security Center sont exécutées avec les privilèges du compte utilisateur du Serveur d'administration pour lequel elles ont été lancées.

Après l'installation de l'application, l'administrateur Kaspersky Security Center peut procéder comme suit :

- Modifier les privilèges accordés aux groupes **KLOperators** ;
- Définir les privilèges d'accès aux fonctions de l'application Kaspersky Security Center aux autres groupes d'utilisateurs et aux utilisateurs particuliers enregistrés sur le poste de travail de l'administrateur ;
- Définir les privilèges d'accès des utilisateurs au travail dans chaque groupe d'administration.

L'administrateur de Kaspersky Security Center peut établir les privilèges d'accès à chaque groupe d'administration ou aux autres objets du Serveur d'administration dans la section **Sécurité** de la fenêtre des propriétés de l'objet sélectionné.

Vous pouvez surveiller les actions de l'utilisateur à l'aide des enregistrements sur les événements dans le fonctionnement du Serveur d'administration. Les enregistrements relatifs aux événements sont affichés dans le nœud **Serveur d'administration** sous l'onglet **Événements**. Ces événements possèdent le niveau d'importance **Message d'information**, les types d'événement commencent par le mot **Audit**.

Conditions de connexion au Serveur d'administration via Internet

Si le Serveur d'administration est un serveur à distance, c'est-à-dire il se trouve en dehors du réseau d'entreprise, les appareils clients se connectent à lui via Internet. Pour la connexion des appareils au Serveur d'administration via Internet, il est nécessaire d'exécuter les conditions suivantes :

- Le Serveur d'administration à distance doit posséder l'adresse IP externe, et sur cette adresse les ports entrants 13000 et 14000 doivent être ouverts.
- Des Agents d'administration doivent être installés sur les appareils.

- Lors de l'installation de l'Agent d'administration sur les appareils, l'adresse IP externe du Serveur d'administration à distance doit être indiquée. Si pour l'installation, le paquet d'installation est utilisé, alors l'adresse IP doit être indiquée manuellement dans les propriétés du paquet d'installation dans la section **Paramètres**.
- Pour administrer les applications et les tâches de l'appareil à l'aide du Serveur d'administration à distance, il faut cocher la case **Maintenir la connexion au Serveur d'administration** dans la fenêtre des propriétés de cet appareil dans la section **Général**. Après avoir coché la case, il faut attendre la synchronisation avec l'appareil distant. La connexion permanente avec le Serveur d'administration peut prendre en charge pas plus de 100 appareils clients en même temps.

Pour accélérer l'exécution des tâches reçues depuis le Serveur d'administration à distance, vous pouvez ouvrir sur les appareils le port 15000. Dans ce cas pour lancer une tâche, le Serveur d'administration envoie un paquet spécial à l'Agent d'administration par le port 15000 sans attendre la synchronisation avec l'appareil.

Connexion sécurisée au Serveur d'administration

L'échange des informations entre les appareils clients et le Serveur d'administration, ainsi que la connexion de la Console d'administration au Serveur d'administration peuvent être exécutées en utilisant le protocole SSL (Secure Socket Layer). Le protocole SSL permet d'identifier les parties, qui coopèrent lors de la connexion, de chiffrer les données transmises et de garantir leur intégrité tout au long de la transmission. L'authentification des parties coopérants et le chiffrement des données par clés ouvertes sont à la base du protocole SSL.

Dans cette section

Authentification du Serveur lors de la connexion de l'appareil	100
Authentification du Serveur lors de la connexion de la Console d'administration	100
Certificat du Serveur d'administration	101

Authentification du Serveur lors de la connexion de l'appareil

Lors de la première connexion de l'appareil client au Serveur d'administration, l'Agent d'administration sur l'appareil reçoit une copie du certificat de Serveur d'administration et le sauvegarde localement.

Lors de l'installation locale de l'Agent d'administration sur l'appareil, le certificat de Serveur d'administration peut être sélectionné à la main.

Selon la copie reçue du certificat, l'analyse des privilèges et des pouvoirs du Serveur d'administration sera réalisée au cours des connexions ultérieures.

Par la suite, lors de chaque connexion de l'appareil au Serveur d'administration, l'Agent d'administration demandera le certificat de Serveur d'administration et le comparera avec sa copie locale. S'ils ne concordent pas, l'accès du Serveur d'administration à l'appareil sera interdit.

Authentification du Serveur lors de la connexion de la Console d'administration

Lors de la première connexion au Serveur d'administration, la Console d'administration demande le certificat de Serveur d'administration et sauvegarde sa copie localement sur le poste de travail de l'administrateur. Selon la copie reçue du certificat, au cours des connexions suivantes de la Console d'administration au Serveur d'administration, l'identification du Serveur d'administration sera exécutée.

Si le certificat de Serveur d'administration ne concorde pas avec la copie du certificat sauvegardée sur le poste de travail de l'administrateur, la Console d'administration affiche une demande afin de pouvoir confirmer la connexion au Serveur d'administration portant le nom attribué et d'obtenir un nouveau certificat. Après la connexion, la Console d'administration sauvegardera la copie du nouveau certificat de Serveur d'administration. Elle sera utilisée ultérieurement pour identifier le Serveur.

Certificat du Serveur d'administration

L'authentification du Serveur d'administration lors de la connexion de la Console d'administration et de l'échange des informations avec les appareils s'effectue selon le *certificat de Serveur d'Administration*. Le certificat est utilisé pour l'authentification lors de l'établissement de la connexion entre les Serveurs d'administration principaux et secondaires.

Le certificat de Serveur d'administration est automatiquement créé en cours de l'installation du module Serveur d'administration et sauvegardé dans le dossier
%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Le certificat de Serveur d'administration n'est créé qu'une seule fois, à l'installation du Serveur d'administration. Pour restaurer le certificat de Serveur d'administration en cas de perte, vous devez réinstaller le module du Serveur d'administration et restaurer les données (cf. section "Copie de sauvegarde et restauration des données du Serveur d'administration" à la p. [394](#)).

Se déconnecter du Serveur d'administration

► *Pour se déconnecter du Serveur d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée correspondant au Serveur d'administration de laquelle il faut se déconnecter.
2. Sélectionnez l'option **Se déconnecter du Serveur d'administration** dans le menu contextuel de l'entrée.

Ajout d'un Serveur d'administration à l'arborescence de la console

► *Pour ajouter un Serveur d'administration à l'arborescence de la console, procédez comme suit :*

1. Dans la fenêtre principale de l'application Kaspersky Security Center, sélectionnez l'entrée **Kaspersky Security Center** dans l'arborescence de la console.
2. Dans le menu contextuel, sélectionnez l'option **Créer** → **Serveur d'administration**.

Une entrée appelée **Serveur d'administration - <nom de l'appareil> (Non connecté)** apparaîtra dans l'arborescence de console. Utilisez cette entrée pour la connecter à n'importe quel Serveur installé sur votre réseau des Serveurs d'administration.

Suppression d'un Serveur d'administration de l'arborescence de la console

► *Pour supprimer un Serveur d'administration de l'arborescence de la console, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée correspondant au Serveur d'administration à supprimer.
2. Sélectionnez l'option **Supprimer** dans le menu contextuel de l'entrée.

Changement du compte utilisateur du service du Serveur d'administration. Utilitaire klsrvswch

S'il vous faut modifier le compte utilisateur du service du Serveur d'administration, défini lors de l'installation de l'application Kaspersky Security Center, vous pouvez utiliser l'utilitaire de changement du compte du service du Serveur d'administration klsrvswch.

Lors de l'installation de Kaspersky Security Center, l'utilitaire est automatiquement copiée dans le dossier d'installation de l'application.

Le nombre de lancements de l'utilitaire est illimité.

► *Pour modifier le compte utilisateur du service du Serveur d'administration, procédez comme suit :*

1. Lancez l'utilitaire klsrvswch depuis le dossier d'installation Kaspersky Security Center.

Finalement, l'Assistant de changement du compte utilisateur du service du Serveur d'administration se lance. Suivez les instructions de l'Assistant.

2. La fenêtre **Compte du service du Serveur d'administration** permet de sélectionner une de deux options de définition du compte utilisateur :

- **Compte du système.** Le service du Serveur d'administration se lance sous le compte utilisateur et avec les privilèges *Compte du système*.

Pour que Kaspersky Security Center fonctionne correctement, il faut que le compte utilisateur possède les droits d'accès d'administrateur des ressources pour le placement de la base des informations du Serveur d'administration au démarrage du service du Serveur d'administration.

- **Compte d'utilisateur.** Le service du Serveur d'administration se lance sous le compte utilisateur inclus dans le domaine. Dans ce cas, le Serveur d'administration initie toutes les opérations avec les privilèges de ce compte utilisateur.

Pour sélectionner l'utilisateur dont le compte utilisateur sera utilisé pour lancer le service du Serveur d'administration, procédez comme suit :

1. Cliquez sur le bouton **Rechercher** et choisissez l'utilisateur dans la fenêtre ouverte **Sélection : « Utilisateur »**.

Fermez la fenêtre **Sélection : « Utilisateur »** et cliquez sur le bouton **Suivant**.

2. La fenêtre **Mot de passe du compte** permet de saisir le mot de passe pour le compte utilisateur de l'utilisateur sélectionné, s'il le faut.

Suite au fonctionnement de l'Assistant, le compte utilisateur du Serveur d'administration change.

Lors de l'utilisation du serveur SQL en mode d'authentification du compte utilisateur par les outils Microsoft Windows, il faut assurer l'accès à la base des données. Le compte utilisateur doit posséder la base de données de Kaspersky Anti-Virus. Par défaut, il faut utiliser le schéma dbo.

Affichage et modification des paramètres du Serveur d'administration

Vous pouvez configurer les paramètres du Serveur d'administration dans la fenêtre des propriétés du Serveur d'administration.

- *Pour ouvrir la fenêtre Propriétés : Serveur d'administration,*
dans le menu contextuel de l'entrée du Serveur d'administration dans l'arborescence de la console, sélectionnez l'option **Propriétés**.

Dans cette section

Configuration des paramètres généraux du Serveur d'administration	105
Traitement et stockage des événements sur le Serveur d'administration	105
Contrôle de l'émergence d'épidémies de virus	106
Restriction du trafic	107
Configuration des paramètres du Serveur Internet.....	107
Travail avec les utilisateurs internes.....	108

Configuration des paramètres généraux du Serveur d'administration

Vous pouvez configurer les paramètres généraux du Serveur d'administration dans les sections **Général**, **Paramètres**, **Conservation des événements** et **Sécurité** de la fenêtre des propriétés du Serveur d'administration.

La section **Sécurité** peut ne pas s'afficher dans la fenêtre de propriétés du Serveur d'administration si son affichage est désactivé dans l'interface de la Console d'administration.

► *Pour activer l'affichage de la section **Sécurité** dans la Console d'administration, procédez comme suit :*

1. Dans le menu **Affichage** de la fenêtre principale de l'application, sélectionnez le point **Configuration de l'interface**.
2. Dans la fenêtre **Configuration de l'interface** qui s'ouvre, cochez la case **Afficher les sections avec les paramètres de sécurité** et cliquez sur le bouton **OK**.
3. Dans la fenêtre avec un message de l'application, cliquez sur le bouton **OK**.

La section **Sécurité** s'affiche dans la fenêtre de propriétés du Serveur d'administration.

Traitement et stockage des événements sur le Serveur d'administration

Les informations sur les événements dans le fonctionnement de l'application et des appareils administrés sont stockées dans la base de données du Serveur d'administration. Chaque événement est lié à un type défini et à un niveau d'importance (Événement critique, Erreur de fonctionnement, Avertissement, Message d'information). En fonction des conditions dans lesquelles l'événement s'est produit, l'application peut attribuer aux événements d'un type unique des niveaux d'importance différents.

Vous pouvez consulter les types et les niveaux d'importance dans la section **Notification sur les événements** de la fenêtre de propriétés du Serveur d'administration. Dans la section **Notification sur les événements**, vous pouvez aussi configurer les paramètres de traitement de chaque événement du Serveur d'administration :

- consignation des événements sur le Serveur d'administration et dans les journaux des événements du système d'exploitation sur l'appareil et sur le Serveur d'administration ;
- mode de notification de l'administrateur sur l'événement (par exemple, SMS, message électronique).

Dans la section **Conservation des événements** de la fenêtre de propriétés du Serveur d'administration, vous pouvez configurer les paramètres de conservation des événements dans la base de données : limiter le nombre d'enregistrements sur les événements et le temps de conservation de ces derniers. Par défaut, la capacité de la base de données du Serveur d'administration est de 400 000 événements. La capacité maximale recommandée de la base de données est de 15 000 000 événements. Si le nombre d'événements dans la base de données atteint la valeur maximale indiquée par l'administrateur, l'application supprime les événements les plus anciens et enregistre les nouveaux.

Contrôle de l'émergence d'épidémies de virus

Kaspersky Security Center vous permet de réagir opportunément à l'apparition des menaces des épidémies de virus. L'évaluation de l'épidémie de virus se réalise par le contrôle de l'activité de virus sur les appareils.

Vous pouvez configurer les règles d'évaluation de l'épidémie de virus et les actions dans le cas de son apparition dans la section **Attaque de virus** de la fenêtre des propriétés du Serveur d'administration.

L'ordre de notification sur l'événement *Attaque de virus* peut être défini dans la section **Notification sur les événements** de la fenêtre des propriétés du Serveur d'administration (cf. section "Traitement et stockage des événements sur le Serveur d'administration" à la page [105](#)), dans la fenêtre des propriétés de l'événement *Attaque de virus*.

L'événement *Attaque de virus* se forme quand l'événement *Objet malveillant détecté* survient dans le fonctionnement des applications de protection. Par conséquent, pour pouvoir identifier une épidémie de virus, les informations sur les événements *Objet malveillant détecté* doivent être enregistrées sur le Serveur d'administration.

Les paramètres d'enregistrement des informations sur l'événement *Objet malveillant détecté* sont définis dans les stratégies des applications de protection.

Sous le titre *Objet malveillant détecté*, les informations en provenance des appareils du Serveur d'administration principal sont prises en compte. Les informations depuis les Serveurs d'administration secondaires ne sont pas prises en compte. Pour chaque Serveur d'administration secondaire, les paramètres de l'événement *Attaque de virus* doivent être configurés individuellement.

Restriction du trafic

Pour diminuer le trafic dans le réseau, il est possible de limiter la vitesse de transfert des données sur le Serveur d'administration depuis les plages IP ou les intervalles IP en particulier.

Vous pouvez créer et configurer les règles de restriction du trafic dans la section **Trafic** de la fenêtre des propriétés du Serveur d'administration.

Configuration des paramètres du Serveur Internet

Le Serveur Internet est utilisé pour publier les paquets d'installation autonomes, les profils MDM iOS, ainsi que les fichiers du dossier partagé.

Vous pouvez configurer les paramètres de connexion du Serveur Internet au Serveur d'administration et définir le certificat de Serveur Internet dans la section **Serveur Internet** de la fenêtre des propriétés du Serveur d'administration.

Travail avec les utilisateurs internes

Les comptes utilisateur des *utilisateurs internes* sont utilisés pour travailler avec les Serveurs d'administration virtuels. Sous le nom du compte utilisateur de l'utilisateur interne, l'administrateur du Serveur virtuel permet de lancer Kaspersky Security Center 10 Web Console pour consulter les informations sur l'état de la protection antivirus du réseau. Dans le cadre de fonctionnalité de l'application Kaspersky Security Center, les utilisateurs internes possèdent les privilèges des utilisateurs réels.

Les comptes utilisateur des utilisateurs internes sont créés et utilisés uniquement à l'intérieur de Kaspersky Security Center. Les informations sur les utilisateurs internes ne sont pas transmises au système d'exploitation. Kaspersky Security Center effectue l'authentification des utilisateurs internes.

Vous pouvez configurer les paramètres des comptes utilisateurs des utilisateurs internes dans le dossier **Comptes utilisateurs** de l'arborescence de la console (cf. section "Utilisation des comptes utilisateur" à la page [178](#)).

Administration des groupes d'administration

Cette section contient les informations sur le travail avec les groupes d'administration.

Avec les groupes d'administration, vous pouvez effectuer les actions suivantes :

- ajouter au groupe d'administration le nombre quelconque des groupes imbriqués de tous les niveaux hiérarchique ;
- ajouter au groupe d'administration des appareils ;
- modifier la hiérarchie des groupes d'administration en déplaçant des appareils individuels ou des groupes entiers dans d'autres groupes ;
- supprimer d'un groupe d'administration les sous-groupes et les appareils ;
- ajouter aux groupes d'administration des Serveurs d'administration virtuels et secondaires ;
- déplacer les appareils des groupes d'administration d'un Serveur vers les groupes d'administration d'un autre Serveur ;
- définir les applications de Kaspersky Lab qui seront installées automatiquement sur les appareils ajoutés au groupe.

Dans cette section

Création des groupes d'administration	109
Déplacement des groupes d'administration	112
Suppression des groupes d'administration	113
Création automatique de structure des groupes d'administration.....	114
Installation automatique des applications sur les appareils du groupe d'administration	116

Création 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 **Appareils 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 dossier **Appareils 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 afficher ce dossier, il faut accéder au menu **Affichage** → **Configuration de l'interface** et dans la fenêtre **Configuration de l'interface** qui s'ouvre, cocher la case **Afficher les Serveurs d'administration secondaires**.

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

Chaque groupe créé, tel que le dossier **Appareils 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 appareils compris dans ce groupe s'affichent sur les onglets correspondants dans la zone de travail de ce groupe.

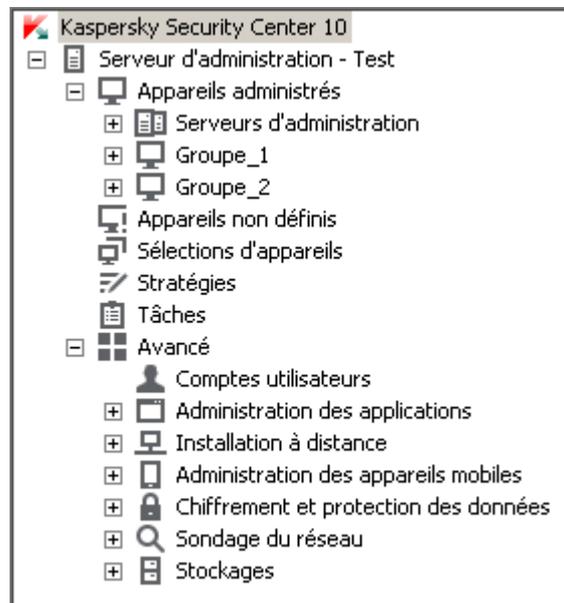


Illustration 9 Consultation des hiérarchies des groupes d'administration

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

1. Dans l'arborescence de la console ouvrez le dossier **Appareils administrés**.
2. Si vous voulez créer un sous-groupe du groupe d'administration existant, dans le dossier **Appareils 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 bouton **Créer un 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.

L'application permet de créer une structure de groupes d'administration sur la base de la structure d'Active Directory ou de la structure du réseau de domaine. Vous pouvez aussi créer une structure de groupes du fichier texte.

► *Pour créer une structure de groupes d'administration, procédez comme suit :*

1. Dans l'arborescence de la console sélectionnez le dossier **Appareils administrés**.
2. Dans le menu contextuel du dossier **Appareils administrés**, sélectionnez l'option **Toutes les tâches** → **Créer une structure de groupes**.

Finalement, l'Assistant de création de la structure des groupes d'administration se lance. Suivez les instructions de l'Assistant.

Déplacement des groupes d'administration

Vous pouvez déplacer les groupes d'administration à l'intérieur de la hiérarchie des groupes.

Le groupe d'administration est déplacé avec tous les sous-groupes, les Serveurs d'administration secondaires, les appareils, les stratégies et les tâches de groupe. Tous les paramètres correspondant à sa nouvelle position dans la hiérarchie des groupes d'administration lui seront appliqués.

Le nom de groupe doit être unique entre groupes du même niveau de hiérarchie. Si dans le dossier dans lequel vous déplacez le groupe d'administration, un groupe avec un tel nom existe déjà, le nom du groupe doit être modifié avec le déplacement. Si vous n'avez pas modifié préalablement le nom du groupe déplacé, le suffixe **<numéro d'ordre>** sera automatiquement ajouté à son nom lors du déplacement, par exemple : **(1)**, **(2)**.

Vous ne pouvez pas renommer le groupe **Appareils administrés**, car il s'agit d'un élément incorporé à la Console d'administration.

► *Pour déplacer le groupe dans un autre dossier de l'arborescence de la console, procédez comme suit :*

1. Sélectionnez le groupe déplacé dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
 - Déplacez le groupe à l'aide du menu contextuel :
 1. Sélectionnez l'option **Couper** dans le menu contextuel du groupe.
 2. Sélectionnez l'option **Coller** dans le menu contextuel du groupe d'administration dans lequel vous voulez déplacer le groupe sélectionné.
 - Déplacez le groupe à l'aide du menu principal de l'application :
 - a. Sélectionnez l'option du menu principal **Action** → **Couper**.
 - b. Sélectionnez dans l'arborescence de la console le groupe d'administration dans lequel vous voulez déplacer le groupe sélectionné.
 - c. Sélectionnez l'option du menu principal **Action** → **Coller**.
 - Déplacez le groupe dans un autre groupe dans l'arborescence de la console à l'aide de la souris.

Suppression des groupes d'administration

Vous pouvez supprimer le groupe d'administration s'il ne contient pas des Serveurs d'administration secondaires, des groupes imbriqués et des appareils clients, et si aucune tâche ou stratégie n'a été créée pour lui.

Avant la suppression du groupe d'administration, il faut supprimer de ce groupe les Serveurs d'administration secondaires, les groupes imbriqués et les appareils clients.

► Pour supprimer un groupe, procédez comme suit :

1. Sélectionnez le groupe d'administration dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
 - sélectionnez l'option **Supprimer** dans le menu contextuel du groupe ;
 - sélectionnez l'option **Action** → **Supprimer** dans le menu principal de l'application ;
 - cliquez sur le bouton **DEL**.

Création automatique de structure des groupes d'administration

Kaspersky Security Center permet de former automatiquement une structure des groupes d'administration à l'aide de l'Assistant de création de la structure des groupes.

L'Assistant crée la structure des groupes d'administration sur la base des données suivantes :

- structure des domaines et des groupes du réseau Windows ;
- structure des groupes Active Directory ;
- contenu du fichier texte créé par l'administrateur à la main.

Lors de la composition du fichier texte, il faut respecter les règles suivantes :

- Le nom de chaque nouveau groupe doit commencer par une nouvelle ligne ; séparateur – traduction de la ligne. Les lignes vides sont ignorées.

Exemple :

Office 1

Office 2

Office 3

Trois groupes hiérarchiques du premier niveau seront formés dans le groupe de destination.

- Il faut indiquer le nom du groupe placé par une barre oblique (/).

Exemple :

Office 1/Subdivision 1/Section 1/Groupe 1

Quatre sous-groupes placés l'un dans l'autre seront formés dans le groupe de destination.

- Pour former quelques groupes placés du même niveau hiérarchique, il faut indiquer "le chemin complet vers le groupe".

Exemple :

Office 1/Subdivision 1/Section 1

Office 1/Subdivision 2/Section 1

Office 1/Subdivision 3/Section 1

Office 1/Subdivision 4/Section 1

Dans le groupe de destination un groupe du premier niveau hiérarchique "Office 1" sera formé. Il sera composé de quatre groupes placés du même niveau hiérarchique "Subdivision 1", "Subdivision 2", "Subdivision 3", "Subdivision 4". Chaque groupe est composé d'un groupe "Section 1".

La création d'une structure de groupes d'administration à l'aide de l'assistant n'atteint pas l'intégrité du réseau : de nouveaux groupes sont ajoutés et ne remplacent pas les groupes existants.

L'appareil client ne peut pas être inclus une seconde fois dans le groupe d'administration, parce que, lors du déplacement de l'appareil dans le groupe d'administration, il se supprime du groupe

Appareils non définis.

Si lors de la création d'une structure des groupes d'administration, l'appareil pour des raisons quelconques n'a pas été inclus dans le groupe **Appareils non définis** (éteint, déconnecté du réseau), il ne sera pas automatiquement déplacé dans le groupe d'administration. Vous pouvez ajouter les appareils dans les groupes d'administration à la main après la fin du fonctionnement de l'Assistant.

► *Pour lancer la création automatique d'une structure des groupes d'administration, procédez comme suit :*

1. Sélectionnez le dossier **Appareils administrés** dans l'arborescence de la console.
2. Dans le menu contextuel du dossier **Appareils administrés**, sélectionnez l'option **Toutes les tâches** → **Créer une structure de groupes**.

Finalement, l'Assistant de création de la structure des groupes d'administration se lance. Suivez les instructions de l'Assistant.

Installation automatique des applications sur les appareils du groupe d'administration

Vous pouvez définir les paquets d'installation à utiliser pour l'installation automatique à distance des applications Kaspersky Lab sur les nouveaux appareils clients qui viennent d'être intégrés au groupe.

► *Afin de configurer l'installation automatique des applications sur les nouveaux appareils 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 appareils 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 appareils 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.

Administration à distance des applications

Cette section contient les informations sur l'administration à distance des applications Kaspersky Lab installées sur les appareils clients à l'aide de stratégies, de profils de stratégie, de tâches et de la configuration des paramètres locaux des applications.

Dans cette section

Administration des stratégies	118
Administration des profils de stratégies	127
Gérer les tâches	134
Consultation et modification des paramètres locaux de l'application	147

Administration des stratégies

La configuration centralisée des paramètres des applications installées sur les appareils clients s'opère à l'aide de la définition de stratégies.

Les stratégies formées pour les applications dans le groupe d'administration s'affichent dans l'espace de travail sous l'onglet **Stratégies**. Une icône figure devant le nom de chaque stratégie et caractérise son état (cf. section "Etats des appareils, des tâches et des stratégies" p. [423](#)).

Après la suppression d'une stratégie ou la fin de ses effets, l'application continue à fonctionner selon les paramètres définis dans la stratégie. Par la suite, il est possible de modifier ces paramètres à la main.

L'application d'une stratégie se déroule de la manière suivante : si des tâches résidentes (tâches de protection en temps réel) sont exécutées sur l'appareil, leur exécution est poursuivie avec les nouvelles valeurs des paramètres. Les tâches lancées périodiquement (analyse à la demande, mise à jour des bases de données de l'application) sont exécutées avec les valeurs non modifiées.

Le nouveau lancement des tâches périodiques est exécuté avec les valeurs modifiées des paramètres.

Dans le cas d'utilisation de la structure hiérarchique des Serveurs d'administration, les Serveurs secondaires obtiennent les stratégies du Serveur d'administration principal et les diffusent vers les appareils clients. Quand le mode d'héritage est activé, les paramètres de la stratégie peuvent être modifiés sur le Serveur d'administration principal. Après cela, les modifications apportées dans les paramètres d'une stratégie se diffusent sur les stratégies héritées des Serveurs d'administration secondaires.

En cas de perte de la connexion entre les Serveurs d'administration principal et secondaire, la stratégie sur le Serveur secondaire continue de fonctionner selon les paramètres précédents. Les paramètres modifiés dans la stratégie sur le Serveur d'administration principal sont propagés vers le Serveur secondaire une fois que la connexion a été rétablie.

Lorsque le mode d'héritage est désactivé, les paramètres de la stratégie peuvent être modifiés sur le Serveur secondaire indépendamment du Serveur principal.

En cas de déconnexion entre le Serveur d'administration et l'appareil client, la stratégie pour les utilisateurs autonomes (si elle a été définie) entre en vigueur sur l'appareil, ou la stratégie continue de fonctionner selon les paramètres précédents jusqu'au rétablissement de la connexion.

Les résultats de la diffusion de la stratégie sur les Serveurs d'administration secondaires figurent dans la fenêtre des propriétés de la stratégie sur le Serveur d'administration principal.

Les résultats de diffusion de la stratégie sur les appareils clients s'affichent dans la fenêtre des propriétés de la stratégie du Serveur d'administration auquel ils sont connectés.

Dans cette section

Création d'une stratégie	120
Affichage des stratégies héritées dans le groupe imbriqué.....	121
Activation d'une stratégie.....	122
Activation automatique d'une stratégie lors d'un événement "Attaque de virus".....	123
Application des stratégies pour les utilisateurs autonomes.....	123

Modification d'une stratégie. Restauration des modifications	124
Suppression d'une stratégie	125
Copie d'une stratégie	125
Exportation d'une stratégie	126
Importation d'une stratégie	126
Conversion des stratégies	127

Création d'une stratégie

Dans la Console d'administration, il est possible de créer des stratégies directement dans le dossier du groupe d'administration pour lequel la stratégie est créée et dans l'espace de travail du dossier **Stratégies**.

► *Pour créer une stratégie dans le dossier du groupe d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut créer une stratégie.
2. Dans l'espace de travail du groupe, sélectionnez l'onglet **Stratégies**.
3. Lancez l'Assistant de création de la stratégie avec le bouton **Création de la stratégie**.

Ceci permet de lancer l'Assistant de création de la stratégie. Suivez les instructions de l'Assistant.

► *Pour créer une stratégie dans l'espace de travail du dossier **Stratégies**, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Stratégies**.
2. Lancez l'Assistant de création de la stratégie avec le bouton **Création de la stratégie**.

Ceci permet de lancer l'Assistant de création de la stratégie. Suivez les instructions de l'Assistant.

Il est possible de créer de nombreuses stratégies pour une application, mais une seule d'entre elles peut être celle active. Lors de la création d'une nouvelle stratégie effective, la stratégie active précédente devient inactive.

Lors de la création de la stratégie, il est possible de configurer un ensemble minimal des paramètres sans lesquels l'application ne fonctionnera pas. Tous les autres paramètres prendront les valeurs par défaut correspondantes à celles définies lors de l'installation locale de l'application. Vous pouvez modifier la stratégie après sa création.

Les paramètres des applications Kaspersky Lab, qui se modifient après l'application des stratégies, sont décrits en détails dans les documentations correspondantes.

Après la création de la stratégie, les paramètres verrouillés (comportant un cadenas ) commencent à agir sur les appareils clients quels que soient les paramètres définis auparavant pour l'application.

Affichage des stratégies héritées dans le groupe imbriqué

► *Pour activer l'affichage des stratégies héritées pour le groupe d'administration imbriqué, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut afficher les stratégies héritées.
2. Sélectionnez l'onglet **Stratégies** pour le groupe sélectionné dans l'espace de travail.
3. Dans le menu contextuel de la liste des stratégies, sélectionnez l'option **Affichage** → **Stratégies héritées**.

Ainsi, les stratégies héritées s'affichent dans la liste des stratégies avec l'icône :

-  – si elles ont été héritées du groupe créé sur le Serveur d'administration principal ;
-  – si elles ont été héritées d'un groupe de niveau supérieur.

Lorsque le mode d'héritage des paramètres est activé, la modification des stratégies héritées n'est possible que dans les groupes où elles ont été créées. La modification de stratégies héritées n'est pas disponible dans le groupe qui hérite les stratégies.

Activation d'une stratégie

► *Pour activer une stratégie pour le groupe sélectionné, procédez comme suit :*

1. Dans l'espace de travail du groupe sous l'onglet **Stratégies**, sélectionnez la stratégie qui doit être active.
2. Pour activer une stratégie, exécutez une des actions suivantes :
 - Dans le menu contextuel de la stratégie, sélectionnez l'option **Stratégie active**.
 - Dans la fenêtre des propriétés de la stratégie, ouvrez la section **Général** et dans le groupe des paramètres **Etat de la stratégie**, sélectionnez l'option **Stratégie active**.

Finalement, la stratégie devient active pour le groupe d'administration sélectionné.

Tout changement de stratégie réalisé simultanément sur un grand nombre d'appareils clients augmente considérablement la charge du Serveur d'administration ainsi que le volume du trafic réseau.

Activation automatique d'une stratégie lors d'un événement "Attaque de virus"

► *Pour que la stratégie soit automatiquement activée lors d'un événement "Attaque de virus", procédez comme suit :*

1. Dans la fenêtre des propriétés du Serveur d'administration, ouvrez la section **Attaque de virus**.
2. Ouvrez la fenêtre **Activation des stratégies** à l'aide du lien **Configurer l'activation des stratégies suite à une "Attaque de virus"** et ajoutez la stratégie dans la liste sélectionnée des stratégies activées lors de la détection d'une activité virale.

Si vous désactivez la stratégie en fonction de l'événement *Attaque de virus*, vous ne pouvez rétablir la stratégie précédente que manuellement.

Application des stratégies pour les utilisateurs autonomes

La stratégie pour les utilisateurs autonomes entre en vigueur sur l'appareil dans le cas de déconnexion du réseau d'entreprise.

► *Pour appliquer la stratégie sélectionnée pour les utilisateurs autonomes,*

dans la fenêtre des propriétés de la stratégie, ouvrez la section **Général** et dans le groupe des paramètres **Etat de la stratégie**, sélectionnez l'option **Stratégie pour les utilisateurs autonomes**.

Finalement, la stratégie commence à agir sur les appareils dans le cas de leur déconnexion du réseau d'entreprise.

Modification d'une stratégie. Restauration des modifications

► *Pour modifier une stratégie, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Stratégies**.
2. Dans l'espace de travail du dossier **Stratégies**, sélectionnez la stratégie et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
3. Apportez les modifications nécessaires.
4. Cliquez sur le bouton **Appliquer**.

Les modifications de la stratégie seront enregistrées dans les propriétés de la stratégie, dans la section **Historique des révisions**.

En cas de besoin, vous pouvez restaurer les modifications de la stratégie.

► *Pour restaurer les modifications de la stratégie, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Stratégies**.
2. Sélectionnez la stratégie dont vous souhaitez restaurer les modifications et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
3. Sélectionnez la section **Historique des révisions** dans la fenêtre des propriétés de la stratégie.
4. Dans la liste des révisions de la stratégie, sélectionnez le numéro de révision dont il faut restaurer les modifications.
5. Cliquez sur le bouton **Avancé** et dans la liste déroulante, sélectionnez la valeur **Restaurer**.

Suppression d'une stratégie

► *Pour supprimer une stratégie, procédez comme suit :*

1. Dans l'espace de travail du groupe d'administration sous l'onglet **Stratégies**, sélectionnez la stratégie qui doit être supprimée.
2. Supprimez la stratégie à l'aide d'un des moyens suivants :
 - Sélectionnez l'option **Supprimer** dans le menu contextuel de la stratégie.
 - A l'aide du lien **Supprimer la stratégie**, situé dans l'espace de travail, dans le groupe de travail avec la stratégie sélectionnée.

Copie d'une stratégie

► *Pour copier une stratégie, procédez comme suit :*

1. Dans l'espace de travail du groupe nécessaire, sélectionnez une stratégie sous l'onglet **Stratégies**.
2. Sélectionnez l'option **Copier** dans le menu contextuel de la stratégie.
3. Sélectionnez dans l'arborescence de la console le groupe à ajouter une stratégie.

La stratégie peut être ajoutée dans le groupe depuis lequel elle a été copiée.

4. Dans le menu contextuel de la liste des stratégies pour le groupe sélectionné sous l'onglet **Stratégies**, sélectionnez l'option **Coller**.

La stratégie est copiée avec tous les paramètres et elle est diffusée sur tous les appareils du groupe où elle a été déplacée. Si vous insérez la stratégie dans le groupe depuis lequel elle a été copiée, le suffixe de type (<numéro d'ordre>) s'ajoute automatiquement au nom de la stratégie, par exemple : **(1)**, **(2)**.

Une stratégie active devient inactive lors de la copie. Le cas échéant, vous pouvez en faire une stratégie active.

Exportation d'une stratégie

► *Pour exporter une stratégie, procédez comme suit :*

1. Exportez la stratégie à l'aide d'un des moyens suivants :
 - Dans le menu contextuel de la stratégie, sélectionnez l'option **Toutes les tâches** → **Exporter**.
 - A l'aide du lien **Exporter la stratégie dans le fichier** situé dans l'espace de travail, dans le groupe de travail avec la stratégie sélectionnée.
2. Dans la fenêtre **Enregistrer sous** qui s'ouvre, indiquez le nom du fichier de la stratégie et le chemin d'accès pour son enregistrement. Cliquez sur **Enregistrer**.

Importation d'une stratégie

► *Pour importer une stratégie, procédez comme suit :*

1. Dans l'espace de travail du groupe nécessaire sous l'onglet **Stratégies**, sélectionnez un des moyens suivants d'importation de la stratégie :
 - Dans le menu contextuel de la liste des stratégies, sélectionnez l'option **Toutes les tâches** → **Importer**.
 - A l'aide du lien **Importer une stratégie à partir d'un fichier** dans le groupe d'administration de la liste des stratégies.
2. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier depuis lequel vous souhaitez importer la stratégie. Cliquez sur **Ouvrir**.

Finalement, la stratégie ajoutée s'affiche dans la liste des stratégies.

Si, dans la liste sélectionnée des stratégies, une stratégie présentant un nom similaire à la stratégie importée existe déjà, le suffixe de type (**<numéro d'ordre>**) sera ajouté au nom de la stratégie importée, par exemple : **(1)**, **(2)**.

Conversion des stratégies

Kaspersky Security Center peut convertir les stratégies des versions précédentes des applications Kaspersky Lab en stratégies des versions actuelles de ces applications.

La conversion est possible pour les stratégies des applications suivantes :

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 ;
- Kaspersky Endpoint Security 8 for Windows ;
- Kaspersky Endpoint Security 10 for Windows.

► *Pour convertir les stratégies, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous voulez convertir les stratégies.
2. Dans le menu contextuel du Serveur d'administration, sélectionnez le point **Toutes les tâches** → **Assistant de conversion en masse des stratégies et des tâches**.

Ensuite, l'Assistant de conversion en masse des stratégies et des tâches se lance. Suivez les instructions de l'Assistant.

Finalement l'Assistant forme des nouvelles stratégies qui utilisent les paramètres des stratégies des versions précédentes des applications Kaspersky Lab.

Administration des profils de stratégie

Cette section contient des informations sur les profils de stratégies utilisés pour gérer efficacement les groupes d'appareils clients. Elle décrit les avantages des profils des stratégies et les modes d'application. La section reprend également les instructions de création, de configuration et de suppression de profils de stratégie.

A propos du profil de stratégie

Un profil de stratégie est un ensemble de paramètres variables d'une stratégie qui est activé sur un ordinateur client (ordinateur ou appareil mobile) lorsque certaines conditions sont remplies. Quand le profil est activé, les paramètres de la stratégie en vigueur sur l'ordinateur avant l'activation du profil sont modifiés. Ces paramètres prennent alors les valeurs reprises dans le profil.

Les profils sont pris en charge uniquement pour les stratégies suivantes :

- stratégies de l'application Kaspersky Endpoint Security 10 Service Pack 1 for Windows et versions supérieures ;
- stratégies de l'application Kaspersky Endpoint Security 10 Service Pack 1 for Mac ;
- stratégies du plug-in Kaspersky Mobile Device Management 10 Service Pack 1 et versions supérieures.

Avantages des profils de stratégies

Les profils de stratégie simplifient la gestion des postes clients à l'aide de stratégies :

- Les profils contiennent uniquement les paramètres qui se différencient des paramètres de la stratégie de base.
- Il n'est pas nécessaire de maintenir et d'appliquer manuellement plusieurs copies d'une stratégie qui se distinguent uniquement par un faible nombre de paramètres.
- Il n'est pas nécessaire de prévoir une stratégie distincte pour des utilisateurs autonomes.
- Les nouveaux profils de stratégies sont faciles à créer. L'importation et l'exportation de profils sont prises en charge ainsi que la création de profils sur la base de profils existants à l'aide de la copie.
- Plusieurs profils de stratégie peuvent être activés simultanément sur un poste client.
- La hiérarchie des stratégies est prise en charge.

Règles d'activation d'un profil. Priorités des profils

Le profil de stratégie s'active sur le poste client quand une règle d'activation est remplie. Une règle

d'activation peut contenir les conditions suivantes :

- L'Agent d'administration sur l'appareil client se connecte au serveur selon une sélection de paramètres de connexion définis (adresse du serveur, numéro de port, etc.).
- L'appareil client se trouve en mode déconnecté.
- Des tags déterminés ont été attribués au poste client.
- L'ordinateur client se trouve dans un sous-groupe déterminé d'Active Directory®, l'ordinateur ou son propriétaire se trouvent dans un groupe de sécurité Active Directory.
- L'ordinateur client appartient à un propriétaire défini ou son propriétaire se trouve dans le groupe de sécurité interne Kaspersky Security Center.

Les profils créés pour une stratégie sont classés par ordre de priorité décroissante. Par exemple, si le profil *X* se trouve avant le profil *Y* dans la liste de profils, cela signifie que la priorité du profil *X* est supérieure à celle du profil *Y*. Les priorités des profils sont indispensables, car plusieurs profils peuvent être activés au même moment sur l'appareil client.

Stratégies dans la hiérarchie des groupes d'administration

Alors que les stratégies exercent une influence l'une sur l'autre en fonction de la hiérarchie des groupes d'administration, les profils qui portent un même nom s'unissent. Les profils d'une stratégie plus "haute" ont une plus grande priorité. Ainsi, la stratégie $P(A)$ du groupe d'administration *A* contient les profils *X1*, *X2* et *X3* par ordre de priorité descendante. Dans le groupe d'administration *B*, qui est un sous-groupe du groupe *A*, la stratégie $P(B)$ est créée avec les profils *X2*, *X4* et *X5*. Alors la stratégie $P(B)$ sera remplacée par la stratégie $P(A)$ de sorte que dans la stratégie $P(B)$, la liste des profils par ordre de priorité décroissante sera *X1*, *X2*, *X3*, *X4*, *X5*. La priorité du profil *X2* dépendra de l'état d'origine de *X2* de la stratégie $P(B)$ et *X2* de la stratégie $P(A)$.

La stratégie active est l'ensemble de la stratégie principale et des profils actifs de cette stratégie, à savoir les profils pour lesquels les règles d'activation sont exécutées. La stratégie active est recalculée au lancement de l'Agent d'administration, lors de l'activation ou de la désactivation du mode déconnecté ou en cas de modification de la liste des tags attribués à l'appareil client.

Propriétés et restrictions d'un profil de stratégie

Les profils possèdent les propriétés suivantes :

- Les profils d'une stratégie inactive n'ont aucun impact sur les postes client.
- Si la stratégie est active en mode déconnecté, les profils de cette stratégie sont appliqués uniquement en mode déconnecté.
- Les profils ne prennent pas en charge l'analyse statistique de l'accès aux fichiers exécutables.
- Une stratégie ne peut pas contenir des paramètres de notification.
- En cas de connexion de l'appareil au Serveur d'administration via le port UDP 15000, il faudra activer le profil de stratégie correspondant dans la minute lors de l'attribution d'un tag à l'appareil.
- Les règles de connexion de l'Agent d'administration au Serveur d'administration peuvent être utilisées lors de la création des règles d'activation du profil.

Création d'un profil de stratégie

La création d'un profil est uniquement possible pour les stratégies de Kaspersky Endpoint Security 10 Service Pack 1 for Windows.

► *Pour créer un profil de stratégie pour un groupe d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut créer un profil de stratégie.
2. Dans l'espace de travail du groupe, sélectionnez l'onglet **Stratégies**.
3. Sélectionnez la stratégie et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
4. Ouvrez la section **Profil de la stratégie** dans les propriétés de la stratégie, puis cliquez sur le bouton **Ajouter**.

5. Dans la fenêtre **Propriétés : Nouveau profil** , configurez les paramètres du profil de la stratégie :

- Dans la section **Général**, spécifiez le nom du profil.

Le nom du profil ne peut pas contenir plus de 100 caractères.

- Activez ou désactivez le profil à l'aide de la case **Activer le profil**.

Si la case est décochée, le profil n'est pas utilisé pour administrer l'appareil.

6. Dans le groupe **Règles d'activation**, créez les règles d'activation du profil :

- Cliquez sur le bouton **Ajouter**.
- Définissez les règles d'activation du profil de stratégie dans la fenêtre **Propriétés : Nouvelle règle**.
- Cliquez sur le bouton **OK**.

7. Modifiez les paramètres de la stratégie dans les sections correspondantes.

8. Une fois que le profil a été configuré et que les règles d'activation ont été créées, enregistrez les modifications en cliquant sur **OK**.

Le profil est enregistré. Le profil sera activé sur l'appareil lors de l'application des règles d'activation.

Les profils créés pour une stratégie sont affichés dans les propriétés de la stratégie, dans la section **Profils des stratégies**. Vous pouvez modifier le profil d'une stratégie et la priorité d'un profil (cf. section "Modification du profil d'une stratégie" à la page [132](#)). Il est également possible de supprimer un profil (cf. section "Suppression d'un profil de stratégie" à la page [133](#)).

Plusieurs profils de stratégie peuvent être activés simultanément lors de l'application des règles d'activation des profils.

Modification du profil d'une stratégie

Modification des paramètres du profil de stratégie

La modification d'un profil est uniquement possible pour les stratégies de Kaspersky Endpoint Security 10 Service Pack 1 pour Windows.

► *Pour modifier un profil de stratégie, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut modifier le profil de stratégie.
2. Dans l'espace de travail du groupe, sélectionnez l'onglet **Stratégies**.
3. Sélectionnez la stratégie et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
4. Ouvrez la section **Profil de la stratégie** dans les propriétés de la stratégie.

La section contient la liste des profils créés pour la stratégie. Les profils de la liste sont affichés conformément à leur priorité.

5. Sélectionnez le profil de stratégie, puis cliquez sur le bouton **Propriétés**.
6. Configurez les paramètres du profil dans la fenêtre des propriétés :
 - Le cas échéant, modifiez dans la section **Général** le nom du profil et activez ou désactivez le profil à l'aide de la case **Activer le profil**.
 - Dans le groupe **Règles d'activation**, modifiez les règles d'activation du profil.
 - Modifiez les paramètres de la stratégie dans les sections correspondantes.
7. Cliquez sur le bouton **OK**.

Les paramètres modifiés entrent en vigueur après la synchronisation de l'appareil avec le Serveur d'administration (si le profil de stratégie est actif), ou après l'exécution de la règle d'activation (si le profil de stratégie est inactif).

Modification de la priorité du profil de stratégie

La priorité des profils de stratégie détermine l'ordre d'activation de ces profils sur l'appareil client. La priorité intervient si différents profils de stratégie sont soumis aux mêmes règles d'activation.

Imaginons deux profils de stratégie : *Profil 1* et *Profil 2* qui se distinguent uniquement par les valeurs d'un paramètre (*Valeur 1* et *Valeur 2*). La priorité du *Profil 1* est supérieure à celle du *Profil 2*. De plus, il existe d'autres profils dont la priorité est inférieure à celle de *Profil 2*. Les règles d'activation des profils correspondent.

En cas d'exécution des règles d'activation, s'est le *Profil 1* qui sera activé. Le paramètre sur l'appareil prend la *Valeur 1*. Si le *Profil 1* est supprimé, c'est le *Profil 2* qui aura la priorité la plus haute et le paramètre prendra la *Valeur 2*.

La liste des profils de stratégie affiche les profils selon leur priorité. La tête de la liste revient au profil possédant la priorité la plus élevée. Pour modifier la priorité d'un profil,

utilisez les boutons  et .

Suppression d'un profil de stratégie

► Pour supprimer un profil de stratégie, procédez comme suit :

1. Sélectionnez dans l'arborescence de la console le groupe d'administration dans lequel vous voulez supprimer le profil de stratégie.
2. Dans l'espace de travail du groupe d'administration, ouvrez l'onglet **Stratégies**.
3. Sélectionnez la stratégie et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
4. Ouvrez la section **Profil de la stratégie** dans les propriétés de la stratégie de Kaspersky Endpoint Security.
5. Sélectionnez le profil de stratégie que vous souhaitez supprimer, puis cliquez sur le bouton **Supprimer**.

Le profil de stratégie sera supprimé. Il sera remplacé par un autre profil de stratégie dont les règles d'activation sont exécutées sur l'appareil ou par une stratégie.

Gérer les tâches

Kaspersky Security Center gère le fonctionnement des applications installées sur les appareils par la création et l'exécution des tâches. Les tâches permettent d'exécuter l'installation, le lancement et l'arrêt des applications, l'analyse des fichiers, la mise à jour des bases de données et des modules des applications, les autres actions avec les applications.

Les tâches sont scindées en types suivants :

- *Tâches de groupe*. Tâches exécutées sur les appareils du groupe d'administration sélectionné.
- *Tâches du Serveur d'administration*. Tâches exécutées sur le Serveur d'administration.
- *Tâches pour les ensembles des appareils*. Tâches exécutées sur les appareils sélectionnés peu importe leur inclusion dans les groupes d'administration.
- *Tâches locales*. Tâches exécutées sur un appareil particulier.

La création des tâches pour l'application est possible uniquement si le poste de travail de l'administrateur est doté du plug-in d'administration de l'application.

La liste des appareils pour lesquels la tâche sera créée peut être formée par une des méthodes suivantes :

- Sélectionner les appareils détectés sur le réseau par le Serveur d'administration.
- Définir la liste des appareils manuellement. Vous pouvez utiliser l'adresse IP (ou l'intervalle IP), le nom NetBIOS ou le nom DNS en tant que l'adresse de l'appareil.
- Importer la liste des appareils depuis le fichier au format TXT, contenant la liste des adresses des appareils ajoutés (chaque adresse doit se trouver dans une ligne séparée).

Si la liste des appareils est importée depuis le fichier ou formée manuellement et les appareils sont identifiés selon le nom, uniquement les appareils dont les informations sont déjà enregistrées dans la base de données du Serveur d'administration peuvent être ajoutés dans la liste lors de la connexion des appareils ou lors du sondage du réseau.

Pour chaque application vous pouvez créer n'importe quel nombre de tâches de groupe, de tâches pour des ensembles d'appareils et des tâches locales.

L'échange des informations sur les tâches entre l'application installée sur l'appareil et la base d'informations de Kaspersky Security Center a lieu au moment de la connexion de l'Agent d'administration au Serveur d'administration.

Vous pouvez modifier les paramètres des tâches, suivre l'exécution des tâches, copier, exporter ou importer, ainsi que supprimer les tâches.

Les tâches ne sont lancées sur un appareil que lorsque l'application pour laquelle les tâches ont été créées est lancée. Si l'application est désactivée, toutes les tâches courantes sont annulées.

Les résultats de l'exécution des tâches sont enregistrés dans les journaux des événements Microsoft Windows et Kaspersky Security Center d'une manière centralisée sur le Serveur d'administration et d'une manière locale sur chaque appareil.

Création d'une tâche de groupe

Dans la Console d'administration, il est possible de créer des tâches directement dans le dossier du groupe d'administration pour lequel la tâche de groupe est créée et dans l'espace de travail du dossier **Tâches**.

► *Pour créer une tâche de groupe dans le dossier du groupe d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut créer une tâche.
2. Dans l'espace de travail du groupe, sélectionnez l'onglet **Tâches**.
3. Lancez le processus de création d'une tâche à l'aide du bouton **Créer une tâche**.

Ceci permet de lancer l'Assistant de création de tâche. Suivez les instructions de l'Assistant.

► *Pour créer une tâche dans l'espace de travail du dossier **Tâches**, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Lancez le processus de création d'une tâche à l'aide du bouton **Créer une tâche**.

Ceci permet de lancer l'Assistant de création de tâche. Suivez les instructions de l'Assistant.

Création d'une tâche du Serveur d'administration

Le Serveur d'administration exécute les tâches suivantes :

- diffusion automatique des rapports ;
- téléchargement des mises à jour dans le stockage ;
- sauvegarde des données du Serveur d'administration ;
- maintenance de la base de données ;
- synchronisation des mises à jour Windows Update ;
- création du paquet d'installation sur la base de l'image du système d'exploitation de l'appareil d'étalon.

Uniquement la tâche de diffusion automatique des rapports est disponible sur le Serveur d'administration virtuel, ainsi que la tâche de création du paquet d'installation sur la base de l'image du système d'exploitation de l'appareil d'étalon. Les mises à jour téléchargées sur le Serveur d'administration principal s'affichent dans le stockage du Serveur virtuel. La copie de sauvegarde des données du Serveur virtuel s'effectue dans le cadre de la copie de sauvegarde des données du Serveur d'administration principal.

► *Pour créer une tâche du Serveur d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Lancez le processus de création de la tâche par un des moyens suivants :
 - Dans l'arborescence de la console, dans le menu contextuel du dossier **Tâches**, sélectionnez le point **Créer** → **Tâche**.
 - A l'aide du bouton **Créer une tâche** dans l'espace de travail du dossier **Tâches**.

Ceci permet de lancer l'Assistant de création de tâche. Suivez les instructions de l'Assistant.

Les tâches **Téléchargement des mises à jour dans le stockage**, **Synchronisation des mises à jour Windows Update**, **Maintenance de la base de données** et **Sauvegarde des données du Serveur d'administration** peuvent exister dans un seul exemplaire. Si les tâches **Téléchargement des mises à jour dans le stockage**, **Maintenance de la base de données**, **Sauvegarde des données du Serveur d'administration** et **Synchronisation des mises à jour Windows Update** ont déjà été créées pour le Serveur d'administration, elles ne s'affichent pas dans la fenêtre de sélection du type de tâche de l'Assistant de création d'une tâche.

Création d'une tâche pour un ensemble d'appareils

Kaspersky Security Center permet de créer une tâche pour un ensemble d'appareils sélectionné d'une manière aléatoire. Les appareils dans l'ensemble peuvent être inclus dans des différents groupes d'administration ou ne faire partie d'un aucun groupe d'administration. Kaspersky Security Center permet d'exécuter les tâches principales suivantes pour un ensemble d'appareils :

- installation à distance de l'application (cf. *Manuel d'implantation de Kaspersky Security Center*) ;
- envoi d'un message à l'utilisateur (cf. section "Envoi d'un message aux utilisateurs des appareils" à la page [165](#)) ;

- modification du Serveur d'administration (cf. section "Modification du Serveur d'administration pour les appareils clients" à la page [163](#)) ;
- administration d'un appareil (cf. section "Démarrage, arrêt et redémarrage à distance des appareils clients" à la page [164](#)) ;
- vérification des mises à jour (cf. section "Analyse des mises à jour récupérées" à la page [333](#)) ;
- diffusion du paquet d'installation (cf. *Manuel d'implantation de Kaspersky Security Center*) ;
- installation à distance de l'application sur les Serveurs d'administration secondaires (cf. *Manuel d'implantation de Kaspersky Security Center*) ;
- tâche de désinstallation à distance de l'application (cf. *Manuel d'implantation de Kaspersky Security Center*).

► *Pour créer une tâche pour un ensemble d'appareils, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
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**, sélectionnez l'option **Créer** → **Tâche**.
 - A l'aide du bouton **Créer une tâche** dans l'espace de travail du dossier **Tâches**.

Ceci permet de lancer l'Assistant de création de tâche. Suivez les instructions de l'Assistant.

Création d'une tâche locale

► *Pour créer une tâche locale pour un appareil, procédez comme suit :*

1. Dans l'espace de travail incluant l'appareil, sélectionnez l'onglet **Appareils**.
2. Dans la liste des appareils, sous l'onglet **Appareils**, sélectionnez l'appareil pour lequel il faut créer une tâche locale.

3. Lancez le processus de création d'une tâche pour l'appareil sélectionné à l'aide d'un des moyens suivants :

- Appuyez sur le bouton **Exécuter l'action** et, dans la liste déroulante, sélectionnez **Créer une tâche**.
- A l'aide du lien **Créer une tâche** dans le groupe de fonctionnement avec l'appareil.
- Depuis la fenêtre des propriétés de l'appareil :
 - a. Dans le menu contextuel de l'appareil, sélectionnez l'option **Propriétés**.
 - b. Dans la fenêtre ouverte des propriétés de l'appareil, sélectionnez la section **Tâches** et cliquez sur le bouton **Ajouter**.

Ceci permet de lancer l'Assistant de création de tâche. Suivez les instructions de l'Assistant.

Pour plus d'informations sur la création et la configuration des tâches locales, reportez-vous à la documentation des applications Kaspersky Lab correspondantes.

Affichage d'une tâche de groupe héritée dans la zone de travail du groupe imbriqué

► *Pour activer l'affichage des tâches héritées du groupe imbriqué dans l'espace de travail, procédez comme suit :*

1. Sélectionnez dans l'espace de travail du groupe imbriqué, l'onglet **Tâches**.
2. Dans l'espace de travail de l'onglet **Tâches**, cliquez sur le bouton **Afficher les tâches héritées**.

Ainsi, les tâches héritées s'affichent dans la liste des tâches avec l'icône :

-  – si elles ont été héritées du groupe créé sur le Serveur d'administration principal ;
-  – si elles ont été héritées d'un groupe de niveau supérieur.

Lorsque le mode d'héritage est activé, la modification des tâches héritées n'est possible que dans les groupes où elles ont été créées. La modification des tâches héritées n'est pas disponible dans le groupe qui hérite les tâches.

Activation automatique des appareils avec le lancement de la tâche

Kaspersky Security Center permet de configurer les paramètres des tâches pour que le système d'exploitation se démarre avant l'exécution de la tâche sur les appareils éteints.

► *Pour configurer le démarrage automatique des appareils avant le lancement de la tâche, procédez comme suit :*

1. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Programmation**.
2. Ouvrez la fenêtre de configuration des actions avec les appareils à l'aide du lien **Avancé**.
3. Dans la fenêtre **Avancé** qui s'ouvre, cochez la case **Activer l'appareil avant lancement de tâche par la fonction Wake On LAN (min.)**. Ensuite, spécifiez le temps souhaité en minutes.

Dès lors, les appareils désactivés seront automatiquement activés dans les délais avant le lancement de la tâche indiqués en minutes et le système d'exploitation sera chargé.

Le démarrage automatique du système d'exploitation est accessible uniquement sur les appareils qui supportent la fonction Wake On Lan.

Arrêt automatique de l'appareil après l'exécution de la tâche

Kaspersky Security Center permet de configurer les paramètres des tâches de telle manière pour qu'après son exécution les appareils, sur lesquels elle est diffusée, soient automatiquement éteints.

► *Pour que les appareils soient automatiquement éteints après l'exécution des tâches, procédez comme suit :*

1. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Programmation**.
2. Ouvrez la fenêtre de configuration des actions avec les appareils à l'aide du lien **Avancé**.
3. Dans la fenêtre qui s'ouvre, cochez la case **Avancé** qui s'ouvre, cochez la case **Eteindre l'appareil après la fin de la tâche**.

Limitation de la durée d'exécution de la tâche

► *Pour limiter la durée d'exécution de la tâche sur les appareils, procédez comme suit :*

1. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Programmation**.
2. Ouvrez la fenêtre de configuration des actions avec les appareils clients à l'aide du lien **Avancé**.
3. Dans la liste déroulante **Avancé**, cochez la case **Stopper si la tâche prend plus de (min.)** et indiquez la durée en minutes.

Finalement, Kaspersky Security Center arrêtera automatiquement l'exécution de la tâche si à l'issue du temps indiqué, l'exécution de la tâche ne se terminera pas sur l'appareil.

Exportation d'une tâche

Vous pouvez exporter les tâches de groupe et les tâches pour les ensembles d'appareils dans un fichier. Les tâches du Serveur d'administration et les tâches locales ne peuvent pas être exportées.

► *Pour exporter une tâche, procédez comme suit :*

1. Dans le menu contextuel de la tâche, sélectionnez l'option **Toutes les tâches** → **Exporter**.
2. Dans la fenêtre **Enregistrer sous** qui s'ouvre, indiquez le nom du fichier et le chemin d'accès pour l'enregistrement.
3. Cliquez sur **Enregistrer**.

Les privilèges des utilisateurs locaux ne sont pas exportés.

Importation d'une tâche

Vous pouvez importer les tâches de groupe et les tâches pour les ensembles d'appareils. Les tâches du Serveur d'administration et les tâches locales ne peuvent pas être importées.

► *Pour importer une tâche, procédez comme suit :*

1. Sélectionnez la liste des tâches dans laquelle il faut importer la tâche :
 - Si vous voulez importer la tâche dans la liste des tâches de groupe, sélectionnez l'onglet **Tâches** dans l'espace de travail du groupe d'administration nécessaire.
 - Si vous voulez importer la tâche dans la liste des ensembles d'appareils, sélectionnez le dossier **Tâches pour les ensembles des appareils** dans l'arborescence de la console.
2. Sélectionnez un des moyens suivants d'importation de la tâche :
 - Dans le menu contextuel de la liste des tâches, sélectionnez l'option **Toutes les tâches** → **Importer**.
 - A l'aide du lien **Importer une tâche à partir d'un fichier** dans le groupe d'administration de la liste des tâches.
3. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier depuis lequel vous souhaitez importer la tâche.
4. Cliquez sur **Ouvrir**.

Suite à l'importation, la tâche s'affiche dans la liste des tâches.

Si, dans la liste sélectionnée, une tâche présentant un nom similaire à la tâche importée existe déjà, le suffixe de type (**<numéro d'ordre>**) sera ajouté au nom de la tâche importée, par exemple : **(1)**, **(2)**.

Conversion des tâches

Kaspersky Security Center permet de convertir les tâches des versions précédentes des applications Kaspersky Lab en tâches des versions actuelles des applications.

La conversion est possible pour les tâches des applications suivantes :

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 ;
- Kaspersky Endpoint Security 8 for Windows ;
- Kaspersky Endpoint Security 10 for Windows.

► *Pour convertir les tâches, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous voulez convertir les tâches.
2. Dans le menu contextuel du Serveur d'administration, sélectionnez le point **Toutes les tâches** → **Assistant de conversion en masse des stratégies et des tâches**.

Ensuite, l'Assistant de conversion en masse des stratégies et des tâches se lance. Suivez les instructions de l'Assistant.

Finalement l'Assistant forme des nouvelles tâches qui utilisent les paramètres des tâches des versions précédentes des applications.

Démarrage et arrêt manuels des tâches

Les tâches peuvent être lancées et arrêtées par deux moyens : à partir du menu contextuel de tâches et dans la fenêtre de propriétés de l'appareil auquel la tâche est affectée.

Seuls les utilisateurs qui appartiennent au groupe **KLAdmins** peuvent lancer des tâches de groupe via le menu contextuel de l'appareil (cf. section "Privilèges d'accès au Serveur d'administration et à ses objets" à la page [96](#)).

► Pour lancer ou arrêter une tâche via le menu contextuel ou la fenêtre des propriétés, procédez comme suit :

1. Sélectionnez une tâche dans la liste des tâches.
2. Lancez ou arrêtez la tâche à l'aide d'un des moyens suivants :
 - Dans le menu contextuel de la tâche, sélectionnez l'option **Démarrer** ou **Arrêter**.
 - Dans la section **Général** de la fenêtre des propriétés de la tâche, cliquez sur le bouton **Démarrer** ou **Arrêter**.

► Pour lancer ou arrêter une tâche via le menu contextuel ou la fenêtre des propriétés de l'appareil, procédez comme suit :

1. Sélectionnez l'appareil dans la liste des appareils.
2. Lancez ou arrêtez la tâche à l'aide d'un des moyens suivants :
 - Dans le menu contextuel de l'appareil, sélectionnez l'option **Toutes les tâches** → **Lancer la tâche**. Sélectionnez la tâche souhaitée dans la liste.

La liste des appareils auxquels la tâche a été affectée se trouvera dans l'appareil sélectionné. La tâche sera lancée.

- Dans la la fenêtre des propriétés de l'appareil, dans la section **Tâches**, cliquez sur le

bouton  ou .

Suspension et reprise manuelles d'une tâche

► *Pour suspendre ou reprendre l'exécution de la tâche lancée, procédez comme suit :*

1. Sélectionnez une tâche dans la liste des tâches.
2. Suspendez ou reprenez l'exécution de la tâche à l'aide d'un des moyens suivants :
 - Dans le menu contextuel de la tâche, sélectionnez l'option **Pause** ou **Reprendre**.
 - Dans la section **Général** de la fenêtre des propriétés de la tâche, cliquez sur le bouton **Pause** ou **Reprendre**.

Suivi et affichage des comptes-rendus d'activité des tâches

► *Pour surveiller l'exécution des tâches,*

Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Général**.

Le milieu de la fenêtre de la section **Général** contient les informations sur l'état actuel de la tâche.

Affichage de l'historique des tâches entreposé sur le Serveur d'administration

Kaspersky Security Center permet de consulter les résultats d'exécution des tâches de groupe, des tâches pour des ensembles d'appareils et des tâches du Serveur d'administration.

La consultation des résultats d'exécution des tâches locales n'est pas disponible.

► *Pour consulter les résultats de l'exécution de la tâche, procédez comme suit :*

1. Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Général**.
2. Sur le lien **Résultats**, ouvrez la fenêtre **Résultats de la tâche**.

Configuration du filtre d'informations sur les résultats de la tâche

Kaspersky Security Center permet de filtrer les informations sur les résultats d'exécution des tâches de groupe, des tâches pour des ensembles d'appareils et des tâches du Serveur d'administration. Le filtrage n'est pas disponible pour les tâches locales.

► *pour configurer le filtrage pour les informations sur les résultats de la tâche, procédez comme suit :*

1. Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Général**.
2. Sur le lien **Résultats**, ouvrez la fenêtre **Résultats de la tâche**.

Le tableau dans la partie supérieure de la fenêtre contient la liste de tous les appareils pour lesquels la tâche a été désignée. Le tableau de la partie inférieure de la fenêtre contient les résultats de l'exécution des tâches sur l'appareil sélectionné.

3. Dans le tableau qui vous intéresse, ouvrez le menu contextuel avec le bouton droit de la souris et sélectionnez le point **Filtre**.
4. Dans la fenêtre ouverte **Appliquer le filtre**, configurez les paramètres du filtre dans les sections de la fenêtre **Événements**, **Appareils** et **Heure**. Cliquez sur le bouton **OK**.

Après cela, les informations qui vérifient les paramètres indiqués dans le filtre seront affichées dans la fenêtre **Résultats de la tâche**.

Modification d'une tâche. Restauration des modifications

► *Pour modifier une tâche, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Dans l'espace de travail du dossier **Tâches**, choisissez la tâche et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.

3. Apportez les modifications nécessaires.

Dans la section **Exclusions de la zone d'action de la tâche**, configurez la liste des sous-groupes auxquels la tâche ne sera pas appliquée.

4. Cliquez sur le bouton **Appliquer**.

Les modifications de la tâche seront enregistrées dans la fenêtre des propriétés de la tâche, dans la section **Historique des révisions**.

En cas de besoin, vous pouvez restaurer les modifications de la tâche.

► *Pour restaurer les modifications d'une tâche, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Sélectionnez la tâche dont il faut restaurer les modifications et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
3. Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Historique des révisions**.
4. Dans la liste des révisions de la tâche, sélectionnez le numéro de la révision pour laquelle il faut restaurer les modifications.
5. Cliquez sur le bouton **Avancé** et dans la liste déroulante, sélectionnez la valeur **Restaurer**.

Consultation et modification des paramètres locaux de l'application

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

Les *Paramètres locaux des applications* sont les paramètres de l'application individuels pour chaque appareil. A l'aide de Kaspersky Security Center, vous pouvez installer les paramètres locaux des applications pour les appareils 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 l'appareil nécessaire, sélectionnez l'onglet **Appareils**.
2. Dans la fenêtre des propriétés de l'appareil 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).

Administration des appareils clients

Cette section contient les informations sur le travail avec les appareils clients.

Dans cette section

Connexion des appareils clients au Serveur d'administration	149
Connexion manuelle de l'appareil client au Serveur d'administration. Utilitaire klmover	151
Connexion en tunnel de l'appareil client avec le Serveur d'administration	153
Connexion à distance au bureau de l'appareil client	154
Paramètres du redémarrage de l'appareil client.....	156
Audit des actions sur un appareil client distant	157
Vérification de la connexion de l'appareil client avec le Serveur d'administration.....	158
Identification des appareils clients sur le Serveur d'administration	161
Ajout d'appareils à un groupe d'administration.....	162
Modification du Serveur d'administration pour les appareils clients.....	163
Démarrage, arrêt et redémarrage à distance des appareils clients	164
Envoi d'un message aux utilisateurs des appareils	165
Contrôle de modification de l'état des machines virtuelles.....	165
Attribution automatique de tags aux appareils	166
Diagnostic à distance des appareils clients. Utilitaire de diagnostic à distance Kaspersky Security Center	169

Connexion des appareils clients au Serveur d'administration

La connexion de l'appareil client au Serveur d'administration se réalise par l'Agent d'administration installé sur l'appareil client.

Lors de la connexion de l'appareil client au Serveur d'administration, les opérations suivantes sont exécutées :

- Synchronisation automatique des données :
 - la synchronisation de la liste des applications installées sur l'appareil client ;
 - la synchronisation des stratégies, des paramètres des applications, des tâches et des paramètres des tâches.
- La réception par le Serveur des informations actuelles sur l'état des applications, sur l'exécution des tâches et sur les statistiques de fonctionnement des applications.
- La transmission sur le Serveur des informations sur les événements qui doivent être traités.

La synchronisation automatique des données s'effectue périodiquement, en fonction des paramètres de l'Agent d'administration (par exemple, une fois toutes les 15 minutes). Vous pouvez définir manuellement l'intervalle entre les connexions.

Les informations sur un événement sont envoyées sur le Serveur d'administration tout de suite après que l'événement a eu lieu.

Kaspersky Security Center permet de configurer la connexion de l'appareil client au Serveur d'administration de telle manière pour que la connexion ne se termine pas à la fin d'exécution des opérations. Une connexion permanente est nécessaire dans le cas, où le contrôle d'état des applications est requis, et que le Serveur d'administration ne peut pas initier la connexion avec l'appareil client (par exemple, la connexion est protégée par un pare-feu, il est interdit d'ouvrir des ports sur l'appareil client, l'adresse IP de l'appareil client est inconnue). Une connexion permanente de l'appareil client au Serveur d'administration peut être établie dans la fenêtre des propriétés de l'appareil client, dans la section **Général** .

Il est recommandé d'établir une connexion permanente avec les appareils les plus importants. Le nombre total de connexions simultanées prises en charge par le Serveur d'administration est limité (plusieurs centaines).

Lors de la synchronisation manuelle, le mode auxiliaire de connexion est utilisé. Le Serveur d'administration initie la connexion dans ce mode. Avant la connexion sur l'appareil client, l'ouverture du port UDP est requise. Le Serveur d'administration envoie une demande de connexion sur le port UDP de l'appareil client. En réponse, l'analyse du certificat de Serveur d'administration est exécutée. Si le certificat de Serveur coïncide avec la copie du certificat sur l'appareil client, la connexion est exécutée.

Le lancement manuel du processus de synchronisation est aussi utilisé pour recevoir les informations actuelles sur l'état des applications, sur l'exécution des tâches et sur les statistiques de fonctionnement des applications.

Connexion manuelle de l'appareil client au Serveur d'administration. Utilitaire klmover

S'il vous faut connecter l'appareil client au Serveur d'administration à la main, vous pouvez utiliser l'utilitaire klmover sur l'appareil client.

Lors de l'installation de l'Agent d'administration sur l'appareil client, l'utilitaire est automatiquement copié dans le dossier d'installation de l'Agent d'administration.

► *Pour connecter l'appareil client au Serveur d'administration à la main à l'aide de l'utilitaire klmover,*

lancez l'utilitaire klmover sur l'appareil depuis la ligne de commande.

Lors du lancement depuis la ligne de commande, l'utilitaire `klmover` exécute les actions suivantes selon les clés utilisées :

- connecte l'Agent d'administration au Serveur d'administration, en utilisant les paramètres indiqués ;
- enregistre les résultats de l'opération dans le fichier journal des événements, ou les affiche à l'écran.

Syntaxe de l'utilitaire :

```
klmover [-logfile <nom du fichier>] [-address <adresse serveur>]  
[-pn <numéro du port>] [-ps < numéro du port SSL>] [-noss1] [-cert  
<chemin d'accès au fichier du certificat>] [-silent][dupfix]
```

Description des paramètres :

- `-logfile <nom du fichier>` : enregistre les résultats de l'exécution dans le fichier journal.

Par défaut, les informations sont conservées dans le flux de sortie standard (`stdout`). Si la clé n'est pas utilisée, les résultats et les messages d'erreur sont affichés à l'écran.

- `-address <adresse du serveur>` : adresse du Serveur d'administration pour la connexion.

L'adresse peut être une adresse IP, un nom NetBIOS ou DNS de l'appareil.

- `-pn <numéro du port>` : numéro de port à utiliser pour une connexion non sécurisée au Serveur d'administration.

Le numéro de port par défaut est 14000.

- `-ps <numéro du port SSL>` : numéro de port SSL à utiliser pour une connexion sécurisée au Serveur d'administration sous protocole SSL.

Le numéro de port par défaut est 13000.

- `-noss1` : utilise une connexion non sécurisée au Serveur d'administration.

Si aucune clé n'est utilisée, la connexion de l'Agent d'administration au Serveur est établie à l'aide du protocole sécurisé SSL.

- `-cert <chemin complet du fichier certificat>` : utilise le fichier de certificat spécifié pour l'authentification, afin d'accéder au Serveur d'administration.

Si aucune clé n'est utilisée, l'Agent d'administration recevra le certificat lors de la première connexion au Serveur d'administration.

- `-silent` : exécute l'utilitaire en mode non interactif.

Cette clé est utile, par exemple, pour exécuter l'outil à partir du scénario de connexion de l'utilisateur.

- `-dupfix` : clé utilisée en cas d'installation de l'Agent d'administration par une méthode différente de la normale (avec le kit de distribution), par exemple, par restauration depuis une image disque.

Connexion en tunnel de l'appareil client avec le Serveur d'administration

La connexion en tunnel de l'appareil client à distance avec le Serveur d'administration est nécessaire si le port de connexion au Serveur d'administration est inaccessible sur l'appareil.

Le port sur l'appareil peut être inaccessible dans les cas suivants :

- L'appareil à distance est connecté au réseau local avec le mécanisme NAT utilisé.
- L'appareil à distance fait partie du réseau local du Serveur d'administration, mais son port est fermé par le navigateur.

► *Pour exécuter une connexion en tunnel de l'appareil client avec le Serveur d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier du groupe dont l'appareil client fait partie.
2. Choisissez un onglet **Appareils** choisissez l'appareil.

3. Dans le menu contextuel de l'appareil, sélectionnez l'option **Toutes les tâches** → **Connexion en tunnel**.

4. Créez un tunnel dans la fenêtre ouverte **Connexion en tunnel**.

Connexion à distance au bureau de l'appareil client

L'administrateur peut obtenir l'accès au bureau de l'appareil client à l'aide de l'Agent d'administration installé sur l'appareil. La connexion à distance à l'appareil client à l'aide de l'Agent d'administration est aussi possible dans le cas si les ports TCP et UDP de l'appareil client ne sont pas accessibles.

Après la connexion à l'appareil, l'administrateur obtient l'accès complet aux informations sur cet appareil et peut administrer les applications installées sur celui-ci.

La connexion à distance à l'appareil client peut être exécutée de deux manières suivantes :

- A l'aide du module standard de Microsoft Windows "Connexion Bureau à distance". La connexion au bureau à distance est exécutée à l'aide de l'utilitaire titulaire de Windows `mstsc.exe` conformément aux paramètres de fonctionnement de cet utilitaire.

La connexion à la session en cours sur le poste de travail distant de l'utilisateur s'établit sans notification. Une fois l'administrateur connecté à la session, l'utilisateur de l'appareil sera déconnecté sans notification.

- A l'aide de la technologie Windows Desktop Sharing. Lors de la connexion à la séance existante du bureau à distance, l'utilisateur de cette séance sur l'appareil recevra une demande de connexion en provenance de l'administrateur. Les informations sur le processus de l'utilisation à distance de l'appareil et sur les résultats de cette utilisation ne sont pas conservées dans les rapports de Kaspersky Security Center.

L'administrateur peut se connecter à la séance existante sur l'appareil client sans la déconnexion de l'utilisateur travaillant dans cette séance. Dans ce cas, l'administrateur et l'utilisateur de la séance sur l'appareil auront un accès collectif au bureau.

L'administrateur peut configurer l'audit des actions sur l'appareil client distant. Lors de l'audit, l'application enregistre les informations relatives aux fichiers que l'administrateur a ouverts et/ou modifiés sur l'appareil client (cf. section "Audit des actions sur un appareil client distant" à la page [157](#)).

Pour se connecter au bureau de l'appareil client à l'aide de Windows Desktop Sharing, les conditions suivantes doivent être réalisées :

- Le système d'exploitation Microsoft Windows Vista ou plus récent est installé sur l'appareil.
 - Le système d'exploitation Microsoft Windows Vista ou plus récent est installé sur le poste de travail de l'administrateur. Le type du système d'exploitation de l'appareil hébergeant le Serveur d'administration ne représente pas une restriction pour la connexion à l'aide de Windows Desktop Sharing.
 - Kaspersky Security Center utilise la licence sur l'Administration système.
- *Pour se connecter au bureau de l'appareil client à l'aide du module "Connexion Bureau à distance", procédez comme suit :*

1. Dans l'arborescence de la console d'administration, sélectionnez l'appareil auquel l'accès doit être obtenu.
2. Dans le menu contextuel de l'appareil, sélectionnez l'option **Toutes les tâches** → **Se connecter à l'appareil** → **Créer une nouvelle session RDP**.

Finalement, l'utilitaire titulaire de Windows mstsc.exe sera lancé pour la connexion au bureau à distance.

3. Suivez les indications dans les fenêtres ouvertes de l'utilitaire.

Après la connexion à l'appareil client, le bureau de l'appareil client est accessible dans la fenêtre de la connexion à distance de Microsoft Windows.

► *Pour se connecter au bureau de l'appareil client à l'aide de la technologie Windows Desktop Sharing, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, sélectionnez l'appareil auquel l'accès doit être obtenu.
2. Dans le menu contextuel de l'appareil, sélectionnez l'option **Toutes les tâches** → **Se connecter à l'appareil** → **Accès en commun au bureau d'utilisateur**.
3. Dans la fenêtre ouverte **Sélection de la session du bureau**, sélectionnez une séance sur l'appareil client auquel il faut se connecter.

Dans le cas d'une connexion réussie à l'appareil client, le bureau de cet appareil sera accessible dans la fenêtre **Kaspersky Remote desktop session viewer**.

4. Pour commencer l'interaction avec l'appareil, dans le menu principal de la fenêtre **Kaspersky Remote desktop session viewer**, sélectionnez l'option **Actions** → **Mode interactif**.

Voir également

| Options de licence de Kaspersky Security Center..... [68](#)

Paramètres du redémarrage de l'appareil client

Au cours de la session, l'installation ou la suppression du Kaspersky Security Center peut nécessiter un redémarrage de l'appareil client. L'application permet de configurer les paramètres de redémarrage des appareils.

► *Pour configurer le redémarrage de l'appareil client, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il est nécessaire de configurer le redémarrage.
2. Dans l'espace de travail du groupe, sélectionnez l'onglet **Stratégies**.

3. Sélectionnez la stratégie de l'Agent d'administration Kaspersky Security Center dans la liste des stratégies, puis sélectionnez l'option **Propriétés** dans le menu contextuel de la stratégie.
4. Sélectionnez la section **Administration du redémarrage** dans la fenêtre des propriétés de la stratégie.
5. Sélectionnez l'action à exécuter si le redémarrage de l'appareil est requis :
 - Sélectionnez **Ne pas redémarrer le système d'exploitation** pour interdire le redémarrage automatique.
 - Sélectionnez **Redémarrer le système d'exploitation automatiquement si cela s'avère nécessaire** pour autoriser le redémarrage automatique.
 - Sélectionnez **Confirmer l'action auprès de l'utilisateur** pour activer la demande de confirmation de redémarrage auprès de l'utilisateur.

Vous pouvez indiquer la fréquence de la demande de redémarrage, activer le redémarrage forcé et forcer la fermeture des applications dans les sessions verrouillées sur l'appareil grâce aux cases prévues à cet effet.

6. Cliquez sur le bouton **OK** pour enregistrer les modifications et fermer la fenêtre des propriétés de la stratégie.

Après cette étape, le redémarrage du système d'exploitation de l'appareil sera configuré.

Audit des actions sur un appareil client distant

L'application permet d'effectuer l'audit des actions de l'administrateur sur l'appareil client distant. Lors de l'audit, l'application enregistre les informations relatives aux fichiers que l'administrateur a ouverts et/ou modifiés sur l'appareil. L'audit des actions de l'administrateur est accessible lorsque les conditions suivantes sont réunies :

- il existe une licence active de Systems Management ;
- l'administrateur est autorisé à lancer l'accès partagé au bureau de l'appareil distant.

► *Pour activer l'audit des actions sur un appareil client distant, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il est nécessaire de configurer l'audit des actions de l'administrateur.
2. Dans l'espace de travail du groupe, sélectionnez l'onglet **Stratégies**.
3. Sélectionnez la stratégie de l'Agent d'administration Kaspersky Security Center et sélectionnez l'option **Propriétés** dans le menu contextuel de la stratégie.
4. Sélectionnez la section **L'accès partagé au poste de travail** dans la fenêtre des propriétés de la stratégie.
5. Cochez la case **Activer l'audit**.
6. Ajoutez les masques des fichiers qui font l'objet d'actions à surveiller dans les listes **Masques des fichiers dont la lecture doit être suivie** et **Masques des fichiers dont les modifications doivent être suivies**.

Par défaut, l'application suit les actions effectuées sur les fichiers txt, rtf, doc, xls, docx, xlsx, odt, pdf.

7. Cliquez sur le bouton **OK** pour enregistrer les modifications et fermer la fenêtre des propriétés de la stratégie.

L'audit des actions de l'administrateur sur l'appareil distant d'un utilisateur se servant d'un accès partagé au poste de travail sera ainsi configuré.

Les enregistrements des actions de l'administrateur sur l'appareil distant sont conservés :

- dans le journal des événements de l'appareil distant ;
- dans un fichier .syslog, situé dans le dossier de l'Agent d'administration sur l'appareil distant (par exemple C:\ProgramData\KasperskyLab\adminkit\1103\logs) ;
- dans la base des événements du Kaspersky Security Center.

Vérification de la connexion de l'appareil client avec le Serveur d'administration

Kaspersky Security Center permet d'analyser les connexions de l'appareil client avec le Serveur d'administration automatiquement ou à la main.

L'analyse automatique de la connexion s'effectue sur le Serveur d'administration. L'analyse manuelle de la connexion s'effectue sur l'appareil.

Dans cette section

Vérification automatique de la connexion de l'appareil client avec le Serveur d'administration.....	159
Vérification manuelle de la connexion de l'appareil client avec le Serveur d'administration. Utilitaire klnagchk.....	160

Vérification automatique de la connexion de l'appareil client avec le Serveur d'administration

► *Pour lancer l'analyse automatique de la connexion de l'appareil client avec le Serveur d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration dont l'appareil fait partie.
2. Dans l'espace de travail du groupe d'administration sous l'onglet **Appareils**, sélectionnez l'appareil.
3. Dans le menu contextuel de l'appareil, sélectionnez l'option **Analyser l'accessibilité de l'appareil**.

Finalement la fenêtre, qui contient l'information sur l'accessibilité de l'appareil, s'ouvre.

Vérification manuelle de la connexion de l'appareil client avec le Serveur d'administration. Utilitaire klnagchk

Vous pouvez vérifier la connexion et recevoir les informations détaillées sur les paramètres de connexion de l'appareil client au Serveur d'administration à l'aide de l'utilitaire klnagchk.

Lors de l'installation de l'Agent d'administration sur l'appareil client, l'utilitaire klnagchk est automatiquement copié dans le dossier d'installation de l'Agent d'administration.

Lors du lancement depuis la ligne de commande, l'utilitaire klnagchk exécute les actions suivantes selon les clés utilisées :

- Renvoie à l'écran ou enregistre dans le fichier journal les valeurs des paramètres de connexion de l'Agent d'administration installé sur l'appareil, utilisés afin de se connecter au Serveur d'administration.
- Enregistre dans le fichier journal les statistiques de l'Agent d'administration (à partir de son dernier démarrage) et les résultats d'exécution de l'utilitaire, ou affiche les informations sur l'écran.
- Tente de connecter l'Agent d'administration au Serveur d'administration.

Si la connexion n'a pas pu être établie, l'utilitaire envoie un paquet ICMP au poste sur lequel est installé le Serveur d'administration afin de vérifier l'état de l'appareil.

► *Pour vérifier la connexion de l'appareil client au Serveur d'administration à l'aide de l'utilitaire klnagchk,*

lancez l'utilitaire klnagchk sur l'appareil depuis la ligne de commande.

Syntaxe de l'utilitaire :

```
klnagchk [-logfile <nom du fichier>] [-sp] [-savecert <chemin  
du fichier certificat>] [-restart]
```

Description des paramètres :

- `-logfile <nom du fichier>` : enregistre les valeurs des paramètres de connexion utilisées par l'Agent d'administration pour se connecter au Serveur, ainsi que les résultats de l'exécution dans le fichier journal.

Par défaut, les informations sont conservées dans le flux de sortie standard (stdout). Si la clé n'est pas utilisée, les paramètres, les résultats et les messages d'erreur sont affichés à l'écran.

- `-sp` : affiche le mot de passe utilisé pour authentifier l'utilisateur sur le serveur proxy.

Ce paramètre est utilisé si la connexion au Serveur d'administration est effectuée via un serveur proxy.

- `-savecert <nom du fichier>` : enregistre le certificat pour l'authentification de l'accès au serveur d'administration dans le fichier spécifié.
- `-restart` : relance l'Agent d'administration après exécution de l'utilitaire.

Identification des appareils clients sur le Serveur d'administration

L'identification des appareils clients est réalisée sur la base de leurs noms. Le nom d'un appareil est unique parmi tous les noms d'appareils connectés au Serveur d'administration.

Le nom de l'appareil est transmis au Serveur d'administration, soit lors du sondage du réseau Windows et de la détection d'un nouvel appareil dans ce réseau, soit lors de la première connexion de l'Agent d'administration, installé sur l'appareil, au Serveur d'administration. Par défaut, le nom concorde avec le nom d'appareil dans le réseau Windows (nom NetBIOS). Si un appareil est déjà enregistré avec ce nom sur le Serveur d'administration, alors un numéro d'ordre sera ajouté à la fin du nom du nouvel appareil, par exemple : **<Nom>-1**, **<Nom>-2**. Sous ce nom, l'appareil sera inclus dans le groupe d'administration.

Ajout d'appareils à un groupe d'administration

► *Pour inclure un ou plusieurs appareils dans un groupe d'administration sélectionné, procédez comme suit :*

1. Dans l'arborescence de la console ouvrez le dossier **Appareils administrés**.
2. Dans le dossier **Appareils administrés** sélectionnez le dossier joint qui correspond au groupe dans lequel les appareils clients seront inclus.

Si vous voulez activer les appareils dans le groupe **Appareils administrés**, cette étape peut être ignorée.

3. Dans l'espace de travail du groupe d'administration sélectionné sous l'onglet **Appareils**, lancez le processus d'inclusion des appareils dans le groupe à l'aide d'un des moyens suivants :
 - Ajoutez des appareils dans le groupe à l'aide du bouton **Ajouter des appareils** dans le groupe d'administration de la liste des appareils.
 - Dans le menu contextuel de la liste des appareils, sélectionnez l'option **Créer** → **Appareil**.

Finalement, l'Assistant d'ajout des appareils sera démarré. Suivez ses instructions et définissez le mode d'ajout des appareils au groupe et composez la liste des appareils appartenant au groupe.

Si vous fournissez la liste des appareils à la main, vous pouvez utiliser l'adresse IP (ou l'intervalle IP), le nom NetBIOS ou le nom DNS en tant que l'adresse de l'appareil. Il est possible d'ajouter manuellement à la liste des appareils uniquement les appareils dont les informations ont été insérées dans la base de données du Serveur d'administration lors de la connexion de l'appareil ou lors du sondage du réseau.

Pour importer la liste des appareils depuis le fichier, il faut indiquer le fichier au format TXT avec la liste des adresses des appareils ajoutés. Chaque adresse doit figurer sur une ligne séparée.

Après la fin de l'Assistant, les appareils sélectionnés sont inclus dans les groupes d'administration et s'affichent dans la liste des appareils sous les noms établis pour eux par le Serveur d'administration.

Il est possible d'ajouter l'appareil dans le groupe d'administration sélectionné, en le déplaçant à l'aide de la souris depuis le dossier **Appareils non définis** dans le dossier du groupe d'administration.

Modification du Serveur d'administration pour les appareils clients

Vous pouvez modifier le Serveur d'administration, sous lequel les appareils clients se trouvent, par un autre Serveur à l'aide de la tâche **Modification du Serveur d'administration**.

► *Pour modifier le Serveur d'administration, sous lequel les appareils clients se trouvent, par un autre Serveur, procédez comme suit :*

1. Connectez-vous au Serveur d'administration, qui administre les appareils.
2. Créez une tâche de modification du Serveur d'administration à l'aide d'un des moyens :
 - S'il faut modifier le Serveur d'administration pour les appareils qui font partie du groupe d'administration sélectionné, créez une tâche pour le groupe sélectionné (cf. section "Création d'une tâche de groupe" à la page [135](#)).
 - S'il faut modifier le Serveur d'administration pour les appareils qui font partie des différents groupes d'administration ou non, créez une tâche pour un ensemble d'appareils (cf. section "Création d'une tâche pour un ensemble d'appareils" à la page [137](#)).

Ceci permet de lancer l'Assistant de création de tâche. Suivez les instructions de l'Assistant. Dans la fenêtre **Type de tâche** de l'Assistant de création d'une tâche, sélectionnez l'entrée **Kaspersky Security Center**, ouvrez le dossier **Avancé** et sélectionnez la tâche **Modification du Serveur d'administration**.

3. Lancez la tâche créée.

Après la fin de la tâche, les appareils clients, pour lesquels elle a été créée, passent sous l'administration du Serveur d'administration indiqué dans les paramètres de la tâche.

Si le Serveur d'administration prend en charge la fonctionnalité d'administration de chiffrement et de protection des données, lors de la création de la tâche **Modification du Serveur d'administration**, un avertissement s'affiche. Cet avertissement signale que lors de la présence des données chiffrées sur les appareils après le passage des appareils sous l'administration d'un autre serveur, les utilisateurs auront l'accès uniquement aux données chiffrées dont ils travaillaient auparavant. Dans les autres cas, l'accès aux données chiffrées ne sera pas octroyé. La description détaillée des scénarios dont l'accès aux données chiffrées ne sera pas offert est décrite dans le Manuel de l'administrateur de Kaspersky Endpoint Security 10 for Windows.

Démarrage, arrêt et redémarrage à distance des appareils clients

Kaspersky Security Center permet de gérer à distance les appareils clients : les démarrer, les arrêter et les redémarrer.

► *Pour administrer à distance les appareils clients, procédez comme suit :*

1. Connectez-vous au Serveur d'administration, qui administre les appareils.
2. Créez une tâche d'administration de l'appareil par un des moyens suivants :
 - S'il faut allumer, éteindre ou redémarrer les appareils qui font partie du groupe d'administration sélectionné, créez une tâche pour le groupe sélectionné (cf. section "Création d'une tâche de groupe" à la page [135](#)).
 - S'il faut allumer, éteindre ou redémarrer les appareils qui font partie des différents groupes d'administration ou non, créez une tâche pour une sélection d'appareils (cf. section "Création d'une tâche pour une sélection d'appareils" à la page [137](#)).

Ceci permet de lancer l'Assistant de création de tâche. Suivez les instructions de l'Assistant. Dans la fenêtre **Type de tâche** de l'Assistant de création d'une tâche, sélectionnez l'entrée **Kaspersky Security Center**, ouvrez le dossier **Avancé** et sélectionnez la tâche **Administration des appareils**.

3. Lancez la tâche créée.

Après la fin du fonctionnement de la tâche, la commande (démarrage, arrêt, redémarrage) sera exécutée sur les appareils sélectionnés.

Envoi d'un message aux utilisateurs des appareils

► *Pour envoyer un message aux utilisateurs des appareils, procédez comme suit :*

1. Connectez-vous au Serveur d'administration, qui administre les appareils.
2. Créez une tâche d'envoi du message aux utilisateurs des appareils par un des moyens suivants :
 - S'il faut envoyer un message aux utilisateurs des appareils qui font partie du groupe d'administration sélectionné, créez une tâche pour le groupe sélectionné (cf. section "Création d'une tâche de groupe" à la page [135](#)).
 - S'il faut envoyer un message aux utilisateurs des appareils clients qui font partie des différents groupes d'administration ou non, créez une tâche pour un ensemble d'appareils (cf. section "Création d'une tâche pour un ensemble d'appareils" à la page [137](#)).

Ceci permet de lancer l'Assistant de création de tâche. Suivez les instructions de l'Assistant. Dans la fenêtre **Type de tâche** de l'Assistant de création d'une tâche, sélectionnez l'entrée **Kaspersky Security Center**, ouvrez le dossier **Avancé** et sélectionnez la tâche **Message pour l'utilisateur**.

3. Lancez la tâche créée.

A la fin du fonctionnement de la tâche, le message créé sera envoyé aux utilisateurs des appareils sélectionnés.

Contrôle de modification de l'état des machines virtuelles

Le Serveur d'administration conserve les informations sur l'état des appareils administrés, par exemple, le registre du matériel et la liste des appareils administrés, les paramètres des

applications administrées, des tâches et des stratégies. Si une machine virtuelle est un appareil administré, l'utilisateur peut à tout moment restaurer son état depuis l'image de la machine virtuelle (snapshot), faite auparavant. Finalement, les informations sur l'état de la machine virtuelle sur le Serveur d'administration peuvent dépasser.

Par exemple, à 12h00 l'administrateur a créé sur le Serveur d'administration une stratégie de protection qui a commencé à fonctionner à 12h01 sur la machine virtuelle VM_1. A 12h30 l'utilisateur de la machine virtuelle VM_1 a modifié son état, en exécutant la restauration depuis l'image faite à 11h00. Suite à ceci, la stratégie de protection devient inactive sur la machine virtuelle. Cependant, le Serveur d'administration contient les informations dépassées sur le fait que la stratégie de protection sur la machine virtuelle VM_1 continue son fonctionnement.

Kaspersky Security Center permet de contrôler la modification de l'état des machines virtuelles.

Après chaque synchronisation avec l'appareil, le Serveur d'administration forme un identificateur unique qui est conservé du côté de l'appareil et du côté du Serveur d'administration. Avant de commencer la synchronisation suivante, le Serveur d'administration compare les valeurs des identificateurs de deux côtés. Si les valeurs des identificateurs ne coïncident pas, le Serveur d'administration considère la machine virtuelle comme une machine restaurée depuis l'image. Le Serveur d'administration remet à zéro les paramètres des tâches et des stratégies, valables pour cette machine virtuelle, et envoie à celle-ci les stratégies à jour, ainsi que la liste des tâches de groupe.

Attribution automatique de tags aux appareils

L'application peut attribuer automatiquement des tags aux appareils. L'attribution automatique de tags aux appareils s'effectue à l'aide des règles. Vous pouvez créer et modifier des règles d'attribution de tags dans la fenêtre de propriétés du Serveur d'administration et/ou dans celle de l'appareil.

► *Pour créer et configurer des règles d'attribution automatique de tags aux appareils, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez la section **Règles d'attribution des tags**.
4. Dans la section **Règles d'attribution des tags**, cliquez sur le bouton **Ajouter**.

Finalement, la fenêtre **Propriété : Nouvelle règle** s'ouvre.

5. Dans la section **Général** de la fenêtre **Propriété : Nouvelle règle**, configurez les propriétés de la règle :

- Indiquez le nom de la règle.

Le nom de la règle ne peut pas contenir plus de 255 symboles et contenir de symboles spéciaux (*<>_?:"|).

- Dans la liste **Tag à attribuer** qui s'affiche, sélectionnez le tag précédemment ajouté ou saisissez-en un nouveau.
- Activez ou désactivez la règle à l'aide de la case **Activer la règle**.

6. Dans la section **Conditions**, cliquez sur le bouton **Ajouter** pour ajouter une nouvelle condition ou sur le bouton **Propriétés** pour modifier la condition existante.

La fenêtre de propriété de la nouvelle condition ou de la condition sélectionnée s'ouvre.

7. Dans la fenêtre affichée, configurer la condition d'attribution de tag :

- Dans la section **Général**, indiquez le nom de la condition.
- Dans la section **Réseau** configurez le traitement de la règle selon les propriétés réseau de l'appareil (noms de l'appareil dans le réseau Windows, appartenance de l'appareil à un domaine, à une plage IP, etc.).

- Dans la section **Active Directory**, configurez le traitement de la règle selon la situation de l'appareil dans la sous-section Active Directory et selon l'appartenance de l'appareil au groupe Active Directory.
 - Dans la section **Applications**, configurez le traitement de la règle selon la présence d'un Agent d'administration sur l'appareil, selon le type, la version et l'architecture du système d'exploitation.
 - Dans la section **Machines virtuelles**, configurez le traitement de la règle selon l'appartenance de l'appareil à différents types de machines virtuelles.
 - Dans la section **Registre des applications**, selon la présence d'applications de divers éditeurs sur l'appareil.
8. Après la configuration de la condition, cliquez sur le bouton **OK** dans la fenêtre **Propriété : Nouvelle règle**.
 9. Ajoutez ou configurez d'autres conditions de règle d'attribution de tag.

Les conditions ajoutées de traitement de la règle sont affichées dans la section **Conditions** de la fenêtre de propriétés de la règle.

10. Cliquez sur le bouton **OK** dans la fenêtre de propriétés de la règle.

La règle d'activation de tag est enregistrée. La règle est appliquée sur les appareils correspondant aux conditions associées. Suite à l'application de la règle aux appareils, un tag est attribué. Plusieurs tags sont automatiquement attribués à l'appareil si les règles d'attribution de ces tags sont appliquées simultanément. Une liste de tous les tags ajoutés peut être consultée dans la fenêtre de propriété de n'importe quel appareil dans la section **Tags**. Dans cette section **Tags**, vous pouvez aussi procéder à la configuration des règles d'attribution automatique de tags sur le lien correspondant.

Diagnostic à distance des appareils clients. Utilitaire de diagnostic à distance Kaspersky Security Center

L'utilitaire de diagnostic à distance Kaspersky Security Center (ci-après : utilitaire de diagnostic à distance) est conçue pour exécuter à distance des opérations suivantes sur les appareils clients :

- activation et désactivation du traçage, modification du niveau de traçage, téléchargement du fichier de traçage ;
- téléchargement des paramètres des applications ;
- téléchargement des journaux des événements ;
- lancement du diagnostic et téléchargement des résultats du diagnostic ;
- lancement et arrêt des applications.

L'utilitaire de diagnostic à distance s'installe automatiquement sur l'appareil conjointement avec la Console d'administration.

Dans cette section

Connexion de l'utilitaire de diagnostic à distance à l'appareil client	170
Activation et désactivation du traçage, téléchargement du fichier de traçage	173
Téléchargement des paramètres des applications	173
Téléchargement des enregistrements des événements	174
Lancement du diagnostic et téléchargement des résultats	175
Lancement, arrêt ou relancement des applications	175

Connexion de l'utilitaire de diagnostic à distance à l'appareil client

► Pour connecter l'utilitaire de diagnostic à distance à l'appareil client, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez n'importe quel groupe d'administration.
2. Dans l'espace de travail sous l'onglet **Appareils** dans le menu contextuel de n'importe quel appareil, sélectionnez l'option **Outils externes** → **Diagnostic à distance**.

Finalement, la fenêtre principale de l'utilitaire de diagnostic à distance s'ouvrira.

3. Dans le champ droit de la fenêtre principale de l'utilitaire de diagnostic à distance, définissez les moyens de connexion à l'appareil :
 - **Accès à l'aide des outils du réseau Microsoft Windows.**
 - **Accès à l'aide des outils du serveur d'administration.**
4. Si dans le premier champ de la fenêtre principale de l'utilitaire, vous avez sélectionné l'option **Accès à l'aide des outils du réseau Microsoft Windows**, procédez comme suit :

- Dans le champ **Appareil**, indiquez l'adresse de l'appareil à se connecter.

L'adresse d'appareil peut être une adresse IP, un nom NetBIOS ou DNS.

Par défaut, l'adresse de l'appareil est indiquée, dont l'utilitaire a été lancé depuis son menu contextuel.

- Indiquez un compte utilisateur pour se connecter à l'appareil :
 - **Se connecter au nom de l'utilisateur en cours** (sélectionné par défaut).
Connexion sous compte utilisateur actuel.
 - **Utiliser, lors de la connexion, le nom d'utilisateur et le mot de passe fournis.**
Connexion sous compte utilisateur indiqué. Indiquez **Nom d'utilisateur** et **Mot de passe** du compte utilisateur nécessaire.

La connexion à l'appareil est possible uniquement sous le compte utilisateur de l'administrateur local de l'appareil.

5. Si dans le premier champ, vous avez sélectionné **Accès à l'aide des outils du serveur d'administration**, procédez comme suit :

- Dans le champ **Serveur d'administration**, indiquez l'adresse du Serveur d'administration depuis lequel il faut se connecter à l'appareil.

L'adresse du Serveur peut être une adresse IP, un nom NetBIOS ou DNS.

Par défaut l'adresse du Serveur, depuis lequel l'utilitaire a été lancé, est indiquée.

- S'il faut, cochez les cases **Utiliser SSL**, **Compresser le trafic** et **L'appareil appartient au Serveur d'administration secondaire**.

Si la case **L'appareil appartient au Serveur d'administration secondaire** est cochée, le champ **Serveur secondaire** permet de sélectionner le Serveur d'administration secondaire sous l'administration duquel l'appareil se trouve, en cliquant sur le bouton **Parcourir**.

6. Pour se connecter à l'appareil, cliquez sur le bouton **Se connecter**.

Finalement, la fenêtre de diagnostic à distance de l'appareil s'ouvrira (cf. ill. ci-après). La partie gauche de la fenêtre reprend les liens pour exécuter les opérations de diagnostic de l'appareil. La partie droite de la fenêtre reprend l'arborescence des objets de l'appareil avec lesquels l'utilitaire peut fonctionner. La partie inférieure de la fenêtre affiche le processus d'exécution des opérations de l'utilitaire.

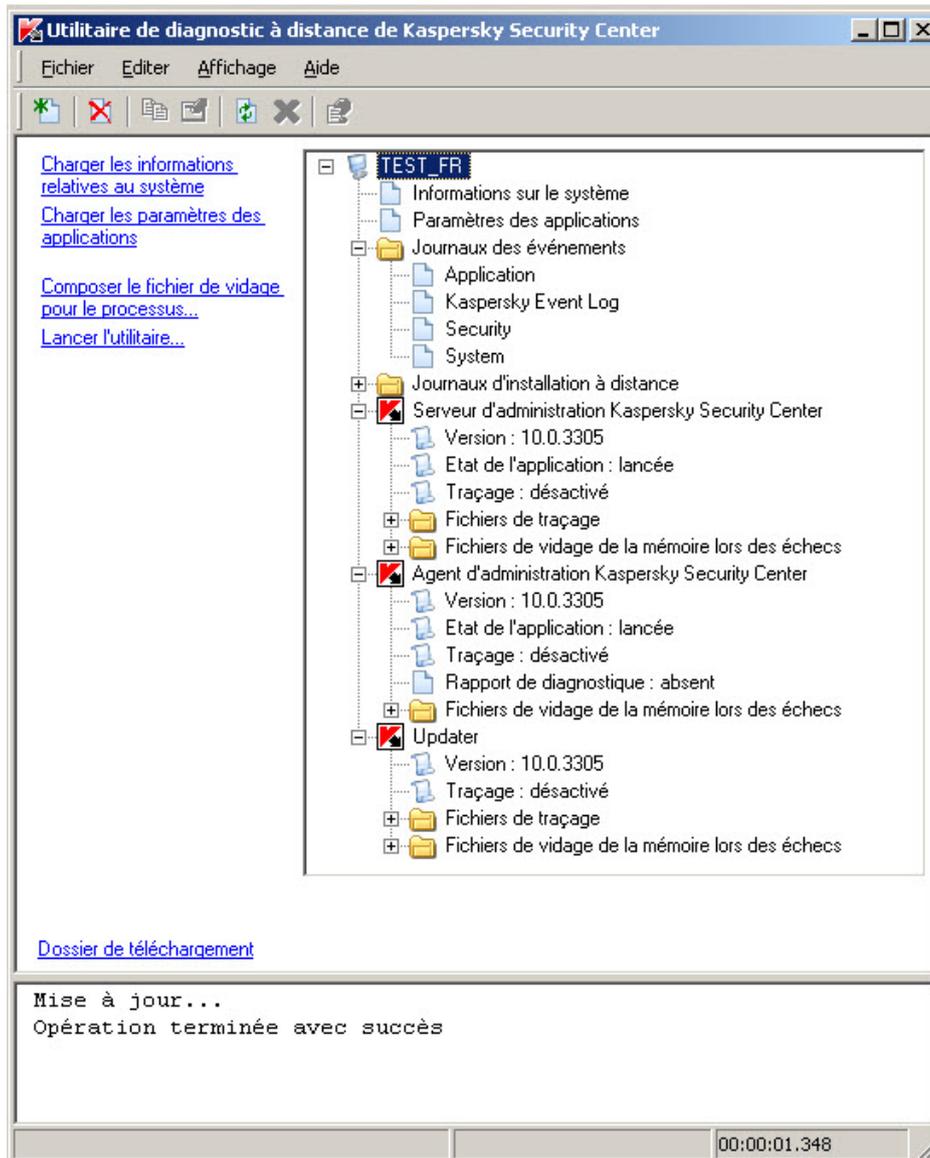


Illustration 10 Utilitaire de diagnostic à distance. Fenêtre de diagnostic à distance de l'ordinateur client

L'utilitaire de diagnostic à distance enregistre les fichiers téléchargés des appareils sur le bureau de l'appareil, depuis lequel il était lancé.

Activation et désactivation du traçage, téléchargement du fichier de traçage

► Pour activer le traçage sur l'appareil distant, télécharger le fichier de traçage ou désactiver le traçage, procédez comme suit :

1. Lancez l'utilitaire de diagnostic à distance et connectez-vous à l'appareil nécessaire.
2. Dans l'arborescence des objets de l'appareil, sélectionnez l'application dont il faut obtenir le traçage, et activez le traçage à l'aide du lien **Activer le traçage** dans la partie gauche de la fenêtre de l'utilitaire de diagnostic à distance.

Activation et désactivation du traçage des applications avec l'autodéfense sont possibles uniquement lors de la connexion à l'appareil via les outils du Serveur d'administration.

Dans certains cas, pour activer le traçage de l'application de protection, il faut relance cette application et sa tâche.

3. L'entrée de l'application pour laquelle le traçage a été activé, dans le dossier **Fichiers de traçage**, sélectionnez le fichier nécessaire et téléchargez-le à l'aide du lien **Télécharger le fichier**. Pour les fichiers de grande taille, il existe une possibilité de télécharger uniquement les dernières parties du traçage.

Vous pouvez supprimer le fichier de traçage sélectionné. La suppression du fichier de traçage est possible après la désactivation du traçage.

4. Désactivez le traçage pour l'application sélectionnée à l'aide du lien **Désactiver le traçage**.

Téléchargement des paramètres des applications

► *Pour télécharger les paramètres des applications depuis l'appareil distant, procédez comme suit :*

1. Lancez l'utilitaire de diagnostic à distance et connectez-vous à l'appareil nécessaire.
2. Dans l'arborescence des objets de la fenêtre de diagnostic à distance de l'appareil, sélectionnez l'entrée supérieure avec le nom de l'appareil et sélectionnez l'action nécessaire dans la partie gauche de la fenêtre :
 - **Charger les informations relatives au système.**
 - **Charger les paramètres des applications.**
 - **Composer le fichier dump pour le processus.**

Dans la fenêtre, ouverte à l'aide du lien, indiquez le fichier exécutable de l'application sélectionnée pour laquelle il faut former le fichier dump de la mémoire.

- **Lancer l'utilitaire.**

Dans la fenêtre, ouverte à l'aide du lien, indiquez le fichier exécutable de l'utilitaire sélectionné et les paramètres de son lancement.

Finalement, l'utilitaire sélectionné sera téléchargé et lancé sur l'appareil.

Téléchargement des journaux des événements

► *Pour télécharger le journal des événements depuis l'appareil distant, procédez comme suit :*

1. Lancez l'utilitaire de diagnostic à distance et connectez-vous à l'appareil nécessaire.
2. Dans le dossier **Journaux des événements** de l'arborescence des objets de l'appareil, sélectionnez le journal nécessaire et téléchargez-le à l'aide du lien **Charger les**

enregistrements des événements Kaspersky dans la partie gauche de la fenêtre de l'utilitaire de diagnostic à distance.

Lancement du diagnostic et téléchargement des résultats

► *Pour lancer le diagnostic de l'application sur l'appareil distant et télécharger les résultats, procédez comme suit :*

1. Lancez l'utilitaire de diagnostic à distance et connectez-vous à l'appareil nécessaire.
2. Dans l'arborescence des objets de l'appareil, sélectionnez l'application nécessaire et lancez le diagnostic à l'aide du lien **Poser le diagnostic**.

Finalement, dans l'entrée de l'application sélectionnée, le rapport de diagnostic apparaîtra dans l'arborescence des objets.

3. Sélectionnez le rapport formé de diagnostic dans l'arborescence des objets et téléchargez-le à l'aide du lien **Télécharger le fichier**.

Lancement, arrêt ou relancement des applications

Le lancement, l'arrêt et le relancement des applications sont possibles uniquement à la connexion à l'appareil par les outils du Serveur d'administration.

► *Pour lancer, arrêter ou relancer l'application, procédez comme suit :*

1. Lancez l'utilitaire de diagnostic à distance et connectez-vous à l'appareil nécessaire.
2. Dans l'arborescence des objets de l'appareil, sélectionnez l'application nécessaire et sélectionnez l'action dans la partie gauche de la fenêtre :
 - **Arrêter l'application.**
 - **Relancer l'application.**
 - **Lancer l'application.**

Selon l'action sélectionnée, l'application sera lancée, arrêtée ou relancée.

Administration des comptes utilisateur

Cette section contient des informations sur les comptes utilisateur et les rôles des utilisateurs pris en charge par l'application. Elle comprend les instructions nécessaires à la création de comptes utilisateur et de rôles des utilisateurs Kaspersky Security Center. Cette section comprend également des instructions relatives à l'utilisation des listes de certificats et d'appareils mobiles pour la distribution de messages aux utilisateurs.

Dans cette section

Utilisation des comptes utilisateur	178
Ajout du compte utilisateur	179
Configuration du contrôle de l'originalité du nom de l'utilisateur interne.....	180
Ajout d'un groupe d'utilisateurs	181
Ajout d'un utilisateur dans le groupe	182
Configuration des autorisations. Rôles des utilisateurs	183
Désignation d'un utilisateur comme propriétaire de l'appareil	186
Diffusion des messages aux utilisateurs.....	186
Consultation de la liste des appareils mobiles de l'utilisateur	188
Installation du certificat pour l'utilisateur	188
Consultation de la liste des certificats octroyés à l'utilisateur	189

Utilisation des comptes utilisateur

Le Kaspersky Security Center permet d'administrer les comptes utilisateur et groupes de comptes utilisateur. L'application prend en charge deux types de comptes utilisateur :

- Comptes utilisateur pour les employés de l'entreprise. Le Serveur d'administration reçoit les données relatives aux comptes utilisateur de ces utilisateurs lors du balayage du réseau de l'entreprise.
- Comptes utilisateur des utilisateurs internes (cf. section "Travail avec les utilisateurs internes" à la page [108](#)). Appliqués pour l'utilisation des Serveurs d'administration virtuels. Les comptes des utilisateurs internes ne peuvent être créés (cf. section "Ajout du compte utilisateur" à la page [179](#)) et utilisés que depuis Kaspersky Security Center.

Tous les comptes utilisateur peuvent être consultés dans le dossier **Comptes utilisateurs** de l'arborescence de la console. Le dossier **Comptes utilisateurs** est placé par défaut dans le dossier **Avancé**.

Les comptes utilisateur et groupes de comptes utilisateur vous permettent d'exécuter les actions suivantes :

- configurer les privilèges d'accès des utilisateurs aux fonctions de l'application à l'aide de rôles (cf. section "Configuration des autorisations. Rôles utilisateur" à la page [183](#)) ;
- envoyer des messages aux utilisateurs par messagerie électronique et SMS (cf. section "Diffusion des messages aux utilisateurs" à la page [186](#)) ;
- consulter la liste des périphériques mobiles d'un utilisateur (cf. section "Consultation de la liste des périphériques mobiles de l'utilisateur" à la page [188](#)) ;
- octroyer et installer des certificats sur les périphériques mobiles d'un utilisateur (cf. section "Installation du certificat pour l'utilisateur" à la page [188](#)) ;
- consulter la liste des certificats octroyés à un utilisateur (cf. section "Consultation de la liste des certificats octroyés à l'utilisateur" à la page [189](#)) ;

Ajout du compte utilisateur

► Pour ajouter un nouveau compte utilisateur Kaspersky Security Center, procédez comme suit :

1. Ouvrez le dossier **Comptes utilisateurs** dans l'arborescence de la console.

Le dossier **Comptes utilisateurs** est placé par défaut dans le dossier **Avancé**.

2. Dans l'espace de travail, cliquez sur le bouton **Ajouter un utilisateur** pour ouvrir la fenêtre **Propriétés**.
3. Dans la fenêtre **Propriétés**, indiquez les paramètres du compte utilisateur et son mot de passe pour connecter l'utilisateur à Kaspersky Security Center.

Le mot de passe doit contenir des caractères latins en majuscules et en minuscules, des chiffres ou des symboles spéciaux (@#\$%^&*-_!+=[]{}|\\\'",. ?/ ~-()\"). La longueur du mot de passe doit être comprise entre huit et seize caractères.

Le nombre de tentatives de saisie du mot de passe par l'utilisateur est limité. Par défaut, le nombre maximal de tentatives de saisie du mot de passe est égal à 10. Le nombre de tentatives de saisie du mot de passe est modifiable dans le registre à l'aide de la clé SrvSpIPpcLogonAttempts.

Si l'utilisateur a incorrectement saisi le mot de passe le nombre de fois indiqué, le compte utilisateur associé est bloqué pour une heure. L'administrateur peut déverrouiller le compte utilisateur uniquement après avoir modifié le mot de passe.

Si la case **Désactiver le compte** est cochée, l'utilisateur interne (par exemple avec les droits d'administrateur ou d'opérateur) ne peut pas se connecter à l'application. Vous pouvez cocher la case en cas, par exemple, de licenciement d'un employé. Celle-ci est décochée par défaut.

4. Cliquez sur le bouton **OK**.

Le compte utilisateur créé apparaît dans l'espace de travail du dossier **Comptes utilisateurs**.

Configuration du contrôle de l'originalité du nom de l'utilisateur interne

Vous pouvez configurer le contrôle de l'originalité du nom de l'utilisateur interne Kaspersky Security Center au moment de l'ajouter dans l'application. Le contrôle de l'originalité du nom de l'utilisateur interne peut être exécuté seulement sur le Serveur virtuel ou le Serveur principal pour lequel un compte utilisateur est créé ou sur tous les Serveurs virtuels et le Serveur principal. Par défaut, le contrôle de l'originalité du nom de l'utilisateur interne est exécuté sur tous les Serveurs virtuels et sur le Serveur d'administration principal.

► *Pour activer le contrôle de l'originalité du nom de l'utilisateur interne dans le cadre du Serveur virtuel ou du Serveur principal, procédez comme suit :*

1. Ouvrez le registre système de l'appareil sur lequel le Serveur d'administration est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.

2. Rendez-vous dans la section :

- Pour un système de 64 bits :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34  
\.core\independent\KLLIM
```

- Pour un système de 32 bits :

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\independ  
ent\KLLIM
```

3. Pour la clé LP_InterUserUniqVsScope (DWORD), sélectionnez la valeur 00000001.

Par défaut, la valeur 0 est indiquée pour cette clé.

4. Relancez le service du Serveur d'administration.

Suite à cette action, le contrôle de l'originalité du nom sera exécuté seulement sur le Serveur virtuel où l'utilisateur interne a été créé ou sur le Serveur principal si l'utilisateur a été créé sur le Serveur principal.

► *Pour activer le contrôle de l'originalité du nom de l'utilisateur interne sur tous les Serveurs virtuels et sur le Serveur principal, procédez comme suit :*

1. Ouvrez le registre système de l'appareil sur lequel le Serveur d'administration est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.

2. Rendez-vous dans la section :

- Pour un système de 64 bits :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34  
\.core\independent\KLLIM
```

- Pour un système de 32 bits :

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\independ  
ent\KLLIM
```

3. Pour la clé LP_InterUserUniqVsScope (DWORD), sélectionnez la valeur 00000000.

Par défaut, la valeur 0 est indiquée pour cette clé.

4. Relancez le service du Serveur d'administration.

Suite à cette action, le contrôle de l'originalité du nom sera exécuté sur tous les Serveurs virtuels et sur le Serveur d'administration principal.

Ajout d'un groupe d'utilisateurs

Vous pouvez ajouter des groupes d'utilisateurs, configurer en toute flexibilité le contenu des groupes et l'accès d'un groupe d'utilisateurs à diverses fonctions de l'application. Ces groupes d'utilisateurs peuvent être nommés en fonction de leurs attributs. Par exemple, le nom peut correspondre à l'emplacement des utilisateurs dans le bureau ou au nom de la sous-section structurelle à laquelle ceux-ci sont rattachés au sein d'une société.

Un seul utilisateur peut appartenir à plusieurs groupes. Le compte utilisateur géré par un Serveur d'administration virtuel peut faire partie uniquement des groupes d'utilisateurs de ce serveur virtuel et avoir des droits d'accès uniquement à celui-ci.

► *Pour ajouter un groupe d'utilisateurs, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Comptes utilisateurs**.

Le dossier **Comptes utilisateurs** est placé par défaut dans le dossier **Avancé**.

2. Cliquez sur le bouton **Ajouter un groupe de sécurité**.

Dans la fenêtre **Propriétés : Nouveau groupe**, configurez les paramètres du groupe d'utilisateurs ajoutés :

3. Dans la section **Général**, indiquez le nom du groupe.

Le nom du groupe ne peut pas contenir plus de 100 caractères. Le nom du groupe doit être unique.

4. Dans la section **Utilisateurs**, ajoutez des comptes utilisateurs dans le groupe.

5. Cliquez sur le bouton **OK**.

Le groupe d'utilisateurs ajouté s'affiche dans le dossier **Comptes utilisateurs** dans l'arborescence de la console.

Ajout d'un utilisateur dans le groupe

► *Pour ajouter un utilisateur dans le groupe, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Comptes utilisateurs**.

Le dossier **Comptes utilisateurs** est placé par défaut dans le dossier **Avancé**.

2. Dans la liste de comptes utilisateurs et de groupes, sélectionnez le groupe auquel ajouter un utilisateur.

3. Dans le menu contextuel du groupe, sélectionnez l'option **Propriétés**.

4. Dans la fenêtre des propriétés du groupe, sélectionnez la section **Utilisateurs du groupe** et cliquez sur le bouton **Ajouter**.

Suite à cette action, la fenêtre s'ouvre avec une liste d'utilisateurs.

5. Dans la liste, sélectionnez les utilisateurs à inclure dans le groupe.
6. Cliquez sur le bouton **OK**.

Suite à cette action, les utilisateurs sont inclus dans le groupe.

Configuration des autorisations. Rôles d'utilisateurs

Vous pouvez configurer de manière flexible l'accès des administrateurs, utilisateurs et des groupes aux différentes fonctions de l'application. Deux méthodes peuvent être employées pour accorder des privilèges d'accès aux fonctions aux utilisateurs :

- configurer les privilèges de chaque utilisateur ou groupe d'utilisateurs séparément ;
- créer des rôles types d'utilisateurs avec un ensemble de privilèges configurés au préalable et attribuer ces rôles aux utilisateurs en fonction de leurs responsabilités.

Un *rôle utilisateur* est un ensemble de privilèges préalablement définis et configurés pour l'accès aux fonctions de l'application. Un rôle peut être attribué à un utilisateur ou à un ensemble d'utilisateurs. L'application de rôles simplifie et accélère les procédures routinières de configuration des privilèges d'accès des utilisateurs à l'application. Les privilèges d'accès des rôles sont configurés en fonction des responsabilités "types" des utilisateurs. Par exemple, le rôle de l'utilisateur peut être limité à la lecture et à l'envoi de commandes à caractère informatif sur les appareils mobiles des autres utilisateurs à l'aide de Self Service Portal.

Ces rôles peuvent être nommés en fonction de leurs attributs. Il est possible de créer un nombre illimité de rôles dans l'application.

Ajout d'un rôle utilisateur

► *Pour ajouter un rôle utilisateur, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.

3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez la section **Rôles d'utilisateurs** et cliquez sur le bouton **Ajouter**.
4. Dans la fenêtre **Propriétés : Nouveau rôle**, configurez les paramètres du rôle :
 - Dans la section **Général**, indiquez le nom du rôle.

Le nom du rôle ne peut pas contenir plus de 100 caractères.
 - Dans la section **Privilèges** configurez l'ensemble de privilèges en cochant les cases **Autoriser** et **Interdire** en regard des fonctions de l'application.
5. Cliquez sur le bouton **OK**.

Le rôle sera ainsi enregistré.

Les rôles d'utilisateurs créés pour le Serveur d'administration apparaissent dans la fenêtre de propriétés du serveur, dans la section **Rôles d'utilisateurs**. Vous pouvez modifier et supprimer les rôles utilisateur, mais aussi attribuer des rôles à des groupes d'utilisateurs (cf. section "Attribution d'un rôle à un utilisateur ou à un groupe d'utilisateurs" à la page [184](#)) ou à des utilisateurs isolés.

La section **Rôles d'utilisateurs** est accessible si la case **Afficher les sections avec les paramètres de sécurité** est cochée dans la fenêtre de configuration de l'interface (cf. section "Configuration de l'interface" à la page [61](#)).

Attribution d'un rôle à un utilisateur ou à un groupe d'utilisateurs

► *Pour attribuer un rôle à un utilisateur ou à un groupe d'utilisateurs, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.

3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez la section **Sécurité**.
4. Dans le champ **Noms de groupes ou d'utilisateurs** sélectionnez l'utilisateur ou le groupe d'utilisateurs auquel vous devez attribuer un rôle.

Si l'utilisateur ou le groupe d'utilisateurs ne s'affiche pas dans le champ, ajoutez-le en cliquant sur le bouton **Ajouter**.

Si vous ajoutez l'utilisateur avec le bouton **Ajouter**, vous pouvez sélectionner le type d'authentification de l'utilisateur (Microsoft Windows ou Kaspersky Security Center). L'authentification par le Kaspersky Security Center permet de sélectionner les compte utilisateur des utilisateurs internes enregistrés qui manipulent les Serveurs d'administration virtuels.

5. Ouvrez l'onglet **Rôles** et cliquez sur le bouton **Ajouter**.

La fenêtre **Rôles d'utilisateurs** s'ouvre. Les rôles utilisateur créés s'affichent dans la fenêtre.

6. Sélectionnez le rôle à attribuer au groupe d'utilisateurs dans la fenêtre **Rôles d'utilisateurs**.
7. Cliquez sur le bouton **OK**.

Le rôle comprenant l'ensemble de privilèges concernant l'utilisation du Serveur d'administration sera ainsi attribué à l'utilisateur ou au groupe d'utilisateurs. Les rôles attribués apparaissent dans l'onglet **Rôles** de la section **Sécurité** de la fenêtre des propriétés du Serveur d'administration.

La section **Sécurité** est accessible uniquement si la case **Afficher les sections avec les paramètres de sécurité** est cochée dans la fenêtre de configuration de l'interface (cf. section "**Configuration de l'interface**" à la page [61](#)).

Désignation d'un utilisateur comme propriétaire de l'appareil

Vous pouvez désigner un utilisateur comme propriétaire de l'appareil pour associer les deux. Si des actions doivent être effectuées avec l'appareil (par exemple une mise à jour de la configuration matérielle), l'administrateur peut en informer le propriétaire et convenir d'actions avec lui.

► *Pour désigner un appareil comme propriétaire de l'appareil, procédez comme suit :*

1. Dans l'arborescence de la console sélectionnez le dossier **Appareils administrés**.
2. Dans l'espace de travail du dossier, dans l'onglet **Appareils**, sélectionnez l'appareil pour lequel un propriétaire doit être désigné.
3. Dans le menu contextuel de l'appareil, sélectionnez l'option **Propriétés**.
4. Dans la fenêtre de propriétés de l'appareil, sélectionnez la section **Informations sur le système** → **Sessions**.
5. Cliquez sur le bouton **Désigner** en regard du champ **Propriétaire de l'appareil**.
6. Dans la fenêtre **Choix de l'utilisateur**, sélectionnez l'utilisateur à désigner comme propriétaire de l'appareil et cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **OK**.

Suite à cette action, le propriétaire de l'appareil est désigné. Par défaut, le champ **Propriétaire de l'appareil** contient la valeur d'Active Directory et est mis à jour à chaque sondage d'Active Directory (cf. section "Affichage et modification des paramètres de sondage des groupes Active Directory" à la page [211](#)). Vous pouvez consulter la liste des propriétaires des appareils dans **Rapport sur les propriétaires des appareils**. Un rapport peut être créé à l'aide de l'assistant de création de rapports (cf. section "Créer le nouveau rapport" p. [191](#)).

Diffusion des messages aux utilisateurs

► *Pour envoyer un message par email à l'utilisateur, procédez comme suit :*

1. Sélectionnez un utilisateur dans le dossier **Comptes utilisateurs** dans l'arborescence de la console.

Le dossier **Comptes utilisateurs** est placé par défaut dans le dossier **Avancé**.

2. Dans le menu contextuel de l'utilisateur, choisissez l'option **Envoyer un message par email**.
3. Remplissez les champs requis dans la fenêtre **Message pour l'utilisateur**, puis cliquez sur le bouton **OK**.

Le message sera envoyé à l'email repris dans les propriétés de l'utilisateur.

► *Pour envoyer un message SMS à l'utilisateur, procédez comme suit :*

1. Sélectionnez un utilisateur dans le dossier **Comptes utilisateurs** dans l'arborescence de la console.
2. Dans le menu contextuel de l'utilisateur, sélectionnez l'option **Envoyer le message SMS**.
3. Remplissez les champs requis dans la fenêtre **Texte SMS**, puis cliquez sur le bouton **OK**.

Le SMS sera envoyé au numéro de l'appareil mobile repris dans les propriétés de l'utilisateur.

Consultation de la liste des appareils mobiles de l'utilisateur

► Pour consulter la liste des appareils mobiles de l'utilisateur, procédez comme suit :

1. Sélectionnez un utilisateur dans le dossier **Comptes utilisateurs** dans l'arborescence de la console.

Le dossier **Comptes utilisateurs** est placé par défaut dans le dossier **Avancé**.

2. Dans le menu contextuel du compte utilisateur, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du compte utilisateur, sélectionnez la section **Appareils mobiles**.

La section **Appareils mobiles** permet de consulter la liste des appareils mobiles de l'utilisateur et les informations qui les concernent. Le bouton **Exporter dans un fichier** permet d'enregistrer la liste des appareils mobiles dans un fichier.

Installation du certificat pour l'utilisateur

Vous pouvez installer trois types de certificats pour l'utilisateur :

- certificat partagé indispensable pour identifier l'appareil mobile de l'utilisateur ;
- certificat de messagerie nécessaire pour la configuration de la messagerie d'entreprise sur l'appareil mobile de l'utilisateur ;
- Certificat VPN nécessaire pour la configuration du réseau privé virtuel sur l'appareil mobile de l'utilisateur.

► *Pour octroyer le certificat à l'utilisateur et l'installer, procédez comme suit :*

1. Sélectionnez un compte utilisateur en ouvrant le dossier **Comptes utilisateurs** de l'arborescence de la console.

Le dossier **Comptes utilisateurs** est placé par défaut dans le dossier **Avancé**.

2. Dans le menu contextuel du compte utilisateur, sélectionnez l'option **Installer le certificat**.

L'Assistant d'installation du certificat se lance. Suivez les instructions de l'Assistant.

Une fois l'Assistant d'installation du certificat terminé, le certificat est créé et installé pour l'utilisateur. Il est possible de consulter et d'exporter sous forme de fichier la liste des certificats installés pour l'utilisateur (cf. section "Consultation de la liste des certificats octroyés à l'utilisateur" à la page [189](#)).

Consultation de la liste des certificats octroyés à l'utilisateur

► *Pour consulter la liste de tous les certificats octroyés à l'utilisateur, procédez comme suit :*

1. Sélectionnez un utilisateur dans le dossier **Comptes utilisateurs** dans l'arborescence de la console.

Le dossier **Comptes utilisateurs** est placé par défaut dans le dossier **Avancé**.

2. Dans le menu contextuel du compte utilisateur, sélectionnez l'option **Propriétés**.

3. Dans la fenêtre des propriétés du compte utilisateur, sélectionnez la section **Certificats**.

La section **Certificats** permet de consulter la liste des certificats de l'utilisateur et les informations qui les concernent. Le bouton **Exporter dans un fichier** permet d'enregistrer la liste des certificats dans un fichier.

Utilisation des rapports, des statistiques et des notifications

Cette section reprend les informations sur l'utilisation des rapports, les statistiques et les sélections d'événements et d'appareils dans Kaspersky Security Center, ainsi que sur la configuration des notifications du Serveur d'administration.

Dans cette section

Utilisation des rapports.....	190
Utilisation des données statistiques	194
Configuration des paramètres de notification sur les événements	195
Création d'un certificat pour le serveur SMTP.....	198
Sélections d'événements.....	199
Exportation des événements dans le système SIEM.....	202
Sélections des appareils.....	204
Stratégies	208
Tâches	208

Utilisation des rapports

Les rapports dans Kaspersky Security Center contiennent les informations sur l'état des appareils administrés. Les rapports se forment à partir des informations enregistrées sur le Serveur d'administration. Vous pouvez créer les rapports pour les objets suivants :

- pour les sélections d'appareils créés selon des paramètres définis ;
- pour les groupes d'administration ;
- pour les ensembles d'appareils issus de divers groupes d'administration ;
- pour tous les appareils dans le réseau (dans le rapport de déploiement).

L'application comporte un ensemble de modèles standard de rapport. La possibilité de créer des modèles de rapports d'utilisateurs. Les rapports s'affichent dans la fenêtre principale de l'application, dans le dossier de l'arborescence de la console **Serveur d'administration**.

Dans cette section

Créer le nouveau rapport.....	191
Génération et affichage des rapports	192
Enregistrement du rapport.....	193
Création d'une tâche d'envoi du rapport	193

Créer le nouveau rapport

► *Pour créer un modèle de rapport, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans la zone de travail du groupe, sélectionnez l'onglet **Rapports**.
3. Cliquez sur le bouton **Créer un modèle de rapport**.

Finalement, l'Assistant de création du modèle du rapport se lancera. Suivez les instructions de l'Assistant.

A la fin du fonctionnement de l'Assistant, le modèle formé du rapport sera ajouté dans le dossier sélectionné **Serveur d'administration** de l'arborescence de la console. Ce modèle peut être utilisé pour créer et afficher des rapports.

Génération et affichage des rapports

► *Pour former et consulter le rapport, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans la zone de travail du groupe, sélectionnez l'onglet **Rapports**.
3. Sélectionnez le modèle de rapport qui vous intéresse dans la liste de modèles.

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 d'appareils ;
- diagramme avec les données générales du rapport ;

- tableau récapitulatif avec les indices énumérés du rapport ;
- tableau avec les données détaillées du rapport.

Enregistrement du rapport

► *Afin de sauvegarder un rapport formé, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans la zone de travail du groupe, sélectionnez l'onglet **Rapports**.
3. Sélectionnez le modèle de rapport qui vous intéresse dans la liste de modèles.
4. 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.

Création d'une tâche d'envoi du rapport

Les rapports peuvent être diffusés par courrier électronique. La diffusion des rapports dans Kaspersky Security Center s'effectue à l'aide de la tâche de diffusion du rapport.

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

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans la zone de travail du groupe, sélectionnez l'onglet **Rapports**.
3. Sélectionnez le modèle de rapport qui vous intéresse dans la liste de rapports.
4. Dans le menu contextuel du modèle du rapport, sélectionnez l'option **Envoi de 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, dans le noeud avec le nom du Serveur d'administration dont vous avez besoin sélectionnez le dossier **Tâches**.
2. Dans l'espace de travail du dossier **Tâches**, cliquez sur le bouton **Créer une tâche**.

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 **Envoi du rapport**.

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

La tâche de diffusion du rapport est créée automatiquement dans le cas où, lors de l'installation de Kaspersky Security Center, des paramètres d'email ont été définis (cf. section "Assistant de configuration initiale du Serveur d'administration" à la p. [75](#)).

Travailler avec les données statistiques

Des statistiques sur l'état du système de protection et des appareils administrés s'affichent dans l'espace de travail de l'entrée **Serveur d'administration** sous l'onglet **Statistiques**. L'onglet **Statistiques** contient plusieurs onglets de deuxième niveau (pages). Chaque page présente des panneaux d'informations avec des statistiques. Les données statistiques sont présentées sur les panneaux d'informations sous forme de tableaux ou de diagrammes camemberts ou colonnes. Les données dans les panneaux d'informations sont actualisées lors du fonctionnement de l'application et reflètent l'état actuel de l'application de protection.

Vous pouvez modifier l'ensemble de pages sous l'onglet **Statistiques**, l'ensemble de panneaux d'informations sur chaque page, ainsi que le mode d'affichage des données dans les panneaux d'informations.

► Pour ajouter une nouvelle page avec des panneaux d'informations, dans l'onglet **Statistiques**, procédez comme suit :

1. Cliquez sur le bouton **Personnaliser Affichage** en haut à droite de l'onglet **Statistiques**.

La fenêtre **Propriétés : Statistiques** s'ouvre. La fenêtre contient une liste des pages figurant dans l'onglet **Statistiques** en temps réel. Dans la fenêtre, vous pouvez modifier l'ordre d'apparition des pages dans l'onglet, ajouter et supprimer des pages, procéder à la configuration des propriétés des pages via le bouton **Propriétés**.

2. Cliquez sur le bouton **Ajouter**.

La fenêtre de propriétés de la nouvelle page s'affiche.

3. Configurez la nouvelle page :

- Dans la section **Général**, indiquez le nom de la page.
- Dans la section **Barres d'informations**, avec le bouton **Ajouter**, ajoutez des panneaux d'informations qui doivent s'afficher sur la page.

Avec le bouton **Propriétés**, dans la section **Barres d'informations**, il est possible de configurer les propriétés des panneaux d'informations ajoutés : nom et affichage du diagramme sur les panneaux, données avec lesquelles le diagramme est créé.

4. Cliquez sur le bouton **OK**.

La page ajoutée et les panneaux d'informations apparaissent dans l'onglet **Statistiques**. Avec le bouton  , il est possible de procéder rapidement à la configuration de la page ou de la barre d'informations sélectionnée sur celle-ci.

Configuration des paramètres de notification sur les événements

Kaspersky Security Center permet de sélectionner le mode de notification de l'administrateur sur les événements survenus sur les appareils client et de configurer les paramètres de ces notifications :

- Courrier électronique. Quand un événement se produit, l'application envoie une notification à l'adresse de messagerie électronique indiquée. Vous pouvez configurer le texte de la notification.
- SMS. Quand un événement se produit, l'application envoie la notification aux numéros de téléphone indiqués. Vous pouvez configurer l'envoi des SMS via la passerelle de messagerie ou à l'aide de l'utilitaire Kaspersky SMS Broadcasting.
- Fichier exécutable. Quand un événement se produit sur l'appareil, le fichier exécutable est lancé sur le poste de travail de l'administrateur. À l'aide du fichier exécutable, l'administrateur peut obtenir les paramètres de l'événement passé (cf. section "Notification relative aux événements via un fichier exécutable" à la p. [380](#)).

► *Pour configurer les paramètres des notifications sur les événements survenus sur les appareils clients, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Événements**.
3. Cliquez sur le lien **Configurer les paramètres des notifications et d'exportation des événements** dans la liste déroulante, puis sélectionnez la valeur **Configurer les paramètres des notifications**.

Finalement, la fenêtre **Propriétés : Événements**.

4. Dans la section **Notification**, sélectionnez le mode de notification (email, SMS, fichier exécutable à lancer) et configurez les paramètres des notifications.

5. Saisissez dans le champ **Texte de la notification** le texte que l'application enverra lorsque l'événement se produira.

Dans la liste déroulante située à droite du champ de texte, choisissez les paramètres prédéfinis avec les détails de l'événement à ajouter au texte (par exemple, la description de l'événement, l'heure à laquelle il s'est produit, etc.).

Si le texte de la notification contient le caractère %, il faut le saisir deux fois pour que le message puisse être envoyé. Par exemple, "La charge du processeur est de 100 %%".

6. Le bouton **Envoyer un message d'essai** permet de vérifier si la notification a été bien configurée.

L'application envoie la notification au destinataire indiqué.

7. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

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

Vous pouvez aussi rapidement configurer les notifications des événements dans la fenêtre de propriétés des événements par les liens **Configurer les paramètres des événements Kaspersky Endpoint Security** et **Configurer les paramètres des événements du Serveur d'administration**.

Voir également

Traitement et stockage des événements sur le Serveur d'administration [105](#)

Création d'un certificat pour le serveur SMTP

► Pour créer un certificat pour le serveur SMTP, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Evénements**.
3. Cliquez sur le lien **Configurer les paramètres des notifications et d'exportation des événements** dans la liste déroulante, puis sélectionnez la valeur **Configurer les paramètres des notifications**.

La fenêtre de propriétés des événements s'affiche.

4. Dans l'onglet **Email**, cliquez sur le lien **Paramètres** pour ouvrir la fenêtre **Paramètres**.
5. Dans la fenêtre **Paramètres**, cliquez sur le lien **Indiquer le certificat** pour ouvrir la fenêtre **Certificat pour la signature**.
6. Dans la fenêtre **Certificat pour la signature**, cliquez sur le bouton **Définir**.

Finalement, la fenêtre **Certificat** s'ouvre.

7. Dans la liste déroulante **Type de certificat**, sélectionnez le type de certificat ouvert ou fermé :
 - Si un certificat de type fermé est sélectionné (**Coffre-fort PKCS#12**), indiquez le fichier de certificat et le mot de passe.
 - Si un certificat de type ouvert est sélectionné (**certificat X.509**) :
 - a. indiquez un fichier de clé fermée (avec l'extension prk ou pem) ;
 - b. indiquez le mot de passe de la clé fermée ;
 - c. indiquez un fichier de clé ouverte (avec l'extension cer).
8. Cliquez sur le bouton **OK**.

Suite à cette action, un certificat pour serveur SMTP est créé.

Sélections d'événements

Les informations sur les événements dans le fonctionnement de Kaspersky Security Center et sur les applications administrés sont enregistrées dans le journal système Microsoft Windows et dans le journal des événements Kaspersky Security Center. Vous pouvez consulter des informations du journal des événements Kaspersky Security Center dans l'espace de travail du nœud **Serveur d'administration** dans l'onglet **Evénements**.

Les informations de l'onglet **Evénements** sont présentées sous forme de liste de sélections d'événements. Chaque sélection inclut seulement les événements d'un certain type. Par exemple, la sélection "État de l'appareil - Critique" contient uniquement les enregistrements du passage des appareils à l'état "Critique". Après l'installation de l'application, l'onglet **Evénements** contient une série de sélections standard d'événements. Vous pouvez créer des sélections complémentaires (d'utilisateurs) d'événements et exporter les informations sur les événements dans un fichier.

Dans cette section

Consultation d'une sélection d'événements	199
Configuration d'une sélection d'événements.....	200
Création d'une requête d'événements	200
Exportation d'une sélection dans le fichier texte	201
Suppression des événements depuis la sélection.....	201

Consultation d'une sélection d'événements

► *Pour consulter une sélection d'événements, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Evénements**.
3. Dans la liste affichée **Evénements de la sélection**, choisissez la sélection d'événements nécessaire.

Si vous souhaitez que les événements de cette sélection s'affichent en permanence dans l'espace de travail, cliquez sur le bouton  en regard de la sélection.

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

Vous pouvez trier les informations dans la liste des événements par ordre croissant ou décroissant des données dans n'importe quelle colonne de la liste.

Configuration d'une sélection d'événements

► *Pour configurer une sélection d'événements, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Evénements**.
3. Ouvrez la fenêtre de la sélection d'événements nécessaire sous l'onglet **Evénements**.
4. Cliquez sur le bouton **Propriétés de la sélection**.

Dans la fenêtre ouverte des propriétés de la sélection d'événements, vous pouvez configurer les paramètres de la sélection.

Création d'une sélection d'événements

► *Pour créer une sélection d'événements, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Evénements**.
3. Cliquez sur le bouton **Créer une sélection**.
4. Dans la fenêtre ouverte **Nouvelle sélection d'événements**, indiquez le nom de la sélection créée et cliquez sur le bouton **OK**.

Suite à cette action, une section avec le nom que vous avez indiqué est créée dans la liste affichée **Requêtes d'événements**.

Par défaut, la sélection d'événements créée contient tous les événements enregistrés sur le Serveur d'administration. Pour que la sélection d'événements affiche uniquement les événements qui vous intéressent, il faut configurer les paramètres de la sélection.

Exportation d'une sélection d'événements dans le fichier texte

► *Pour exporter la sélection d'événements dans un fichier texte, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Evénements**.
3. Cliquez sur le bouton **Importation/Exportation**.
4. Dans la liste affichée, sélectionnez **Exporter les événements dans un fichier**.

Finalement, l'Assistant d'exportation des événements se lancera. Suivez les instructions de l'Assistant.

Suppression des événements depuis la sélection

► Pour supprimer des événements de la sélection, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Evénements**.
3. Sélectionnez les événements à supprimer à l'aide de la souris et des touches **Shift** ou **Ctrl**.
4. Supprimez les événements sélectionnés par un des moyens suivants :
 - Dans le menu contextuel du n'importe quel événement parmi les événements sélectionnés, sélectionnez l'option **Supprimer**.

Lors de la sélection de l'option du menu contextuel **Supprimer tout**, tous les événements affichés, peu importe les événements que vous avez sélectionnés pour supprimer, seront supprimés de la requête.

- A l'aide du lien **Supprimer l'événement** si un événement a été sélectionné, ou à l'aide du lien **Supprimer les événements** si plusieurs événements ont été sélectionnés dans le groupe de travail avec les événements sélectionnés.

Suite à cette action, les événements sélectionnés sont supprimés.

Exportation des événements dans le système SIEM

L'application permet d'exporter les événements survenus au cours du fonctionnement du Serveur d'administration et des autres applications Kaspersky Lab installées sur les appareils clients dans le système SIEM (Security Information and Event Management).

► *Pour configurer l'exportation des événements dans le système SIEM, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Événements**.
3. Sur le lien **Configurer les paramètres des notifications et d'exportation des événements** dans la liste affichée, sélectionnez **Configurer l'exportation vers le système SIEM**.

La fenêtre des propriétés des événements de la section **Exportation des événements** s'ouvre.

4. Cochez la case **Exporter automatiquement les événements dans la base du système SIEM**.
5. Dans la liste déroulante **Système SIEM**, sélectionnez le système qui recevra les événements.

Il est possible d'exporter les événements dans les systèmes SIEM QRadar (format LEEF), ArcSight (format CEF) et Splunk (format CEF) et format Syslog (RFC 5424). Le système ArcSight (format CEF) est sélectionné par défaut.

6. Indiquez l'adresse du serveur du système SIEM et le port de connexion au serveur dans les champs prévus à cet effet.

Le bouton **Exporter l'archive** permet à l'application d'exporter les événements déjà créés dans la base du système SIEM à partir de la date indiquée. Par défaut, l'application exporte les événements à la date du jour.

7. Cliquez sur le bouton **OK**.

Suite à l'activation de la case **Exporter automatiquement les événements dans la base du système SIEM** et à la configuration de la connexion au serveur, l'application exportera automatiquement tous les événements concernant le Serveur d'administration et les autres applications Kaspersky Lab dans le système SIEM.

Pour obtenir de plus amples informations sur l'exportation des événements, consultez l'aide en ligne sur la ressource Web de Kaspersky Lab

<https://stage.help.kaspersky.com/KSC/EventExport/en-US/140015.htm>.

Sélections d'appareils

Les informations sur l'état des appareils se trouvent dans l'arborescence de la console dans le dossier **Sélections d'appareils**.

Les informations dans le dossier de **Sélections d'appareils** sont présentées sous forme de liste de sélection des appareils. Chaque sélection comprend les appareils répondant aux conditions définies. Par exemple, la sélection **Appareils avec l'état "Critique"** contient uniquement les appareils avec l'état *Critique*. Une fois que l'application a été installée, le dossier **Sélections d'appareils** contient diverses sélections standard. Vous pouvez créer des sélections complémentaires d'appareils (définies par l'utilisateur), exporter les paramètres des sélections dans un fichier, et créer des sélections avec les paramètres importés depuis un fichier.

Dans cette section

Affichage d'une sélection d'appareils	204
Configuration d'une sélection d'appareils	205
Création d'une sélection d'appareils	205
Exportation des paramètres de la sélection d'appareils dans un fichier	206
Création d'une sélection d'appareils selon les paramètres importés	206
Suppression des appareils depuis les groupes d'administration dans la sélection	207

Affichage d'une sélection d'appareils

► *Pour afficher une sélection d'appareils, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Sélections d'appareils**.
2. Dans la liste déroulante **Appareils de la sélection** du dossier, choisissez la sélection d'appareils dont vous avez besoin.

Si vous souhaitez que les appareils de cette sélection s'affichent en permanence dans l'espace de travail, cliquez sur le bouton  en regard de la sélection.

Finalement, l'espace de travail présentera la liste des appareils qui répondent aux paramètres de la sélection.

Vous pouvez trier les informations dans la liste des appareils en ordre croissant ou décroissant à partir de n'importe quel paramètre.

Configuration d'une sélection d'appareils

► *Pour configurer la sélection d'appareils, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Sélections d'appareils**.
2. Choisissez la sélection d'appareils dont vous avez besoin.
3. Cliquez sur le bouton **Propriétés de la sélection**.
4. Dans la fenêtre des propriétés qui s'ouvre, configurez les propriétés générales de la sélection et les critères d'inclusion des appareils dans la sélection.
5. Cliquez sur le bouton **OK**.

Création d'une sélection d'appareils

► *Pour créer une sélection d'appareils, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Sélections d'appareils**.
2. Dans l'espace de travail du dossier, appuyez sur le bouton **Avancé**, et dans la liste déroulante, sélectionnez **Créer une sélection**.
3. Dans la fenêtre ouverte **Nouvelle sélection d'appareils**, indiquez le nom de la sélection créée et cliquez sur le bouton **OK**.

Finalement, dans l'arborescence de la console dans le dossier **Sélections d'appareils** un nouveau dossier avec le nom, que vous avez indiqué, sera créé. Par défaut, la sélection d'appareils créée contient tous les appareils inclus dans les groupes d'administration du Serveur sous l'administration duquel la sélection a été créée. Pour que la sélection d'événements affiche uniquement les appareils qui vous intéressent, il faut configurer les paramètres de la sélection en appuyant sur le bouton **Propriétés de la sélection**.

Exportation des paramètres de la sélection d'appareils dans un fichier

► *Pour exporter les paramètres de la sélection d'appareils dans le fichier texte, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Sélections d'appareils**.
2. Dans l'espace de travail du dossier, appuyez sur le bouton **Avancé**, et dans la liste déroulante, sélectionnez **Exporter les paramètres**.
3. Dans la fenêtre ouverte **Enregistrer sous**, définissez le nom du fichier d'exportation des paramètres de la sélection, sélectionnez le dossier dans lequel le fichier sera enregistré et cliquez sur le bouton **Enregistrer**.

Les paramètres de la sélection d'appareils seront enregistrés dans le fichier indiqué.

Création d'une sélection d'appareils selon les paramètres importés

► *Créer une sélection d'appareils selon les paramètres importés :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Sélections d'appareils**.
2. Dans l'espace de travail du dossier, appuyez sur le bouton **Avancé**, et dans la liste déroulante, sélectionnez **Importer**.
3. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier depuis lequel vous souhaitez importer les paramètres de la sélection. Cliquez sur **Ouvrir**.

Finalement, dans le dossier **Sélections d'appareils** la sélection **Nouvelle sélection** dont les paramètres ont été importés depuis le fichier indiqué sera créée.

Si dans le dossier **Sélections d'appareils** une sélection portant le nom **Nouvelle sélection** existe déjà, le suffixe de type (<numéro d'ordre>) sera ajouté au nom de la sélection créée, par exemple : **(1)**, **(2)**.

Suppression des appareils depuis les groupes d'administration dans la sélection

Lors de l'utilisation de la sélection d'appareils, vous pouvez supprimer les appareils des groupes d'administration directement dans la sélection sans avoir à supprimer les appareils des groupes d'administration.

► *Pour supprimer les appareils depuis les groupes d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Sélections d'appareils**.
2. Sélectionnez les appareils à supprimer à l'aide des boutons **Shift** ou **Ctrl**.
3. Supprimez les appareils sélectionnés depuis les groupes d'administration à l'aide d'un des moyens suivants :
 - Dans le menu contextuel de n'importe quel appareil parmi les appareils sélectionnés, sélectionnez l'option **Supprimer**.
 - Appuyez sur le bouton **Exécuter l'action** et, dans la liste déroulante, sélectionnez **Supprimer du groupe**.

Finalement, les appareils sélectionnés seront supprimés depuis les groupes d'administration dont ils faisaient partie.

Stratégies

Le dossier **Stratégies** contient des informations sur les stratégies.

Le dossier **Stratégies** reprend la liste des stratégies créées dans les groupes d'administration. Après l'installation de l'application, le dossier contient les stratégies créées automatiquement. Vous pouvez mettre à jour la liste de stratégies, créer des stratégies ainsi que consulter les propriétés de la stratégie sélectionnée dans la liste.

Le diagramme montre la progression de l'application de la stratégie sur les appareils clients auxquels elle est appliquée. Quand la couleur du diagramme devient entièrement vert, cela signifie que la stratégie est appliquée à tous les appareils clients.

Tâches

Le dossier **Tâches** contient des informations sur les tâches.

Le dossier **Tâches** reprend la liste des tâches attribuées aux appareils clients dans les groupes d'administration et au Serveur d'administration. Après l'installation de l'application, le dossier contient la liste des tâches créées automatiquement. Vous pouvez mettre à jour la liste de tâches, créer des tâches ainsi que consulter les propriétés des tâches, lancer ou arrêter des tâches.

Appareils non définis

Cette section reprend les informations sur l'utilisation des appareils du réseau de l'entreprise, non inclus dans les groupes d'administration.

Dans cette section

Sondage du réseau.....	209
Travail avec les domaines Windows. Affichage et modification des paramètres du domaine ..	213
Travail avec les plages IP.....	213
Travail avec les groupes Active Directory. Affichage et modification des paramètres du groupe.....	215
Création des règles de déplacement automatique des appareils dans un groupe d'administration.....	215
Utilisation du mode dynamique VDI sur les appareils clients	216

Sondage du réseau

Le Serveur d'administration obtient les informations relatives à la structure du réseau et aux appareils qu'elle héberge lors des sondages réguliers du réseau Windows, des plages IP ou d'Active Directory ayant lieu dans le réseau de l'entreprise. Le contenu du dossier **Appareils non définis** est actualisé sur la base du résultat de ces requêtes.

Le Serveur d'administration peut réaliser les types de sondage du réseau suivants :

- **Sondage du réseau Windows.** Il existe deux types de sondages du réseau Windows : ce rapide et complet. Lors du sondage rapide, le serveur ne reçoit que les informations relatives à la liste des noms NetBIOS des appareils de tous les domaines et des groupes de travail du réseau. Pendant le sondage entier, les informations suivantes sont demandées à partir de chaque appareil client : nom du système d'exploitation, adresse IP, nom DNS et nom NetBIOS.
- **Sondage des plages IP.** Le Serveur d'administration sonde les intervalles IP créés à l'aide de paquets ICMP et reçoit toutes les informations sur les appareils appartenant aux plages IP.
- **Sondage des groupes Active Directory.** Les données du Serveur d'administration permettent d'enregistrer des informations relatives à la structure des groupes Active Directory, ainsi qu'aux noms DNS des appareils du groupe Active Directory.

Sur la base des informations obtenues et des données sur la structure du réseau de l'entreprise, Kaspersky Security Center actualise le contenu des dossiers **Appareils non définis** et **Appareils administrés**. Si dans le réseau de l'entreprise le déplacement automatique des appareils dans les groupes d'administration est configuré, les appareils détectés dans le réseau sont inclus dans les groupes d'administration.

Dans cette section

Affichage et modification des paramètres de sondage du réseau Windows	211
Affichage et modification des paramètres de sondage des groupes Active Directory	211
Affichage et modification des paramètres de sondage des plages IP	212

Affichage et modification des paramètres de sondage du réseau Windows

► *Pour modifier les paramètres du sondage du réseau Windows, procédez comme suit :*

1. Dans l'arborescence de la console dans le dossier **Sondage du réseau**, sélectionnez le sous-dossier **Domaines**.

Vous pouvez passer au dossier **Sondage du réseau** depuis le dossier **Appareils non définis** à l'aide du bouton **Analyser maintenant**.

2. Cliquez sur le bouton **Configurer les paramètres du sondage** dans l'espace de travail du dossier **Domaines**.

Cela entraîne l'ouverture de la fenêtre **Propriétés : Domaines**. Celle-ci permet de modifier les paramètres de sondage du réseau Windows.

Sur le Serveur d'administration virtuel l'affichage et la modification des paramètres du sondage du réseau Windows sont effectués dans la fenêtre des propriétés de l'agent de mises à jour, dans la section **Sondage du réseau**.

Affichage et modification des paramètres de sondage des groupes Active Directory

► *Pour modifier les paramètres de sondage des groupes Active Directory, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Sondage du réseau**, sélectionnez le sous-dossier **Active Directory**.

Vous pouvez passer au dossier **Sondage du réseau** depuis le dossier **Appareils non définis** à l'aide du bouton **Analyser maintenant**.

2. Le lien **Configurer les paramètres du sondage** ouvre la fenêtre **Propriétés : Active Directory**.

La fenêtre **Propriétés : Active Directory** permet de consulter et de modifier les paramètres de sondage des groupes Active Directory.

Sur le Serveur d'administration virtuel l'affichage et la modification des paramètres du sondage des groupes Active Directory sont effectués dans la fenêtre des propriétés de l'agent de mises à jour, dans la section **Sondage du réseau**.

Affichage et modification des paramètres de sondage des plages IP

► *Pour modifier les paramètres du sondage des plages IP, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Sondage du réseau**, sélectionnez le sous-dossier **Plages IP**.

Vous pouvez passer au dossier **Sondage du réseau** depuis le dossier **Appareils non définis** à l'aide du bouton **Analyser maintenant**.

2. Le lien **Configurer les paramètres du sondage** ouvre la fenêtre **Propriétés : Plages IP**.

La fenêtre **Propriétés : Plages IP** permet de consulter et de modifier les paramètres du sondage des plages IP.

Sur le Serveur d'administration virtuel l'affichage et la modification des paramètres du sondage des plages IP sont effectués dans la fenêtre des propriétés de l'agent de mises à jour, dans la section **Sondage du réseau**. Les appareils clients, trouvés suite au sondage des plages IP, s'affichent dans le dossier **Domaines** du Serveur virtuel.

Travail avec les domaines Windows.

Affichage et modification des paramètres du domaine

► Pour modifier les paramètres du domaine, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Sondage du réseau**, sélectionnez le sous-dossier **Domaines**.
2. Sélectionnez le domaine et ouvrez la fenêtre de ses propriétés à l'aide d'un des moyens suivants :
 - Dans le menu contextuel du domaine, sélectionnez l'option **Propriétés**.
 - A l'aide du lien **Afficher les propriétés du groupe**.

Finalement, la fenêtre **Propriétés : <Nom de domaine>** s'ouvre qui permet de configurer les paramètres du domaine sélectionnée.

Travail avec les plages IP

Vous pouvez configurer les paramètres des plages IP existantes, ainsi que créer les nouvelles plages IP.

Dans cette section

Création de la plage IP	214
Affichage et modification des paramètres de plage IP	214

Création de la plage IP

► *Pour créer une plage IP, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Sondage du réseau**, sélectionnez le sous-dossier **Plages IP**.
2. Dans le menu contextuel du dossier, sélectionnez l'option **Créer** → **Plage IP**.
3. Dans la fenêtre ouverte **Nouvelle plage IP**, configurez les paramètres de la plage IP créée.

Finalement, la plage IP créée apparaîtra dans le dossier **Plages IP**.

Affichage et modification des paramètres de plage IP

► *Pour modifier les paramètres de la plage IP, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Sondage du réseau**, sélectionnez le sous-dossier **Plages IP**.
2. Sélectionnez la plage IP et ouvrez la fenêtre de ses propriétés à l'aide d'un des moyens suivants :
 - Dans le menu contextuel de la plage IP, sélectionnez l'option **Propriétés**.
 - A l'aide du lien **Afficher les propriétés du groupe**.

Finalement, la fenêtre **Propriétés : <Nom de plage IP>** s'ouvre qui permet de configurer les paramètres de la plage IP sélectionnée.

Travail avec les groupes Active Directory. Affichage et modification des paramètres du groupe

► *Pour modifier les paramètres du groupe Active Directory, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Sondage du réseau**, sélectionnez le sous-dossier **Active Directory**.
2. Sélectionnez le groupe Active Directory et ouvrez la fenêtre de ses propriétés à l'aide d'un des moyens suivants :
 - Dans le menu contextuel du groupe, sélectionnez l'option **Propriétés**.
 - A l'aide du lien **Afficher les propriétés du groupe**.

Finalement, la fenêtre **Propriétés : <Nom du groupe Active Directory>** s'ouvre qui permet de configurer les paramètres du groupe Active Directory sélectionné.

Création des règles de déplacement automatique des appareils dans un groupe d'administration

Vous pouvez configurer le déplacement automatique des appareils, détectés lors du sondage du réseau de l'entreprise, dans les groupes d'administration.

► *Pour configurer la règle de déplacement automatique des appareils dans les groupes d'administration, procédez comme suit :*

1. Dans l'arborescence de la console sélectionnez le dossier **Appareils non définis**.
2. Dans l'espace de travail du dossier, cliquez sur le bouton **Configurer les règles**.

Finalement, la fenêtre **Propriétés : Appareils non définis** s'ouvre. Configurez la règle de déplacement automatique des appareils dans le groupe d'administration dans la section **Déplacement des appareils**.

Utilisation du mode dynamique VDI sur les appareils clients

Le réseau de l'entreprise peut contenir une infrastructure virtuelle sur la base de machines virtuelles temporaires. Kaspersky Security Center détecte les machines virtuelles temporaires et ajoute les données qui les concernent à la base de données du serveur d'administration. Une fois que l'utilisateur a terminé de travailler avec la machine virtuelle temporaire, celle-ci est supprimée de l'infrastructure virtuelle. Toutefois, l'entrée relative à la machine virtuelle supprimée peut être conservée dans la base de données du serveur d'administration. De plus, les machines virtuelles inexistantes peuvent apparaître dans la Console d'administration.

Pour éviter de conserver des données relatives à des machines virtuelles qui n'existent pas, Kaspersky Security Center prend en charge le mode dynamique pour Virtual Desktop Infrastructure (VDI). L'administrateur peut activer la prise en charge du mode dynamique pour VDI dans les propriétés du paquet d'installation de l'agent d'administration qui sera installé sur la machine virtuelle temporaire (cf. section "Activation du mode dynamique VDI dans les propriétés du paquet d'installation de l'Agent d'administration" à la page [217](#)).

Lors de l'arrêt de la machine virtuelle temporaire, l'agent d'administration informe le serveur d'administration de l'arrêt. Si la machine virtuelle a bien été arrêtée, elle est supprimée de la liste des appareils connectés au Serveur d'administration. Si l'arrêt de la machine virtuelle n'est pas réalisé comme il se doit et que l'agent d'administration n'a pas notifié le serveur d'administration de l'arrêt, c'est le scénario de réserve qui est suivi. D'après ce scénario, la machine virtuelle est supprimée de la liste des appareils connectés au Serveur d'administration après trois tentatives échouées de synchronisation avec le Serveur.

Dans cette section

Activation du mode dynamique VDI dans les propriétés du paquet d'installation de l'Agent d'administration.....	217
Recherche d'appareils qui font partie de VDI.....	218
Déplacement dans le groupe d'administration des appareils qui font partie de VDI	218

Activation du mode dynamique VDI dans les propriétés du paquet d'installation de l'Agent d'administration

► *Pour activer le mode dynamique VDI, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
2. Dans le menu contextuel du paquet d'installation de l'Agent d'administration, sélectionnez l'option **Propriétés**.

La fenêtre **Paramètres : Agent d'administration de Kaspersky Security Center** s'ouvre.

3. Dans la fenêtre **Propriétés : Agent d'administration Kaspersky Security Center**, sélectionnez la section **Avancé**.
4. Dans la section **Avancé**, cochez la case **Activer le mode dynamique pour VDI**.

L'appareil sur lequel l'Agent d'administration s'installe sera une partie de Virtual Desktop Infrastructure.

Recherche d'appareils qui font partie de VDI

► *Pour rechercher les appareils qui font partie de VDI, procédez comme suit :*

1. Dans le menu contextuel du dossier **Appareils non définis**, sélectionnez l'option **Recherche**.
2. Dans la fenêtre **Recherche** sous l'onglet **Machines virtuelles** dans la liste déroulante **Membre d'une Virtual Desktop Infrastructure**, sélectionnez l'option **Oui**.
3. Cliquez sur le bouton **Rechercher**.

La recherche d'appareils membres de Virtual Desktop Infrastructure sera exécutée.

Déplacement dans le groupe d'administration des appareils qui font partie de VDI

► *Pour déplacer les appareils qui font partie de VDI dans le groupe d'administration, procédez comme suit :*

1. Dans l'espace de travail du dossier **Appareils non définis**, cliquez sur le bouton **Configurer les règles**.

Finalement, la fenêtre des propriétés du dossier **Appareils non définis** s'ouvre.

2. Dans la fenêtre des propriétés du dossier **Appareils non définis** dans la section **Déplacement des appareils**, cliquez sur le bouton **Ajouter**.

La fenêtre **Nouvelle règle** s'ouvre.

3. Dans la fenêtre **Nouvelle règle**, sélectionnez la section **Machines virtuelles**.
4. Dans la liste déroulante **Membre d'une Virtual Desktop Infrastructure**, sélectionnez l'option **Oui**.

La règle de déplacement des appareils dans le groupe d'administration sera créée.

Administration des applications sur les appareils clients

Kaspersky Security Center permet d'administrer les applications de Kaspersky Lab et d'autres éditeurs installées sur les appareils clients.

L'administrateur peut exécuter les actions suivantes :

- créer les catégories d'applications sur la base des critères définis ;
- administrer les catégories d'applications à l'aide des règles spécialement créées ;
- administrer le lancement des applications sur les appareils;
- exécuter l'inventaire et suivre le registre du logiciel installé sur les appareils ;
- fermer les vulnérabilités du logiciel installé sur les appareils ;
- installer les mises à jour Windows Update et d'autres éditeurs du logiciel sur les appareils ;
- surveiller l'utilisation des clés pour les groupes des applications sous licence.

Dans cette section

Groupes des applications	219
Vulnérabilités dans les applications	232
Mises à jour du logiciel	236

Groupes des applications

Cette section décrit l'utilisation des groupes des applications installées sur les appareils.

Création des catégories d'applications

Kaspersky Security Center permet de créer les catégories d'applications installées sur les appareils.

Il est possible de créer les catégories d'applications à l'aide des moyens suivants :

- L'administrateur indique le dossier dont les fichiers exécutables se trouvent dans la catégorie sélectionnée.
- L'administrateur indique l'appareil dont les fichiers exécutables se trouvent dans la catégorie sélectionnée.
- L'administrateur définit les critères selon lesquels les applications se trouvent dans la catégorie sélectionnée.

Quand une catégorie d'applications est créée, l'administrateur peut définir les règles pour cette catégorie. Les règles définissent le comportement des applications qui sont incluses dans la catégorie indiquée. Par exemple, il est possible d'interdire ou d'autoriser le lancement des applications qui font partie de la catégorie.

Administration du lancement des applications sur les appareils

Kaspersky Security Center permet de gérer le lancement des applications sur les appareils en mode "Liste blanche" (pour plus d'informations, cf. Manuel de l'administrateur pour l'application Kaspersky Endpoint Security 10 for Windows). Le mode "Liste blanche" signifie que le lancement uniquement des applications, qui font partie des catégories indiquées, sera autorisé sur les appareils sélectionnés. L'administrateur peut consulter les résultats de l'analyse statique des règles de lancement des applications sur les appareils pour chaque utilisateur.

Inventaire du logiciel installé sur les appareils

Kaspersky Security Center permet d'exécuter l'inventaire du logiciel sur les appareils. L'Agent d'administration obtient les informations sur toutes les applications installées sur les appareils. Les informations obtenues suite à l'inventaire s'affichent dans l'espace de travail du dossier **Registre**

des applications. L'administrateur peut consulter les informations détaillées sur chaque application, y compris la version et l'éditeur.

Le nombre de fichiers exécutables reçus d'un appareil ne peut pas dépasser 150 000. Une fois cette restriction atteinte, Kaspersky Security Center ne recevra pas de nouveaux fichiers.

Administration des groupes des applications sous licence

Kaspersky Security Center permet de créer les groupes des applications sous licence. Le groupe des applications sous licence inclut les applications qui répondent aux critères définis par l'administrateur. L'administrateur peut indiquer les critères suivants pour les groupes des applications sous licence :

- nom de l'application ;
- version de l'application ;
- éditeur ;
- tag de l'application.

Les applications qui correspondent à un ou plusieurs critères sont placées automatiquement dans le groupe. Pour créer le groupe des applications sous licence, au moins un critère d'inclusion des applications dans ce groupe doit être défini.

Chaque groupe des applications sous licence possède sa clé. La clé du groupe des applications sous licence définit le nombre admissible des installations pour les applications qui font partie du groupe. Si le nombre d'installations dépasse la restriction définie dans la clé, l'événement d'informations s'enregistre sur le Serveur d'administration. L'administrateur peut indiquer la date de fin de validité de la clé. Lorsque cette date survient, l'événement d'informations est enregistré sur le Serveur d'administration.

Consultation des informations sur les fichiers exécutables

Kaspersky Security Center reçoit toutes les informations sur les fichiers exécutables qui ont été lancés sur les appareils dès l'installation du système d'exploitation sur ceux-ci. Les informations collectées sur les fichiers exécutables s'affichent dans la fenêtre principale de l'application, dans l'espace de travail du dossier **Fichiers exécutables**.

Dans cette section

Création des catégories d'applications	222
Configuration d'administration du lancement des applications sur les appareils clients.....	223
Consultation des résultats de l'analyse statique des règles de lancement des fichiers exécutables	225
Affichage du registre des applications	225
Création des groupes des applications de licence	227
Administration des clés pour les groupes des applications de licence.....	228
Inventaire du logiciel Kaspersky Security Center	229
Inventaire des fichiers exécutables	230
Consultation des informations sur les fichiers exécutables.....	231

Création des catégories d'applications

► *Pour créer une catégorie d'applications, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Catégories d'applications**.
2. Le lien **Créer une catégorie** permet de lancer l'Assistant de création de la catégorie d'utilisateur.

3. Sélectionnez le type de la catégorie d'utilisateur dans la fenêtre de l'Assistant :
 - **Catégorie complétée à la main.** Dans ce cas, vous pouvez définir manuellement les critères selon lesquels les fichiers exécutables feront partie de la catégorie créée.
 - **Catégorie complétée automatiquement.** Dans ce cas, vous pouvez indiquer le dossier dont les fichiers exécutables seront automatiquement placés dans la catégorie créée.

Lors de la création de la catégorie d'applications remplie automatiquement, l'application exécute l'inventaire des formats de fichiers suivants : exe, com, dll, sys, bat, ps1, cmd, js, vbs, reg, msi, msc, cpl, html, htm, drv, ocx, scr.

- **Catégorie incluant les fichiers exécutables depuis les appareils sélectionnés.** Dans ce cas, vous pouvez indiquer l'appareil. Les fichiers exécutables détectés sur l'appareil seront automatiquement placés dans la catégorie.

4. Suivez les instructions de l'Assistant.

Suite au fonctionnement de l'Assistant, la catégorie d'applications définie par l'utilisateur est créée. Les catégories créées peuvent être consultées dans la liste de catégories de l'espace de travail du dossier **Catégories d'applications**.

Configuration d'administration du lancement des applications sur les appareils clients

► *Pour configurer la gestion du lancement des applications sur les appareils clients, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Catégories d'applications**.
2. Dans la zone de travail du dossier **Catégories d'applications**, créez une catégorie d'applications (cf. section "Création des catégories d'applications" à la page [222](#)) dont vous voulez gérer le lancement.

3. Dans le dossier **Appareils administrés** sous l'onglet **Stratégies** à l'aide du lien **Créer une stratégie de Kaspersky Endpoint Security**, lancez l'Assistant de création de la stratégie pour l'application Kaspersky Endpoint Security 10 for Windows et suivez les consignes de l'Assistant.

Si une telle stratégie déjà existe, cette étape peut être ignorée. L'administration du lancement des applications dans la catégorie indiquée peut être configurée dans les paramètres de cette stratégie. La stratégie créée s'affiche dans le dossier **Appareils administrés** sous l'onglet **Stratégies**.

4. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés** pour l'application Kaspersky Endpoint Security 10 for Windows.

La fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security 10 for Windows s'ouvre.

5. Dans la fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security 10 for Windows dans la section **Contrôle du lancement des applications**, cliquez sur le bouton **Ajouter**.

La fenêtre **Règle de contrôle du lancement des applications** s'ouvre.

6. Dans la fenêtre **Règle de contrôle du lancement des applications** dans la liste déroulante **Catégorie**, sélectionnez la catégorie d'applications pour laquelle la règle du lancement sera diffusée. Configurez les paramètres de la règle du lancement pour la catégorie sélectionnée des applications.

Pour plus de détails sur les règles de contrôle du lancement des applications, cf. Manuel de l'administrateur de Kaspersky Endpoint Security 10 for Windows.

7. Cliquez sur le bouton **OK**.

Le lancement des applications sur les appareils qui font partie de la catégorie indiquée sera exécuté conformément à la règle créée. La règle créée s'affichent dans la fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security 10 for Windows dans la section **Contrôle du lancement des applications**.

Consultation des résultats de l'analyse statique des règles de lancement des fichiers exécutables

► *Pour consulter les informations sur le lancement des fichiers exécutables interdits par l'utilisateur, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Appareils administrés**, sélectionnez l'onglet **Stratégies**.

2. Dans le menu contextuel **Stratégies de protection**, choisissez l'option **Propriétés**.

La fenêtre des propriétés de la stratégie de protection s'ouvre.

3. Dans la fenêtre des propriétés de la stratégie de protection, sélectionnez la section **Contrôle du lancement des applications** et cliquez sur le bouton **Analyse statique**.

La fenêtre **Analyse de la liste des privilèges d'accès** s'ouvre.

4. La partie gauche de la fenêtre **Analyse de la liste des privilèges d'accès** affiche la liste des utilisateurs composée sur la base des données Active Directory.

5. Sélectionnez l'utilisateur dans la liste.

La partie droite de la fenêtre affichera les catégories d'applications désignées à cet utilisateur.

6. Pour consulter les fichiers exécutables dont le lancement est interdit par l'utilisateur, cliquez sur le bouton **Consulter les fichiers** dans la fenêtre **Analyse de la liste des privilèges d'accès**.

La fenêtre s'ouvre. Cette fenêtre affiche la liste des fichiers exécutables dont le lancement est interdit par l'utilisateur.

7. Pour consulter la liste de fichiers exécutables qui font partie d'une catégorie,, sélectionnez la catégorie d'applications et cliquez sur le bouton **Consulter les fichiers de la catégorie**.

La fenêtre s'ouvre. Cette fenêtre affiche la liste des fichiers exécutables qui font partie de la catégorie d'applications.

Affichage du registre des applications

La fonctionnalité d'obtention d'informations sur les applications installées est prise en charge uniquement pour les systèmes d'exploitation Microsoft Windows.

► *Pour consulter le registre des applications installées sur les appareils clients,*

dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Registre des applications**.

L'espace de travail du dossier **Registre des applications** affiche la liste des applications détectées sur les appareils par l'Agent d'administration installés sur ces appareils.

Vous pouvez consulter les informations détaillées concernant une application en sélectionnant dans le menu contextuel de cette application l'option **Propriétés**. La fenêtre des propriétés de l'application affiche les informations générales sur l'application et les informations sur les fichiers exécutables de l'application, ainsi que la liste des appareils sur lesquels l'application est installée.

Pour consulter les applications qui satisfont les critères définis, vous pouvez utiliser les champs de filtrage dans l'espace de travail du dossier **Registre des applications**.

Les informations relatives aux applications de Kaspersky Lab et d'autres éditeurs sur les appareils connectés aux Serveurs d'administration secondaires et virtuels sont également enregistrées dans le registre des applications du Serveur d'administration principal. Vous pouvez consulter ces informations à l'aide du rapport sur le registre des applications, en incluant dans le rapport les données de la part des Serveurs d'administration virtuels et secondaires.

► *Pour inclure dans le rapport sur le registre des applications les informations provenant des Serveurs d'administration secondaires, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans la zone de travail du groupe, sélectionnez l'onglet **Rapports**.
3. Dans l'onglet **Rapports**, sélectionnez **Rapport sur les versions des logiciels de Kaspersky Lab**.

4. Dans le menu contextuel du rapport, sélectionnez l'option **Propriétés**.

La fenêtre **Propriétés : Rapport sur les versions des logiciels de Kaspersky Lab** s'ouvre.

5. Dans la section **Hiérarchie des Serveurs d'administration**, cochez la case **Utiliser les données à partir des Serveurs d'administration secondaires et virtuels**.
6. Cliquez sur le bouton **OK**.

Les informations provenant des serveurs d'administration virtuels et secondaires seront alors incluses dans le **Rapport sur les versions des logiciels de Kaspersky Lab**.

Création des groupes des applications sous licence

► *Pour créer un groupe des applications sous licence, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Compte des licences tierces**.
2. A l'aide du lien **Ajouter un groupe d'applications sous licence**, lancez **Assistant d'ajout du groupe des applications sous licence**.
3. Suivez les instructions de l'Assistant.

Suite à l'exécution de l'Assistant, un groupe des applications sous licence est créé. Ce groupe s'affiche dans le dossier **Compte des licences tierces**.

Gestion des clés pour les groupes des applications sous licence

► *Pour créer une clé pour le groupe des applications sous licence, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Compte des licences tierces**.
2. Dans l'espace de travail du dossier **Compte des licences tierces**, cliquez sur le lien **Administrer les clés d'applications sous licence** et ouvrez la fenêtre **Administration des clés des applications sous licence**.
3. Dans la fenêtre **Administration des clés des applications sous licence**, cliquez sur le bouton **Ajouter**.

Le fenêtre **Clé** s'ouvre.

4. Dans la fenêtre **Clé**, indiquez les paramètres de la clé et les restrictions que cette clé impose sur le groupe des applications sous licence.

- **Nom**. Le nom de la clé.
- **Commentaires**. Les remarques de la clé sélectionnée.
- **Limite**. Le nombre d'appareils sur lesquels l'application, utilisant cette clé, peut être installée.
- **Date d'expiration**. La date d'expiration de validité de la clé.

Les clés créées s'affichent dans le dossier **Administration des clés des applications sous licence**.

► *Pour appliquer une clé au groupe des applications sous licence, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Compte des licences tierces**.
2. Dans le dossier **Compte des licences tierces**, sélectionnez le groupe des applications sous licence auquel vous souhaitez appliquer la clé.

3. Dans le menu contextuel du groupe des applications sous licence, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés du groupe des applications sous licence s'ouvre.

4. Dans la fenêtre des propriétés du groupe des applications sous licence dans la section **Clés**, sélectionnez l'option **Contrôler la violation des restrictions de licence définie**.
5. Cliquez sur le bouton **Ajouter**.

La fenêtre **Sélection de la clé** s'ouvre.

6. Dans la fenêtre **Sélection de la clé**, sélectionnez la clé que vous voulez appliquer au groupe des applications sous licence.
7. Cliquez sur le bouton **OK**.

Les restrictions pour le groupe des applications sous licence indiquées dans la clé seront diffusées sur le groupe des applications sous licence sélectionné.

Inventaire du logiciel Kaspersky Security Center

Kaspersky Security Center procède à l'inventaire du logiciel installé sur les appareils clients administrés.

L'Agent d'administration constitue une liste des applications installées sur l'appareil et la transmet au Serveur d'administration. L'Agent d'administration reçoit automatiquement des informations sur les applications installées du registre Windows.

Pour enregistrer les ressources de l'appareil, par défaut, l'Agent d'administration comment à recevoir des informations sur les applications installées 10 minutes après le lancement de son service.

► Pour modifier la durée du début d'inventaire du logiciel de l'appareil après le lancement du service de l'Agent d'administration, procédez comme suit :

1. Ouvrez le registre système de l'appareil sur lequel l'Agent d'administration est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.
2. Rendez-vous dans la section :

- Pour un système de 64 bits :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34  
\1103\1.0.0.0\NagentFlags
```

- Pour un système de 32 bits :

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\N  
agentFlags
```

3. Pour la clé KLINV_INV_COLLECTOR_START_DELAY_SEC, cochez la valeur de votre choix en secondes.

La valeur par défaut est égale à 600 secondes.

4. Relancez le service de l'Agent d'administration.

Suite à cette action, la durée du début d'inventaire du logiciel après le lancement du service de l'Agent d'administration est modifiée.

Inventaire des fichiers exécutables

L'inventaire des fichiers exécutables sur les appareils clients peut être effectué à l'aide de la tâche d'inventaire. La fonction d'inventaire des fichiers exécutables est réalisée dans l'application Kaspersky Endpoint Security 10 for Windows.

Le nombre de fichiers exécutables reçus d'un appareil ne peut pas dépasser 150 000. Une fois cette limite atteinte, Kaspersky Endpoint Security 10 ne recevra pas de nouveaux fichiers.

► *Pour créer une tâche d'inventaire des fichiers exécutables sur les appareils clients, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Dans l'espace de travail du dossier **Tâches**, cliquez sur le bouton **Créer une tâche**.

Ceci permet de lancer l'Assistant de création de tâche.

3. Dans la fenêtre de l'assistant **Sélection du type de tâche**, sélectionnez le type de tâche **Kaspersky Endpoint Security**, puis le sous-type de tâche **Inventaire** et cliquez sur le bouton **Suivant**.

4. Suivez les étapes ultérieures de l'assistant.

Suite à l'exécution de l'assistant, une tâche d'inventaire est créée pour Kaspersky Endpoint Security. La tâche créée est affichée dans la liste de tâches de l'espace de travail du dossier **Tâches**.

Suite à l'exécution de l'inventaire, la liste des fichiers exécutables détectés sur les appareils s'affiche dans l'espace de travail **Fichiers exécutables**.

Pendant l'exécution de l'inventaire, l'application détecte les fichiers exécutables des formats suivants : m3u, com, ms-dos, pe, ne, sys, cmd, bat, ps1, js, vbs, reg, msi, cpl, dll, jar, ainsi que les fichiers HTML.

Consultation des informations sur les fichiers exécutables

► *Pour consulter la liste de tous les fichiers exécutables détectés sur les appareils clients,*

dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Fichiers exécutables**.

L'espace de travail du dossier **Fichiers exécutables** affiche la liste des fichiers exécutables qui ont été lancés sur les appareils dès le moment d'installation du système d'exploitation ou

qui ont été détectés pendant le fonctionnement de la tâche d'inventaire de Kaspersky Endpoint Security 10 for Windows.

Pour consulter les données sur les fichiers exécutables qui satisfont les critères définis, vous pouvez utiliser le filtrage.

► *Pour consulter les propriétés du fichier exécutable,*

dans le menu contextuel du fichier, sélectionnez l'option **Propriétés**.

La fenêtre qui contient les informations sur le fichier exécutable s'ouvre, ainsi que la liste des appareils sur lesquels le fichier exécutable est présent.

Vulnérabilités dans les applications

Le dossier **Vulnérabilités dans les applications** du dossier **Administration des applications** contient la liste des vulnérabilités applicatives que l'Agent d'administration a détectées sur les appareils clients où il est installé.

La fonction d'analyse des informations sur les vulnérabilités dans les applications est prise en charge uniquement pour les systèmes d'exploitation Microsoft Windows.

En ouvrant la fenêtre des propriétés de l'application sélectionnée dans le dossier **Vulnérabilités dans les applications**, vous pouvez recevoir les informations générales sur la vulnérabilité, sur l'application dans laquelle la vulnérabilité a été détectée, consulter la liste des appareils sur lesquels la vulnérabilité a été détectée, ainsi que les informations sur la correction de la vulnérabilité.

Vous pouvez recevoir des informations sur les vulnérabilités détectées dans les applications sur le site Kaspersky Lab (<https://threats.kaspersky.com>).

Consultation des informations relatives aux vulnérabilités dans les applications

- *Pour consulter la liste des vulnérabilités détectées sur les appareils clients,*

dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Vulnérabilités dans les applications**.

L'espace de travail du dossier affiche la liste des vulnérabilités dans les applications détectées sur les appareils par l'Agent d'administration installé sur ces appareils.

- *Pour obtenir les informations sur la vulnérabilité sélectionnée,*

dans le menu contextuel de la vulnérabilité, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés de la vulnérabilité s'ouvre. Cette fenêtre affiche les informations suivantes :

- l'application contenant la vulnérabilité ;
- la liste des appareils avec la vulnérabilité détectée ;
- les informations sur la correction de la vulnérabilité.

- *Pour consulter le rapport sur toutes les vulnérabilités détectées,*

dans le dossier **Vulnérabilités dans les applications**, utilisez le lien **Consulter le rapport sur les vulnérabilités dans les applications**.

Le rapport sur les vulnérabilités dans les applications installées sur les appareils sera créé. Le rapport peut être consulté dans le nœud portant le nom du Serveur d'administration dont vous avez besoin sous l'onglet Rapports.

La fonction d'obtention d'informations sur les vulnérabilités dans les applications est prise en charge uniquement pour les systèmes d'exploitation Microsoft Windows.

Recherche de vulnérabilités dans les applications

Si vous avez exécuté la configuration de l'application à l'aide de l'Assistant de configuration initiale, la tâche de recherche de vulnérabilités est créée automatiquement. Il est possible de consulter la tâche dans le dossier **Appareils administrés** sous l'onglet **Tâches**.

► *Pour créer une tâche de recherche de vulnérabilités dans les applications installées sur les appareils clients, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Vulnérabilités dans les applications**.
2. A l'aide du lien **Configurer la recherche de vulnérabilités** dans l'espace de travail, lancez l'Assistant de création de la tâche de recherche de vulnérabilités et de mises à jour requises.

La fenêtre de l'Assistant de création de la tâche s'ouvre.

3. Suivez les instructions de l'Assistant.

Suite au fonctionnement de l'Assistant, la tâche **Recherche de vulnérabilités et de mises à jour requises** est créée. Cette tâche s'affiche dans la liste des tâches dans le dossier **Appareils administrés** sous l'onglet **Tâches**.

À la suite de l'exécution de la tâche **Recherche de vulnérabilités et de mises à jour requises** sur le Serveur d'administration, apparaît la liste des vulnérabilités détectées dans le logiciel installé sur l'appareil, les mises à jour du logiciel requises appliquées aux appareils du réseau, par exemple, les nouvelles versions des applications.

L'agent d'administration reçoit les informations sur les mises à jour Windows disponibles et du logiciel du Centre de mises à jour Windows ou du Serveur d'administration, si le Serveur d'administration est utilisé comme serveur WSUS. Les informations sont transmises au moment du lancement des applications (si c'est configuré dans la stratégie) et du lancement périodique de la tâche **Synchronisation des mises à jour Windows Update** sur les appareils clients.

Vous pouvez recevoir des informations sur les logiciels d'éditeurs étrangers qu'il est possible de mettre à jour à l'aide de Kaspersky Security Center sur le site Internet du Support Technique, à la page Kaspersky Security Center, dans la section Administration du serveur (<http://support.kaspersky.com/fr/9327>).

Fermeture de vulnérabilités dans les applications

Si, dans l'Assistant de configuration initiale, dans la fenêtre **Paramètres d'administration des mises à jour**, vous avez sélectionné l'option **Rechercher et installer les mises à jour requises**, la tâche **Installation des mises à jour requises et correction des vulnérabilités** est créée automatiquement. La tâche s'affiche dans le dossier **Appareils administrés** sous l'onglet **Tâches**.

► *Pour créer une tâche de fermeture des vulnérabilités à l'aide des mises à jour disponibles pour les applications, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Appareils administrés** sous l'onglet **Tâches**.
2. Le lien **Créer une tâche** permet de lancer l'Assistant de création d'une tâche.
3. Dans la fenêtre de l'Assistant **Sélection du type de tâche**, indiquez le type de tâche **Installation des mises à jour requises et correction des vulnérabilités**.
4. Suivez les instructions de l'Assistant.

Suite au fonctionnement de l'Assistant, la tâche **Installation des mises à jour requises et correction des vulnérabilités** est créée. Cette tâche s'affiche dans le dossier **Tâches**.

► *Pour corriger la vulnérabilité sélectionnée à l'aide des mises à jour disponibles pour l'application, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Vulnérabilités dans les applications**.
2. Dans le dossier **Mises à jour du logiciel** cliquez sur le bouton **Lancer l'Assistant de correction de la vulnérabilité**.

L'Assistant de correction de la vulnérabilité s'ouvre.

La fonctionnalité de l'Assistant de correction de la vulnérabilité est accessible en présence d'une licence pour le fonctionnement de l'Administration système.

3. Suivez les instructions de l'Assistant.

Une fois l'Assistant terminé, la tâche **Installation des mises à jour requises et correction des vulnérabilités** est créée et s'affiche dans le dossier **Tâches**, ou la règle de correction de la vulnérabilité sera ajoutée à la tâche existante **Installation des mises à jour requises et correction des vulnérabilités**.

Mises à jour du logiciel

Kaspersky Security Center permet d'administrer les mises à jour du logiciel installé sur les appareils clients et de fermer les vulnérabilités dans les applications de Microsoft et d'autres éditeurs du logiciel à l'aide de l'installation des mises à jour nécessaires.

Kaspersky Security Center permet d'exécuter la recherche de mises à jour à l'aide de la tâche de recherche de mises à jour et télécharge les mises à jour dans le stockage des mises à jour. Après la fin de la recherche de mises à jour, l'application offre à l'administrateur les informations sur les mises à jour disponibles et sur les vulnérabilités dans les applications qui peuvent être fermées à l'aide de ces mises à jour.

Les informations sur les mises à jour Microsoft Windows disponibles sont transmises en provenance du centre des mises à jour Windows. Le Serveur d'administration peut être utilisé dans le rôle du serveur Windows Update (WSUS). Pour utiliser le Serveur d'administration dans le rôle du serveur Windows Update, il faut configurer la synchronisation des mises à jour avec le centre des mises à jour Windows. Après la configuration de la synchronisation des données avec le centre des mises à jour Windows, le Serveur d'administration, avec une fréquence définie, fournit les mises à jour aux services Windows Update sur les appareils.

Il est aussi possible d'administrer les mises à jour du logiciel à l'aide de la stratégie de l'Agent d'administration. Pour ce faire, il faut créer la stratégie de l'Agent d'administration et de configurer les paramètres des mises à jour du logiciel dans les fenêtres correspondantes de l'Assistant de création de la stratégie.

L'administrateur peut consulter la liste des mises à jour disponibles dans le dossier **Mises à jour du logiciel** qui fait partie du dossier **Administration des applications**. Ce dossier contient la liste des mises à jour obtenues par le Serveur d'administration des applications de Microsoft et d'autres éditeurs du logiciel qui peuvent être diffusées sur les appareils. Après la consultation des informations sur les mises à jour disponibles, l'administrateur peut exécuter l'installation des mises à jour sur les appareils.

La mise à jour de certaines applications Kaspersky Security Center s'effectue par la suppression de la version précédente de l'application et par l'installation d'une nouvelle version.

Avant l'installation des mises à jour sur tous les appareils, il est possible d'exécuter l'installation de contrôle pour s'assurer que les mises à jour installées ne provoquent pas d'échecs dans le fonctionnement des applications sur les appareils.

Vous pouvez recevoir des informations sur les logiciels d'éditeurs étrangers qu'il est possible de mettre à jour à l'aide de Kaspersky Security Center sur le site Internet du Support Technique, à la page Kaspersky Security Center, dans la section Administration du serveur (<http://support.kaspersky.com/fr/9327>).

Dans cette section

Consultation des informations sur les mises à jour disponibles.....	238
Synchronisation des mises à jour Windows Update avec le Serveur d'administration	238
Installation automatique des mises à jour pour Kaspersky Endpoint Security sur les appareils.....	239
Modèle hors ligne d'obtention des mises à jour	242
Activation et désactivation d'un modèle hors ligne d'obtention des mises à jour	245
Installation manuelle des mises à jour sur les appareils	246
Configuration des mises à jour Windows dans la stratégie de l'Agent d'administration	249

Consultation des informations sur les mises à jour disponibles

- *Pour consulter la liste des mises à jour disponibles pour les applications installées sur les appareils clients,*

dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Mises à jour du logiciel**.

Dans l'espace de travail du dossier, vous pouvez consulter la liste des mises à jour existantes pour les applications installées sur les appareils.

- *Pour consulter les propriétés de la mise à jour,*

dans l'espace de travail du dossier **Mises à jour du logiciel** dans le menu contextuel de la mise à jour, sélectionnez l'option **Propriétés**.

Les informations suivantes sont accessibles à la consultation dans la fenêtre des propriétés de la mise à jour :

- la liste des appareils clients pour lesquels la mise à jour est applicable (*appareils ciblés*) ;
- la liste des modules système général (préaccessoires) qui doivent être installés avec l'installation de la mise à jour (si de tels modules existent) ;
- les vulnérabilités dans les applications que cette mise à jour ferme.

Synchronisation des mises à jour Windows Update avec le Serveur d'administration

Si dans l'Assistant de configuration initiale dans la fenêtre **Paramètres d'administration des mises à jour**, vous avez sélectionné l'option **Utiliser le Serveur d'administration dans le rôle du serveur WSUS**, la tâche de synchronisation des mises à jour Windows Update est automatiquement créée. Il est possible de lancer la tâche dans le dossier **Tâches**. La fonctionnalité de mise à jour du logiciel Microsoft est disponible uniquement après une réussite de l'exécution de la tâche **Synchronisation des mises à jour Windows Update**.

► *Pour créer la tâche de synchronisation des mises à jour Windows Update avec le Serveur d'administration, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Mises à jour du logiciel**.
2. Cliquez sur le bouton **Actions supplémentaires** et dans le menu déroulant, choisissez l'option **Configurer la synchronisation des mises à jour Windows Update**.

Cette action lance l'Assistant de création d'une tâche d'obtention des données depuis le centre des mises à jour Windows.

3. Suivez les instructions de l'Assistant.

Suite au fonctionnement de l'Assistant, la tâche **Synchronisation des mises à jour Windows Update** est créée. Cette tâche s'affiche dans le dossier **Tâches**.

La tâche de synchronisation des mises à jour Windows Update peut être aussi créée dans le dossier **Tâches** avec le bouton **Créer une tâche**.

La tâche **Synchronisation des mises à jour Windows Update** télécharge sur les serveurs Microsoft seulement les métadonnées. Si le réseau n'utilise pas de serveur WSUS, chaque appareil client télécharge indépendamment les mises à jour Microsoft sur des serveurs externes.

Installation automatique des mises à jour pour Kaspersky Endpoint Security sur les appareils

Vous pouvez configurer automatiquement la mise à jour des bases et des modules de l'application Kaspersky Endpoint Security sur les appareils clients.

► *Pour configurer le téléchargement et l'installation automatique des mises à jour de Kaspersky Endpoint Security sur les appareils, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Créez une tâche de type **Mise à jour** selon l'un des procédés suivants :
 - Dans le menu contextuel du dossier de l'arborescence de la console **Tâches**, sélectionnez l'option **Créer** → **Tâche**.
 - Dans l'espace de travail du dossier **Tâches**, cliquez sur le bouton **Créer une tâche**.

Ceci permet de lancer l'Assistant de création de tâche.

3. Dans la fenêtre de l'assistant **Sélection du type de tâche**, sélectionnez le type de tâche **Kaspersky Endpoint Security**, puis le sous-type de tâche **Mise à jour** et cliquez sur le bouton **Suivant**.
4. Suivez les étapes ultérieures de l'assistant.

Suite à l'exécution de l'assistant, une tâche de mise à jour est créée pour Kaspersky Endpoint Security. La tâche créée est affichée dans la liste de tâches de l'espace de travail du dossier **Tâches**.

5. Sélectionnez la tâche de mise à jour créée dans l'espace de travail du dossier **Tâches**.
6. Dans le menu contextuel de la tâche, sélectionnez l'option **Propriétés**.
7. Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Paramètres**.

La section **Paramètres** permet de configurer les paramètres de la tâche de mise à jour en mode local ou déconnecté :

- **Paramètres de mise à jour en mode local** : la communication est établie entre l'appareil et le Serveur d'administration.
- **Paramètres de mise à jour en mode déconnecté** : la communication n'est pas établie entre l'appareil et Kaspersky Security Center (par exemple, si l'appareil n'est pas connecté à Internet).

8. Cliquez sur le bouton **Configuration** pour sélectionner la source de mises à jour.
9. Cochez la case **Télécharger les mises à jour des modules** pour télécharger et installer simultanément les mises à jour des modules de l'application avec les bases de l'application.

Si la case est cochée, Kaspersky Endpoint Security notifie l'utilisateur sur la présence de mises à jour disponibles pour les modules de l'application. En outre, au cours de l'exécution de la tâche, Kaspersky Endpoint Security inclut les mises à jour de l'application au paquet de mises à jour. Configurez l'application des modules de mises à jour :

- **Installer les mises à jour critiques et approuvées.** En présence de mises à jour de modules de l'application, Kaspersky Endpoint Security installe automatiquement celles avec l'état *Critique* et les autres mises à jour de modules de l'application après l'approbation de leur installation par l'administrateur.

Pour approuver les mises à jour du logiciel, procédez comme suit :

- a. Ouvrez le dossier **Mises à jour du logiciel** dans l'arborescence de la console.
- b. Dans la fenêtre de propriétés de la mise à jour, dans la section **Général**, dans le champ **Approbation de la mise à jour**, cochez la valeur **Approuvée**.

Par défaut, la valeur **Non défini** est cochée.

Si lors de la configuration des propriétés de la mise à jour pour les applications Kaspersky Lab impossibles à désinstaller, dans le champ **Approbation de la mise à jour**, vous indiquez la valeur **Rejetée**, Kaspersky Security Center ne désinstallera pas cette mise à jour des appareils sur lesquels elle était auparavant installée.

L'impossibilité de supprimer la mise à jour pour les applications Kaspersky Lab s'affiche dans la fenêtre des propriétés de la mise à jour sous l'onglet **Général** dans le champ **Exigence lors de l'installation**.

- **Installer uniquement les mises à jour confirmées.** Si des mises à jours des modules de l'application sont disponibles, Kaspersky Endpoint Security les installe après approbation, en local via l'interface de l'application ou du côté de Kaspersky Security Center.

Si la mise à jour des modules implique de consulter et d'accepter les conditions du Contrat de licence, l'application installe la mise à jour après que l'utilisateur a accepté ces conditions.

10. Cochez la case **Copier les mises à jour dans un dossier** pour que l'application enregistre les mises à jour téléchargées dans un dossier indiqué à l'aide du bouton **Parcourir**.

11. Cliquez sur le bouton **OK**.

Lors de l'exécution de la tâche **Mise à jour**, l'application envoie des requêtes aux serveurs de mise à jour de Kaspersky Lab.

Certaines mises à jour requièrent l'installation des dernières versions des plug-ins des applications administrées.

Modèle hors ligne d'obtention des mises à jour

Les Agents d'administration sur les appareils administrés ne peuvent pas toujours se connecter au Serveur d'administration pour la réception des mises à jour. Par exemple, l'Agent d'administration peut être installé sur un ordinateur portable qui, parfois, n'est pas connecté à Internet et au réseau local. L'administrateur peut également limiter la durée de connexion des appareils au réseau. Dans ces cas, les Agents d'administration ne peuvent pas recevoir les mises à jour provenant du Serveur d'administration conformément à l'emploi du temps. Si la mise à jour des applications administrées est configurée (par exemple, Kaspersky Endpoint Security) à l'aide de l'Agent d'administration, la mise à jour nécessite une connexion au Serveur d'administration. Lorsque l'Agent d'administration et le Serveur d'administration ne sont pas connectés, la mise à jour est impossible. La connexion de l'Agent d'administration au serveur peut être configurée de manière à s'effectuer seulement dans un délai défini. Au pire des cas, si les périodes de connexion configurées sont dépassées, lorsque la connexion est absente, les bases ne sont jamais mises à jour. Dans certaines situations, également, de nombreuses applications administrées s'adressent simultanément au Serveur d'administration pour des mises à jour. Dans ce cas, le Serveur d'administration peut arrêter de répondre aux requêtes (comme pendant une attaque DDOS).

Pour éviter les problèmes décrits, Kaspersky Security Center prévoit un modèle hors ligne d'obtention de la mise à jour des bases de données et des modules des applications administrées. Ce modèle assure la fiabilité du mécanisme de diffusion des mises à jour quels que soient les problèmes temporaires d'indisponibilité des canaux de communication du Serveur d'administration et réduit la charge sur le Serveur d'administration.

Fonctionnement du modèle hors ligne d'obtention des mises à jour

Chaque fois que le Serveur d'administration reçoit les mises à jour, il indique aux Agents d'administration les mises à jour exigées par les applications administrées. Lorsque les Agents d'administration savent quelles mises à jour nécessiteront bientôt les applications administrées, ils téléchargent de manière anticipée les fichiers nécessaires à partir du Serveur d'administration. Lors de la première connexion à l'Agent d'administration, le serveur initialise le téléchargement des mises à jour par cet agent. Pour répartir le téléchargement sur le Serveur d'administration, les Agents d'administration commencent à se connecter au serveur et à télécharger les mises à jour de manière aléatoire au cours du délai défini par le serveur. Ce délai dépend du nombre d'Agents d'administration qui téléchargent les mises à jour et de la taille de celles-ci. Une fois que l'Agent d'administration sur l'appareil a téléchargé toutes les mises à jour, celles-ci deviennent accessibles aux applications situées sur ce même appareil.

Pour réduire la surcharge sur le Serveur d'administration, vous pouvez utiliser les Agents d'administration comme agents de mises à jour.

Lorsque l'application administrée sur l'appareil s'adresse à l'Agent d'administration pour obtenir des mises à jour, l'Agent vérifie s'il a les mises à jour nécessaires. Si des mises à jour ont été reçues du Serveur d'administration au plus tôt 25 heures après la requête de l'application administrée, l'Agent d'administration ne se connecte pas au Serveur d'administration et fournit à l'application administrée des mises à jour du cache local. La connexion au Serveur d'administration peut alors être absente mais n'est pas obligatoire pour la mise à jour. Dans le cas contraire, l'installation de mises à jour s'effectue en mode ordinaire, conformément à la programmation de tâche d'obtention de mises à jour.

Par défaut, le modèle hors ligne d'obtention de mises à jour est activé. Le modèle hors ligne de récupération des mises à jour intervient uniquement pour les appareils administrés pour lesquels la planification de la tâche de récupération des mises à jour par les applications administrées possède la valeur "A la fin de la tâche serveur de récupération des mises à jour". Pour les autres appareils administrés, la récupération des mises à jour s'opère via le système traditionnel en temps réel de récupération depuis le Serveur d'administration.

Il est recommandé de désactiver le modèle hors ligne de récupération des mises à jour via les paramètres des stratégies de l'Agent d'administration des groupes d'administration correspondant si dans les applications administrées, la récupération des mises à jour est configurée pour avoir lieu non pas depuis le Serveur d'administration, mais depuis les serveurs de Kaspersky Lab ou depuis un dossier réseau et la planification de cette tâche a la valeur "A la fin de la tâche serveur de récupération des mises à jour".

Avantages et défauts du modèle hors ligne d'obtention des mises à jour

Le modèle hors ligne d'obtention des mises à jour comporte les avantages suivants :

- Kaspersky Security Center peut définir en toute indépendance quand télécharger les mises à jour en évitant ainsi les erreurs dans les mises à jour des applications administrées. Les applications bénéficieront toujours d'un accès sécurisé aux dernières mises à jour qui peuvent être téléchargées à partir du Serveur d'administration.
- Celui-ci peut contrôler le téléchargement lors de la diffusion des mises à jour.

Le modèle hors ligne d'obtention des mises à jour comporte les défauts suivants :

- Le trafic réseau entre le Serveur d'administration et l'Agent d'administration peut être accru, car dans le modèle hors ligne, les mises à jour sont diffusées sur les Agents d'administration chaque fois que le Serveur d'administration en obtient de nouvelles. En mode normal, les mises à jour sont diffusées selon la programmation des tâches de mise à jour.
- Le Serveur d'administration risque de subir une charge supplémentaire car il définit les mises à jour nécessaires pour chaque appareil administré.

Recommandations sur l'utilisation du modèle hors ligne de mises à jour

- Il y a toujours un délai entre le moment où le Serveur d'administration obtient les nouvelles mises à jour des applications et le moment où l'Agent d'administration télécharge les mises à jour à partir du Serveur d'administration. Si la tâche de mise à jour commence pendant cet intervalle de temps, les appareils administrés obtiennent les anciennes mises à jour des bases de données à partir de l'Agent d'administration.

Il est recommandé de définir la programmation de la tâche de mise à jour pour qu'elle démarre une fois que le Serveur d'administration a obtenu les mises à jour. Dans ce cas, Kaspersky Security Center effectue la tâche de mise à jour et les applications obtiennent les mises à jour le plus tôt possible.

- Si la tâche de téléchargement des mises à jour est lancée trop fréquemment, l'Agent d'administration risque de ne pas disposer d'un délai suffisant pour les télécharger toutes avant le prochain lancement de la tâche.

Il est recommandé d'augmenter l'intervalle entre les lancements de la tâche de téléchargement des mises à jour dans le stockage.

Activation et désactivation d'un modèle hors ligne d'obtention des mises à jour

► *Pour activer ou désactiver le modèle de récupération hors ligne des mises à jour pour le groupe d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut activer le modèle de récupération hors ligne des mises à jour.
2. Dans l'espace de travail du groupe, ouvrez l'onglet **Stratégies**.
3. Dans l'onglet **Stratégies**, choisissez la stratégie de l'Agent d'administration.
4. Dans le menu contextuel de la stratégie, choisissez l'option **Propriétés**.

La fenêtre des propriétés de la stratégie de l'Agent d'administration s'ouvre.

5. Sélectionnez la section **Administration des correctifs et des mises à jour** dans la fenêtre des propriétés de la stratégie.
6. Cochez ou décochez la case **Télécharger au préalable les mises à jour et les bases antivirus depuis le Serveur d'administration** pour activer ou désactiver le modèle de récupération hors ligne des mises à jour.

Par défaut, le modèle hors ligne d'obtention de mises à jour est activé.

Suite à cette action, le modèle de récupération hors ligne des mises à jour est activé ou désactivé.

► Pour insérer ou désactiver modèle de récupération hors ligne des mises à jour simultanément pour tous les groupes d'administration, procédez comme suit :

1. Ouvrez le registre système de l'appareil sur lequel le Serveur d'administration est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.
2. Rendez-vous dans la section :

- Pour un système de 64 bits :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34  
\1093\1.0.0.0\ServerFlags
```

- Pour un système de 32 bits :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Components\34\1093\1.0.0.0\ServerFlags
```

3. Pour la clé SrvDisableOfflineUpdates (DWORD), définissez une des valeurs : 0 – pour activer le modèle de récupération hors ligne des mises à jour ; 1 – pour désactiver le modèle de récupération hors ligne des mises à jour.

Par défaut, la valeur 0 est indiquée pour cette clé (le modèle hors ligne d'obtention des mises à jour est activé).

4. Relancez le service du Serveur d'administration.

Suite à cette action, le modèle de récupération hors ligne des mises à jour sera désactivé pour tous les groupes d'administration.

Installation manuelle des mises à jour sur les appareils

Si, dans l'Assistant de configuration initiale, dans la fenêtre **Paramètres d'administration des mises à jour**, vous avez sélectionné l'option **Rechercher et installer les mises à jour requises**, la tâche **Installation des mises à jour requises et correction des vulnérabilités** est créée automatiquement. Il est possible d'arrêter ou de lancer la tâche dans le dossier **Appareils administrés** sous l'onglet **Tâches**.

Si dans l'Assistant de configuration initiale vous avez sélectionné l'option **Rechercher les mises à jour requises pour l'installation**, vous pouvez installer les mises à jour du logiciel sur les appareils clients à l'aide de la tâche **Installation des mises à jour requises et correction des vulnérabilités**.

► *Pour créer une nouvelle tâche d'installation des mises à jour, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Mises à jour du logiciel**.
2. Dans le dossier **Mises à jour du logiciel**, ouvrez le menu contextuel de la mise à jour et sélectionnez l'option **Installer la mise à jour** → Nouvelle tâche ou utilisez le lien **Installer la mise à jour (créer la tâche)** dans le groupe de fonctionnement avec les mises à jour sélectionnées.

L'Assistant de création de la tâche d'installation des mises à jour et de correction des vulnérabilités s'ouvre.

3. Suivez les instructions de l'Assistant.

Suite au fonctionnement de l'Assistant, la tâche **Installation des mises à jour requises et correction des vulnérabilités** est créée. Cette tâche s'affiche dans le dossier **Tâches**.

Dans les paramètres de la tâche d'installation des mises à jour et de correction des vulnérabilités, vous pouvez autoriser l'installation automatique des modules du système général (prérequis) qui doivent être installés avant l'installation des mises à jour. Dans ce cas, avant l'installation d'une mise à jour, une installation de tous les modules système général sera exécutée. La liste de ces modules est à consulter dans les propriétés de la mise à jour.

Dans les paramètres de la tâche d'installation des mises à jour et de correction des vulnérabilités, vous pouvez autoriser l'installation des mises à jour, suites auxquelles une nouvelle version de l'application sera installée.

Si dans les paramètres de la tâche, sont configurées les règles d'installation des mises à jour d'éditeurs étrangers, le Serveur d'administration télécharge sur le site des éditeurs les mises à jour requises. Les mises à jour sont conservées dans le stockage du Serveur d'administration et ensuite sont diffusées et sont installées sur les appareils où elles sont appliquées.

Si dans les paramètres de la tâche sont configurées les règles d'installation des mises à jour Microsoft et que le Serveur d'administration est utilisé comme serveur WSUS, le Serveur d'administration télécharge les mises à jour requises dans le stockage et les diffuse ensuite aux appareils administrés. Si le réseau n'utilise pas de serveur WSU, chaque appareil de client télécharge indépendamment les mises à jour Microsoft sur les serveurs externes.

► *Pour créer une tâche d'installation d'une mise à jour sélectionnée, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Mises à jour du logiciel**.
2. Dans le dossier **Mises à jour du logiciel**, cliquez sur le bouton **Lancer l'Assistant d'installation de la mise à jour**.

L'Assistant d'installation de la mise à jour s'ouvre.

La fonctionnalité de l'Assistant d'installation des mises à jour est accessible en présence d'une licence pour le fonctionnement de l'Administration système.

3. Suivez les instructions de l'Assistant.

Une fois l'Assistant terminé, la tâche **Installation des mises à jour requises et correction des vulnérabilités** est créée et s'affiche dans le dossier **Tâches**, ou une nouvelle règle d'installation de la mise à jour sera ajoutée à la tâche existante **Installation des mises à jour requises et correction des vulnérabilités**.

Après l'installation de la nouvelle version de l'application, le fonctionnement d'autres applications, installées sur les appareils et qui dépendent du fonctionnement de l'application installée, peut être troublé.

Dans les paramètres de la tâche d'installation des mises à jour, vous pouvez configurer l'installation de contrôle des mises à jour.

► *Pour configurer l'installation de contrôle des mises à jour, procédez comme suit :*

1. Dans l'arborescence de la console dans le dossier **Appareils administrés** sous l'onglet **Tâches**, sélectionnez la tâche **Installation des mises à jour requises et correction des vulnérabilités**.

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

La fenêtre des propriétés de la tâche **Installation des mises à jour requises et correction des vulnérabilités** s'ouvre.

3. Dans la fenêtre des propriétés de la tâche dans la section **Installation de contrôle**, sélectionnez une des options disponibles de l'installation de contrôle :

- **Ne pas analyser**. Sélectionnez cette option si vous ne voulez pas exécuter l'installation de contrôle des mises à jour.
- **Exécuter l'analyse sur les appareils indiqués**. Sélectionnez cette option si vous voulez vérifier l'installation des mises à jour sur certains appareils. Cliquez sur le bouton **Ajouter** et sélectionnez les appareils qui requièrent l'exécution de l'installation de contrôle des mises à jour.
- **Exécuter l'analyse sur les appareils dans le groupe indiqué**. Sélectionnez cette option si vous voulez vérifier l'installation des mises à jour sur le groupe d'appareils. Dans le champ **Définissez le groupe test**, indiquez le groupe d'appareils à exécuter l'installation de contrôle.
- **Exécuter l'analyse sur le pourcentage indiqué des appareils**. Sélectionnez cette option si vous voulez lancer l'analyse des mises à jour sur une partie des appareils. Dans le champ **Le pourcentage des appareils test du nombre total des appareils ciblés**, indiquez le pourcentage des appareils qui requièrent l'exécution de l'installation de contrôle des mises à jour.

4. Lors de la sélection de toutes les options sauf la première dans le champ **Temps pour prendre la décision sur la suite d'installation**, indiquez le nombre d'heures à passer après l'installation de contrôle des mises à jour avant le début d'installation des mises à jour sur tous les appareils.

Configuration des mises à jour Windows dans la stratégie de l'Agent d'administration

► Pour configurer les mises à jour Windows dans la stratégie de l'Agent d'administration, procédez comme suit :

1. Dans le dossier **Appareils administrés** sous l'onglet **Stratégies**, sélectionnez la stratégie de l'Agent d'administration.
2. Dans le menu contextuel de la stratégie, choisissez l'option **Propriétés**.
La fenêtre des propriétés de la stratégie de l'Agent d'administration s'ouvre.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez la section **Mises à jour et vulnérabilités dans les applications**.
4. Cochez la case **Utiliser le Serveur d'administration dans le rôle du serveur WSUS** pour télécharger les mises à jour Windows sur le Serveur d'administration puis les diffuser sur les appareils clients à l'aide des Agents d'administration.

Si la case est décochée, les mises à jour Windows ne sont pas téléchargées sur le Serveur d'administration. Le cas échéant, les appareils clients reçoivent les mises à jour Windows de manière autonome.

5. Sélectionnez le mode de recherche des mises à jour Windows Update :
 - **Actif**. Le Serveur d'administration initie la demande de l'agent de mises à jour Windows sur l'appareil client à la source de mises à jour : Windows Update Servers ou WSUS. Ensuite, l'Agent d'administration transmet sur le Serveur d'administration les informations obtenues en provenance de l'agent de mises à jour Windows.
 - **Passif**. Dans ce mode, l'Agent d'administration transmet périodiquement sur le Serveur d'administration les informations sur les mises à jour obtenues lors de la dernière synchronisation de l'agent de mises à jour Windows avec la source des mises à jour. Si la synchronisation de l'agent de mises à jour Windows avec la source des mises à jour n'est pas exécutée, les données sur les mises à jour sur le Serveur d'administration deviennent obsolètes.
 - **Inactif**. Le Serveur d'administration ne reçoit pas les informations sur les mises à jour.
6. Cliquez sur le bouton **Appliquer**.

Installation à distance des systèmes d'exploitation et des applications

Kaspersky Security Center permet de créer les images des systèmes d'exploitation et de les déployer sur les appareils clients par le réseau, ainsi que d'exécuter l'installation à distance des applications de Kaspersky Lab et d'autres éditeurs du logiciel.

Prise des images des systèmes d'exploitation

Kaspersky Security Center permet d'exécuter la prise des images des systèmes d'exploitation des appareils et de livrer ces images sur le Serveur d'administration. Finalement, les images reçues des systèmes d'exploitation sont conservées sur le Serveur d'administration dans le dossier partagé. La prise et la création de l'image du système d'exploitation de l'appareil d'étalon est exécutée à l'aide de la tâche de création du paquet d'installation (cf. section "Création des paquets d'installation des applications" à la page [260](#)).

Pour créer les images du système d'exploitation, le paquet d'outils Windows Automated Installation Kit (WAIK) doit être installé sur le Serveur d'administration.

La fonctionnalité de prise de l'image du système d'exploitation a des particularités suivantes :

- Il est interdit de prendre l'image du système d'exploitation de l'appareil sur lequel le Serveur d'administration est installé.
- Pendant la prise de l'image du système d'exploitation, la remise à zéro des paramètres de l'appareil d'étalon se passe par l'utilitaire sysprep.exe. En cas de nécessité de restaurer les paramètres de l'appareil d'étalon, il faut cocher la case **Conserver la copie de sauvegarde de l'état de l'appareil** dans l'Assistant de création de l'image du système d'exploitation.
- Durant la prise de l'image, le redémarrage de l'appareil d'étalon est exécuté.

Déploiement des images des systèmes d'exploitation sur les nouveaux appareils

L'administrateur peut utiliser les images reçues pour le déploiement sur les nouveaux appareils dans le réseau sur lesquels le système d'exploitation n'a pas encore été installé. Pour ce but, la

technologie Preboot eXecution Environment (PXE) est utilisée. L'administrateur désigne l'appareil dans le réseau qui sera utilisé en tant que serveur PXE. Cet appareil doit répondre aux exigences suivantes :

- L'Agent d'administration doit être installé sur l'appareil.
- Le serveur DHCP ne doit pas fonctionner sur l'appareil parce que le serveurs PXE utilise les mêmes ports que DHCP.
- Le segment du réseau qui fait partie de l'appareil ne doit pas avoir d'autres serveurs PXE.

Pour déployer le système d'exploitation, il faut que l'appareil possède la carte réseau, l'ordinateur soit connecté au réseau, et l'option d'installation Network boot soit sélectionnée pendant le démarrage de l'appareil dans l'environnement BIOS.

Le déploiement du système d'exploitation est exécuté dans la séquence suivante :

1. Le serveur PXE établit la connexion avec le nouvel l'appareil client lors du démarrage de l'appareil client.
2. L'appareil client est inclus dans l'environnement Windows Preinstallation Environment (WinPE).

Pour inclure l'appareil dans l'environnement WinPE, la configuration de la composition des pilotes pour l'environnement WinPE peut être requise.

3. L'appareil client est enregistré sur le Serveur d'administration.
4. L'administrateur désigne à l'appareil client le paquet d'installation avec l'image du système d'exploitation.

L'administrateur peut ajouter les pilotes nécessaires dans le paquet d'installation avec l'image du système d'exploitation et indiquer les fichiers de configuration avec les paramètres du système d'exploitation (le fichier des réponses) qui doivent être appliqués pendant l'installation.

5. Le déploiement du système d'exploitation est exécuté sur l'appareil client.

L'administrateur peut manuellement indiquer les adresses MAC des appareils clients non connectés et désigner à ceux-ci le paquet d'installation avec l'image du système d'exploitation. Quand les appareils clients indiqués se connectent au serveur PXE, l'installation du système d'exploitation est automatiquement exécutée sur ces appareils.

Déploiement des images des systèmes d'exploitation sur les appareils avec le système d'exploitation déjà installé

Le déploiement des images du système d'exploitation sur les appareils clients qui possèdent déjà le système d'exploitation de travail est exécuté à l'aide de la tâche d'installation à distance pour les ensembles d'appareils.

Installation des applications de Kaspersky Lab et d'autres éditeurs du logiciel

L'administrateur peut créer les paquets d'installation de toutes les applications, y compris les applications indiquées par l'utilisateur, et installer ces applications sur les appareils clients à l'aide de la tâche d'installation à distance.

Dans cette section

Création des images des systèmes d'exploitation	254
Ajout des pilotes pour l'environnement de préinstallation Windows (WinPE)	254
Ajout des pilotes dans le paquet d'installation avec l'image du système d'exploitation	255
Configuration des paramètres de l'utilitaire sysprep.exe.....	256
Déploiement des systèmes d'exploitation sur les nouveaux appareils dans le réseau	257
Déploiement des systèmes d'exploitation sur les appareils clients.....	259
Création des paquets d'installation des applications	260
Établissement d'un certificat pour les paquets d'installation des applications	261
Installation des applications sur les appareils clients.....	262

Création des images des systèmes d'exploitation

La création des images des systèmes d'exploitation est exécutée à l'aide de la tâche de prise d'image du système d'exploitation de l'appareil d'étalon.

► *Pour créer la tâche de prise d'image du système d'exploitation, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
2. Avec le bouton **Créer un paquet d'installation**, lancez l'Assistant de création du paquet d'installation.
3. Dans la fenêtre de l'Assistant **Sélection du type de paquet d'installation**, cliquez sur le bouton **Créer le paquet d'installation avec l'image du S.E.**
4. Suivez les instructions de l'Assistant.

Suite au fonctionnement de l'Assistant, la tâche du Serveur d'administration **Prise de l'image du S.E. à partir de l'appareil d'étalon** est créée. Il est possible de consulter la tâche dans le dossier **Tâches**.

Suite à l'exécution de la tâche **Prise de l'image du S.E. à partir de l'appareil d'étalon**, le paquet d'installation est créé. Ce paquet peut être utilisé pour déployer le système d'exploitation sur les appareils clients à l'aide du serveur PXE ou à l'aide de la tâche d'installation à distance. Il est possible de consulter le paquet d'installation dans le dossier **Paquets d'installation**.

Ajout des pilotes pour l'environnement de préinstallation Windows (WinPE)

► Pour ajouter les pilotes pour l'environnement WinPE, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Installation à distance**, sélectionnez le dossier joint **Déploiement des images des appareils**.
2. Dans l'espace de travail du dossier **Déploiement des images des appareils**, cliquez sur le bouton **Actions supplémentaires** et dans le menu déroulant, choisissez l'option **Configurer la synchronisation des mises à jour Windows Update**.

La fenêtre **Pilotes pour l'environnement de préinstallation Windows** s'ouvre.

3. Dans la fenêtre **Pilotes pour l'environnement de préinstallation Windows**, cliquez sur le bouton **Ajouter**.

La fenêtre **Ajout du pilote** s'ouvre.

4. Dans la fenêtre **Ajout du pilote**, indiquez le nom du pilote et le chemin d'accès au paquet d'installation du pilote. Le chemin d'accès au paquet d'installation peut être indiqué lorsque vous cliquez sur le bouton **Sélectionner** dans la fenêtre **Ajout du pilote**.
5. Cliquez sur le bouton **OK**.

Le pilote sera ajouté dans le stockage du Serveur d'administration. Le pilote ajouté dans le stockage s'affiche dans la fenêtre **Sélection du pilote**.

6. Cliquez sur le bouton **OK** dans la fenêtre **Sélection du pilote**.

Le pilote sera ajouté dans l'environnement de préinstallation Windows (WinPE).

Ajout des pilotes dans le paquet d'installation avec l'image du système d'exploitation

► Pour ajouter des pilotes dans le paquet d'installation avec l'image du système d'exploitation, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
2. Dans le menu contextuel du paquet d'installation avec l'image du système d'exploitation, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés du paquet d'installation s'ouvre.

3. Dans la fenêtre des propriétés du paquet d'installation, sélectionnez la section **Pilotes complémentaires**.
4. Dans la section **Pilotes complémentaires**, cliquez sur le bouton **Ajouter**.

La fenêtre **Sélection du pilote** s'ouvre.

5. Dans la fenêtre **Sélection du pilote**, sélectionnez les pilotes que vous voulez ajouter dans le paquet d'installation avec l'image du système d'exploitation.

Les nouveaux pilotes peuvent être ajoutés dans le stockage du Serveur d'administration, en cliquant sur le bouton **Ajouter** dans la fenêtre **Sélection du pilote**.

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

Les pilotes ajoutés s'affichent dans la section **Pilotes complémentaires** dans la fenêtre des propriétés du paquet d'installation avec l'image du système d'exploitation.

Configuration des paramètres de l'utilitaire sysprep.exe

L'utilitaire sysprep.exe est utilisé pour préparer l'appareil à la création de l'image du système d'exploitation de celui-ci.

► *Pour configurer la requête de l'utilitaire sysprep.exe, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
2. Dans le menu contextuel du paquet d'installation avec l'image du système d'exploitation, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés du paquet d'installation s'ouvre.

3. Dans la fenêtre des propriétés du paquet d'installation, sélectionnez la section **Paramètres de sysprep.exe**.
4. Dans la section **Paramètres de sysprep.exe**, indiquez le fichier de configuration qui sera utilisé lors du déploiement du système d'exploitation sur l'appareil client :
 - **Utiliser le fichier de configuration par défaut.** Sélectionnez cette option pour utiliser le fichier-réponse créé par défaut pendant la prise de l'image du système d'exploitation.
 - **Définir les valeurs d'utilisateur des paramètres principaux.** Sélectionnez cette option pour définir les valeurs des paramètres à l'aide de l'interface d'utilisateur.
 - **Définir le fichier de configuration.** Sélectionnez cette option pour utiliser votre propre fichier-réponse.
5. Cliquez sur le bouton **Appliquer** pour que les modifications apportées entrent en vigueur.

Déploiement des systèmes d'exploitation sur les nouveaux appareils dans le réseau

► *Pour déployer le système d'exploitation sur les nouveaux appareils qui ne possèdent pas encore de système d'exploitation, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Installation à distance**, sélectionnez le dossier joint **Déploiement des images des appareils**.
2. Cliquez sur le bouton **Actions supplémentaires** et dans le menu déroulant, choisissez l'option **Administrer la liste des serveurs PXE sur le réseau**.

Le lien ouvre la fenêtre **Propriétés : Déploiement des images des appareils** dans la section **Serveurs PXE**.

3. Dans la section **Serveurs PXE**, cliquez sur le bouton **Ajouter** et dans la fenêtre ouverte **Serveurs PXE**, sélectionnez l'appareil qui sera utilisé en tant que serveur PXE.

L'appareil ajouté s'affichera dans la section **Serveurs PXE**.

4. Dans la section **Serveurs PXE** sélectionnez le serveur PXE et cliquez sur le bouton **Propriétés**.
5. Dans la fenêtre des propriétés du serveur PXE sélectionné dans la section **Paramètres de connexion au serveur PXE**, exécutez la configuration des paramètres de connexion du Serveur d'administration au serveur PXE.
6. Exécutez le démarrage de l'appareil client sur lequel vous voulez déployer le système d'exploitation.
7. Dans l'environnement BIOS de l'appareil client, sélectionnez l'option d'installation Network boot.

L'appareil client se connecte au serveur PXE et s'affiche dans l'espace de travail du dossier **Déploiement des images des appareils**.

8. Dans le groupe **Actions** à l'aide du lien **Désigner le paquet d'installation**, sélectionnez le paquet d'installation qui sera utilisé pour installer le système d'exploitation sur l'appareil sélectionné.

Après l'ajout de l'appareil et la désignation du paquet d'installation pour celui-ci, le déploiement du système d'exploitation sur cet appareil commence automatiquement.

9. Pour annuler le déploiement du système d'exploitation sur l'appareil client, utilisez le lien **Annuler l'installation des images du S.E** dans le groupe **Actions**.

► *Pour ajouter les appareils par l'adresse MAC,*

- à l'aide du lien **Ajouter l'adresse MAC de l'appareil ciblé** dans le dossier **Déploiement des images des appareils**, ouvrez la fenêtre **Nouvel appareil** et indiquez l'adresse MAC de l'appareil que vous voulez ajouter ;
- à l'aide du lien **Importer les adresses MAC des appareils ciblés à partir d'un fichier** dans le dossier **Déploiement des images des appareils**, sélectionnez le fichier qui contient la liste des adresses MAC de tous les appareils sur lesquels vous voulez déployer le système d'exploitation.

Déploiement des systèmes d'exploitation sur les appareils clients

► *Pour exécuter le déploiement du système d'exploitation sur les appareils clients avec le système d'exploitation déjà installé, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, cliquez sur le lien **Déployer le paquet d'installation sur les appareils administrés (postes de travail)** pour lancer l'Assistant du déploiement de la protection.
2. Dans la fenêtre de l'Assistant **Sélection du paquet d'installation**, indiquez le paquet d'installation avec l'image du système d'exploitation.
3. Suivez les instructions de l'Assistant.

Suite au fonctionnement de l'Assistant, la tâche d'installation à distance du système d'exploitation sur les appareils clients est créée. Il est possible de lancer ou d'arrêter la tâche dans le dossier **Tâches**.

Création des paquets d'installation des applications

► Afin de créer le paquet d'installation de l'application, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
2. Avec le bouton **Créer un paquet d'installation**, lancez l'Assistant de création du paquet d'installation.
3. Dans la fenêtre de l'Assistant **Sélection du type de paquet d'installation**, cliquez sur un des boutons :
 - **Générer un paquet d'installation pour l'application de Kaspersky Lab.**
Sélectionnez cette option si vous voulez créer le paquet d'installation pour l'application de Kaspersky Lab.
 - **Générer un paquet d'installation pour l'application indiquée par l'utilisateur.**
Sélectionnez cette option si vous voulez créer le paquet d'installation pour l'application demandée par l'utilisateur.
 - **Créer le paquet d'installation avec l'image du S.E. de l'appareil d'étalon.**
Sélectionnez cette option si vous voulez créer le paquet d'installation avec l'image du système d'exploitation de l'appareil d'étalon.

Suite au fonctionnement de l'Assistant, la tâche du Serveur d'administration **Prise de l'image du S.E. à partir de l'appareil d'étalon** est créée. Suite à l'exécution de cette tâche, le paquet d'installation est créé. Ce paquet peut être utilisé pour déployer l'image du système d'exploitation à l'aide du serveur PXE ou à l'aide de la tâche d'installation à distance.

4. Suivez les instructions de l'Assistant.

Suite au fonctionnement de l'Assistant, le paquet d'installation est créé. Ce paquet peut être utilisé pour installer l'application sur les appareils clients. Il est possible de consulter le paquet d'installation dans le dossier **Paquets d'installation**.

Pour plus d'informations sur le fonctionnement avec les paquets d'installation, cf. *Manuel d'implantation de Kaspersky Security Center*.

Établissement d'un certificat pour les paquets d'installation des applications

► Afin de calculer un certificat pour un paquet d'installation d'application, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.

Le dossier **Installation à distance** est placé par défaut dans le dossier **Avancé**.

2. Dans le menu contextuel du dossier **Paquets d'installation**, sélectionnez l'option **Propriétés**.

Ainsi, la fenêtre des propriétés du dossier **Paquets d'installation** s'ouvre.

3. Dans la fenêtre des propriétés du dossier **Paquets d'installation**, sélectionnez la section **Signature des paquets autonomes**.

4. Dans la section **Signature des paquets autonomes**, cliquez sur le bouton **Définir**.

Finalement, la fenêtre **Certificat** s'ouvre.

5. Dans le champ **Type de certificat**, sélectionnez le type de certificat ouvert ou fermé :

- Si la valeur **Coffre-fort PKCS#12** est sélectionnée, indiquez le fichier de certificat et le mot de passe.
- Si la valeur **Certificat X.509** est sélectionnée :
 - a. indiquez un fichier de clé fermée (avec l'extension prk ou pem) ;
 - b. indiquez le mot de passe de la clé fermée ;
 - c. indiquez un fichier de clé ouverte (avec l'extension cer).

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

Suite à cette action, un certificat est établi pour le paquet d'installation de l'application.

Installation des applications sur les appareils clients

► Pour installer l'application sur les appareils clients, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, cliquez sur le lien **Déployer le paquet d'installation sur les appareils administrés (postes de travail)** pour lancer l'Assistant du déploiement de la protection.
2. Dans la fenêtre de l'Assistant **Sélection du paquet d'installation**, indiquez le paquet d'installation de l'application que vous voulez installer.
3. 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. Il est possible de lancer ou d'arrêter la tâche dans le dossier **Tâches**.

Vous pouvez installer l'Agent d'administration sur les appareils clients fonctionnant sous les systèmes d'exploitation Windows, Linux et MacOS à l'aide de l'Assistant de déploiement de la protection.

Avant l'exécution de l'installation à distance de l'Agent d'administration sur l'appareil fonctionnant sous le système d'exploitation Linux, il est nécessaire de préparer l'appareil (cf. section "Préparation de l'appareil fonctionnant sous le système d'exploitation Linux à l'installation à distance de l'Agent d'administration" à la page [392](#)).

Administration des appareils mobiles

Cette section décrit l'administration des appareils mobiles connectés au Serveur d'administration. Les informations sur la connexion des appareils mobiles sont décrites dans le *Manuel d'implantation du Kaspersky Security Center*.

Dans cette section

Administration des appareils mobiles à l'aide d'une stratégie MDM	263
Utilisation des commandes pour les périphériques mobiles.....	266
Utilisation des certificats	274
Ajout d'un appareil mobile à la liste des appareils administrés.....	279
Gestion des appareils mobiles via les outils Exchange ActiveSync.....	284
Administration des appareils MDM iOS	290
Administration des appareils KES.....	306

Administration des appareils mobiles à l'aide d'une stratégie MDM

Pour administrer les appareils MDM iOS et EAS, vous pouvez utiliser le plug-in d'administration Kaspersky Mobile Device Management 10 Service Pack1 inclus dans la distribution du Kaspersky Security Center. Kaspersky Mobile Device Management permet de créer des stratégies de groupe pour la configuration des paramètres des appareils MDM iOS et EAS. Une stratégie de groupe qui permet de configurer les paramètres des appareils MDM iOS et EAS sans passer par l'iPhone Configuration Utility ni le profil d'administration Exchange Active Sync s'appelle une stratégie MDM.

La stratégie MDM offre les possibilités suivantes à l'administrateur :

- pour la gestion des appareils EAS :
 - configurer les paramètres du mot de passe pour le déverrouillage de l'appareil ;
 - configurer la conservation des données sur l'appareil sous forme chiffrée ;
 - configurer les paramètres de synchronisation de la messagerie d'entreprise ;
 - configurer les fonctions matérielles des appareils mobiles, par exemple, l'utilisation de disques amovibles, de l'appareil photo et du Bluetooth ;
 - configurer les restrictions des apps mobiles pouvant être utilisées sur l'appareil.
- pour la gestion des appareils MDM iOS :
 - configurer les paramètres de sécurité de l'utilisation du mot de passe sur l'appareil ;
 - configurer des restrictions pour l'utilisation des fonctions matérielles de l'appareil, ainsi que des restrictions relatives à l'installation et à la suppression d'apps mobiles ;
 - configurer des restrictions pour l'utilisation des apps mobiles de série sur l'appareil. Par exemple, YouTube™, iTunes Store, Safari ;
 - configurer des restrictions sur la consultation du contenu multimédia (par exemple, les films et les émissions télévisées) en fonction de la région où se trouve l'appareil ;
 - configurer les paramètres de connexion à Internet via le serveur proxy (proxy HTTP mondial) ;
 - configurer les paramètres du compte utilisateur unique via lequel l'utilisateur accède aux apps et services d'entreprise (technologie d'entrée unique) ;
 - contrôler l'utilisation d'Internet (sites Internet consultés) sur les appareils mobiles ;
 - configurer les paramètres des réseaux sans fil (Wi-Fi), des points d'accès (APN) et des réseaux privés virtuels (VPN) à l'aide de différents mécanismes d'authentification et protocoles réseau ;

- configurer les paramètres de connexion aux appareils AirPlay pour la transmission de photographies, de musique et de vidéos sur le réseau ;
- configurer les paramètres de connexion aux imprimantes AirPrint pour l'impression sans fil de documents à partir de l'appareil ;
- configurer les paramètres de synchronisation avec le serveur Microsoft Exchange et les comptes utilisateurs pour la messagerie d'entreprise sur les appareils ;
- configurer les identifiants de l'utilisateur pour la synchronisation à partir du service des catalogues LDAP ;
- configurer les identifiants de l'utilisateur pour la connexion aux services CalDAV et CardDAV, ce qui permet à l'utilisateur d'exploiter les calendriers et listes de contacts de l'entreprise ;
- configurer les paramètres de l'interface iOS sur l'appareil de l'utilisateur, par exemple les polices et les icônes pour certains sites Internet ;
- ajouter de nouveaux certificats de sécurité à l'appareil ;
- configurer les paramètres du serveur SCEP pour que l'appareil obtienne automatiquement les certificats à partir du Centre de certification ;
- ajouter des paramètres spécifiques pour le fonctionnement des apps mobiles.

Les principes généraux de fonctionnement de la stratégie MDM sont semblables aux principes de fonctionnement des stratégies définies pour l'administration d'autres applications. La particularité de la stratégie MDM repose dans son attribution à un groupe d'administration intégrant le Serveur MDM iOS et le Serveur des appareils mobiles Exchange ActiveSync (ci-après, les serveurs des appareils mobiles). Tous les paramètres définis dans la stratégie MDM sont d'abord diffusés sur les serveurs des appareils mobiles, puis sur les appareils mobiles qu'ils régissent. En cas d'utilisation d'une structure hiérarchisée de groupes d'administration, les serveurs secondaires des appareils mobiles y étant rattachés reçoivent les paramètres de la stratégie MDM en provenance des serveurs principaux des appareils mobiles, puis les diffusent sur les appareils mobiles.

Pour en savoir plus sur l'utilisation de la stratégie MDM dans la Console d'administration du Kaspersky Security Center, consultez le Manuel de l'administrateur relatif à l'utilisation avancée de Kaspersky Security for Mobile.

Utilisation des commandes pour les appareils mobiles

Cette section contient des informations sur les commandes d'administration des appareils mobiles prises en charge par l'application. Elle comporte également des instructions relatives à l'envoi de commandes aux appareils mobiles et à la consultation de l'état de l'exécution de ces commandes dans le journal dédié.

Commandes d'administration de l'appareil mobile

L'application prend en charge les commandes d'administration des appareils mobiles.

Ces commandes sont utilisées pour assurer l'administration à distance des appareils mobiles. Par exemple, si l'appareil mobile a été perdu, une commande vous permet de supprimer les données d'entreprise qu'il contient.

Les commandes peuvent être utilisées sur trois types d'appareils mobiles :

- appareil MDM iOS ;
- appareil KES ;
- appareil EAS.

Chaque type d'appareil prend en charge son propre ensemble de commandes. Le tableau ci-dessous reprend la liste des commandes pour chaque type d'appareil mobile.

Tous les appareils visés par la commande **Restaurer les paramètres par défaut** envoyée depuis l'appareil mobile verront toutes les données supprimées de l'appareil mobile et leurs paramètres réinitialisés en configuration de sortie d'usine.

Les appareils MDM iOS visés par la commande **Supprimer les données d'entreprise** envoyée depuis l'appareil mobile verront tous leurs profils de configuration, tous leurs profils provisioning, leur profil MDM iOS et toutes leurs apps supprimés si la case **Supprimer avec le profil MDM iOS** avait été cochée pour chacun d'entre eux.

Les appareils KES visés par la commande **Supprimer les données d'entreprise** envoyée depuis l'appareil mobile verront leurs données d'entreprise, leurs entrées dans les Contacts, leur historique des SMS, leur journal des appels, leur calendrier, leurs paramètres de connexion à Internet et leurs comptes utilisateurs (sauf leur compte utilisateur Google) supprimés. Les appareils KES verront également les données de leur carte mémoire supprimées.

Tableau 2. Liste des commandes prises en charge

Type d'appareil mobile	Commandes	Résultat de la commande
Appareil MDM iOS	Bloquer	L'appareil mobile est bloqué.
	Débloquer	Le verrouillage d'appareil mobile est activé par le code PIN. Le code PIN installé précédemment est réinitialisé.
	Restaurer les paramètres par défaut	Toutes les données sont supprimées de l'appareil mobile, et les paramètres reprennent leur configuration d'usine.

Type d'appareil mobile	Commandes	Résultat de la commande
	Supprimer les données corporatives	Suppression de tous les profils de configuration, de tous les profils provisioning, du profil iOS MDM et de toutes les apps dont la case Supprimer avec le profil MDM iOS avait été cochée.
	Synchroniser l'appareil	Les données de l'appareil mobile sont synchronisées avec le Serveur d'administration.
	Installer le profil	Le profil de configuration est installé sur l'appareil mobile.
	Supprimer le profil	Le profil de configuration est supprimé de l'appareil mobile.
	Installer le profil provisioning	Le profil provisioning est installé sur l'appareil mobile.
	Supprimer le profil provisioning	Le profil provisioning est supprimé de l'appareil mobile.
	Installer l'app	L'app est installée sur l'appareil mobile.
	Supprimer l'app	L'app est supprimée de l'appareil mobile.
	Saisir le code de rédemption	Saisit le code de rédemption d'une app payante.

Type d'appareil mobile	Commandes	Résultat de la commande
	Configurer l'itinérance	Active ou désactive l'itinérance des données et l'itinérance vocale.
	Installer Kaspersky Safe Browser	L'app Kaspersky Safe Browser est installée sur l'appareil mobile.
Appareil KES	Bloquer	L'appareil mobile est bloqué.
	Débloquer	Le verrouillage d'appareil mobile est activé par le code PIN. Le code PIN installé précédemment est réinitialisé.
	Restaurer les paramètres par défaut	Toutes les données sont supprimées de l'appareil mobile, et les paramètres reprennent leur configuration d'usine.
	Supprimer les données corporatives	Suppression de tous les profils de configuration, de tous les profils provisioning, du profil iOS MDM et de toutes les apps dont la case Supprimer avec le profil MDM iOS avait été cochée.
	Synchroniser l'appareil	Les données de l'appareil mobile sont synchronisées avec le Serveur d'administration.

Type d'appareil mobile	Commandes	Résultat de la commande
	Définir l'emplacement	L'appareil mobile est géolocalisé sur une carte Google Maps™. L'opérateur de téléphonie mobile facture l'envoi de SMS et l'utilisation d'Internet.
	Photographier	L'appareil mobile est bloqué. Une photographie est prise avec l'appareil photo frontal de l'appareil et enregistrée sur le Serveur d'administration. Les photographies peuvent être consultées dans le journal des commandes. L'opérateur de téléphonie mobile facture l'envoi de SMS et l'utilisation d'Internet.
	Emettre un signal sonore	L'appareil mobile émet un signal sonore.
Appareil EAS	Restaurer les paramètres par défaut	Toutes les données sont supprimées de l'appareil mobile, et les paramètres reprennent leur configuration d'usine.

Utilisation de Google Firebase Cloud Messaging

Pour une livraison opportune des commandes sur les appareils KES sous le système d'exploitation Android, le mécanisme des notifications push est utilisé dans Kaspersky Security Center. Les notifications push entre les appareils KES et le Serveur d'administration sont exécutées à l'aide du service Google Firebase Cloud Messaging. La Console d'administration de Kaspersky Security Center permet d'indiquer les paramètres du service Google Firebase Cloud Messaging pour connecter les appareils KES à ce service.

Pour obtenir les paramètres de Google Firebase Cloud Messaging, l'administrateur doit avoir un compte utilisateur Google. Pour plus d'informations sur l'obtention des paramètres de Google Firebase Cloud Messaging, consultez l'article de la Base de connaissances sur le site Internet du Support Technique <http://support.kaspersky.com/fr/11770>.

► *Pour configurer les paramètres de Google Firebase Cloud Messaging, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.
2. Dans le menu contextuel du dossier **Appareils mobiles**, sélectionnez l'option **Propriétés**.
Finalement, la fenêtre des propriétés du dossier **Appareils mobiles** s'ouvre.
3. Sélectionnez la section **Paramètres de Google Firebase Cloud Messaging**.
4. Dans le champ **Identificateur de l'expéditeur**, indiquez le nom du projet Google API que vous avez reçu lors de la création du projet dans la Console du développeur Google.
5. Dans le champ **Clé API**, saisissez la clé API standard que vous avez créée dans la console du développeur Google.

Lors de la synchronisation suivantes avec le Serveur d'administration, les appareils KES sous le système d'exploitation Android seront connectés au service Google Firebase Cloud Messaging.

Vous pouvez modifier les paramètres de Google Firebase Cloud Messaging à l'aide du bouton **Abandonner les paramètres**.

Envoi d'une commande

► Pour envoyer la commande à l'appareil mobile de l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Sélectionnez l'appareil mobile de l'utilisateur qui doit recevoir la commande.
3. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.
4. Dans la fenêtre **Commandes d'administration de l'appareil mobile**, ouvrez la section portant le nom de la commande qui doit être envoyée sur l'appareil mobile et cliquez sur le bouton **Envoyer la commande**.

Selon la commande que vous avez sélectionnée en cliquant sur le bouton **Envoyer la commande**, il est possible qu'une fenêtre de configuration de paramètres complémentaires s'ouvre. Par exemple, lors de l'envoi de la commande de suppression du profil provisioning sur l'appareil mobile, l'application propose de sélectionner le profil provisioning qui doit être supprimé. Dans la fenêtre, indiquez les paramètres complémentaires de la commande et confirmez votre choix. La commande sera ainsi envoyée à l'appareil mobile.

Le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile.

Le bouton **Annuler** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

Le groupe **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et l'état de leur exécution. Le bouton **Actualiser** permet d'actualiser la liste des commandes.

5. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes d'administration des appareils mobiles**.

Consultation de l'état des commandes dans le journal des commandes

L'application conserve les informations relatives à toutes les commandes envoyées aux appareils mobiles dans le journal des commandes. Le journal des commandes stocke des données telles que la date et l'heure d'envoi des commandes à l'appareil mobile, l'état des commandes, et certains détails concernant le résultat de leur exécution. Par exemple, en cas d'échec d'exécution d'une commande, la cause de l'erreur apparaît dans ce journal. Les enregistrements sont conservés pendant 30 jours dans le journal des commandes.

Les commandes envoyées aux appareils mobiles peuvent présenter les états suivants :

- *En cours d'exécution* : la commande est envoyée à l'appareil mobile ;
- *Terminée* : l'exécution de la commande a réussi ;
- *Terminée avec une erreur*: échec de l'exécution de la commande ;
- *Suppression en cours* : la commande est supprimée de la file d'attente des commandes envoyées à l'appareil mobile ;
- *Supprimée* : la commande a bien été supprimée de la file d'attente des commandes envoyées à l'appareil mobile ;
- *Suppression terminée sur une erreur* : la commande n'a pas pu être supprimée de la file d'attente des commandes envoyées à l'appareil mobile.

L'application tient un journal des commandes pour chaque appareil mobile.

► *Pour consulter le journal des commandes envoyées sur l'appareil mobile, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans la liste, sélectionnez l'appareil mobile dont vous souhaitez consulter le journal des commandes.

3. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

La fenêtre **Commandes de gestion des appareils mobiles** s'ouvre. Les sections de la fenêtre **Commandes de gestion des appareils mobiles** comportent les commandes qu'il est possible d'envoyer à l'appareil mobile.

4. Sélectionnez les sections comportant les commandes dont vous avez besoin et consultez les informations relatives à leur envoi et à leur exécution dans le groupe **Journal des commandes**.

Le groupe **Journal des commandes** permet de consulter la liste des commandes envoyées à l'appareil mobile et les informations les concernant. Le filtre **Afficher les commandes** permet d'afficher uniquement les commandes ayant le statut sélectionné dans la liste.

Utilisation des certificats

Cette section contient les informations sur l'utilisation de certificats des appareils mobiles. Elle comporte également des instructions concernant l'installation des certificats sur les appareils mobiles des utilisateurs et sur la configuration des règles d'octroi des certificats. Enfin, elle reprend des instructions relatives à l'intégration de l'application à l'infrastructure de clés ouvertes et à la configuration de la prise en charge de Kerberos.

Installation d'un certificat

Vous pouvez installer trois types de certificats sur l'appareil mobile de l'utilisateur :

- certificats généraux pour l'identification de l'appareil mobile ;
- certificats de messagerie pour la configuration de la messagerie corporative sur l'appareil mobile ;
- certificat VPN pour la configuration du réseau privé virtuel sur l'appareil mobile.

► *Pour installer le certificat sur l'appareil mobile de l'utilisateur, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Certificats**.
2. Dans l'espace de travail du dossier **Certificats**, cliquez sur le lien **Ajouter un certificat** pour lancer l'Assistant d'installation du certificat.

Suivez les instructions de l'Assistant.

A la fin de l'exécution de l'Assistant, le certificat sera créé et ajouté à la liste des certificats de l'utilisateur. De plus, l'utilisateur recevra une notification contenant un lien pour qu'il puisse télécharger et installer le certificat sur son appareil mobile. Il est possible de consulter et d'exporter sous forme de fichier la liste de tous les certificats (cf. section "Consultation de la liste des certificats octroyés à l'utilisateur" à la page [189](#)). Il est également possible de supprimer et d'octroyer à nouveau les certificats, ainsi que de consulter leurs propriétés.

Configuration des règles d'octroi de certificats

► *Pour configurer les règles d'octroi des certificats, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Certificats**.

Le dossier **Administration des appareils mobiles** est placé par défaut dans le dossier **Avancé**.

2. Dans l'espace de travail du dossier **Certificats**, cliquez sur le bouton **Configurer les règles d'émission des certificats**, pour ouvrir la fenêtre **Règles d'émission des certificats**.

3. Affichez la section au nom du type du certificat :

Emission des certificats de type général : pour la configuration de l'octroi des certificats généraux ;

Emission des certificats de messagerie : pour la configuration de l'octroi des certificats de messagerie ;

Emission des certificats VPN : pour la configuration de l'octroi des certificats VPN.

4. Dans le groupe **Paramètres d'émission**, configurez l'émission du certificat :

- Indiquez la durée de validité du certificat en jours.
- Sélectionnez une source de certificats (**Serveur d'administration** ou **Les certificats sont définis manuellement**).

Le Serveur d'administration est sélectionné en tant que source de certificats par défaut.

- Définissez un modèle de certificat (**Modèle par défaut**, **Autre modèle**).

La configuration des modèles est accessible si l'intégration à l'infrastructure à clé publique a été configurée dans la section **Intégration avec PKI** (à la page [277](#)).

5. Dans le groupe **Paramètres de la mise à jour automatique**, configurez la mise à jour automatique du certificat :

- Dans le champ **Mettre à jour lorsqu'il reste le nombre de jours indiqué ici avant la fin de la durée de validité (jours)**, indiquez le moment, en nombre de jours avant la fin de la durée de validité, où vous souhaitez exécuter une mise à jour du certificat.
- Pour activer la mise à jour automatique des certificats, cochez la case **Rééditer automatiquement le certificat si possible**.

Les certificats généraux ne peuvent être ré-octroyés que manuellement.

6. Dans le groupe **Paramètres de chiffrement**, activez et configurez le chiffrement des certificats octroyés.

Le chiffrement est uniquement disponible pour les certificats de type général.

- a. Cochez la case **Activer le chiffrement des certificats**.
- b. Servez-vous du curseur pour configurer la quantité maximale de caractères dans le mot de passe de chiffrement.

7. Cliquez sur le bouton **OK**.

Intégration à l'infrastructure de clés ouvertes

Il est indispensable d'intégrer l'application à l'infrastructure à clé publique (Public Key Infrastructure, PKI) pour simplifier l'octroi des certificats aux utilisateurs de domaine. Suite à cette intégration, l'émission des certificats est automatique.

Il est indispensable de configurer un compte utilisateur pour l'intégration PKI. Ce compte utilisateur doit répondre aux conditions suivantes :

- être utilisateur du domaine et administrateur de l'appareil hébergeant le Serveur d'administration ;
- disposer du privilège SeServiceLogonRight sur l'appareil hébergeant le Serveur d'administration.

Pour créer le profil permanent de l'utilisateur, il est nécessaire d'ouvrir au moins une fois une session du compte utilisateur configuré sur l'appareil hébergeant le Serveur d'administration. Installez le certificat de l'Agent d'enregistrement accordé par l'administrateur du domaine dans le stockage des certificats de cet utilisateur, sur l'appareil hébergeant le Serveur d'administration.

► *Pour configurer l'intégration à l'infrastructure de clés ouvertes, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Certificats**.

Le dossier **Administration des appareils mobiles** est placé par défaut dans le dossier **Avancé**.

2. Dans l'espace de travail, cliquez sur le bouton **Intégrer à l'infrastructure de clés ouvertes** pour ouvrir la section **Intégration avec PKI** de la fenêtre **Règles d'émission des certificats**.

Cette action entraîne l'ouverture de la section **Intégration avec PKI** de la fenêtre **Règles d'émission des certificats**.

3. Cochez la case **Intégrer la délivrance des certificats avec PKI**.

4. Dans le champ **Compte**, indiquez le nom du compte utilisateur de l'utilisateur qui sera utilisé pour l'intégration à l'infrastructure de clés ouvertes.
5. Dans le champ **Mot de passe**, saisissez le mot de passe du domaine du compte utilisateur.
6. Dans la liste **Indiquez le nom du modèle de certificat dans le système PKI**, sélectionnez le modèle qui servira de base à l'émission de certificats pour les utilisateurs du domaine.

Un service spécialisé est lancé sur Kaspersky Security Center à partir de ce compte utilisateur pour émettre les certificats de domaine des utilisateurs. Ce service se lance lors du téléchargement de la liste des modèles de certificats avec le bouton **Actualiser la liste** ou lors de l'émission du certificat.

7. Cliquez sur le bouton **OK** afin d'enregistrer les paramètres.

Suite à cette intégration, l'émission des certificats est automatique.

Activation de la prise en charge de Kerberos Constrained Delegation

L'application prend en charge l'utilisation de Kerberos Constrained Delegation.

► *Pour activer la prise en charge de Kerberos Constrained Delegation, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles**.
2. Dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.
3. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur MDM iOS.
4. Dans le menu contextuel du Serveur MDM iOS, sélectionnez l'option **Propriétés**.
5. Dans la fenêtre des propriétés du Serveur MDM iOS, sélectionnez la section **Paramètres**.

6. Dans la section **Paramètres**, cochez la case **Assurer la conformité avec Kerberos Constraint Delegation**.
7. Cliquez sur le bouton **OK**.

Ajout d'un appareil mobile à la liste des appareils administrés

Pour ajouter un appareil mobile de l'utilisateur à la liste des appareils administrés, il faut ajouter et installer un certificat commun sur l'appareil. Les certificats communs sont utilisés par le Serveur d'administration pour identifier les appareils mobiles. Après l'ajout et l'installation d'un certificat commun sur l'appareil mobile, celui-ci apparaît dans la liste des appareils administrés. L'ajout des appareils mobiles de l'utilisateur à la liste des appareils administrés est effectué grâce à un Assistant.

Lancement de l'Assistant d'ajout d'un nouvel appareil

► *Pour lancer l'Assistant d'ajout d'un nouvel appareil mobile, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Comptes utilisateurs**.

Par défaut, le dossier **Comptes utilisateurs** est placé dans le dossier **Avancé**.

2. Sélectionnez le compte utilisateur, et l'appareil mobile que vous souhaitez ajouter à la liste des appareils administrés.
3. Dans le menu contextuel du compte utilisateur, sélectionnez l'option **Ajouter un appareil mobile**.

L'Assistant d'ajout d'un nouvel appareil mobile démarre.

4. Dans la fenêtre **Système d'exploitation**, sélectionnez le type de système d'exploitation de l'appareil mobile (*Android, iOS*).

Les actions suivantes de l'Assistant d'ajout d'un nouvel appareil mobile dépendent du type de système d'exploitation de l'appareil mobile que vous avez choisi (cf. instructions ci-dessous).

Ajout d'un appareil mobile lorsque le certificat commun est fourni via un lien vers l'App Store

► Pour installer l'app Kaspersky Safe Browser sur un appareil iOS à partir de l'App Store, puis le connecter au Serveur d'administration :

1. Dans la fenêtre de l'Assistant **Système d'exploitation**, sélectionnez le type de système d'exploitation de l'appareil mobile **iOS**.
2. Dans la fenêtre de l'Assistant **Mode de protection des appareils MDM iOS**, sélectionnez l'option **Installer Kaspersky Safe Browser à partir du lien vers l'AppStore**.
3. Dans la fenêtre de l'assistant **Source du certificat**, il faut indiquer le mode de création du certificat commun à l'aide duquel le Serveur d'administration identifie un appareil mobile. Il existe deux manières de fournir un certificat commun :
 - créer automatiquement un certificat commun à l'aide du Serveur d'administration et l'ajouter à l'appareil mobile ;
 - indiquer le fichier du certificat commun.
4. Dans la fenêtre **Mode de notification des utilisateurs** de l'assistant, configurez les paramètres de la notification, par message SMS ou email, de l'utilisateur d'un appareil mobile à propos de la création du certificat.
5. Dans la fenêtre **Résultat** de l'assistant, cliquez sur le bouton **Terminé** pour fermer l'Assistant d'installation de certificats.

Suite à l'exécution de l'assistant sur l'appareil mobile de l'utilisateur, un lien et un code QR seront envoyés pour télécharger Kaspersky Safe Browser depuis l'App Store. L'utilisateur clique sur le lien et scanne le code QR. Ensuite, le système d'exploitation de l'appareil mobile demande à l'utilisateur son accord pour l'installation de Kaspersky Safe Browser. L'utilisateur installe Kaspersky Safe Browser sur l'appareil mobile. Après l'installation de Kaspersky Safe Browser, l'utilisateur scanne de nouveau le code QR pour recevoir les paramètres de connexion au Serveur d'administration. Après avoir scanné de nouveau le code QR dans Safe Browser, l'utilisateur reçoit les paramètres de connexion au Serveur d'administration et le certificat commun. L'appareil mobile se connecte au Serveur d'administration et télécharge le certificat commun. Après l'installation du certificat sur l'appareil mobile, celui-ci apparaît dans le

sous-dossier **Appareils mobiles** du dossier **Administration des appareils mobiles** de l'arborescence de la console.

Si Kaspersky Safe Browser a été installé auparavant sur l'appareil mobile, les paramètres de connexion au Serveur d'administration doivent être saisis indépendamment. Ensuite, il faut installer le certificat général sur l'appareil (cf. section "Installation du certificat" à la page [274](#)). Dans ce cas, Kaspersky Safe Browser n'est ni téléchargé ni installé.

Ajout d'un appareil mobile lorsque le certificat commun est intégré au Profil MDM iOS

► *Pour connecter au Serveur d'administration l'appareil iOS via le protocole MDM iOS, procédez comme suit :*

1. Dans la fenêtre de l'Assistant **Système d'exploitation**, sélectionnez le type de système d'exploitation de l'appareil mobile **iOS**.
2. Dans la fenêtre de l'Assistant **Mode de protection des appareils MDM iOS**, sélectionnez l'option **Utiliser le profil MDM iOS du Serveur MDM iOS**.

Dans le champ qui apparaît ci-dessous, sélectionnez le Serveur MDM iOS.

3. Dans la fenêtre de l'assistant **Source du certificat**, il faut indiquer le mode de création du certificat commun à l'aide duquel le Serveur d'administration identifie un appareil mobile. Il existe deux manières de fournir un certificat commun :
 - créer automatiquement un certificat commun à l'aide du Serveur d'administration et l'ajouter à l'appareil mobile ;
 - indiquer le fichier du certificat commun.
4. Dans la fenêtre **Mode de notification des utilisateurs** de l'assistant, configurez les paramètres de la notification, par message SMS ou email, de l'utilisateur d'un appareil mobile à propos de la création du certificat.
5. Dans la fenêtre **Résultat** de l'assistant, cliquez sur le bouton **Terminé** pour fermer l'Assistant d'installation de certificats.

Le profil MDM iOS est alors automatiquement publié sur le serveur Internet de Kaspersky Security Center. L'utilisateur de l'appareil mobile reçoit une notification avec un lien permettant

de télécharger le profil MDM iOS sur le serveur Internet. L'utilisateur clique lui-même sur le lien reçu. Ensuite, le système d'exploitation de l'appareil mobile demande à l'utilisateur son accord pour l'installation du profil MDM iOS. Si l'utilisateur est d'accord, le profil MDM iOS est téléchargé sur l'appareil mobile. Après le téléchargement du profil MDM iOS et après la synchronisation avec le Serveur d'administration, l'appareil mobile est affiché dans le sous-dossier **Appareils mobiles** du dossier **Administration des appareils mobiles** de l'arborescence de la console.

Pour que l'utilisateur puisse accéder au serveur Internet de Kaspersky Security Center via le lien reçu, l'appareil mobile doit pouvoir se connecter au Serveur d'administration sur le port 8061.

Ajout d'un appareil mobile lorsque le certificat commun est fourni via un lien vers Google Play

► *Pour installer l'app Kaspersky Endpoint Security for Android sur un appareil KES à partir de Google Play, puis le connecter au Serveur d'administration, procédez comme suit :*

1. Dans la fenêtre de l'Assistant **Système d'exploitation**, sélectionnez le type de système d'exploitation de l'appareil mobile **Android**.
2. Dans la fenêtre de l'Assistant **Mode d'installation de Kaspersky Endpoint Security for Android**, sélectionnez l'option **Via le lien vers Google Play**.
3. Dans la fenêtre de l'assistant **Source du certificat**, il faut indiquer le mode de création du certificat commun à l'aide duquel le Serveur d'administration identifie un appareil mobile. Il existe deux manières de fournir un certificat commun :
 - créer automatiquement un certificat commun à l'aide du Serveur d'administration et l'ajouter à l'appareil mobile ;
 - indiquer le fichier du certificat commun.

4. Dans la fenêtre **Mode de notification des utilisateurs** de l'assistant, configurez les paramètres de la notification, par message SMS ou email, de l'utilisateur d'un appareil mobile à propos de la création du certificat.
5. Dans la fenêtre **Résultat** de l'assistant, cliquez sur le bouton **Terminé** pour fermer l'Assistant d'installation de certificats.

Suite au fonctionnement de l'assistant sur l'appareil mobile de l'utilisateur, un lien et un code QR seront envoyés pour le téléchargement de Kaspersky Endpoint Security for Android. L'utilisateur clique sur le lien et scanne le code QR. Ensuite, le système d'exploitation de l'appareil mobile demande à l'utilisateur son accord pour l'installation de Kaspersky Endpoint Security for Android. Après le téléchargement et l'installation de Kaspersky Endpoint Security for Android, l'appareil mobile se connecte au Serveur d'administration et télécharge le certificat commun. Après l'installation du certificat sur l'appareil mobile, celui-ci apparaît dans le sous-dossier **Appareils mobiles** du dossier **Administration des appareils mobiles** de l'arborescence de la console.

Ajout d'un appareil mobile lorsque le certificat commun est intégré à l'app mobile

- *Pour installer l'app Kaspersky Endpoint Security for Mobile Devices sur l'appareil Android, puis le connecter au Serveur d'administration, procédez comme suit :*

L'app Kaspersky Endpoint Security for Mobile Devices disponible sur le Serveur d'administration est utilisée pour l'installation.

1. Dans la fenêtre de l'Assistant **Système d'exploitation**, sélectionnez comme type de système d'exploitation de l'appareil mobile **Android**.
2. Dans la fenêtre de l'Assistant **Mode d'installation de Kaspersky Endpoint Security for Android**, sélectionnez l'option **Via un lien vers votre serveur Web**.

Dans le champ qui apparaît ci-dessous, sélectionnez le paquet d'installation ou créez un nouveau paquet d'installation à l'aide du bouton **Nouveau**.

3. Dans la fenêtre de l'assistant **Source du certificat**, il faut indiquer le mode de création du certificat commun à l'aide duquel le Serveur d'administration identifie un appareil mobile. Il existe deux manières de fournir un certificat commun :
 - créer automatiquement un certificat commun à l'aide du Serveur d'administration et l'ajouter à l'appareil mobile ;
 - indiquer le fichier du certificat commun.
4. Dans la fenêtre **Mode de notification des utilisateurs** de l'assistant, configurez les paramètres de la notification, par message SMS ou email, de l'utilisateur d'un appareil mobile à propos de la création du certificat.
5. Dans la fenêtre **Résultat** de l'assistant, cliquez sur le bouton **Terminé** pour fermer l'Assistant d'installation de certificats.

Le paquet de l'application mobile Kaspersky Endpoint Security for Android est automatiquement publié sur le serveur Internet de Kaspersky Security Center. Le paquet de l'application mobile contient l'app, les paramètres de connexion de l'appareil mobile au Serveur d'administration et le certificat. L'utilisateur de l'appareil mobile reçoit une notification contenant un lien pour télécharger le paquet sur le serveur Internet. L'utilisateur clique lui-même sur le lien reçu. Ensuite, le système d'exploitation de l'appareil demande à l'utilisateur son accord pour l'installation du paquet de l'application mobile. Si l'utilisateur est d'accord, le paquet est téléchargé sur l'appareil mobile. Après le téléchargement du paquet et après la synchronisation avec le Serveur d'administration, l'appareil mobile est affiché dans le sous-dossier **Appareils mobiles** du dossier **Administration des appareils mobiles** de l'arborescence de la console.

Gestion des appareils mobiles via les outils Exchange ActiveSync

Cette section décrit les options complémentaires de gestion des appareils EAS à partir de Kaspersky Security Center.

En plus d'administrer les appareils EAS via des commandes, l'administrateur peut :

- Créer des profils d'Administration des appareils EAS et les attribuer aux boîtes aux lettres des utilisateurs (à la page [285](#)). Un *profil de gestion des appareils EAS* est une stratégie Exchange ActiveSync utilisée sur le serveur Microsoft Exchange pour administrer les appareils EAS. Ce profil permet de configurer les groupes de paramètres suivants :
 - paramètres de gestion du mot de passe utilisateur ;
 - paramètres de synchronisation du courrier ;
 - restrictions des fonctions pouvant être utilisées sur l'appareil mobile ;
 - restrictions des apps mobiles pouvant être utilisées sur l'appareil mobile.

Les paramètres du profil d'administration peuvent n'être appliqués que partiellement selon le modèle de l'appareil mobile. Vous pouvez consulter l'état d'application de la stratégie Exchange ActiveSync dans les propriétés de l'appareil mobile.

- Consulter les informations sur les paramètres d'Administration des appareils EAS (à la page [288](#)). Par exemple, dans les propriétés d'un appareil mobile, l'administrateur peut consulter l'heure de la dernière synchronisation de l'appareil mobile avec le serveur Microsoft Exchange, l'identifiant d'appareil EAS, le nom de la stratégie Exchange ActiveSync et son statut d'application sur l'appareil mobile.
- Désactiver l'Administration des appareils EAS inutilisés (à la page [289](#)).
- Configurer les paramètres du sondage d'Active Directory par le Serveur des appareils mobiles Exchange ActiveSync, qui permettent de mettre à jour les informations relatives aux boîtes aux lettres des utilisateurs et à leurs appareils mobiles.

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

Ajout d'un profil d'administration

Pour gérer les appareils EAS, vous pouvez créer des profils d'administration des appareils EAS et leur attribuer les boîtes aux lettres Microsoft Exchange de votre choix.

Chaque boîte aux lettres Microsoft Exchange ne peut être associée qu'à un seul profil d'administration des appareils EAS.

► *Pour ajouter un profil d'administration des appareils EAS à une boîte aux lettres Microsoft Exchange, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles**.
2. Dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.
3. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur des appareils mobiles Exchange ActiveSync.
4. Dans le menu contextuel du Serveur des appareils mobiles Exchange ActiveSync, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés du Serveur des appareils mobiles s'ouvre.

5. Dans la fenêtre des propriétés du **Serveur des appareils mobiles Exchange ActiveSync**, sélectionnez la section **Boîtes aux lettres**.
6. Sélectionnez une boîte aux lettres et cliquez sur le bouton **Désigner le profil**.

Le fenêtre **Profils des stratégies** s'ouvre.

7. Dans la fenêtre **Profils des stratégies**, cliquez sur le bouton **Ajouter**.

La fenêtre **Nouveau profil** s'ouvre.

8. Configurez les paramètres du profil dans les onglets de la fenêtre **Nouveau profil** :

- Si vous souhaitez définir le nom du profil et la fréquence de ses mises à jour, sélectionnez l'onglet **Général**.
- Si vous souhaitez configurer les paramètres du mot de passe utilisateur de l'appareil mobile, sélectionnez l'onglet **Mot de passe**.
- Si vous souhaitez configurer les paramètres de la synchronisation avec le serveur Microsoft Exchange, sélectionnez l'onglet **Paramètres de synchronisation**.
- Si vous souhaitez configurer les paramètres de restriction des fonctions de l'appareil mobile, sélectionnez l'onglet **Appareil**.
- Si vous souhaitez configurer les paramètres de restriction de l'utilisation des apps mobiles sur l'appareil mobile, sélectionnez l'onglet **Applications pour l'appareil**.

9. Cliquez sur le bouton **OK**.

Le nouveau profil s'affichera dans la liste des profils de la fenêtre **Profils des stratégies**.

Si vous souhaitez que ce profil soit automatiquement attribué aux nouvelles boîtes aux lettres et aux boîtes aux lettres dont le profil a été supprimé, sélectionnez-le dans la liste des profils et cliquez sur **Définir comme le profil par défaut**.

Il est impossible de supprimer le profil par défaut. Pour supprimer le profil par défaut actuel, il faut désigner la propriété "profil par défaut" à un autre profil.

10. Cliquez sur le bouton **OK** dans la fenêtre **Profils des stratégies**.

Les paramètres du profil d'administration seront appliqués à l'appareil EAS lors de la synchronisation suivante de l'appareil avec le Serveur des appareils mobiles Exchange ActiveSync.

Suppression d'un profil d'administration

► Pour supprimer le profil de gestion des appareils EAS d'une boîte aux lettres Microsoft Exchange, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles**.
2. Dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.
3. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur des appareils mobiles Exchange ActiveSync.
4. Dans le menu contextuel du Serveur des appareils mobiles Exchange ActiveSync, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés du Serveur des appareils mobiles s'ouvre.

5. Dans la fenêtre des propriétés du Serveur des appareils mobiles Exchange ActiveSync, sélectionnez la section **Boîtes aux lettres**.
6. Sélectionnez une boîte aux lettres et cliquez sur le bouton **Modifier les profils**.

Le fenêtre **Profils des stratégies** s'ouvre.

7. Dans la fenêtre **Profils des stratégies**, sélectionnez le profil à supprimer et cliquez sur le bouton de suppression représentant un X rouge.

Le profil sélectionné sera supprimé de la liste des profils d'administration. Les appareils EAS qui étaient administrés par le profil supprimé passeront sous le contrôle du profil par défaut actif.

Si vous souhaitez supprimer le profil par défaut actif, attribuez la propriété "Profil par défaut" à un autre profil, puis supprimez le profil désiré.

Affichage des informations sur l'appareil EAS

► *Pour consulter les informations relatives à un appareil EAS, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, filtrez les appareils EAS par type de protocole d'administration (EAS).
3. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Propriétés**.

Cette action entraîne l'ouverture de la fenêtre des propriétés de l'appareil EAS.

La fenêtre des propriétés de l'appareil mobile affiche des informations sur l'appareil EAS connecté.

Désactivation de l'administration d'un appareil EAS

► *Pour désactiver l'administration d'un appareil EAS par le Serveur des appareils mobiles Exchange ActiveSync, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, filtrez les appareils EAS par type de protocole d'administration (EAS).
3. Sélectionnez l'appareil mobile dont vous souhaitez désactiver l'administration par le Serveur des appareils mobiles Exchange ActiveSync.
4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Supprimer**.

L'appareil EAS est marqué pour suppression avec une icône en forme de croix rouge. La suppression réelle de l'appareil mobile de la liste des appareils administrés a lieu après son élimination de la base de données du Serveur des appareils mobiles Exchange ActiveSync. Pour ce faire, l'administrateur doit supprimer le compte utilisateur sur le serveur Microsoft Exchange.

Administration des appareils MDM iOS

Cette section décrit les options complémentaires d'administration des appareils MDM iOS à partir de Kaspersky Security Center. Pour administrer les appareils MDM iOS, l'application permet de :

- Configurer de manière centralisée les paramètres des appareils MDM iOS administrés et restreindre les fonctions de l'appareil à l'aide de profils de configuration. Vous pouvez ajouter et modifier les profils de configuration et installer des profils sur l'appareil mobile.
- Installer des apps sur l'appareil mobile, sans passer par l'App Store, à l'aide de profils provisioning. Les profils provisioning vous permettent par exemple d'installer sur l'appareil mobile des utilisateurs les apps d'entreprise conçues en interne. Le profil provisioning contient des informations sur l'app et sur l'appareil mobile.
- Installer une app sur l'appareil MDM iOS via l'App Store. L'app doit être ajoutée sur le Serveur MDM iOS avant son installation sur l'appareil MDM iOS.

Une notification PUSH est envoyée à tous les appareils MDM iOS connectés toutes les 24 heures pour synchroniser les données avec le Serveur MDM iOS.

Les informations sur l'installation du Serveur MDM iOS sont décrites dans le *Manuel d'implantation de Kaspersky Security Center*.

Les informations relatives au profil de configuration et au profil provisioning, ainsi qu'aux applications installées sur l'appareil iOS MDM, peuvent être consultées dans la fenêtre des propriétés de l'appareil (cf. section "Affichage des informations sur l'appareil MDM iOS" à la page [305](#)).

Établissement d'un certificat de profil MDM iOS

Vous pouvez établir un certificat de profil MDM iOS pour l'authentification par appareil mobile.

► *Pour créer un certificat de profil MDM iOS, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

Le dossier **Administration des appareils mobiles** est placé par défaut dans le dossier **Avancé**.

2. Dans le menu contextuel du dossier **Appareils mobiles**, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre de propriétés du dossier, sélectionnez la section **Paramètres de connexion des appareils iOS**.
4. Cliquez sur le bouton **Définir** en regard du champ **Sélectionnez le certificat**.

Finalement, la fenêtre **Certificat** s'ouvre.

5. Dans le champ **Type de certificat**, sélectionnez le type de certificat ouvert ou fermé :
 - Si la valeur **Coffre-fort PKCS#12** est sélectionnée, indiquez le fichier de certificat et le mot de passe.
 - Si la valeur **Certificat X.509** est sélectionnée :
 - a. indiquez un fichier de clé fermée (avec l'extension prk ou pem) ;
 - b. indiquez le mot de passe de la clé fermée ;
 - c. indiquez un fichier de clé ouverte (avec l'extension cer).
6. Cliquez sur le bouton **OK**.

Suite à cette action, un certificat de profil MDM iOS est créé.

Ajout du profil de configuration

Pour créer le profil de configuration, il faut installer l'application iPhone Configuration Utility sur l'appareil avec la Console d'administration déjà installée. L'application iPhone Configuration Utility doit être téléchargée préalablement depuis le site de Apple Inc. et installée par les outils titulaires du système d'exploitation.

► *Pour créer le profil de configuration et l'ajouter sur le Serveur MDM iOS, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Administration des appareils mobiles**.

Le dossier **Administration des appareils mobiles** est placé par défaut dans le dossier **Avancé**.

2. Dans l'espace de travail du dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Serveurs des appareils mobiles**.

3. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur MDM iOS.

4. Dans le menu contextuel du Serveur MDM iOS, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés du Serveur des appareils mobiles s'ouvre.

5. Dans la fenêtre des propriétés du Serveur MDM iOS, sélectionnez l'option **Profils de configuration**.

6. Dans la section **Profils de configuration**, cliquez sur le bouton **Créer**.

La fenêtre **Ajout du nouveau profil de configuration** s'ouvre.

7. Dans la fenêtre **Ajout du nouveau profil de configuration**, indiquez le nom et l'identificateur du profil.

L'identificateur du profil de configuration doit être unique, la valeur de l'identificateur doit être définie au format Reverse-DNS, par exemple, *com.companyname.identifier*.

8. Cliquez sur le bouton **OK**.

Lancez l'application iPhone Configuration Utility.

9. Exécutez la configuration des paramètres du profil dans l'application iPhone Configuration Utility.

La description des paramètres du profil et les instructions de sa configuration sont décrites dans la documentation pour l'application iPhone Configuration Utility.

Après la configuration des paramètres du profil dans l'application iPhone Configuration Utility, un nouveau profil de configuration s'affiche dans la section **Profils de configuration** de la fenêtre des propriétés du Serveur MDM iOS.

Le bouton **Modifier** permet de modifier le profil de configuration.

Le bouton **Importer** permet de télécharger le profil de configuration dans l'application.

Le bouton **Exporter le filtre** permet d'enregistrer le profil de configuration dans un fichier.

Le profil créé doit être installé sur les appareils MDM iOS (cf. section "Installation du profil de configuration sur l'appareil" à la page [293](#)).

Définition du profil de configuration sur l'appareil

► *Pour installer le profil de configuration sur l'appareil mobile, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, filtrez les appareils MDM iOS par protocole d'administration *MDM iOS*.
3. Sélectionnez l'appareil mobile de l'utilisateur sur lequel vous devez installer le profil de configuration

Vous pouvez sélectionner plusieurs appareils mobiles pour y installer le profil de façon simultanée.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.
5. Dans la fenêtre **Commandes d'administration des appareils mobiles**, ouvrez la section **Installer le profil** et cliquez sur le bouton **Envoyer la commande**.

Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant l'option **Toutes les commandes** dans le menu contextuel de cet appareil mobile, puis **Installer le profil**.

Cette opération ouvre la fenêtre **Sélection des profils** contenant la liste des profils. Dans la liste, sélectionnez le profil que vous devez installer sur l'appareil mobile. Vous pouvez sélectionner et installer simultanément plusieurs profils sur l'appareil mobile. Pour sélectionner une plage de profils, utilisez **SHIFT**. Pour réunir des profils séparés dans un groupe, utilisez **CTRL**.

6. Cliquez sur le bouton **OK** pour envoyer la commande à l'appareil mobile.

Suite à l'exécution de cette commande, le profil de configuration sélectionné sera installé sur l'appareil mobile de l'utilisateur. Parallèlement, l'état de la commande du journal des commandes affichera la valeur *Progression*.

Le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile.

Le bouton **Annuler** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

Le groupe **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et l'état de leur exécution. Le bouton **Actualiser** permet d'actualiser la liste des commandes.

7. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes d'administration des appareils mobiles**.

Il est possible de consulter le profil installé et de le supprimer en cas de besoin (cf. section "Suppression du profil de configuration sur le périphérique" à la page [295](#)).

Suppression du profil de configuration de l'appareil

► Pour supprimer le profil de configuration de l'appareil mobile, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, sélectionnez les appareils MDM iOS en cliquant sur le lien **MDM iOS**.
3. Sélectionnez l'appareil mobile de l'utilisateur duquel vous devez supprimer le profil de configuration.

Vous pouvez sélectionner plusieurs appareils mobiles pour supprimer le profil de façon simultanée.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.
5. Dans la fenêtre **Commandes pour la gestion des appareils mobiles**, ouvrez la section **Supprimer le profil** et cliquez sur le bouton **Envoyer la commande**.

Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant l'option **Toutes les commandes** dans le menu contextuel de cet appareil, puis **Supprimer le profil**.

Cette opération ouvre la fenêtre **Suppression des profils** contenant la liste des profils.

6. Dans la liste, sélectionnez le profil que vous devez supprimer de l'appareil mobile. Vous pouvez sélectionner et supprimer simultanément plusieurs profils de l'appareil mobile. Pour sélectionner une plage de profils, utilisez **SHIFT**. Pour réunir des profils séparés dans un groupe, utilisez **CTRL**.

7. Cliquez sur le bouton **OK** pour envoyer la commande à l'appareil mobile.

Suite à l'exécution de cette commande, le profil de configuration sélectionné sera supprimé de l'appareil mobile de l'utilisateur. Parallèlement, l'état de la commande affichera la valeur *Terminée*.

Le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile.

Le bouton **Annuler** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

Le groupe **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et l'état de leur exécution. Le bouton **Actualiser** permet d'actualiser la liste des commandes.

8. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes de gestion des appareils mobiles**.

Ajout du profil provisioning

► *Pour ajouter le profil provisioning sur le Serveur MDM iOS, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles**.
2. Dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.
3. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur MDM iOS.
4. Dans le menu contextuel du Serveur MDM iOS, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés du Serveur des appareils mobiles s'ouvre.

5. Dans la fenêtre des propriétés du **Serveur MDM iOS**, sélectionnez l'option **Profils provisioning**.
6. Dans la section **Profils provisioning**, cliquez sur le bouton **Importer** et indiquez le chemin d'accès au fichier du profil provisioning.

Le profil sera ajouté dans les paramètres du Serveur MDM iOS.

Le bouton **Exporter le profil** permet d'enregistrer le profil provisioning dans un fichier.

Le profil provisioning importé peut être installé sur l'appareil MDM iOS (cf. section "Installation du profil provisioning sur l'appareil" à la page [297](#)).

Définition du profil provisioning sur l'appareil

► *Pour installer le profil provisioning sur l'appareil mobile, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, filtrez les appareils MDM iOS par protocole d'administration *MDM iOS*.
3. Sélectionnez l'appareil mobile de l'utilisateur sur lequel vous devez installer le profil provisioning.

Vous pouvez sélectionner plusieurs appareils mobiles pour y installer le profil provisioning de façon simultanée.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.
5. Dans la fenêtre **Commandes pour la administration des appareils mobiles**, ouvrez la section **Installer le profil provisioning** et cliquez sur le bouton **Envoyer la commande**.

Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant l'option **Toutes les commandes** dans le menu contextuel de cet appareil mobile, puis **Installer le profil provisioning**.

Cette opération ouvre la fenêtre **Sélection des profils provisioning** contenant la liste des profils provisioning. Dans la liste, sélectionnez le profil provisioning que vous devez installer sur l'appareil mobile. Vous pouvez sélectionner et installer plusieurs profils provisioning

simultanément sur l'appareil mobile. Afin de sélectionner une plage de profils provisioning, utilisez **SHIFT**. Afin de réunir des profils provisioning séparés dans un groupe, utilisez **CTRL**.

6. Cliquez sur le bouton **OK** pour envoyer la commande à l'appareil mobile.

Suite à l'exécution de cette commande, le profil provisioning sélectionné sera installé sur l'appareil mobile de l'utilisateur. Parallèlement, l'état de la commande du journal des commandes affichera la valeur *Terminée*.

Le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile.

Le bouton **Annuler** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

Le groupe **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et l'état de leur exécution. Le bouton **Actualiser** permet d'actualiser la liste des commandes.

7. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes d'administration des appareils mobiles**.

Il est possible de consulter le profil installé et de le supprimer en cas de besoin (cf. section "Suppression du profil provisioning sur le périphérique" à la page [298](#)).

Suppression du profil provisioning de l'appareil

► *Pour supprimer un profil provisioning de l'appareil mobile, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, filtrez les appareils MDM iOS par protocole d'administration *MDM iOS*.

3. Sélectionnez l'appareil mobile de l'utilisateur duquel vous devez supprimer le profil provisioning.

Vous pouvez sélectionner plusieurs appareils mobiles pour supprimer le profil provisioning de façon simultanée.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

5. Dans la fenêtre **Commandes pour la gestion des appareils mobiles**, ouvrez la section **Supprimer le profil provisioning** et cliquez sur le bouton **Envoyer la commande**.

Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant l'option **Toutes les commandes** dans le menu contextuel de cet appareil, puis **Supprimer le profil provisioning**.

Cette opération ouvre la fenêtre **Suppression des profils provisioning** contenant la liste des profils.

6. Dans la liste, sélectionnez le profil provisioning que vous devez supprimer de l'appareil mobile. Vous pouvez sélectionner et supprimer plusieurs profils provisioning simultanément de l'appareil mobile. Afin de sélectionner une plage de profils provisioning, utilisez **SHIFT**. Afin de réunir des profils provisioning séparés dans un groupe, utilisez **CTRL**.

7. Cliquez sur le bouton **OK** pour envoyer la commande à l'appareil mobile.

Suite à l'exécution de cette commande, le profil provisioning sélectionné sera supprimé de l'appareil mobile de l'utilisateur. Les apps liées au profil provisioning supprimé ne fonctionneront plus. Parallèlement, l'état de la commande affichera la valeur *Terminée*.

Le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile.

Le bouton **Annuler** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

Le groupe **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et l'état de leur exécution. Le bouton **Actualiser** permet d'actualiser la liste des commandes.

8. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes de gestion des appareils mobiles**.

Ajout d'une app administrée

L'app doit être ajoutée sur le Serveur MDM iOS avant son installation sur l'appareil MDM iOS. L'app est administrée si elle a été installée sur l'appareil à l'aide de Kaspersky Security Center. Il est possible de gérer à distance les apps administrées à l'aide de Kaspersky Security Center.

► *Pour ajouter l'app administrée sur le Serveur MDM iOS, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles**.
2. Dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.
3. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur MDM iOS.
4. Dans le menu contextuel du Serveur MDM iOS, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés du Serveur MDM iOS s'ouvre.

5. Dans le menu contextuel du Serveur MDM iOS, sélectionnez la section **Apps administrées**.
6. Dans la section **Apps administrées**, cliquez sur le bouton **Ajouter**.

La fenêtre **Ajout de l'app** s'ouvre.

7. Dans la fenêtre **Ajout de l'app**, dans le champ **Nom de l'app**, indiquez le nom de l'app ajoutée.
8. Dans le champ **Apple ID de l'app ou le lien vers l'app dans l'App Store**, indiquez l'identifiant Apple de l'app ajoutée ou le lien vers le fichier-manifeste permettant de télécharger l'app.
9. Si vous souhaitez que l'app administrée soit supprimée en cas de suppression du profil MDM iOS en même temps que le profil de l'appareil mobile de l'utilisateur, cochez la case **Supprimer avec le profil MDM iOS**.

10. Si vous souhaitez interdire la sauvegarde des données de l'app à l'aide des outils iTunes, cochez la case **Interdire la création des copies de sauvegarde des données**.

11. Cliquez sur le bouton **OK**.

L'app ajoutée s'affiche dans la section **Apps administrées** de la fenêtre des propriétés du Serveur MDM iOS.

Installation de l'app sur l'appareil mobile

► *Pour installer l'app sur l'appareil mobile MDM iOS, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

Le dossier **Administration des appareils mobiles** est placé par défaut dans le dossier **Avancé**. La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Sélectionnez l'appareil MDM iOS sur lequel vous devez installer l'app.

Vous pouvez sélectionner plusieurs appareils mobiles pour y installer l'app en même temps.

3. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

4. Dans la fenêtre **Commandes pour la gestion des appareils mobiles**, ouvrez la section **Installer l'app** et cliquez sur le bouton **Envoyer la commande**.

Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant l'option **Toutes les commandes** dans le menu contextuel de cet appareil, puis **Installer l'app**.

Cette opération ouvre la fenêtre **Sélection des apps** contenant la liste des apps. Dans la liste, sélectionnez l'app que vous devez installer sur l'appareil mobile. Vous pouvez sélectionner et installer plusieurs apps en même temps sur l'appareil mobile. Pour sélectionner une plage d'apps, utilisez la touche **SHIFT**. Pour regrouper plusieurs apps, utilisez la touche **CTRL**.

5. Cliquez sur le bouton **OK** pour envoyer la commande à l'appareil mobile.

Suite à l'exécution de cette commande, l'app sélectionnée sera installée sur l'appareil mobile de l'utilisateur. Parallèlement, l'état de la commande du journal des commandes affiche la valeur *Terminée*.

Le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile. Le bouton **Annuler** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

Le groupe **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et l'état de leur exécution. Le bouton **Actualiser** permet d'actualiser la liste des commandes.

6. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes de gestion des appareils mobiles**.

Des informations sur l'application installée sont affichées dans les propriétés de l'appareil mobile MDM iOS (cf. section "Affichage des informations sur l'appareil MDM iOS" à la p. [305](#)). Vous pouvez supprimer une application à partir de l'appareil mobile à l'aide du journal des commandes ou à partir du menu contextuel de l'appareil (cf. section "Suppression de l'application sur l'appareil" à la page [302](#)).

Suppression de l'app de l'appareil

► *Pour supprimer l'app de l'appareil mobile, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, filtrez les appareils MDM iOS par protocole d'administration *MDM iOS*.
3. Sélectionnez l'appareil mobile de l'utilisateur contenant l'app à supprimer.

Vous pouvez sélectionner plusieurs appareils mobiles pour supprimer l'app en même temps.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.
5. Dans la fenêtre **Commandes pour la gestion des appareils mobiles**, ouvrez la section **Supprimer l'app** et cliquez sur le bouton **Envoyer la commande**.

Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant l'option **Toutes les commandes** dans le menu contextuel de cet appareil, puis **Supprimer une app**.

Cette opération ouvre la fenêtre **Suppression des apps** contenant la liste des profils.

6. Dans la liste, sélectionnez l'app que vous devez supprimer de l'appareil mobile. Vous pouvez sélectionner et supprimer plusieurs apps en même temps sur l'appareil. Pour sélectionner une plage d'apps, utilisez la touche **SHIFT**. Pour regrouper plusieurs apps, utilisez la touche **CTRL**.
7. Cliquez sur le bouton **OK** pour envoyer la commande à l'appareil mobile.

Suite à l'exécution de cette commande, l'app sélectionnée sera supprimée de l'appareil mobile de l'utilisateur. Parallèlement, l'état de la commande affichera la valeur *Terminée*.

Le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile.

Le bouton **Annuler** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

Le groupe **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et l'état de leur exécution. Le bouton **Actualiser** permet d'actualiser la liste des commandes.

8. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes de gestion des appareils mobiles**.

Installation de l'app Kaspersky Safe Browser sur l'appareil mobile

► Pour installer l'app Kaspersky Safe Browser sur l'appareil mobile MDM iOS, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

Le dossier **Administration des appareils mobiles** est placé par défaut dans le dossier **Avancé**. La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier **Administration des appareils mobiles**.

2. Sélectionnez l'appareil MDM iOS sur lequel vous devez installer l'app Kaspersky Safe Browser.

Vous pouvez sélectionner plusieurs appareils mobiles pour y installer l'app Kaspersky Safe Browser en même temps.

3. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

4. Dans la fenêtre **Commandes pour l'administration des appareils mobiles**, ouvrez la section **Installer Kaspersky Safe Browser** et cliquez sur le bouton **Envoyer la commande**.

Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant l'option **Toutes les commandes** dans le menu contextuel de cet appareil, puis **Installer Kaspersky Safe Browser**.

Suite à l'exécution de cette commande, l'app Kaspersky Safe Browser sera installée sur l'appareil mobile de l'utilisateur. Parallèlement, l'état de la commande du journal des commandes affiche la valeur *Terminée*.

Le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile. Le bouton **Annuler** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

Le groupe **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et l'état de leur exécution. Le bouton **Actualiser** permet d'actualiser la liste des commandes.

5. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes d'administration des appareils mobiles**.

Des informations sur l'application installée Kaspersky Safe Browser sont affichées dans les propriétés de l'appareil mobile MDM iOS (cf. section "Affichage des informations sur l'appareil MDM iOS" à la p. [305](#)). Vous pouvez supprimer une application à partir de l'appareil mobile à l'aide du journal des commandes ou à partir du menu contextuel de l'appareil (cf. section "Suppression de l'application sur l'appareil" à la page [302](#)).

Affichage des informations sur l'appareil MDM iOS

► *Pour consulter les informations relatives à l'appareil MDM iOS, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, sélectionnez les appareils MDM iOS en cliquant sur le lien **MDM iOS**.
3. Sélectionnez l'appareil mobile dont vous souhaitez consulter les informations.
4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Propriétés**.

Cela ouvre la fenêtre des propriétés de l'appareil MDM iOS.

La fenêtre des propriétés de l'appareil mobile affiche des informations sur l'appareil MDM iOS connecté.

Désactivation de l'administration de l'appareil MDM iOS

► Pour désactiver l'appareil MDM iOS du Serveur MDM iOS, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, sélectionnez les appareils MDM iOS en cliquant sur le lien **MDM iOS**.
3. Sélectionnez l'appareil mobile désiré.
4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Supprimer**.

L'appareil MDM iOS est marqué pour suppression. L'appareil mobile sera automatiquement supprimé de la liste des appareils administrés après sa suppression de la base de données du Serveur MDM iOS. La suppression de l'appareil mobile sur la base de données du Serveur MDM iOS s'effectue en une minute.

Suite de la désactivation de l'administration de l'appareil iOS MDM, tous les profils de configuration installés seront supprimés, ainsi que le profil MDM iOS et toutes les applications pour lesquelles la case **Supprimer en même temps que le profil MDM iOS** avait été cochée (cf. section "**Ajout d'une application administrée**" à la page [300](#)).

Administration des appareils KES

Le Kaspersky Security Center prend en charge les possibilités de gestion des appareils mobiles KES suivantes :

- administrer les appareils KES de façon centralisée à l'aide de commandes (cf. section "Commandes d'administration de l'appareil mobile" à la page [266](#)) ;
- consulter des informations sur les paramètres d'administration des appareils KES (cf. section "Affichage des informations sur l'appareil KES" à la page [309](#)) ;

- installer les applications à l'aide de paquets des applications mobiles (cf. section "Création du paquet des applications mobiles pour les appareils KES" à la page [307](#)) ;
- déconnecter les appareils KES de l'administration (cf. section "Désactivation d'un appareil KES de l'administration" à la page [310](#)).

Pour en savoir plus sur l'utilisation des appareils KES et sur la connexion des appareils KES au Serveur d'administration, consultez le *Manuel d'implantation de Kaspersky Security Center 10*.

Création du paquet des apps mobiles pour les appareils KES

Une licence Kaspersky Endpoint Security 10 for Mobile Devices est indispensable pour la création d'un paquet des applications mobiles destiné aux appareils KES.

► *Pour créer un paquet des applications mobiles, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.

Le dossier **Installation à distance** est placé par défaut dans le dossier **Avancé**.

2. Cliquez sur le bouton **Actions supplémentaires** et, dans la liste affichée, sélectionnez l'option **Administrer les paquets d'apps mobiles**.
3. Dans la fenêtre **Administration des paquets des applications mobiles**, cliquez sur le bouton **Nouveau**.
4. L'Assistant de création du paquet des applications mobiles se lancera. Suivez les instructions de l'Assistant.
5. Si vous voulez placer l'app dans un coffre-fort, cochez la case **Créer un coffre-fort avec l'app sélectionnée** dans la fenêtre de l'Assistant **Paramètres**.

Le paquet des applications mobiles créé s'affiche dans la fenêtre **Administration des paquets des apps mobiles**.

Les conteneurs sont utilisés pour contrôler l'activité des applications lancées sur l'appareil mobile de l'utilisateur. Les règles de la stratégie de sécurité peuvent être appliquées aux applications placées dans le coffre-fort. Les règles pour l'application peuvent être configurées dans la fenêtre des propriétés de la stratégie de l'application Kaspersky Endpoint Security 10 for Mobile Devices dans la section **Conteneurs**. Les informations détaillées sur les coffres-forts et sur leur utilisation sont décrites dans la documentation pour l'application Kaspersky Endpoint Security 10 for Mobile Devices.

Vous pouvez placer une application tierce dans le conteneur. Il est interdit de placer le distributif de Kaspersky Endpoint Security 10 for Mobile Devices dans le coffre-fort.

Activation de l'authentification à deux facteurs des appareils KES

► Pour activer l'authentification à deux facteurs des appareils KES, procédez comme suit :

1. Ouvrez le registre système de l'appareil client sur lequel le Serveur d'administration est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.

2. Rendez-vous dans la section :

- Pour un système de 64 bits :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\
\core\independent\KLLIM
```

- Pour un système de 32 bits :

```
HKLM\Software\KasperskyLab\Components\34\core\independent\KLLIM
```

3. Créez une clé appelée LP_MobileMustUseTwoWayAuthOnPort13292.

4. Définissez le type de clé REG_DWORD.

5. Indiquez la valeur 1 pour la clé.
6. Relancez le service du Serveur d'administration.

Ensuite, une authentification à deux facteurs obligatoire des appareils KES avec utilisation d'un certificat commun sera activée après le lancement du service du Serveur d'administration.

Lors de la première connexion d'un appareil KES au Serveur d'administration, la présence d'un certificat n'est pas obligatoire.

Par défaut, l'authentification à deux facteurs des appareils KES est désactivée.

Affichage des informations sur l'appareil KES

► *Pour consulter les informations relatives à un appareil KES, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, filtrez les appareils KES selon le protocole d'administration *KES*.
3. Sélectionnez l'appareil mobile dont vous souhaitez consulter les informations.
4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Propriétés**.

Cette action entraîne l'ouverture de la fenêtre des propriétés de l'appareil KES.

La fenêtre des propriétés de l'appareil mobile affiche des informations sur l'appareil KES connecté.

Désactivation d'un appareil KES de l'administration

Pour désactiver un appareil KES de l'administration, l'utilisateur doit supprimer l'Agent d'administration de l'appareil mobile concerné. Suite à la suppression de l'Agent d'administration par l'utilisateur, les informations relatives à l'appareil mobile sont supprimées de la base de données du Serveur d'administration. De même, l'administrateur peut supprimer l'appareil mobile de la liste des appareils administrés.

► *Pour supprimer l'appareil KES de la liste des appareils administrés, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, filtrez les appareils KES selon le protocole d'administration *KES*.
3. Sélectionnez l'appareil mobile dont il faut désactiver de l'administration.
4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Supprimer**.

Ainsi, l'appareil mobile sera supprimé de la liste des appareils administrés.

Si Kaspersky Endpoint Security for Android n'est pas supprimé de l'appareil mobile, la prochaine synchronisation avec le Serveur d'administration entraînera la réapparition de cet appareil mobile dans la liste des appareils administrés.

Self Service Portal

Cette section contient des informations sur le Self Service Portal. Cette section contient des informations relatives à l'autorisation d'accès des utilisateurs au Self Service Portal, à la création de comptes utilisateur Self Service Portal et à l'ajout d'appareils mobiles sur le Self Service Portal.

Dans cette section

Présentation du Self Service Portal.....	311
Ajout d'un périphérique.....	314
Connexion de l'utilisateur au Self Service Portal	315

Présentation du Self Service Portal

Le Self Service Portal est un portail Internet qui permet à l'administrateur de déléguer une partie des opérations de gestion des appareils mobiles aux utilisateurs. L'utilisateur ayant obtenu une autorisation d'accès au Self Service Portal peut ajouter lui-même son appareil mobile sur ce portail. Lors de l'ajout d'un appareil mobile, le profil MDM iOS est ajouté à l'appareil MDM iOS, Kaspersky Endpoint Security for Android est installé sur les appareils KES et l'appareil [est soumis aux stratégies de l'entreprise](#) (cf. section "[Ajout d'un appareil](#)" à la page [314](#)). L'appareil mobile devient ainsi un appareil administré.

Le Self Service Portal prend en charge l'autorisation automatique d'accès des utilisateurs à l'aide de Kerberos Constrained Delegation et de l'autorisation de domaine.

Le Self Service Portal prend en charge les appareils mobiles dotés des systèmes d'exploitation iOS et Android.

Sur le Self Service Portal, l'utilisateur peut effectuer les actions suivantes :

- Télécharger l'application sur la boutique d'applications de l'entreprise. Les apps doivent être préalablement ajoutées à la boutique d'apps de l'entreprise dans Kaspersky Security Center 10 Web Console. Pour en savoir plus sur l'ajout d'apps à la boutique d'apps, consultez le *Manuel de l'utilisateur de Kaspersky Security Center 10 Web Console*. Pour télécharger des apps sur le Self Service Portal, l'utilisateur doit sélectionner l'onglet **Apps** dans la fenêtre Self Service Portal.
- Envoyer lui-même des commandes à l'appareil mobile administré, par exemple en cas de vol ou de perte de celui-ci. Pour envoyer une commande, l'utilisateur doit sélectionner l'onglet **Appareils** dans la fenêtre du Self Service Portal. Chaque type d'appareil mobile prend en charge un ensemble spécifique de commandes (cf. tableau ci-dessous).
- Déverrouiller lui-même un appareil mobile à l'aide du lien **Afficher le code de déverrouillage**, en cas de verrouillage de l'appareil mobile.

Tableau 3. Liste des commandes prises en charge

Type d'appareil mobile	Commandes	Résultat de la commande
Appareil MDM iOS	Bloquer	L'appareil mobile est bloqué.
	Restaurer les paramètres par défaut	Toutes les données sont supprimées de l'appareil mobile, ses paramètres reprennent leur configuration d'usine et l'appareil mobile n'est plus administré.
	Supprimer les données corporatives	Suppression des données d'entreprise, du profil MDM iOS et de l'Agent d'administration. L'appareil mobile n'est plus administré.

Type d'appareil mobile	Commandes	Résultat de la commande
Appareil KES	Bloquer	L'appareil mobile est bloqué.
	Restaurer les paramètres par défaut	Toutes les données sont supprimées de l'appareil mobile, ses paramètres reprennent leur configuration d'usine et l'appareil mobile n'est plus administré.
	Supprimer les données corporatives	Suppression des données d'entreprise, du profil MDM iOS et de l'Agent d'administration. L'appareil mobile n'est plus administré.
	Définir l'emplacement	L'appareil mobile est géolocalisé sur une carte Google Maps. L'opérateur de téléphonie mobile facture l'envoi de SMS et l'utilisation d'Internet.
	Emettre un signal sonore	L'appareil mobile émet un signal sonore.
	Photographier	L'appareil mobile est bloqué. Une photographie est prise avec l'appareil photo frontal de l'appareil mobile et enregistrée sur le Serveur d'administration. Les photographies peuvent être consultées dans le journal des commandes du Self Service Portal. L'opérateur de téléphonie mobile facture l'envoi de SMS et l'utilisation d'Internet.

Le Self Service Portal utilise la liste complète des utilisateurs du Kaspersky Security Center. La liste est complétée automatiquement via l'importation depuis Active Directory (cf. section "Affichage et modification des paramètres de sondage des groupes Active Directory" à la page [211](#)) ou manuellement (cf. section "Ajout d'un compte utilisateur" à la page [179](#)).

Si l'autorisation de domaine est interdite par l'administrateur sur le Self Service Portal, les utilisateurs peuvent se servir d'alias. La création de pseudonymes pour obtenir une autorisation d'accès au Self Service Portal est disponible dans les propriétés des comptes des utilisateurs (cf. section "Création d'un compte utilisateur Self Service Portal" à la page [315](#)).

L'administrateur peut attribuer les privilèges suivants aux utilisateurs sur le Self Service Portal :

- Lecture;
- Modification;
- Connexion des nouveaux appareils;
- Envoi uniquement des commandes d'information aux appareils mobiles (qui ne modifient pas l'état de l'appareil mobile) ;

Les commandes **Photographier** et **Définir l'emplacement** sont des commandes d'information.

- Envoi des commandes sur les appareils mobiles.

Ajout d'un appareil

Avant de pouvoir ajouter un appareil mobile sur le Self Service Portal, l'utilisateur doit accepter le Contrat de Licence Utilisateur Final du Self Service Portal et obtenir une autorisation d'accès.

L'algorithme d'ajout d'un appareil mobile d'utilisateur sur le Self Service Portal inclut les étapes suivantes :

1. L'utilisateur ouvre la page principale du portail.
2. Le Self Service Portal crée un paquet d'installation, puis affiche un lien à usage unique pour le téléchargement du paquet et un code QR chiffrant ce lien. L'écran affiche la période de

disponibilité du lien pour le téléchargement du paquet d'installation. Le message contenant le lien pour le téléchargement du paquet d'installation est envoyé à l'utilisateur via email.

Le paquet d'installation est nécessaire pour l'installation de l'Agent d'administration sur l'appareil mobile et l'application de la stratégie d'entreprise.

Il est possible de créer un nouveau paquet d'installation après la suppression du paquet créé précédemment.

3. En cliquant sur le lien **Créer un paquet pour l'installation sur un nouvel appareil**, l'utilisateur accède à la page de téléchargement du paquet d'installation depuis l'appareil mobile qu'il est nécessaire d'ajouter au Self Service Portal.
4. Le Self Service Portal définit le système d'exploitation de l'appareil mobile de l'utilisateur.

Si le système d'exploitation de l'appareil mobile peut être défini automatiquement, la page de téléchargement du paquet d'installation s'ouvre. S'il est impossible de le définir automatiquement, la fenêtre de sélection manuelle du système d'exploitation s'ouvre.

5. L'utilisateur télécharge le paquet d'installation et installe l'Agent d'administration sur l'appareil mobile.
6. Après l'installation de l'Agent d'administration, le périphérique se connecte au Serveur d'administration.

Ainsi, l'appareil mobile est ajouté à la liste des appareils administrés et les stratégies d'entreprise lui sont appliquées. Le lien redirigeant vers les informations relatives à la connexion au Serveur d'administration est envoyé à l'email de l'utilisateur.

Connexion de l'utilisateur au Self Service Portal

Si l'utilisation de l'autorisation de domaine des utilisateurs est interdite dans Self Service Portal, vous pouvez créer des alias utilisateurs (alias accounts) dans la Console d'administration. Les utilisateurs peuvent se servir des alias pour obtenir l'autorisation d'accès au Self Service Portal.

► *Pour connecter l'utilisateur (sous l'alias) au Self Service Portal, procédez comme suit :*

1. Dans le dossier **Administration des appareils mobiles**, choisissez le sous-dossier **Self Service Portal**.
2. Dans l'espace de travail du dossier **Self Service Portal**, cliquez sur le bouton **Envoyer l'invitation de connexion au Self Service Portal**.

Cette opération lancera l'Assistant de connexion de l'utilisateur au Self Service Portal. Suivez les étapes de l'assistant.

3. Dans la fenêtre **Configuration des droits** de l'Assistant, cliquez sur le lien **Configuration** pour configurer les autorisations d'accès au Self Service Portal pour les utilisateurs et les groupes d'utilisateurs.

Si la case **Ne plus afficher ce message** est cochée, la fenêtre **Configuration des droits** ne sera pas affichée au prochain lancement de l'Assistant.

4. La fenêtre **Sélection de l'adresse du Self Service Portal** permet de renseigner l'adresse du Self Service Portal auquel l'utilisateur se connectera.

Vous pouvez ignorer l'étape de la sélection de l'adresse de Self Service Portal. Dans ce cas, il faudra saisir l'adresse du Self Service Portal manuellement dans le texte de l'invitation.

5. Indiquez, dans la fenêtre **Sélection des utilisateurs pour la connexion au Self Service Portal**, les utilisateurs qui il faut connecter au Self Service Portal.
6. Dans la fenêtre de l'Assistant **Configuration des alias de comptes utilisateurs**, configurez l'utilisation des alias et des comptes de domaine des utilisateurs pour la connexion au **Self Service Portal** :

- Cochez la case **Utiliser les alias des comptes utilisateurs pour l'accès au Self Service Portal** afin de configurer l'envoi aux utilisateurs sélectionnés des invitations de connexion au Self Service Portal.

Si la case est décochée, l'invitation pour la connexion au Self Service Portal sera envoyée uniquement aux utilisateurs de domaine choisis à l'étape précédente de l'Assistant.

- Choisissez l'option **Créer des alias pour les utilisateurs qui n'en ont pas** pour que Kaspersky Security Center crée automatiquement les alias pour tous les comptes

utilisateurs qui n'ont pas d'alias. Les invitations pour la connexion au Self Service Portal seront envoyées aux utilisateurs pour lesquels des alias avaient été créés. Kaspersky Security Center ne crée pas d'alias pour les utilisateurs qui en ont déjà.

- Choisissez l'option **Envoyer une invitation sur un compte de domaine aux utilisateurs sans pseudonyme** pour que l'application ne crée pas automatiquement d'alias pour les utilisateurs de domaine qui n'ont pas d'alias. Si l'utilisateur n'a pas d'alias, l'invitation pour la connexion au Self Service Portal sera envoyée sur l'entrée de domaine.
- Cochez la case **Créer de nouveaux mots de passe pour les alias** pour que Kaspersky Security Center crée les mots de passe pour tous les alias (nouveaux et créés antérieurement). Les informations relatives aux mots de passe ancien et nouveau seront envoyées aux utilisateurs dans le texte de l'invitation de connexion au Self Service Portal.

Si la case est décochée, le mot de passe sera généré uniquement pour les alias à nouveau créés.

- Déterminez le nombre de caractères du mot de passe de connexion au Self Service Portal pour les alias des utilisateurs. La longueur par défaut du mot de passe est de 16 caractères.

7. La fenêtre **Envoi des invitations sur Self Service Portal** permet de choisir le mode d'envoi de l'invitation au Self Service Portal aussi bien pour les nouveaux utilisateurs que pour les utilisateurs existants.

8. Cliquez sur le lien **Modifier le message** pour consulter le texte de l'invitation et le modifier le cas échéant.

A l'issue des opérations de l'Assistant, les utilisateurs sélectionnés recevront une invitation avec les informations nécessaires à la connexion au Self Service Portal. Il est possible de créer un nombre illimité d'alias pour le Self Service Portal pour un seul et même utilisateur. Une fois que l'alias a été créé, il s'affiche dans la fenêtre des propriétés du compte utilisateur dans la section **Pseudonymes de l'utilisateur pour Self Service Portal**. Une fois que l'alias de l'utilisateur pour Self Service Portal a été créé, il ne peut plus être modifié. Vous pouvez supprimer l'alias sélectionné en cliquant sur le bouton marqué d'une croix rouge qui se trouve à droite de la liste des alias pour Self Service Portal.

Chiffrement et protection des données

Le chiffrement des données diminue les risques de fuite d'informations en cas de vol ou de perte d'un appareil portable, d'un disque amovible ou d'un disque dur, ou en cas d'accès aux données par des utilisateurs et des applications non autorisés.

La fonction de chiffrement est assurée par l'application Kaspersky Endpoint Security 10 for Windows. Kaspersky Endpoint Security 10 for Windows permet de chiffrer les fichiers enregistrés sur les disques locaux de l'appareil et sur les supports amovibles, ainsi que les disques amovibles et les disques durs entièrement.

La configuration des règles de chiffrement est exécutée à l'aide de Kaspersky Security Center via la définition de stratégies. Le chiffrement et le déchiffrement selon les règles définies sont exécutés lors de l'application de la stratégie.

La disponibilité de la fonctionnalité d'administration du chiffrement est définie par les paramètres de l'interface d'utilisateur (cf. section "Configuration de l'interface" à la page [61](#)).

L'administrateur peut exécuter les actions suivantes :

- configurer et exécuter le chiffrement et le déchiffrement des fichiers sur les disques locaux de l'appareil ;
- configurer et exécuter le chiffrement des fichiers sur les disques amovibles ;
- former les règles d'accès des applications aux fichiers chiffrés ;
- créer et transmettre à l'utilisateur le fichier clé d'accès aux fichiers chiffrés si l'appareil de l'utilisateur a des restrictions de la fonctionnalité de chiffrement des fichiers ;
- configurer et exécuter le chiffrement des disques durs ;
- administrer l'accès des utilisateurs aux disques durs chiffrés et aux disques amovibles (administrer les comptes de l'agent d'authentification, former et transmettre aux utilisateurs les groupes de réponse sur la demande de restauration du nom et du mot de passe du compte utilisateur et les clés d'accès aux appareils chiffrés) ;
- consulter les états de chiffrement et les rapports sur le chiffrement des fichiers.

Ces opérations sont exécutées à l'aide des outils de l'application Kaspersky Endpoint Security 10 for Windows. Les instructions détaillées sur l'exécution des opérations et la description des particularités de fonctionnalité de chiffrement sont décrites dans le *Manuel de l'administrateur de Kaspersky Endpoint Security 10 for Windows*.

Dans cette section

Consultation de la liste des périphériques chiffrés	319
Consultation de la liste des événements de chiffrement	320
Exportation de la liste des événements de chiffrement dans le fichier texte	322
Formation et consultation des rapports sur le chiffrement	322

Consultation de la liste des appareils chiffrés

► *Pour consulter la liste des appareils dont les informations ont été chiffrées, procédez comme suit :*

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console du Serveur d'administration.
2. Passez à la liste des appareils chiffrés à l'aide d'un des moyens suivants :
 - A l'aide du lien **Accéder à la liste des appareils chiffrés** dans le groupe **Administration des appareils chiffrés**.
 - Dans l'arborescence de la console, sélectionnez le dossier joint **Appareils chiffrés**.

Finalement, l'espace de travail reprend les informations sur les appareils présents dans le réseau sur lesquels il y a des fichiers chiffrés et les informations sur les appareils chiffrés au niveau des disques. Après le déchiffrement des informations sur l'appareil, celui-ci sera automatiquement supprimé de la liste.

Vous pouvez trier les informations dans la liste des appareils en ordre croissant ou décroissant à partir de n'importe quel paramètre.

La présence ou l'absence du dossier **Chiffrement et protection des données** dans l'arborescence de la console est définie par les paramètres de l'interface d'utilisateur (cf. section "Configuration de l'interface" à la page [61](#)).

Consultation de la liste des événements du chiffrement

Pendant l'exécution des tâches de chiffrement et de déchiffrement des données sur les appareils, Kaspersky Endpoint Security 10 for Windows envoie dans Kaspersky Security Center les informations sur les événements survenus des types suivants :

- il est impossible de chiffrer/déchiffrer le fichier ou créer l'archive chiffrée à cause de l'insuffisance d'espace sur le disque ;
- il est impossible de chiffrer/déchiffrer le fichier ou créer l'archive chiffrée à cause des problèmes avec la licence ;
- il est impossible de chiffrer/déchiffrer le fichier ou créer l'archive chiffrée à cause de l'absence des privilèges d'accès ;
- l'accès au fichier chiffré est interdit à l'application ;
- les erreurs inconnues.

► *Pour consulter la liste des événements survenus lors du chiffrement des données sur les appareils, procédez comme suit :*

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console du Serveur d'administration.
2. Passez à la liste des événements survenus lors du chiffrement à l'aide d'un des moyens suivants :
 - A l'aide du lien **Accéder à la liste des erreurs** dans le groupe d'administration **Erreurs de chiffrement des données**.
 - Dans l'arborescence de la console, sélectionnez le dossier joint **Événements de chiffrement**.

L'espace de travail reprend enfin les informations sur les problèmes survenus lors du chiffrement des données sur les appareils clients.

Vous pouvez exécuter les actions suivantes avec la liste des événements du chiffrement :

- trier les enregistrements dans l'ordre croissant ou décroissant des données dans n'importe quelle colonne ;
- exécuter la recherche rapide selon les enregistrements (selon la coïncidence de texte avec la sous-ligne dans n'importe quel champ de la liste) ;
- exporter la liste formée des événements dans le fichier texte.

La présence ou l'absence du dossier **Chiffrement et protection des données** dans l'arborescence de la console est définie par les paramètres de l'interface d'utilisateur (cf. section "Configuration de l'interface" à la page [61](#)).

Exportation de la liste des événements du chiffrement dans le fichier texte

► Pour exporter la liste des événements du chiffrement dans un fichier texte, procédez comme suit :

1. Formez la liste des événements du chiffrement (cf. section "Consultation de la liste des événements du chiffrement" à la page [320](#)).
2. Dans le menu contextuel de la liste des événements, sélectionnez l'option **Exporter la liste**.

La fenêtre **Exporter la liste** s'ouvre.

3. Dans la fenêtre **Exporter la liste**, indiquez le nom du fichier texte avec la liste des événements, sélectionnez le dossier dans lequel la liste sera enregistrée et cliquez sur le bouton **Enregistrer**.

La liste des événements du chiffrement sera enregistrée dans le fichier indiqué.

Formation et consultation des rapports sur le chiffrement

L'administrateur peut former les rapports suivants :

- le rapport sur l'état du chiffrement des périphériques de stockage de masse qui contient les informations sur l'état de chiffrement des appareils pour tous les groupes des appareils ;
- le rapport sur les privilèges d'accès aux appareils chiffrés qui contient les informations sur l'état des comptes utilisateurs qui possèdent l'accès aux appareils chiffrés ;
- le rapport sur les erreurs de chiffrement des fichiers et des dossiers qui contient les erreurs survenues lors de l'exécution des tâches de chiffrement et de déchiffrement des données sur les appareils ;

- le rapport sur l'état de chiffrement des appareils administrés qui contient les informations sur la conformité de l'état de chiffrement des appareils à la stratégie de chiffrement ;
- le rapport sur le blocage d'accès aux fichiers qui contient les informations sur le blocage d'accès des apps aux fichiers chiffrés.

► *Pour consulter le rapport sur le chiffrement des appareils, procédez comme suit :*

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
 - A l'aide du lien **Rapport sur le chiffrement des appareils**, lancez l'Assistant de création du modèle du rapport.
 - Sélectionnez le dossier joint **Appareils chiffrés**, puis à l'aide du bouton **Rapport sur le chiffrement des appareils**, lancez l'Assistant de création du modèle du rapport.
3. Suivez les étapes de l'Assistant de création du modèle du rapport.

Dans le nœud **Serveur d'administration** sous l'onglet **Rapports** apparaît un nouveau rapport. Le processus de formation du rapport est lancé. Le rapport s'affichera dans l'espace de travail de l'onglet **Rapports**.

► *Pour consulter le rapport sur les privilèges d'accès aux appareils chiffrés, procédez comme suit :*

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
 - A l'aide du lien **Rapport sur les privilèges d'accès aux appareils chiffrés** dans le groupe **Administration des appareils chiffrés**, lancez l'Assistant de création du modèle du rapport.
 - Sélectionnez le dossier joint **Appareils chiffrés**, puis à l'aide du lien **Rapport sur les privilèges d'accès aux appareils chiffrés**, lancez l'Assistant de création du modèle du rapport.
3. Suivez les étapes de l'Assistant de création du modèle du rapport.

Dans le nœud **Serveur d'administration** sous l'onglet **Rapports** apparaît un nouveau rapport. Le processus de formation du rapport est lancé. Le rapport s'affichera dans l'espace de travail de l'onglet **Rapports**.

► *Pour consulter le rapport sur les erreurs de chiffrement des fichiers et des dossiers, procédez comme suit :*

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
 - A l'aide du lien **Rapport sur les erreurs de chiffrement des dossiers et des fichiers** dans le groupe d'administration **Erreurs de chiffrement des données**, lancez l'Assistant de création du modèle du rapport.
 - Sélectionnez le sous-dossier **Événements de chiffrement**, puis à l'aide du lien **Rapport sur les erreurs de chiffrement des fichiers et des dossiers**, lancez l'Assistant de création du modèle du rapport.
3. Suivez les étapes de l'Assistant de création du modèle du rapport.

Dans l'entrée du Serveur d'administration, sous l'onglet **Rapports**, un nouveau rapport s'affichera. Le processus de formation du rapport est lancé. Le rapport s'affichera dans l'espace de travail de l'onglet **Rapports**.

► *Pour consulter le rapport sur l'état de chiffrement des appareils, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans la zone de travail du groupe, sélectionnez l'onglet **Rapports**.
3. Le bouton **Créer un modèle de rapport** permet de lancer l'Assistant de création du modèle du rapport.

4. Suivez les indices de l'Assistant de création du modèle du rapport. Dans la fenêtre **Sélection du type de modèle de rapport** dans la section **Autre**, sélectionnez l'option **Rapport d'état de chiffrage des appareils**.

A la fin de l'Assistant de création du modèle du rapport, un nouveau modèle de rapport apparaîtra dans l'entrée Serveur d'administration sous l'onglet **Rapports**.

5. Dans l'entrée du Serveur d'administration requis, sous l'onglet **Rapports**, choisissez le modèle de rapport créé aux étapes antérieures.

Le processus de formation du rapport est lancé. Le rapport s'affichera dans l'espace de travail de l'onglet **Rapports**.

Les informations sur la conformité des états de chiffrage des appareils et des disques amovibles à la stratégie de chiffrage sont aussi consultables dans les panneaux d'information sous l'onglet **Statistiques** de l'entrée Serveur d'administration (cf. section "Travailler avec les données statistiques" à la page [194](#)).

► *Pour consulter le rapport sur le blocage d'accès aux fichiers, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans la zone de travail du groupe, sélectionnez l'onglet **Rapports**.
3. Le bouton **Créer un modèle de rapport** permet de lancer l'Assistant de création du modèle du rapport.
4. Suivez les indices de l'Assistant de création du modèle du rapport. Dans la fenêtre **Sélection du type de modèle de rapport** dans la section **Autre**, sélectionnez l'option **Rapport sur le blocage d'accès aux fichiers**.

A la fin de l'Assistant de création du modèle du rapport, un nouveau modèle de rapport apparaîtra dans l'entrée **Serveur d'administration** sous l'onglet **Rapports**.

5. Dans l'entrée **Serveur d'administration**, sous le signets **Rapports**, choisissez le modèle du rapport créé aux étapes antérieures.

Le processus de formation du rapport est lancé. Le rapport s'affichera dans l'espace de travail de l'onglet **Rapports**.

Inventaire du matériel détecté dans le réseau

Kaspersky Security Center obtient les informations sur le matériel détecté suite au sondage du réseau. Tout matériel connecté au réseau de l'entreprise est soumis à l'inventaire. A chaque sondage du réseau, les informations sur le matériel sont mises à jour. La liste du matériel détecté peut contenir les types suivants des appareils :

- Appareils ;
- appareils mobiles ;
- périphériques réseau ;
- appareils virtuels ;
- modules d'ordinateur ;
- périphérie d'ordinateur ;
- appareils connectés ;
- téléphonie VoIP ;
- stockages réseau.

Le matériel détecté durant le sondage du réseau s'affiche dans le dossier **Stockages** placé dans le dossier **Matériel** de l'arborescence de la console.

L'administrateur peut manuellement ajouter les nouveaux appareils à la liste du matériel ou modifier les informations sur le matériel déjà présent dans le réseau. Il est possible de consulter et de modifier les informations détaillées sur les appareils dans les propriétés de l'appareil.

L'administrateur peut attribuer l'indice "Matériel corporatif" aux appareils détectés. Cet indice peut être manuellement attribué dans les propriétés de l'appareil ou définir les critères pour son attribution automatique. Dans ce cas, l'indice "Matériel corporatif" est attribué selon le type

d'appareil. A l'aide de l'indice "Matériel corporatif", il est possible d'autoriser ou d'interdire la connexion du matériel au réseau.

Kaspersky Security Center permet d'exécuter l'amortissement du matériel. Pour ce faire, il faut cocher la case **L'appareil est retiré du service** dans les propriétés de l'appareil. Un tel appareil ne s'affiche pas dans la liste du matériel.

Dans cette section

Ajout d'informations sur les nouveaux périphériques.....	327
Configuration des critères de définition des périphériques corporatifs.....	328

Ajout d'informations sur les nouveaux appareils

► *Pour ajouter les informations sur les nouveaux appareils dans le réseau, procédez comme suit :*

1. Dans l'arborescence de la console **Stockages**, sélectionnez le dossier joint **Matériel**.
2. Dans l'espace de travail du dossier **Matériel** à l'aide du bouton **Ajouter un appareil**, ouvrez la fenêtre **Nouvel appareil**.

La fenêtre **Nouvel appareil** s'ouvre.

3. Dans la fenêtre **Nouvel appareil** dans la liste déroulante **Type**, sélectionnez le type d'appareil que vous voulez ajouter.
4. Cliquez sur le bouton **OK**.

La fenêtre des propriétés de l'appareil dans la section **Général** s'ouvre.

5. Dans la section **Général**, remplissez les champs de saisie par les données sur l'appareil. Les paramètres suivants sont disponibles dans la section **Général** :

- **Appareil d'entreprise.** Cochez la case si vous voulez attribuer l'indice "Corporatif" à l'appareil. Selon cet indice, il est possible d'exécuter la recherche d'appareils dans le dossier **Matériel**.
- **L'appareil est retiré du service.** Cochez la case si vous ne voulez pas afficher l'appareil dans la liste des appareils dans le dossier **Matériel**.

6. Cliquez sur le bouton **Appliquer**.

Le nouvel appareil s'affiche dans l'espace de travail du dossier **Matériel**.

Configuration des critères de définition des appareils d'entreprise

► *Pour configurer les critères de définition des appareils d'entreprise, procédez comme suit :*

1. Dans l'arborescence de la console **Stockages**, sélectionnez le dossier joint **Matériel**.
2. Dans l'espace de travail du dossier **Matériel** à l'aide du lien **Configurer les critères de définition des appareils de l'entreprise**, ouvrez la fenêtre des propriétés du matériel.
3. Dans la fenêtre des propriétés du matériel dans la section **Appareils d'entreprise**, sélectionnez le mode d'attribution de l'indice "Corporatif" :
 - **Etablir manuellement la caractéristique "D'entreprise" pour l'appareil.** L'indice "Appareil corporatif" est attribué à l'appareil manuellement dans la fenêtre des propriétés de l'appareil dans la section **Général**.
 - **Etablir automatiquement la caractéristique "D'entreprise" pour l'appareil.** Dans le groupe des paramètres **Selon le type d'appareil**, indiquez les types des appareils auxquels l'application va automatiquement attribuer l'indice "Corporatif".
4. Cliquez sur le bouton **Appliquer**.

Mise à jour des bases de données et des modules d'application

Cette section décrit le téléchargement et la diffusion des mises à jour des bases de données et des modules d'application à l'aide de Kaspersky Security Center.

Pour maintenir le système de protection, il faut opportunément actualiser les bases et les modules des applications Kaspersky Lab administrés à l'aide de Kaspersky Security Center.

Pour actualiser les bases de données et les modules des applications Kaspersky Lab administrés à l'aide de Kaspersky Security Center, la tâche du Serveur d'administration **Téléchargement des mises à jour dans le stockage** est utilisée. Suite à l'exécution de la tâche, les bases et les mises à jour des modules de l'application sont téléchargées sur le Serveur d'administration depuis la source des mises à jour.

La tâche **Téléchargement des mises à jour dans le stockage** n'est pas disponible sur les Serveurs d'administration virtuels. Les mises à jour téléchargées sur le Serveur d'administration principal s'affichent dans le stockage du Serveur virtuel.

Vous pouvez configurer l'analyse des mises à jour reçues sur la productivité et sur la présence des erreurs avant l'installation sur les appareils clients.

Pour permettre le téléchargement des versions nécessaires des bases et des modules de l'application, les informations suivantes sont automatiquement transmises aux serveurs de mise à jour de Kaspersky Lab lors de l'exécution de la tâche **Téléchargement des mises à jour dans le stockage** :

- identifiant et version de l'application ;
- identifiant de l'installation de l'application ;
- identifiant de la clé active ;
- identifiant du lancement de la tâche **Téléchargement des mises à jour dans le stockage**.

Les informations transmises ne contiennent aucune donnée personnelle ou autre donnée confidentielle. AO Kaspersky Lab protège les informations obtenues conformément aux exigences définies par la loi.

Dans cette section

Création d'une tâche de téléchargement des mises à jour dans le stockage	330
Création d'une tâche de téléchargement des mises à jour dans les stockages des agents de mises à jour	332
Configuration des paramètres de la tâche de téléchargement des mises à jour dans le stockage.....	333
Analyse des mises à jour récupérées.....	333
Configuration des stratégies de vérification et des tâches auxiliaires	336
Affichage des mises à jour récupérées.....	337
Déploiement de mises à jour automatique.....	338
Annulation des mises à jour installées.....	346

Création d'une tâche de téléchargement des mises à 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**.
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**, sélectionnez l'option **Créer → Tâche**.
 - A l'aide du bouton **Créer 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 stockage**, les mises à jour des bases et des modules des applications sont copiées depuis la source définie vers le dossier partagé. Si une tâche est créée pour un groupe d'administration, elle est diffusée uniquement aux agents d'administration inclus dans le groupe d'administration indiqué.

Les mises à jour du dossier partagé sont diffusées sur les appareils 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'appareil 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.

Création d'une tâche de téléchargement des mises à jour dans les stockages des agents de mises à jour

► *Pour créer la tâche de téléchargement des mises à jour dans le stockage des agents de mises à jour pour le groupe d'administration sélectionné, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. A l'aide du bouton **Créer une tâche** dans l'espace de travail du dossier, lancez l'Assistant de création de la tâche.
3. Dans la fenêtre **Type de tâche** de l'Assistant de création de la tâche, sélectionnez le nœud **Serveur d'administration de Kaspersky Security Center 10**, déployez le dossier **Avancé** et sélectionnez la tâche **Téléchargement forcé des mises à jour dans les stockages des agents de mises à jour**.
4. Suivez les étapes de l'assistant.

Une fois l'Assistant de création de la tâche terminé, le **Téléchargement forcé des mises à jour dans les stockages des agents de mises à jour** apparaîtra dans la liste des tâches de l'Agent d'administration dans le groupe d'administration correspondant et dans le dossier **Tâches**.

Suite à l'exécution de la tâche **Téléchargement forcé des mises à jour dans les stockages des agents de mises à jour**, les mises à jour des bases de données et des modules des applications sont copiées depuis la source de mises à jour et placées dans le dossier partagé. Les résultats de l'exécution de la tâche seront utilisés uniquement par les agents de mises à jour faisant partie

du groupe d'administration indiqué pour lesquels il n'y a pas la tâche précise du Serveur d'administration **Téléchargement des mises à jour dans le stockage**.

Configuration des paramètres de la tâche de téléchargement des mises à jour dans le stockage

► *Pour configurer les paramètres de la tâche de téléchargement des mises à jour dans le stockage, procédez comme suit :*

1. Dans l'espace de travail du dossier de l'arborescence de la console **Tâches**, 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.

Finalement, la fenêtre des propriétés de la tâche **Téléchargement des mises à jour dans le stockage** s'ouvrira. Cette fenêtre permet de configurer les paramètres de téléchargement des mises à jour dans le stockage du Serveur d'administration.

Analyse des mises à jour récupérées

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

1. Dans la zone de travail du dossier **Tâches** 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 ouverte des propriétés des tâches dans la section **Vérification des mises à jour**, cochez la case **Vérifier les mises à jour avant de les déployer** et sélectionnez la tâche d'analyse des mises à jour à l'aide d'un des moyens suivants :
 - Cliquez sur le bouton **Sélectionner** pour sélectionner une tâche d'analyse des mises à jour déjà créée.
 - Cliquez sur le bouton **Créer** pour créer une tâche d'analyse des mises à jour.

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

Lors de la création de la tâche d'analyse des mises à jour, il faut sélectionner le groupe d'administration sur les appareils depuis lesquels la tâche sera exécutée. Les appareils de ce groupe sont appelés *appareils d'essai*.

Pour les appareils d'essai, il est recommandé d'utiliser des appareils 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 appareils d'essai, la tâche d'analyse 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 stockage 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 stockage temporaire vers le dossier partagé du Serveur d'administration (<Dossier d'installation Kaspersky Security Center>\Share\Updates), puis seront diffusées vers les appareils clients pour lesquels le Serveur d'administration est une source de mise à jour.

Si, à la fin de la tâche d'analyse 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 une des conditions suivantes est remplie sur au moins un appareil d'essai :

- 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 de protection 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 appareils d'essai, alors les mises à jour sont considérées comme correctes et la tâche d'analyse des mises à jour a réussi.

Configuration des stratégies de vérification et des tâches auxiliaires

Lors de la création d'une tâche d'analyse des mises à jour, le Serveur d'administration crée des stratégies de vérification, ainsi que des tâches de groupe auxiliaires de mise à jour et d'analyse à la demande.

L'exécution des tâches de groupe auxiliaires de mise à jour et de l'analyse à la demande prend un certain temps. Ces tâches sont exécutées dans le cadre d'exécution de la tâche d'analyse des mises à jour. La tâche d'analyse des mises à jour est exécutée dans le cadre d'exécution de la tâche de téléchargement des mises à jour dans le stockage. Le temps d'exécution de la tâche de téléchargement des mises à jour dans le stockage inclut le temps d'exécution des tâches de groupe auxiliaires de mise à jour et de l'analyse à la demande.

Vous pouvez modifier les paramètres des stratégies de vérification et des tâches auxiliaires.

► *Pour modifier les paramètres de la stratégie de vérification ou de la tâche auxiliaire, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe pour lequel la tâche d'analyse des mises à jour sera formée.
2. L'espace de travail permet de sélectionner un des onglets suivants :
 - **Stratégies** si vous voulez modifier les paramètres de la stratégie de vérification ;
 - **Tâches** si vous voulez modifier les paramètres de la tâche auxiliaire.
3. Dans l'espace de travail de l'onglet, sélectionnez la stratégie ou la tâche les paramètres de laquelle vous voulez modifier.
4. Ouvrez la fenêtre des propriétés de cette stratégie (tâche) à l'aide d'un des moyens suivants :
 - Dans le menu contextuel de la stratégie (tâche), sélectionnez l'option **Propriétés**.
 - A l'aide du lien **Modifier les paramètres de la stratégie (Modifier les paramètres de la tâche)** dans le groupe de travail avec la stratégie (la tâche) sélectionnée.

Pour que l'analyse des mises à jour soit exécutée correctement, il faut suivre les restrictions suivantes sur la modification des paramètres des stratégies de vérification et des tâches auxiliaires :

- Dans les paramètres des tâches auxiliaires :
 - Enregistrer sur le Serveur d'administration tous les événements correspondant aux niveaux d'importance **Événement critique** et **Erreur de fonctionnement**. Sur la base des événements de ce type, le Serveur d'administration analyse le fonctionnement des applications.
 - Utiliser le Serveur d'administration en tant que source des mises à jour.
 - Définir le type de programmation des tâches : **Mode manuel**.
- Dans les paramètres des stratégies de vérification :
 - Ne pas utiliser les technologies iChecker, iSwift et iStream d'accélération de l'analyse.
 - Sélectionner l'action sur les objets infectés : **Ne pas requérir / Laisser passer / Enregistrer les données dans le rapport**.
- Dans les paramètres des stratégies de vérification et des tâches auxiliaires :

Si le redémarrage de l'appareil est requis après l'installation des mises à jour des modules logiciels, il faut l'exécuter sans attendre. Si l'appareil n'est pas redémarré, il sera impossible de vérifier ce type de mise à jour. Pour certaines applications, l'installation de mises à jour qui requièrent un redémarrage peut être interdites ou réalisées uniquement après confirmation de l'utilisateur. Ces restrictions doivent être désactivées dans les paramètres des stratégies de vérification et des tâches auxiliaires.

Affichage des mises à jour récupérées

► *Pour consulter la liste des mises à jour reçues,*

dans l'arborescence de la console du dossier **Stockages**, sélectionnez le sous-dossier **Mises à jour et correctifs de Kaspersky Lab**.

L'espace de travail du dossier **Mises à jour et correctifs de Kaspersky Lab** présente la liste des mises à jour enregistrées sur le Serveur d'administration.

Déploiement de mises à jour automatique

Kaspersky Security Center permet de diffuser et d'installer automatiquement les mises à jour sur les appareils clients et sur les Serveurs d'administration secondaires.

Dans cette section

Déploiement automatique des mises à jour sur les appareils clients	338
Redistribution automatique des mises à jour sur les Serveurs d'administration secondaires ...	340
Installation automatique des mises à jour des modules d'application des Agents d'administration.....	341
Désignation d'appareils comme agents de mises à jour	342
Suppression d'un appareil de la liste des agents de mises à jour	344
Récupération des mises à jour par les agents de mises à jour	345

Déploiement automatique des mises à jour sur les appareils clients

► Pour que les mises à jour de l'application sélectionnée se diffusent automatiquement sur les appareils 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 administre les appareils clients.
2. Créez une tâche de diffusion des mises à jour de cette application pour les appareils clients sélectionnées par un des moyens suivants :
 - S'il faut diffuser les mises à jour sur les appareils clients qui font partie du groupe d'administration sélectionné, créez une tâche pour le groupe sélectionné (cf. section "Création d'une tâche de groupe" à la page [135](#)).
 - S'il faut diffuser les mises à jour sur les appareils clients qui font partie des différents groupes d'administration ou non, créez une tâche pour un ensemble d'appareils (cf. section "Création d'une tâche pour un ensemble d'appareils" à la page [137](#)).

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**, dépend 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 **Programmation** dans le champ **Programmation**, sélectionnez l'option de lancement **Lors du téléchargement des mises à jour dans le stockage**.

Ainsi, la tâche de diffusion des mises à jour créée sera lancée pour les appareils 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 appareils sélectionnés et que vous souhaitez une diffusion automatique des mises à jour sur les appareils clients, ouvrez la fenêtre des propriétés de la tâche et, dans la section **Programmation**, sélectionnez l'option de lancement **Lors du téléchargement des mises à jour dans le stockage** dans le champ **Programmation**.

Redistribution automatique des mises à jour sur les Serveurs d'administration secondaires

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

1. Dans l'arborescence de la console dans l'entrée du Serveur d'administration principal, sélectionnez le dossier **Tâches**.
2. Dans la liste des tâches de l'espace de travail, sélectionnez la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration.
3. Ouvrez la section **Paramètres** de la fenêtre des propriétés de la tâche sélectionnée via l'un des moyens suivants :
 - Dans le menu contextuel de la tâche, sélectionnez l'option **Propriétés**.
 - A l'aide du lien **Modifier les paramètres** dans le groupe d'utilisation de la tâche sélectionnée.
4. Dans la section **Paramètres** de la fenêtre de la tâche, ouvrez la fenêtre **Autres paramètres** à l'aide du lien **Personnaliser** dans la sous-section **Autres paramètres**.
5. Dans la fenêtre ouverte **Autres paramètres**, cochez la case **Forcer la mise à jour des serveurs secondaires**.

Dans les paramètres de la tâche de récupération des mises à jour par le Serveur d'administration, sous l'onglet **Paramètres** de la fenêtre des propriétés de la tâche, cochez la case **Forcer la mise à jour des Serveurs secondaires**.

Immédiatement après la réception des mises à jour par le Serveur d'administration principal, des tâches de téléchargement des mises à jour par les Serveurs d'administration secondaires seront automatiquement lancées, indépendamment de la programmation prévue dans la configuration de ces tâches.

Installation automatique des mises à jour des modules d'application des Agents d'administration

► *Pour que les mises à jour des modules d'applications des Agents d'administration s'installent automatiquement après leur téléchargement dans le stockage du Serveur d'administration, procédez comme suit :*

1. Dans l'arborescence de la console dans l'entrée du Serveur d'administration principal, sélectionnez le dossier **Tâches**.
2. Dans la liste des tâches dans l'espace de travail, sélectionnez la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration.
3. Ouvrez la fenêtre des propriétés de la tâche sélectionnée 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** dans le groupe d'utilisation de la tâche sélectionnée.
4. Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Paramètres**.
5. Cliquez sur le lien **Personnaliser** du groupe **Autres paramètres** pour ouvrir la fenêtre **Autres paramètres**.

6. Dans la fenêtre ouverte **Autres paramètres**, cochez la case **Actualiser les modules des Agents d'administration**.

Si la case est cochée, la mise à jour des modules logiciels de l'Agent d'administration seront installés automatiquement après leur chargement dans le stockage du Serveur d'administration. Quand la case est décochée, l'installation automatique des mises à jour de l'Agent d'administration n'a pas lieu. Les mises à jour récupérées peuvent être installées manuellement. Par défaut, la case est cochée.

L'installation automatique des modules logiciels des Agents d'administration est disponible uniquement pour les Agents d'administration de la version 10 Service Pack 1 et versions inférieures.

7. Cliquez sur le bouton **OK**.

Les mises à jour des modules logiciels des Agents d'administration seront donc installés automatiquement.

Désignation d'appareils comme agents de mises à jour

Kaspersky Security Center permet de désigner des appareils comme agents de mises à jour. La désignation peut être effectuée automatiquement (à l'aide du Serveur d'administration) et manuellement.

Si la structure des groupes d'administration reflète la topologie du réseau ou si des parties séparées du réseau correspondent à un groupe d'administration, il est possible d'utiliser la désignation automatique des agents de mises à jour.

Si la composition de la structure des groupes d'administration ne reflète pas la topologie du réseau, il est recommandé de désactiver la désignation automatique des agents de mises à jour et, dans chaque partie séparée du réseau, de désigner manuellement un ou plusieurs appareils comme agents de mises à jour.

Il est recommandé de désigner des agents de mises à jour manuellement avec une proportion de 100 à 200 appareils desservis par agent de mises à jour.

► *Pour désigner manuellement un appareil en tant qu'agent de mises à jour, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
2. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.
3. Dans la fenêtre de propriétés du Serveur d'administration, sélectionnez la section **Agents de mises à jour** et cliquez sur le bouton **Ajouter**.

Suite à cette action, la fenêtre **Ajout d'un agent de mises à jour**.

4. Dans la fenêtre **Ajout d'un agent de mises à jour**, procédez comme suit :
 - a. Sélectionnez l'appareil qui jouera le rôle d'agent de mises à jour (sélectionnez-le dans le groupe d'administration ou indiquez l'adresse IP de l'appareil). Lors de la sélection de l'appareil, prenez en compte les particularités de fonctionnement des agents de mises à jour et les exigences pour l'appareil qui joue le rôle d'agent de mises à jour (cf. section "Agent de mises à jour" à la page [89](#)).
 - b. Indiquez un ensemble d'appareils sur lesquels l'agent de mises à jour diffusera les mises à jour. Vous pouvez indiquer un groupe d'administration ou le sous-réseau Network Location Awareness (NLA).
5. Cliquez sur le bouton **OK**.

L'agent de mises à jour ajouté s'affiche dans la liste d'agents de mises à jour, dans la section **Agents de mises à jour**.

6. Sélectionnez l'agent de mises à jour dans la liste et, via le bouton **Propriétés**, ouvrez la fenêtre de ses propriétés.
7. Configurez les paramètres de l'agent de mises à jour dans la fenêtre des propriétés :
 - Dans la section **Général**, indiquez le numéro de port SSL (diffusion), l'adresse et le numéro du port IP pour une diffusion sur plusieurs adresses IP, ainsi que le contenu des données diffusées par l'agent de mises à jour (celui-ci peut diffuser des mises à jour et/ou des paquets d'installation).
 - Dans la section **Zone d'action**, indiquez la zone sur laquelle l'agent de mises à jour diffuse les mises à jour (groupes d'administration et/ou sous-réseau NLA).

- Dans la section **Sondage du réseau**, configurez les paramètres de sondage par l'agent de mises à jour des domaines Windows, Active Directory et des plages IP.
- Dans la section **Avancé**, indiquez le dossier que l'agent de mises à jour doit utiliser pour l'enregistrement des données diffusées.

Suite à cette action, les appareils sélectionnés joueront le rôle d'agents de mises à jour.

► *Pour désigner des agents de mises à jour automatiquement à l'aide du Serveur d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
2. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.
3. Dans la fenêtre de propriétés du Serveur d'administration, dans la section **Agents de mises à jour**, cochez la case **Désigner automatiquement des agents de mises à jour**.

Si la désignation automatique des appareils comme agents de mises à jour est activée, il est impossible de configurer manuellement les paramètres des agents de mises à jour, ainsi que de modifier la liste de ces agents.

4. Cliquez sur le bouton **OK**.

Suite à cette action, le Serveur d'administration désignera les agents de mises à jour et configurera leurs paramètres, le tout automatiquement.

Suppression d'un appareil de la liste des agents de mises à jour

► *Pour supprimer un appareil de la liste d'agents de mises à jour, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
2. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.
3. Dans la fenêtre de propriétés du Serveur d'administration, dans la section **Agents de mises à jour** sélectionnez l'appareil qui remplit les fonctions d'agent de mises à jour et cliquez sur **Supprimer**.

Suite à cette action, l'appareil est supprimé de la liste d'agents de mises à jour et arrête de remplir les fonctions d'agent de mises à jour.

Il est impossible de supprimer un appareil de la liste d'agents de mises à jour s'il a été désigné par le Serveur d'administration automatiquement (cf. section "Désignation d'appareils comme agents de mises à jour" à la page [342](#)).

Récupération des mises à jour par les agents de mises à jour

Kaspersky Security Center permet aux agents de mises à jour d'obtenir des mises à jour à partir du Serveur d'administration, des serveurs Kaspersky Lab, du dossier local ou réseau.

- ▶ *Pour configurer l'obtention des mises à jour pour l'agent de mises à jour, procédez comme suit :*
 1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
 2. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.
 3. Dans la fenêtre des propriétés du Serveur d'administration, dans la section **Agents de mises à jour**, sélectionnez l'agent de mises à jour via lequel les mises à jour seront livrées sur les appareils clients.
 4. Via le bouton **Propriétés**, ouvrez la fenêtre de propriétés de l'agent de mises à jour sélectionné.
 5. Sélectionnez la section **Source de mises à jour** dans la fenêtre des propriétés de l'agent.
 6. Sélectionnez la source de mises à jour pour l'agent de mises à jour :
 - Pour que l'agent de mises à jour obtienne les mises à jour à partir du Serveur d'administration, sélectionnez l'option **Obtenir à partir du Serveur d'administration**.
 - Pour que l'agent de mises à jour obtienne les mises à jour à l'aide d'une tâche, sélectionnez l'option **Utiliser la tâche d'obtention des mises à jour**:
 - Cliquez sur le bouton **Sélectionner** pour sélectionner une tâche déjà formée de récupération des mises à jour par l'agent de mises à jour.
 - Cliquez sur le bouton **Nouvelle tâche** pour créer une tâche de récupération des mises à jour par l'agent de mises à jour.

La tâche d'obtention des mises à jour par l'agent de mises à jour est une tâche locale. Chaque appareil remplissant le rôle d'agent de mises à jour exige que la tâche d'obtention des mises à jour soit créée individuellement.

Suite à cette action, l'agent de mises à jour obtient des mises à jour à partir de la source indiquée.

Annulation des mises à jour installées

► *Pour annuler les mises à jour installées, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Mises à jour du logiciel**.
2. Dans l'espace de travail du dossier **Mises à jour du logiciel**, sélectionnez la mise à jour à annuler.
3. Dans le menu contextuel de la mise à jour, sélectionnez **Supprimer les fichiers des mises à jour**.
4. Lancez la tâche de mise à jour (cf. section "Installation automatique des mises à jour pour Kaspersky Endpoint Security sur les appareils" à la page [239](#)).

Suite à l'exécution de cette tâche, la mise à jour installée sur l'appareil client sera annulée et présentera l'état **Non installé**.

Travail avec les clés des applications

Cette section décrit les possibilités de Kaspersky Security Center sur l'utilisation des clés des applications administrées de Kaspersky Lab.

Kaspersky Security Center permet de diffuser de manière centralisée les clés des applications de Kaspersky Lab sur les appareils clients, suivre l'utilisation des clés et de prolonger la durée de validité des licences.

Lors de l'ajoute de la clé à l'aide de Kaspersky Security Center, les propriétés de la clé sont enregistrées sur le Serveur d'administration. Sur la base de ces informations, l'application crée un rapport sur les clés utilisées et notifie l'administrateur de l'expiration des licences et du dépassement des restrictions de licence énoncées dans les propriétés des clés. Vous pouvez configurer les paramètres de notifications sur l'utilisation des clés dans la composition des paramètres du Serveur d'administration.

Dans cette section

Consultation des informations sur les clés utilisées	348
Ajout de la clé dans le stockage du Serveur d'administration	349
Suppression de la clé du Serveur d'administration.....	349
Diffusion des clés sur les appareils clients.....	350
Diffusion automatique de la clé.....	350
Création et consultation du rapport d'utilisation des clés	351

Consultation des informations sur les clés utilisées

► Pour consulter les informations sur les clés utilisées,

dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Licences pour les logiciels de Kaspersky Lab**.

L'espace de travail du dossier affiche la liste des clés utilisées sur les appareils clients.

A côté de chaque clé, une icône, correspondant au type de son utilisation, s'affiche :

-  : l'information sur la clé utilisée est reçue depuis l'appareil client connecté au Serveur d'administration. Le fichier de cette clé n'est pas enregistré sur le Serveur d'administration.
-  : le fichier clé se trouve dans le stockage du Serveur d'administration. La diffusion automatique de cette clé est désactivée.
-  : le fichier clé se trouve dans le stockage du Serveur d'administration. La diffusion automatique de cette clé est activée.

Vous pouvez consulter des informations sur les clés utilisées pour l'application sur l'appareil client dans la section **Applications** de la fenêtre de propriétés de l'appareil client (cf. section "Consultation et modifications des paramètres locaux de l'application" à la page [147](#)).

Pour déterminer les paramètres actuels des clés du Serveur d'administration virtuel, le Serveur d'administration envoie la requête sur les serveurs d'activation de Kaspersky Lab au moins une fois par jour.

Ajout de la clé dans le stockage du Serveur d'administration

► *Pour ajouter une clé dans le stockage du Serveur d'administration, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Licences pour les logiciels de Kaspersky Lab**.
2. Lancez la tâche d'ajout de la clé à l'aide d'un des moyens suivants :
 - dans le menu contextuel de la liste des clés, sélectionnez l'option **Ajouter une clé** ;
 - à l'aide du lien **Ajouter une clé** dans le groupe d'administration de la liste des clés.

Finalement l'Assistant d'ajout d'une clé est lancé. Suivez les instructions de l'Assistant.

Suppression de la clé du Serveur d'administration

► *Pour supprimer une clé du Serveur d'administration, procédez comme suit :*

1. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.
2. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, sélectionnez la section **Clés**.
3. Supprimez la clé active ou complémentaire en cliquant sur le bouton **Supprimer**.

La clé sera supprimée.

Si une clé additionnelle a été ajoutée, la clé additionnelle devient automatiquement active à l'expiration de la clé active.

Une fois la clé active du Serveur d'administration supprimée, les fonctions suivantes ne sont plus accessibles : **Administration système** (cf. section "**Options de licence de Kaspersky Security Center**" à la page [68](#)) et **Administration des périphériques mobiles** (cf. section "**Options**

de licence de Kaspersky Security Center" à la page [68](#)). Il est possible de rétablir la clé supprimée ou d'ajouter une autre clé (cf. section "Ajout de la clé dans le stockage du Serveur d'administration" à la page [349](#)).

Diffusion des clés sur les appareils clients

Kaspersky Security Center permet de diffuser la clé sur les appareils clients à l'aide de la tâche de diffusion de la clé.

► *Afin de diffuser une clé sur les appareils clients, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Licences pour les logiciels de Kaspersky Lab**.
2. Cliquez sur le bouton **Diffuser la clé sur les appareils administrés** dans le groupe d'administration de la liste des clés.

Finalement, l'Assistant de création de la tâche de diffusion de la clé sera lancé. Suivez les instructions de l'Assistant.

Les tâches créées à l'aide de l'Assistant de création de la tâche de diffusion de la clé sont des tâches pour des ensembles d'appareils situées dans le dossier **Tâches** de l'arborescence de console.

Vous pouvez aussi créer une tâche de groupe ou une tâche locale de diffusion de la clé à l'aide de l'Assistant de création de la tâche pour le groupe d'administration et pour l'appareil client.

Diffusion automatique de la clé

Kaspersky Security Center permet de diffuser automatiquement sur les appareils administrés les clés placées dans le stockage des clés sur le Serveur d'administration.

► *Afin de diffuser automatiquement une clé sur les appareils administrés, procédez comme suit :*

1. Dans l'arborescence de la console du dossier **Administration des applications**, sélectionnez le sous-dossier **Licences pour les logiciels de Kaspersky Lab**.
2. Dans l'espace de travail du dossier, sélectionnez la clé que vous souhaitez diffuser automatiquement sur l'appareil.
3. Ouvrez la fenêtre des propriétés de la clé sélectionnée à l'aide d'un des moyens suivants :
 - dans le menu contextuel de la clé, sélectionnez l'option **Propriétés** ;
 - à l'aide du lien **Consulter les propriétés de la clé** dans le groupe de travail avec la clé sélectionnée.
4. Dans la fenêtre ouverte des propriétés de la clé, cochez la case **Clé diffusée automatiquement**. Fermez la fenêtre des propriétés de la clé.

Suite à cette action, la clé sera diffusée automatiquement en qualité de clé active ou complémentaire sur les appareils auxquels elle convient.

La diffusion de la clé est exécutée via les moyens de l'Agent d'administration. Avec cela les tâches auxiliaires de diffusion de la clé pour l'application ne se forment pas.

Lors de la diffusion automatique de la clé en qualité de clé active ou additionnelle, la restriction de licence sur le nombre d'appareils énoncée dans les propriétés de la clé est prise en compte. Si la limite liée à la restriction de licence est atteinte, la diffusion de la clé sur les appareils s'arrête automatiquement.

Création et consultation du rapport d'utilisation des clés

► *Pour créer le rapport sur les clés utilisées sur les appareils clients, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans la zone de travail du groupe, sélectionnez l'onglet **Rapports**.
3. Choisissez le modèle du rapport **Rapport sur l'utilisation des clés** ou créez un modèle de rapport du même type.

Ainsi, l'espace de travail du rapport sur les clés utilisées affichera les informations sur les clés actives et additionnelles utilisées sur les appareils clients. Le rapport contient aussi les informations sur les appareils sur lesquels les clés sont utilisées, ainsi que les informations sur les restrictions définies dans les paramètres des clés.

Stockages des données

Cette section contient les informations sur les données enregistrées sur le Serveur d'administration et utilisées pour suivre les états des appareils clients et leur service.

Les données, utilisées pour surveiller l'état des appareils clients et leur service s'affichent dans le dossier de l'arborescence de la console **Stockages**.

Le dossier **Stockages** contient les objets suivants :

- les mises à jour, reçues par le Serveur d'administration, qui se diffusent sur les appareils clients (cf. section "Affichage des mises à jour reçues" à la page [337](#)) ;
- la liste de l'inventaire détecté dans le réseau ;
- les clés détectées sur les appareils clients (cf. section "Travail avec les clés des applications" à la page [347](#)) ;
- fichiers placés par les applications de protection dans les dossiers de quarantaine sur les appareils;
- fichiers placés dans les dossiers de sauvegarde des appareils clients ;
- fichiers pour lesquels les applications de protection ont décidé d'une analyse ultérieure.

Dans cette section

Exportation de la liste des objets en quarantaine dans le fichier texte	353
Paquets d'installation	354
Quarantaine et dossier de sauvegarde.....	354
Fichiers en traitement différé	360

Exportation de la liste des objets en quarantaine dans le fichier texte

Vous pouvez exporter de la liste des objets en quarantaine dans le fichier texte.

► *Pour exporter de la liste des objets en quarantaine dans le fichier texte, procédez comme suit :*

1. Dans l'arborescence de la console **Stockages**, sélectionnez le dossier joint du stockage nécessaire.
2. Dans le menu contextuel de la liste des objets du stockage, sélectionnez l'option **Exporter la liste**.

Finalement, la fenêtre **Exporter la liste** s'ouvrira. Cette fenêtre permet d'indiquer le nom du fichier texte et l'adresse du dossier dans lequel il sera placé.

Paquets d'installation

Kaspersky Security Center place dans les stockages de données les paquets d'installation des applications de Kaspersky Lab et des applications des éditeurs tiers.

Le *Paquet d'installation* représente l'ensemble de fichiers nécessaires pour installer l'application. Le paquet d'installation contient les paramètres du processus d'installation et de la configuration initiale de l'application installée.

Si vous voulez installer n'importe quelle application sur l'appareil client, il faut créer un paquet d'installation (cf. section "Création des paquets d'installation des applications" à la page [260](#)) pour cette application ou utiliser le paquet d'installation déjà créé. La liste des paquets d'installation créés se trouvent dans le dossier de l'arborescence de la console **Installation à distance**, du dossier joint **Paquets d'installation**.

Pour plus d'informations sur le fonctionnement avec les paquets d'installation, cf. *Manuel d'implantation de Kaspersky Security Center*.

Quarantaine et sauvegarde

Les applications antivirus de Kaspersky Lab installées sur les appareils clients peuvent placer les fichiers en quarantaine ou dans le dossier de sauvegarde lors de l'analyse des appareils.

La *Quarantaine* est un stockage spécial qui contient les fichiers probablement infectés par les virus ou irréparables lors de la découverte.

La *Sauvegarde* est conçue pour enregistrer les copies de sauvegarde des fichiers qui ont été supprimés ou modifiés lors de la désinfection.

Kaspersky Security Center forme une liste générale des fichiers placés en quarantaine ou dans le dossier de sauvegarde par les applications de Kaspersky Lab sur les appareils clients. Les Agents d'administration des appareils clients transmettent les informations sur les fichiers en quarantaine et dans les dossiers de sauvegarde sur le Serveur d'administration. Via la Console d'administration il est possible de consulter les propriétés des fichiers qui se trouvent dans les stockages sur les appareils, lancer l'analyse antivirus des stockages et en supprimer les fichiers.

L'utilisation de la quarantaine et de la sauvegarde est accessible à Kaspersky Anti-Virus for Windows Workstations et Kaspersky Anti-Virus for Windows Servers des versions 6.0 supérieures, et à Kaspersky Endpoint Security 10 for Windows.

Kaspersky Security Center ne copie pas les fichiers depuis les stockages sur le Serveur d'administration. Tous les fichiers sont placés dans les stockages des appareils. La restauration des fichiers s'exécute sur l'appareil où est installée l'application de protection ayant placé le fichier dans le stockage.

Dans cette section

Activation de la gestion à distance des fichiers dans les stockages	356
Consultation des propriétés du fichier placé dans le stockage.....	357
Suppression des fichiers depuis le stockage	357
Restauration des fichiers depuis le stockage	358
Enregistrement du fichier depuis le stockage sur le disque	358
Analyse des fichiers en quarantaine.....	359

Activation de la gestion à distance des fichiers dans les stockages

L'administration à distance des fichiers dans les stockages sur les appareils clients est désactivée par défaut.

► *Pour activer l'administration à distance des fichiers dans les stockages sur les appareils clients, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut activer la gestion à distance des fichiers dans les stockages.
2. Dans l'espace de travail du groupe, ouvrez l'onglet **Stratégies**.
3. Sous l'onglet **Stratégies**, sélectionnez la stratégie de l'application de protection qui place les fichiers dans les stockages sur les appareils clients.
4. Dans la fenêtre des propriétés de la stratégie dans le groupe **Informé le Serveur d'administration**, cochez les cases qui correspondent aux stockages pour lesquels vous voulez activer l'administration à distance.

L'emplacement du groupe **Informé le Serveur d'administration** dans la fenêtre des propriétés de la stratégie et les noms des cases dans le groupe sont individuels pour chaque application de protection.

Consultation des propriétés du fichier placé dans le stockage

► *Pour consulter les propriétés du fichier placé en quarantaine ou dans le dossier de sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Quarantaine** ou **Sauvegarde**.
2. Dans l'espace de travail du dossier **Quarantaine (Sauvegarde)** sélectionnez le fichier dont les paramètres requièrent la consultation.
3. Ouvrez la fenêtre des propriétés du fichier à l'aide d'un des moyens suivants :
 - Dans le menu contextuel du fichier, sélectionnez l'option **Propriétés**.
 - A l'aide du lien **Ouvrir les propriétés de l'objet** dans le groupe de travail avec le fichier sélectionné.

Suppression des fichiers depuis le stockage

► *Pour supprimer le fichier placé en quarantaine ou dans le dossier de sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Quarantaine** ou **Sauvegarde**.
2. Dans l'espace de travail du dossier **Quarantaine (Sauvegarde)**, sélectionnez les fichiers à supprimer à l'aide des touches **Shift** et **Ctrl**.
3. Supprimez les fichiers à l'aide d'un des moyens suivants :
 - Sélectionnez l'option **Supprimer** dans le menu contextuel des fichiers.
 - A l'aide du lien **Supprimer les objets (Supprimer l'objet** lors de la suppression d'un fichier) dans le groupe de travail avec les fichiers sélectionnés.

Ainsi, les applications de protection qui ont placé les fichiers sélectionnés dans les stockages sur les appareils clients suppriment les fichiers de ces stockages.

Restauration des fichiers depuis le stockage

► *Pour restaurer le fichier depuis la quarantaine ou le dossier de sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Quarantaine** ou **Sauvegarde**.
2. Dans l'espace de travail du dossier **Quarantaine (Sauvegarde)**, sélectionnez les fichiers à restaurer à l'aide des touches **Shift** et **Ctrl**.
3. Lancez le processus de restauration des fichiers à l'aide d'un des moyens suivants :
 - Sélectionnez l'option **Restaurer** dans le menu contextuel des fichiers.
 - A l'aide du lien **Restaurer** dans le groupe de travail avec les fichiers sélectionnés.

Ainsi, les applications de protection, qui ont placé les fichiers dans les stockages sur les appareils clients, restaurent les fichiers dans les dossiers d'origine.

Enregistrement du fichier depuis le stockage sur le disque

Kaspersky Security Center permet d'enregistrer sur le disque les copies des fichiers placés par l'application de protection en quarantaine ou dans le dossier de sauvegarde sur l'appareil client. Les fichiers sont copiés dans le dossier indiqué sur l'appareil avec Kaspersky Security Center installé.

► *Pour enregistrer une copie du fichier de la quarantaine ou du dossier de sauvegarde sur le disque, procédez comme suit :*

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Quarantaine** ou **Sauvegarde**.
2. Dans l'espace de travail du dossier **Quarantaine (Sauvegarde)**, sélectionnez le fichier à copier sur le disque.
3. Lancez le processus de copie du fichier à l'aide d'un des modes suivants :
 - Dans le menu contextuel du fichier, sélectionnez l'option **Enregistrer sur le disque**.
 - A l'aide du lien **Enregistrer sur le disque** dans le groupe de travail avec le fichier sélectionné.

L'application de protection qui avait placé ce fichier en quarantaine sur l'appareil client sauvegardera la copie du fichier dans le dossier indiqué.

Analyse des fichiers en quarantaine

► *Pour analyser les fichiers en quarantaine, procédez comme suit :*

1. Dans l'arborescence de la console **Stockages**, sélectionnez le dossier joint **Quarantaine**.
2. Dans l'espace de travail du dossier **Quarantaine**, sélectionnez les fichiers à analyser à l'aide des touches **Shift** et **Ctrl**.
3. Lancez le processus d'analyse des fichiers à l'aide d'un des modes suivants :
 - Dans le menu contextuel du fichier, sélectionnez l'option **Analyser les objets en quarantaine**.
 - A l'aide du lien **Vérifier** dans le groupe de travail avec les fichiers sélectionnés.

Ainsi, pour les applications de protection qui ont placé les fichiers en quarantaine, la tâche d'analyse à la demande sera lancée sur les appareils clients sur lesquels les fichiers sélectionnés se trouvent en quarantaine.

Fichiers avec traitement différé

Les informations sur les fichiers avec traitement différé détectés sur les appareils clients se trouvent dans le dossier **Stockages**, dans le sous-dossier **Fichiers avec traitement différé**.

Le traitement différé et la désinfection des fichiers de l'application de protection sont effectués à la demande ou après la survenue d'un événement déterminé. Vous pouvez configurer les paramètres de désinfection différée des fichiers.

Désinfection du fichier avec traitement différé

► *Pour lancer la désinfection du fichier avec traitement différé, procédez comme suit :*

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Fichiers avec traitement différé**.
2. Dans l'espace de travail du dossier **Fichiers avec traitement différé**, sélectionnez le fichier à désinfecter.
3. Lancez le processus de désinfection du fichier à l'aide d'un des modes suivants :
 - Dans le menu contextuel du fichier, sélectionnez l'option **Réparer**.
 - A l'aide du lien **Réparer** dans le groupe de travail avec le fichier sélectionné.

Cela entraîne la tentative de désinfection du fichier.

Si le fichier est réparé, l'application de protection installée sur l'appareil client le restaure dans le dossier d'origine. L'enregistrement sur le fichier est supprimé de la liste du dossier **Fichiers avec traitement différé**. Si la désinfection du fichier est impossible, l'application de protection installée sur l'appareil supprime le fichier de l'appareil. L'enregistrement sur le fichier est supprimé de la liste du dossier **Fichiers avec traitement différé**.

Enregistrement du fichier avec traitement différé sur le disque

Kaspersky Security Center permet d'enregistrer les copies des fichiers sur les appareils clients avec traitement différé sur le disque. Les fichiers sont copiés dans le dossier indiqué sur l'appareil avec Kaspersky Security Center installé.

► *Pour enregistrer une copie du fichier avec traitement différé sur le disque, procédez comme suit :*

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Fichiers avec traitement différé**.
2. Dans l'espace de travail du dossier **Fichiers avec traitement différé**, sélectionnez les fichiers à copier sur le disque.
3. Lancez le processus de copie du fichier à l'aide d'un des modes suivants :
 - Dans le menu contextuel du fichier, sélectionnez l'option **Enregistrer sur le disque**.
 - A l'aide du lien **Enregistrer sur le disque** dans le groupe de travail avec le fichier sélectionné.

Ainsi, l'application de protection de l'appareil client sur lequel le fichier sélectionné avec traitement différé a été détecté, enregistre une copie du fichier dans le dossier indiqué.

Suppression des fichiers du dossier

"Fichiers avec traitement différé"

► Pour supprimer le fichier du dossier **Fichiers avec traitement différé**, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Fichiers avec traitement différé**.
2. Dans l'espace de travail du dossier **Fichiers avec traitement différé**, sélectionnez les fichiers à supprimer à l'aide des touches **Shift** et **Ctrl**.
3. Supprimez les fichiers à l'aide d'un des moyens suivants :
 - Sélectionnez l'option **Supprimer** dans le menu contextuel des fichiers.
 - A l'aide du lien **Supprimer les objets** (**Supprimer l'objet** lors de la suppression d'un fichier) dans le groupe de travail avec les fichiers sélectionnés.

Ainsi, les applications de protection qui ont placé les fichiers sélectionnés dans les stockages sur les appareils clients suppriment les fichiers de ces stockages. Les enregistrements sur les fichiers sont supprimés de la liste dans le dossier **Fichiers avec traitement différé**.

Kaspersky Security Network (KSN)

Cette section explique l'utilisation de l'infrastructure de services en ligne Kaspersky Security Network (KSN). Elle comporte des informations relatives à KSN, ainsi que des instructions pour l'activation de KSN, la configuration de l'accès à KSN et la consultation des statistiques d'utilisation du serveur proxy KSN.

A propos de KSN

Kaspersky Security Network (KSN) est une infrastructure de services en ligne qui donne accès à la base opérationnelle des connaissances de Kaspersky Lab concernant la réputation des fichiers, des ressources Internet et des logiciels. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky Lab sur les menaces, augmente l'efficacité de fonctionnement de certains modules de la protection, ainsi que diminue la possibilité des faux positifs. KSN permet de recevoir des informations sur les applications installées sur les appareils clients. Ces informations se trouvent dans les bases de réputation de Kaspersky Lab.

En participant au KSN, vous acceptez de transmettre automatiquement à Kaspersky Lab les informations relatives au fonctionnement des applications de Kaspersky Lab installées sur les appareils clients administrés par le Kaspersky Security Center. Ceci conformément aux conditions de KSN. La transmission des informations s'effectue conformément aux paramètres d'accès à KSN définis (cf. section "Configuration de l'accès à KSN" à la page [365](#)).

L'application propose de se connecter à KSN lors de son installation et de l'exécution de l'Assistant de configuration initiale (cf. section "Assistant de configuration initiale du Serveur d'administration" à la page [75](#)). Vous pouvez commencer à utiliser KSN ou refuser le service KSN à tout moment du fonctionnement de l'application (cf. section "Activation et désactivation de KSN" à la page [367](#)).

Les appareils clients administrés par le Serveur d'administration interagissent avec KSN à l'aide du service du serveur proxy KSN. Ce service fournit les possibilités suivantes :

- Les appareils clients peuvent exécuter les demandes à KSN et transmettre dans KSN les informations même s'ils n'ont pas d'accès Internet direct.
- Le serveur proxy KSN met en cache les données traitées en diminuant la charge sur le canal du réseau externe et en accélérant l'obtention des informations demandées par l'appareil client.

Vous pouvez configurer les paramètres du serveur proxy KSN dans la section **Serveur proxy KSN** de la fenêtre des propriétés du Serveur d'administration (cf. section "Configuration de l'accès à KSN" à la page [365](#)).

A propos des données

En participant au Kaspersky Security Network, vous acceptez de transmettre automatiquement à Kaspersky Lab les informations relatives au fonctionnement des applications de Kaspersky Lab installées sur les appareils clients administrés par le Kaspersky Security Center. Les experts de Kaspersky Lab utiliseront les informations transmises par les appareils clients pour résoudre les problèmes de fonctionnement des applications de Kaspersky Lab ou pour modifier leurs fonctionnalités.

En participant au programme Kaspersky Security Network, vous acceptez de transmettre automatiquement à Kaspersky Lab les informations suivantes, obtenues suite à l'utilisation de Kaspersky Security Center sur l'appareil :

- nom, version et langue d'utilisation du logiciel auquel correspond la mise à jour ;
- version de la base de données des mises à jour utilisée par l'application lors de l'installation ;
- résultat de l'installation de la mise à jour ;
- identifiant de l'appareil et version de l'Agent d'administration utilisé ;
- paramètres de l'application utilisés lors de l'installation de la mise à jour, identifiants des opérations effectuées et codes de résultat des opérations effectuées.

Si vous refusez de participer au programme Kaspersky Security Network, les données citées ci-dessus ne sont pas transmises à Kaspersky Lab.

Les informations obtenues sont protégées par Kaspersky Lab conformément aux exigences établies par la loi et aux politiques de Kaspersky Lab. Kaspersky Lab utilise les informations obtenues uniquement de manière impersonnelle et sous forme de statistiques. Les statistiques générales sont créées de manière automatique à partir des informations initiales obtenues et ne contiennent pas de données personnelles ou d'autres données confidentielles. Les informations initiales obtenues sont enregistrées sous forme cryptée et supprimées au fur et à mesure de leur collecte (deux fois par an). Les statistiques générales sont conservées pour une durée indéterminée.

Les données sont envoyées sur une base volontaire. La fonction d'envoi des données peut être activée ou désactivée à tout moment dans la fenêtre des paramètres de l'application.

Configuration de l'accès à KSN

► Afin de configurer l'accès du Serveur d'administration à KSN, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous devez configurer l'accès à KSN.
2. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez la section **Paramètres du serveur proxy KSN** dans la section **Serveur proxy KSN**.
4. Cochez la case **Utiliser le Serveur d'administration comme serveur proxy** pour activer le service du serveur proxy KSN.

La transmission des informations depuis les appareils clients vers KSN est régie par la stratégie Kaspersky Endpoint Security active sur ces appareils. Si la case est décochée, la transmission des données depuis le Serveur d'administration ou les appareils clients vers KSN via le Kaspersky Security Center ne s'exécute pas. Toutefois, selon leur configuration, les appareils clients peuvent transmettre directement les données à KSN (et non via le Kaspersky Security Center). La stratégie de Kaspersky Endpoint Security for Windows appliquée sur les appareils clients définit quelles données de ces appareils sont envoyées directement à KSN (et non via le Kaspersky Security Center).

5. Cochez la case **J'accepte de participer au Kaspersky Security Network**.

Si la case est cochée, les appareils clients transmettent les résultats de l'installation des correctifs à Kaspersky Lab. Une fois que vous avez coché la case, vous devez lire et accepter les Conditions de KSN.

Si vous utilisez KSN privé (infrastructure KSN qui ne se trouve pas sur les serveurs de Kaspersky Lab mais, par exemple, sur le réseau du fournisseur Internet), cochez la case **Configurer le KSN privé** et cliquez sur le bouton **Choix du fichier de paramètres KSN** pour télécharger les paramètres du KSN privé (fichiers .pkcs7, .pem). Suite au téléchargement des paramètres, l'interface affiche le nom du fournisseur, ses coordonnées et la date de création du fichier avec les paramètres de KSN privé.

L'utilisation du KSN privé est prise en charge par les applications suivantes de Kaspersky Lab :

- Kaspersky Security Center 10 Service Pack 1 et versions supérieures ;
- Kaspersky Endpoint Security 10 Service Pack 1 et versions supérieures ;
- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 ;
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent.

Si vous utilisez le KSN privé via des versions de l'application antérieures à Kaspersky Security for Virtualization 3.0 Protection Agentless Service Pack 2 ou à Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent, il est recommandé d'utiliser les Serveurs d'administration secondaires pour lesquels l'utilisation du KSN privé n'a pas été configurée.

6. Configurez les paramètres de connexion du Serveur d'administration au service du serveur proxy KSN :

- Dans le champ **Port TCP**, indiquez le numéro du port TCP via lequel la connexion au serveur proxy KSN sera établie. Par défaut, la connexion au serveur proxy KSN est exécutée via le port 13111.
- Pour que le Serveur d'administration se connecte au serveur proxy KSN via un port UDP, cochez la case **Utiliser le port UDP** et indiquez le numéro du port dans le champ **Port UDP**. La case est décochée par défaut et la connexion au serveur proxy KSN est établie via le port UDP 15111.

7. Cochez la case **Connecter les Serveurs d'administration secondaires au KSN via le Serveur principal**.

Si la case est cochée, les Serveurs d'administration secondaires utilisent le Serveur d'administration principal comme serveur proxy KSN. Si la case est décochée, les Serveurs d'administration secondaires se connectent au KSN indépendamment. Dans ce cas, les appareils administrés utilisent les Serveurs d'administration secondaires comme serveurs proxy KSN.

Les Serveurs d'administration secondaires utilisent le Serveur d'administration principal comme serveur proxy si dans les propriétés des Serveurs d'administration secondaires dans la section **Serveur proxy KSN**, la case **Utiliser le Serveur d'administration comme serveur proxy** est également cochée.

8. Cliquez sur le bouton **OK**.

Cela enregistre les paramètres d'accès à KSN.

Activation et désactivation de KSN

► *Pour activer KSN, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous devez activer KSN.
2. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez la sous-section **Paramètres du serveur proxy KSN** dans la section **Serveur proxy KSN**.
4. Cochez la case **Utiliser le Serveur d'administration comme serveur proxy**.

Suite à cette action, le service du serveur proxy KSN est activé.

5. Cochez la case **J'accepte de participer au Kaspersky Security Network**.

KSN est ainsi activé.

Si la case est cochée, les appareils clients transmettent les résultats de l'installation des correctifs à Kaspersky Lab. Une fois que vous avez coché la case, vous devez lire et accepter les Conditions de KSN.

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

► *Pour désactiver KSN, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous devez activer KSN.
2. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez la sous-section **Paramètres du serveur proxy KSN** dans la section **Serveur proxy KSN**.
4. Décochez la case **Utiliser le Serveur d'administration comme serveur proxy**, pour activer le service du serveur proxy KSN ou décochez la case **J'accepte de participer au Kaspersky Security Network**.

Si la case est décochée, les appareils clients ne transmettent pas les résultats de l'installation des correctifs à Kaspersky Lab.

Si vous utilisez un KSN privé, décochez la case **Configurer le KSN privé**

KSN est ainsi désactivé.

5. Cliquez sur le bouton **OK**.

Consulter les statistiques du serveur proxy KSN

Le *serveur proxy KSN* est un service qui assure l'interaction entre l'infrastructure de Kaspersky Security Network et les appareils clients administrés par le Serveur d'administration.

L'utilisation du serveur proxy KSN fournit les possibilités suivantes :

- Les appareils clients peuvent exécuter les demandes à KSN et transmettre dans KSN les informations même s'ils n'ont pas d'accès Internet direct.
- Le serveur proxy KSN met en cache les données traitées en diminuant la charge sur le canal du réseau externe et en accélérant l'obtention des informations demandées par l'appareil client.

Dans la fenêtre de propriétés du Serveur d'administration, vous pouvez configurer les paramètres du serveur proxy KSN et consulter des statistiques sur son utilisation.

► *Pour consulter les statistiques du serveur proxy KSN, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous devez afficher les statistiques de KSN.
2. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez la section **Statistiques du serveur proxy KSN** dans la section **Serveur proxy KSN**.

Cette section affiche les statistiques de fonctionnement du serveur proxy KSN. Si nécessaire, procédez comme suit :

- via le bouton **Actualiser**, mettez à jour les statistiques sur l'utilisation du serveur proxy KSN ;
 - via le bouton **Exporter dans un fichier**, exportez les statistiques dans un fichier au format CSV ;
 - via le bouton **Vérifier la connexion à KSN**, vérifiez si le Serveur d'administration est actuellement connecté à KSN.
4. Cliquez sur **OK** pour fermer la fenêtre de propriétés du Serveur d'administration.

Contacteur le Support Technique

Cette section contient des informations sur les moyens et les conditions d'accès à l'assistance technique.

Dans cette section

Moyens de bénéficier de l'assistance technique	370
Assistance technique par téléphone.....	371
Assistance technique via le Kaspersky CompanyAccount.....	371

Moyens de bénéficier de l'assistance technique

Si vous n'avez pas trouvé de solution à votre problème dans la documentation de l'application ou dans d'autres sources d'informations sur l'application (cf. section "Sources d'informations sur l'application" à la page [21](#)), nous vous recommandons de contacter le Support Technique. Les experts du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application.

L'assistance technique est uniquement accessible aux utilisateurs qui ont acheté une licence commerciale pour l'application. Les utilisateurs qui disposent d'une licence d'évaluation n'ont pas droit à l'assistance technique.

Avant de contacter le Support Technique, il est recommandé de lire les règles d'octroi du Support Technique (<http://support.kaspersky.fr/support/rules>).

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

- contacter le Support Technique par téléphone (<http://support.kaspersky.fr/support/contacts>) ;
- envoyer une demande au Support Technique de Kaspersky Lab via le portail Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

Assistance technique par téléphone

Vous pouvez téléphoner aux experts du Support Technique dans la plupart des régions du monde entier. Vous pouvez trouver des informations sur les moyens de bénéficier de l'aide de l'assistance technique dans votre région ainsi que les coordonnées du Support Technique sur le site Internet du Support Technique de Kaspersky Lab (<http://support.kaspersky.com/b2b>).

Avant de contacter le Support Technique, il est recommandé de lire les règles d'octroi de l'assistance technique (<http://support.kaspersky.com/fr/support/rules>).

Assistance technique via le Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) est un portail dédié aux entreprises utilisant les applications Kaspersky Lab. Le portail Kaspersky CompanyAccount vise à permettre l'interaction entre les utilisateurs et les experts de Kaspersky Lab via des requêtes électroniques. Il permet de suivre le traitement des requêtes électroniques par les experts de Kaspersky Lab et de conserver un historique de ces requêtes.

Vous pouvez enregistrer tous les employés de votre entreprise dans un seul compte utilisateur Kaspersky CompanyAccount. Ce compte utilisateur unique vous permet de centraliser l'administration des requêtes électroniques envoyées à Kaspersky Lab et provenant des employés enregistrés. Il vous permet également d'administrer les privilèges de ces employés Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

- anglais ;
- espagnol ;
- italien ;
- allemand ;
- polonais ;
- portugais ;
- russe ;
- français ;
- japonais.

Pour en savoir plus sur le Kaspersky CompanyAccount, veuillez consulter le site Internet du Service de Support Technique(http://support.kaspersky.fr/faq/companyaccount_help).

Appendice

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

Dans cette section

Possibilités complémentaires.....	373
Particularités d'utilisation de l'interface d'administration	405
Aide.....	407

Possibilités complémentaires

Cette section aborde les possibilités complémentaires de Kaspersky Security Center prévues pour étendre les fonctions d'administration centralisée des applications sur les appareils.

Dans cette section

Automatisation du fonctionnement de Kaspersky Security Center. Utilitaire klakaut	375
Utilisateurs autonomes	375
Événements dans le fonctionnement des applications	379
Définition du niveau d'importance de l'événement de dépassement de la restriction de licence	380
Notification relative aux événements via un fichier exécutable	380
Utilisation de l'application Kaspersky Security pour les environnements protégés	382
Suivi de l'état de la protection antivirus à l'aide d'informations du registre système	382
Clusters et matrices des serveurs	384
Algorithme d'installation du correctif pour l'application Kaspersky Lab dans le modèle de cluster	385
Recherche d'appareils	386
Connexion aux appareils à l'aide de Windows Desktop Sharing	388
A propos des comptes utilisés	388
Fonctionnement avec les outils externes	389
Exportation des listes depuis les fenêtres de dialogue	390
Mode de clonage du disque de l'Agent d'administration	390
Préparation de l'appareil fonctionnant sous le système d'exploitation Linux à l'installation à distance de l'Agent d'administration	392
Copie de sauvegarde et restauration des données du Serveur d'administration	394
Sauvegarde et restauration des données en mode interactif	401
Installation de l'application à l'aide des stratégies de groupe Active Directory	402

Automatisation du fonctionnement de Kaspersky Security Center.

Utilitaire klakaut

Vous pouvez automatiser le fonctionnement de Kaspersky Security Center à l'aide de l'utilitaire klakaut. L'utilitaire klakaut et son système d'aide se trouvent dans le dossier d'installation Kaspersky Security Center.

Utilisateurs autonomes

L'application Kaspersky Security Center prévoit la possibilité de transférer l'Agent d'administration des appareils clients sur d'autres Serveurs d'administration en cas de modification des caractéristiques du réseau suivantes :

- Présence dans le sous-réseau : modification de l'adresse et du masque du sous-réseau.
- Présence dans le domaine DNS : modification du suffixe DNS du sous-réseau.
- Adresse de la passerelle principale : modification de la passerelle principale du réseau.
- Adresse du serveur DHCP : modification de l'adresse IP du serveur DHCP dans le réseau.
- Adresse du serveur DNS : modification de l'adresse IP du serveur DNS dans le réseau.
- Adresse du serveur WINS : modification de l'adresse IP du serveur WINS dans le réseau.
- Accès au domaine Windows : modification de l'état du domaine Windows auquel l'appareil client est connecté.

Cette fonctionnalité est prise en charge pour les systèmes d'exploitation suivants : Microsoft Windows XP/Windows Vista ; Microsoft Windows Server 2003/2008.

Paramètres de connexion d'origine de l'Agent d'administration au Serveur lors de l'installation de l'Agent d'administration. Par la suite, quand des règles de permutation de l'Agent d'administration sur d'autres Serveurs d'administration sont rédigées, l'Agent d'administration réagit aux modifications des caractéristiques du réseau de la manière suivante :

- Si les caractéristiques du réseau correspondent à une des règles formées, l'Agent d'administration se connecte au Serveur d'administration indiqué dans cette règle. Si la règle le prévoit, les applications installées sur les appareils clients adopteront les stratégies pour les utilisateurs autonomes.
- Si une des règles n'est pas exécutée, l'Agent d'administration revient aux paramètres d'origine de connexion au Serveur d'administration définis lors de l'installation. Les applications installées sur les appareils clients reviennent aux stratégies actives.
- Si le Serveur d'administration est inaccessible, l'Agent d'administration utilise les stratégies pour les utilisateurs autonomes.

Par défaut, l'Agent d'administration passe à la stratégie pour les utilisateurs autonomes si le Serveur d'administration est inaccessible pendant plus de 45 minutes.

Les paramètres de connexion de l'Agent d'administration au Serveur d'administration sont préservés dans le profil de connexion. Le profil de connexion permet de créer des règles de permutation des appareils clients vers les stratégies pour les utilisateurs autonomes, ainsi que de configurer le profil de sorte qu'il soit uniquement utilisé pour le téléchargement des mises à jour.

Dans cette section

Création du profil de connexion au Serveur d'administration pour les utilisateurs déconnectés	376
Création de la règle de permutation de l'Agent d'administration	378

Création du profil de connexion au Serveur d'administration pour les utilisateurs déconnectés

► *Pour créer le profil de connexion de l'Agent d'administration au Serveur d'administration pour les utilisateurs déconnectés, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour les appareils dont il faut créer le profil de connexion de l'Agent d'administration au Serveur.
2. Exécutez une des actions suivantes :
 - Si vous voulez créer le profil de connexion pour tous les appareils du groupe, dans l'espace de travail du groupe sous l'onglet **Stratégies**, sélectionnez la stratégie de l'Agent d'administration. Ouvrez la fenêtre de la stratégie sélectionnée.
 - Si vous voulez créer le profil de connexion pour l'appareil sélectionné dans le groupe, dans l'espace de travail du groupe sous l'onglet **Appareils**, sélectionnez l'appareil et procédez comme suit :
 - a. Ouvrez la fenêtre des propriétés de l'appareil sélectionné.
 - b. Dans la section **Applications** de la fenêtre des propriétés de l'appareil, sélectionnez l'Agent d'administration.
 - c. Ouvrez la fenêtre des propriétés de l'Agent d'administration.
3. Dans la fenêtre ouverte des propriétés dans la section **Réseau**, sélectionnez le sous-dossier **Connexion**.
4. Dans le groupe **Profils de connexion au Serveur d'administration**, cliquez sur le bouton **Ajouter**.

La liste des profils de connexion contient uniquement par défaut le profil <Sans connexion>. Ce profil ne peut être modifié ou supprimé. Il ne contient pas de Serveur pour la connexion et en cas de sélection de ce profil, l'Agent d'administration ne tentera pas de se connecter à un serveur quelconque tandis que les applications installées sur les appareils clients utilisent les stratégies pour les utilisateurs autonomes. Le profil <Sans connexion> est invoqué quand les appareils sont déconnectés du réseau.
5. Dans la fenêtre ouverte **Nouveau profil**, configurez les paramètres du profil de connexion et cochez la case **Activer les stratégies déconnectées**.

Finalement, le profil de connexion de l'Agent d'administration au Serveur d'administration pour les utilisateurs déconnectés sera créé. Lors de la connexion de l'Agent d'administration au Serveur via ce profil de l'application, les applications installées sur l'appareil client utiliseront les stratégies pour les utilisateurs autonomes.

Création de la règle de permutation de l'Agent d'administration

- ▶ *Afin de créer la règle de permutation de l'Agent d'administration d'un Serveur d'administration sur un autre, lors de la modification des caractéristiques du réseau, procédez comme suit :*
 1. Dans l'arborescence de la console, sélectionnez le groupe d'administration dont les appareils requièrent la création de la règle de permutation de l'Agent d'administration.
 2. Exécutez une des actions suivantes :
 - Si vous voulez créer la règle de permutation pour tous les appareils du groupe, dans l'espace de travail du groupe sous l'onglet **Stratégies**, sélectionnez la stratégie de l'Agent d'administration. Ouvrez la fenêtre de la stratégie sélectionnée.
 - Si vous voulez créer la règle de permutation pour l'appareil sélectionné du groupe, dans l'espace de travail du groupe sous l'onglet **Appareils**, sélectionnez l'appareil et procédez comme suit :
 - a. Ouvrez la fenêtre des propriétés de l'appareil sélectionné.
 - b. Dans la section **Applications** de la fenêtre des propriétés de l'appareil, sélectionnez l'Agent d'administration.
 - c. Ouvrez la fenêtre des propriétés de l'Agent d'administration.
 3. Dans la fenêtre ouverte des propriétés dans la section **Réseau**, sélectionnez le sous-dossier **Connexion**.
 4. Dans le groupe **Permutation des profils**, cliquez sur le bouton **Ajouter**.
 5. Dans la fenêtre ouverte **Nouvelle règle**, configurez les paramètres de la règle de permutation et cochez la case **Règle activée** pour activer l'utilisation de la règle.

Finalement, la règle de permutation sera créée. Lors de l'exécution de cette règle, l'Agent d'administration sera utilisé pour se connecter au Serveur d'administration indiqué dans la règle du profil de connexion.

La vérification de la correspondance entre les règles de permutation et les caractéristiques du réseau s'opère dans l'ordre de présentation dans la liste. Si les caractéristiques du réseau correspondent à plusieurs règles, c'est la première d'entre elles qui sera appliquée. Vous

pouvez modifier l'ordre de suivi des règles dans la liste à l'aide des boutons



et



Événements dans le fonctionnement des applications

Kaspersky Security Center permet d'obtenir les informations sur les événements dans le fonctionnement du Serveur d'administration et d'autres applications Kaspersky Lab installées sur les appareils clients.

Pour les applications Kaspersky Lab, quatre degrés d'importance des événements sont prévus :

- **Événement critique ;**
- **Erreur de fonctionnement ;**
- **Avertissement ;**
- **Message d'information.**

Vous pouvez configurer les règles de traitement des événements séparément pour chaque niveau d'importance.

Voir également

Configuration des paramètres généraux du Serveur d'administration [105](#)

Définition du niveau d'importance de l'événement de dépassement de la restriction de licence

Kaspersky Security Center permet d'obtenir des informations sur les événements de dépassement de la restriction de licence des applications Kaspersky Lab installées sur les appareils clients.

Le niveau d'importance des événements de dépassement de la restriction de licence est défini conformément aux règles suivantes :

- Si le nombre d'unités de licence utilisées se trouve entre 90 et 100 % du total des unités de licence de cette licence, l'événement avec le niveau d'importance **Message d'information** est publié.
- Si le nombre d'unités de licence utilisées se trouve entre 100 et 110 % du total d'unités de licence de cette licence, l'événement avec le niveau d'importance **Avertissement** est publié.
- Si le nombre d'unités de licence utilisées dépasse 110 % du total d'unités de licence de cette licence, l'événement avec le niveau d'importance **Événement critique** est publié.

Voir également

Configuration des paramètres généraux du Serveur d'administration [105](#)

Notification relative aux événements via un fichier exécutable

Kaspersky Security Center permet de lancer un fichier exécutable afin de signaler à l'administrateur les événements survenus sur les appareils clients. Le fichier exécutable doit contenir un autre fichier exécutable avec les paramètres variables à envoyer à l'administrateur.

Tableau 4. Paramètres variables de description de l'événement

Variable	Description du paramètre secondaire
%SEVERITY%	Niveau d'importance de l'événement
%COMPUTER%	Nom de l'appareil où l'événement s'est produit
%DOMAIN%	Domaine
%EVENT%	Événement
%DESCR%	Description d'événement
%RISE_TIME%	Heure à laquelle l'événement s'est produit
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nom de la tâche
%KL_PRODUCT%	Agent d'administration Kaspersky Security Center
%KL_VERSION%	Numéro de la version de l'Agent d'administration
%HOST_IP%	Adresse IP
%HOST_CONN_IP%	Adresse IP de la connexion

Exemple

La notification de l'événement s'opère via un fichier exécutable (par exemple, *script1.bat*) au sein duquel un autre fichier exécutable (par exemple, *script2.bat*) contenant la variable %COMPUTER% est lancé. Quand l'événement se produit, le fichier *script1.bat* est lancé sur l'appareil de l'administrateur. Ce fichier lance à son tour le fichier *script2.bat* avec la variable %COMPUTER%. L'administrateur reçoit le nom de l'appareil sur lequel l'événement s'est produit.

Utilisation de l'application Kaspersky Security pour les environnements protégés

Kaspersky Security Center prend en charge la possibilité de connecter les machines virtuelles au Serveur d'administration. L'administration des machines virtuelles est réalisée à l'aide de l'application Kaspersky Security pour les environnements protégés 3.0. Pour plus de détails, cf. Manuel de l'administrateur de Kaspersky Security pour les environnements protégés 3.0.

Suivi de l'état de la protection antivirus à l'aide d'informations du registre système

► Pour suivre l'état de la protection antivirus sur l'appareil client à l'aide des informations enregistrées par l'Agent d'administration dans le registre système, procédez comme suit :

1. Ouvrez le registre système de l'appareil client (par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**).
2. Rendez-vous dans la section :

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103  
\1.0.0.0\Statistics\AVState
```

Ainsi, le registre système affichera les informations sur l'état de la protection antivirus de l'appareil client.

Les valeurs spécifiques des clés, décrites dans le tableau ci-dessous, correspondent à chaque état de la protection antivirus.

Tableau 5. Clés du registre et leurs valeurs possibles

Clé (type de données)	Valeur	Description
Protection_AdmServer (REG_SZ)	<Nom du Serveur d'administration>	Nom du Serveur d'administration qui administre l'appareil.
Protection_AvInstalled (REG_DWORD)	Différent de 0	L'application de protection est installée sur l'appareil.

Clé (type de données)	Valeur	Description
Protection_AvRunning (REG_DWORD)	Différent de 0	Protection en temps réel de l'appareil active.
Protection_HasRtp (REG_DWORD)	Différent de 0	Module de protection en temps réel installé.
	Etat de la protection en temps réel :	
	0	Inconnu.
	2	Inactive.
	3	Suspendu(e).
	4	Lancement en cours.
	5	Active.
	6	Active, niveau élevé (protection maximale).
	7	Active, utilisation des paramètres par défaut (recommandés).
	8	Active, utilisation des paramètres configurés par l'utilisateur.
9	Erreur.	

Clé (type de données)	Valeur	Description
Protection_LastFscan (REG_SZ)	JJ-MM-AAAA HH-MM-SS	Date et heure (au format UTC) de la dernière analyse complète.
Protection_BasesDate (REG_SZ)	JJ-MM-AAAA HH-MM-SS	Date et heure (au format UTC) d'édition des bases de l'application.
Protection_LastConnected (REG_SZ)	JJ-MM-AAAA HH-MM-SS	Date et heure (au format UTC) de la dernière connexion au Serveur d'administration.

Clusters et matrices des serveurs

Kaspersky Security Center prend en charge la technologie de cluster. Si l'Agent d'administration transmet au Serveur d'administration les informations sur le fait que l'application installée sur l'appareil client est une partie de la matrice du serveur, alors l'appareil client devient le nœud du cluster. Le cluster sera ajouté comme un objet séparé dans le dossier **Appareils administrés**

dans l'arborescence de la console avec l'icône .

Il est possible de choisir plusieurs propriétés types du cluster :

- Le cluster et toutes ses entrées se trouvent toujours dans un groupe d'administration.
- Si l'administrateur tente de déplacer une entrée quelconque du cluster, l'entrée reviendra dans l'emplacement d'origine.
- Si l'administrateur tente de déplacer le cluster dans un autre groupe, toutes ses entrées seront aussi déplacées avec celui-ci.

Algorithme d'installation du correctif pour l'application Kaspersky Lab dans le modèle de cluster

Kaspersky Security Center prend uniquement en charge l'installation manuelle des correctifs pour les applications Kaspersky Lab dans le modèle de cluster.

Pour installer le correctif pour l'application Kaspersky Lab, procédez comme suit :

1. Téléchargez le correctif sur chaque nœud du cluster.
2. Lancez l'installation du correctif sur le nœud actif.

Attendez que le correctif soit bien installé.

3. Lancez successivement le correctif sur tous les nœuds secondaires du cluster.

Au moment du lancement du correctif depuis la ligne de commande, utilisez la clé "`-CLUSTER_SECONDARY_NODE`".

Suite à ces actions, le correctif sera installé sur chaque nœud du cluster.

4. Lancez manuellement les services de cluster de Kaspersky Lab.

Chaque nœud du cluster s'affichera dans la Console d'administration en tant qu'appareil sur lequel l'Agent d'administration est installé.

Les informations sur les correctifs installés peuvent être consultées dans le dossier **Mises à jour du logiciel** ou dans le rapport sur les versions de mises à jour des modules logiciels des applications Kaspersky Lab.

Voir également

| Configuration des paramètres généraux du Serveur d'administration [105](#)

Recherche d'appareils

Kaspersky Security Center permet de rechercher les appareils sur la base des critères définis. Vous pouvez enregistrer les résultats de la recherche dans un fichier de texte.

La fonction de recherche permet de trouver les appareils suivants :

- les appareils clients dans les groupes d'administration du Serveur d'administration et de ses Serveurs secondaires ;
- les appareils non définis sous l'administration du Serveur d'administration et ses Serveurs secondaires.

► *Pour rechercher les appareils clients du groupe d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier du groupe d'administration.
2. Dans le menu contextuel du dossier du groupe d'administration, sélectionnez l'option **Recherche** ;
3. Sous les onglets de la fenêtre **Recherche**, indiquez les critères selon lesquels il faut rechercher les appareils clients et cliquez sur le bouton **Rechercher**.

Ainsi, les appareils qui correspondent aux critères définis de recherche s'afficheront dans le tableau dans la partie inférieure de la fenêtre **Recherche**.

► *Pour rechercher les appareils non définis, procédez comme suit :*

1. Dans l'arborescence de la console sélectionnez le dossier **Appareils non définis**.
2. Dans le menu contextuel du dossier **Appareils non définis**, sélectionnez l'option **Recherche** ;
3. Sous les onglets de la fenêtre **Recherche**, indiquez les critères selon lesquels il faut rechercher les appareils clients et cliquez sur le bouton **Rechercher**.

Ainsi, les appareils qui correspondent aux critères définis de recherche s'afficheront dans le tableau dans la partie inférieure de la fenêtre **Recherche**.

► *Pour rechercher les appareils qui appartiennent ou non au groupe d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration – <Nom du Serveur>**.
2. Sélectionnez l'option **Recherche** dans le menu contextuel de l'entrée.
3. Sous les onglets de la fenêtre **Recherche**, indiquez les critères selon lesquels il faut rechercher les appareils clients et cliquez sur le bouton **Rechercher**.

Ainsi, les appareils qui correspondent aux critères définis de recherche s'afficheront dans le tableau dans la partie inférieure de la fenêtre **Recherche**.

La fenêtre **Recherche** vous permet aussi de rechercher les groupes d'administration et les Serveurs d'administration secondaires à l'aide de la liste déroulante dans le coin en haut à droite de la fenêtre. La recherche des groupes d'administration et des Serveurs d'administration secondaires n'est pas disponible lors de l'ouverture de la fenêtre **Recherche** du dossier **Appareils non définis**.

Pour rechercher les appareils, vous pouvez utiliser des expressions régulières dans les champs de saisie de la fenêtre **Recherche** (cf. section "Utilisation des expressions régulières dans la ligne de recherche" à la page [427](#)).

La recherche en texte intégral dans la fenêtre **Recherche** est accessible :

- sur l'onglet **Réseau** dans le champ **Commentaires** ;
- sur l'onglet **Matériel** dans les champs **Appareil**, **Editeur**, **Description**.

Connexion aux appareils à l'aide de Windows Desktop Sharing

► Pour se connecter à l'appareil client à l'aide de la technologie Windows Desktop Sharing, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Appareils administrés** sous l'onglet **Appareils**.

La liste des appareils s'affiche dans l'espace de travail du dossier.

2. Dans le menu contextuel de l'appareil client auquel vous voulez vous connecter, sélectionnez l'option **Se connecter à l'appareil** → **Windows Desktop Sharing**.

La fenêtre **Sélection de la session du bureau**.

3. Dans la fenêtre **Sélection de la session du bureau**, sélectionnez la session du bureau qui sera utilisée pour se connecter à l'appareil.

4. Cliquez sur le bouton **OK**.

La connexion à l'appareil sera effectuée.

A propos des comptes utilisateur utilisés

Vous pouvez indiquer le compte utilisateur sous lequel la tâche doit être lancée.

Par exemple, pour une tâche d'analyse à la demande, il faut avoir un droit d'accès à l'objet analysé, tandis que pour une tâche de mise à jour, il faut des droits d'utilisateur autorisé sur serveur proxy. Ceci permet d'éviter des erreurs lors de l'exécution de tâches d'analyse à la demande ou de mise à jour si l'utilisateur lance une tâche sans jouir des privilèges nécessaires.

Dans les tâches d'installation et de désinstallation à distance de l'application, le compte utilisateur est utilisé pour télécharger sur les appareils clients des fichiers nécessaires pour l'installation (la suppression) si l'Agent d'administration n'est pas installé ou n'est pas accessible sur l'appareil. Si l'Agent d'administration est installé ou accessible, le compte utilisateur est utilisé si, selon les paramètres d'une tâche, la remise des fichiers s'effectue uniquement par les moyens de Microsoft Windows du dossier partagé.

Dans ce cas le compte utilisateur doit posséder les droits sur l'appareil suivant :

- le droit sur le lancement des applications à distance ;
- les droits sur une ressource Admin\$;
- le droit *Connexion en tant que service*.

Si l'Agent d'administration effectue la remise des fichiers sur les appareils, le compte utilisateur ne sera pas utilisé. L'Agent d'administration effectuera toutes les opérations de copie et d'installation des fichiers sous le compte utilisateur **Système local (Local System Account)**.

Fonctionnement avec les outils externes

Kaspersky Security Center permet de configurer une liste des *outils externes* (ci-après, les *outils*) : des applications qui sont appelées pour l'appareil client depuis la Console d'administration à l'aide du groupe du menu contextuel **Outils externes**. Pour chaque outil de la liste, une commande de menu est créée, ce qui permet à la console d'administration de lancer l'application qui correspond à l'outil.

L'application se lance sur le poste de travail de l'administrateur. L'application peut accepter en guise d'arguments de la ligne de commande les attributs de l'appareil client distant (nom NetBIOS, nom DNS, adresse IP). La connexion à l'appareil peut être exécutée à l'aide d'une connexion en tunnel.

Par défaut, la liste des outils externes contient les services suivants pour chaque appareil client :

- **Diagnostic à distance** : utilitaire de diagnostic à distance Kaspersky Security Center.
- **Bureau distant** : composant standard de Microsoft Windows "Connexion en cours au poste de travail distant".
- **Administration de l'ordinateur** : composant Microsoft Windows standard.

► *Pour ajouter ou supprimer les outils externes et de modifier leurs paramètres,*

dans le menu contextuel de l'appareil client, sélectionnez l'option **Outils externes** → **Configurer les outils externes**.

Finalement, la fenêtre **Outils externes** s'ouvrira. Cette fenêtre permet d'ajouter et de supprimer les outils externes et de configurer leurs paramètres à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**.

Exportation des listes depuis les fenêtres de dialogue

Dans les fenêtres de dialogue de l'application, vous pouvez exporter les listes des fichiers dans les fichiers de texte.

L'exportation de la liste des objets est possible pour les sections de la fenêtre de dialogue qui contiennent le bouton **Exporter dans un fichier**.

Mode de clonage du disque de l'Agent d'administration

Le clonage du disque dur de l'appareil "étalon" est une méthode répandue pour l'installation d'un logiciel sur de nouveaux appareils. Si l'Agent d'administration sur le disque dur de l'appareil "étalon" fonction en mode normal pendant le clonage, le problème suivant survient :

Après le déploiement de l'image de disque étalon dotée de l'Agent d'administration sur de nouveaux appareils, ces derniers apparaissent sous la même icône dans la Console d'administration. Ce problème survient parce que lors de la copie sur les nouveaux appareils, les données internes identiques sont conservées. Ces données permettent au Serveur d'administration d'associer l'appareil à l'icône dans la Console d'administration.

Pour éviter les problèmes liés à l'affichage incorrect des nouveaux appareils dans la Console d'administration après la copie, vous pouvez utiliser le *mode spécial de clonage de disque de l'Agent d'administration*. Utilisez ce mode si vous déployez une application (avec l'Agent d'administration) sur de nouveaux appareils via le clonage du disque.

En mode de clonage du disque, l'Agent d'administration fonctionne, mais il ne se connecte pas au Serveur d'administration. Une fois sorti du mode de clonage, l'Agent d'administration supprime les données internes qui faisaient que le Serveur d'administration associait plusieurs appareils à une icône dans la Console d'administration. A l'issue de la copie de l'image de l'appareil "étalon", les

nouveaux appareils apparaissent normalement dans la Console d'administration (avec leur propre icône).

Scénarios d'utilisation du mode de clonage du disque de l'Agent d'administration

1. L'administrateur installe l'Agent d'administration sur l'appareil "étalon".
2. L'administrateur vérifie la connexion de l'Agent d'administration au Serveur d'administration à l'aide de l'utilitaire klnagchk (cf. section "Vérification manuelle de la connexion de l'appareil client avec le Serveur d'administration. Utilitaire klnagchk" à la page [160](#)).
3. L'Administrateur active le mode de clonage du disque de l'Agent d'administration.
4. L'administrateur installe sur l'appareil l'application, les correctifs et redémarre l'appareil autant de fois que nécessaire.
5. L'administrateur clone le disque de l'appareil "étalon" sur n'importe quelle quantité d'appareils.
6. Les conditions suivantes doivent être remplies pour chaque copie clonée :
 - a. le nom de l'appareil est modifié ;
 - b. l'appareil a redémarré ;
 - c. le mode de clonage du disque est désactivé.

Activation et désactivation du mode de clonage du disque à l'aide de l'utilitaire klmover

► *Pour activer/désactiver le mode de clonage du disque de l'Agent d'administration, procédez comme suit :*

1. Lancez l'utilitaire klmover sur l'appareil doté de l'Agent d'administration qu'il faut cloner.

L'utilitaire klmover se trouve dans le dossier d'installation de l'Agent d'administration.
2. Pour activer le mode de clonage du disque, saisissez la commande `klmover -cloningmode 1` dans la ligne de commande Windows.

L'Agent d'administration passe au mode de clonage du disque.

3. Pour connaître l'état actuel du mode de clonage du disque, saisissez `klmover -cloningmode` dans la ligne de commande.

La fenêtre de l'utilitaire affiche les informations qui indiquent sur le mode de clonage du disque est activé ou non.

4. Pour désactiver le mode de clonage du disque, saisissez `klmover -cloningmode 0` dans la ligne de commande.

Préparation de l'appareil fonctionnant sous le système d'exploitation Linux à l'installation à distance de l'Agent d'administration

- *Pour préparer l'appareil fonctionnant sous le système d'exploitation Linux à l'installation à distance de l'Agent d'administration, procédez comme suit :*

1. Lancez l'analyse de la configuration de l'appareil :
 - a. Vérifiez que la connexion à l'appareil à l'aide de l'application client SSH (par exemple, l'application PuTTY) est possible.

Si vous ne pouvez pas vous connecter à l'appareil, ouvrez le fichier `/etc/ssh/sshd_config` et veillez à ce que les paramètres suivants aient les valeurs :

- `PasswordAuthentication` – non
- `ChallengeResponseAuthentication` – oui

Enregistrez le fichier (si besoin) et relancez le service SSH à l'aide de la commande `sudo service ssh restart`.

- b. Désactivez le mot de passe de la demande Sudo pour le compte utilisateur utilisé pour la connexion à l'appareil.

Utilisez la commande `sudo visudo` pour ouvrir le fichier de configuration `sudoers`. Dans le fichier qui s'ouvre, indiquez : `username ALL = (ALL) NOPASSWD: ALL`. Le nom du compte utilisateur et le mot de passe sont utilisés pour la connexion à l'appareil.

- c. Enregistrez et fermez le fichier `sudoers`.
- d. Connectez-vous à nouveau à l'appareil via SSH et vérifiez que le service Sudo ne requiert pas de mot de passe à l'aide de la commande `sudo whoami`.

2. Téléchargez et créez le paquet d'installation :

- a. Vérifiez que Libc est installé sur l'appareil : `apt-get install libc6-i386`
- b. Téléchargez le paquet d'installation de l'Agent d'administration.
- c. Pour la création du paquet d'installation à distance, utilisez les fichiers :
 - `klnagent.kpd`
 - `akinstall.sh`
 - `klnagent_8.5.0-662_i386.deb`
- d. Avant la création du paquet d'installation, modifiez dans le fichier `akinstall.sh` la ligne 81 : `Mkdir -p "$ LogDir"`

3. Créez la tâche d'installation à distance de l'application avec les paramètres :

- Dans la fenêtre **Paramètres** de l'Assistant de création de la tâche, cochez la case **Via le système d'exploitation à l'aide du Serveur d'administration**. Décochez toutes les autres cases.
- Dans la fenêtre **Sélection du compte** pour le lancement de la tâche, indiquez les paramètres du compte utilisateur utilisé pour la connexion à l'appareil via SSH.

4. Installez Network Emulator Toolkit.

Une fois Network Emulator Toolkit installé, diminuez la capacité de transmission jusqu'à 100 Kbit pour le canal sur l'appareil.

5. Lancez la tâche d'installation à distance de l'application.

L'exécution de la tâche peut prendre jusqu'à 20 minutes.

Copie de sauvegarde et restauration des données du Serveur d'administration

La copie de sauvegarde des données permet de déplacer le Serveur d'administration d'un appareil à un autre sans perte d'informations. A l'aide de la copie sauvegarde, vous pouvez restaurer les données lors du déplacement de la base d'information du Serveur d'administration à un autre appareil ou lors de la permutation sur la version plus récente de Kaspersky Security Center.

Vous pouvez créer une copie de sauvegarde des données du Serveur d'administration à l'aide d'une des options suivantes :

- Créer et lancer la tâche de copie de sauvegarde des données via la Console d'administration.
- Lancez l'utilitaire klbackup sur l'appareil où le Serveur d'administration est installé. Cet outil est fourni avec le paquet de distribution Kaspersky Security Center et se trouve à la racine du dossier d'installation indiqué après l'installation du Serveur d'administration.

La copie de sauvegarde des données du Serveur d'administration enregistre les données suivantes :

- la base de données du Serveur d'administration (stratégie, tâches, paramètres des applications, événements enregistrés sur le Serveur d'administration) ;
- les données de configuration de la structure du groupe d'administration et des appareils clients ;
- le stockage des distributifs des applications pour l'installation à distance ;
- le certificat de Serveur d'administration.

La restauration des données du Serveur d'administration est possible uniquement à l'aide de l'utilitaire klbackup.

Dans cette section

Création d'une tâche de copie de sauvegarde des données.....	395
Utilitaire de copie de sauvegarde et de restauration des données (klbackup).....	396
Sauvegarde et restauration des données en mode interactif	396
Sauvegarde et restauration des données en mode non interactif	398
Déplacement du Serveur d'administration sur un autre appareil	400

Création d'une tâche de copie de sauvegarde des données

La tâche de la copie de sauvegarde est une tâche du Serveur d'administration et elle est créée par l'Assistant de configuration initiale. Si la tâche de copie de sauvegarde, créée par l'Assistant de configuration initiale, a été supprimée, vous pouvez la créer manuellement.

► *Pour créer une tâche de copie de sauvegarde des données du Serveur d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
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**, sélectionnez l'option **Créer → Tâche**.
 - A l'aide du bouton **Créer 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 **Sauvegarde des données du Serveur d'administration**.

La tâche **Sauvegarde des données du Serveur d'administration** peut être créée dans un seul exemplaire. Si la tâche de sauvegarde des données du Serveur d'administration a déjà été créée pour le Serveur d'administration, alors elle ne s'affiche pas dans la fenêtre de sélection du type de tâche de l'Assistant de création d'une tâche.

Utilitaire de copie de sauvegarde et de restauration des données (klbackup)

Vous pouvez exécuter la copie des données du Serveur d'administration pour sauvegarder et restaurer successivement à l'aide de l'utilitaire klbackup qui fait partie du distributif Kaspersky Security Center.

L'utilitaire klbackup peut fonctionner en deux modes :

- interactif (cf. section "Sauvegarde et restauration des données en mode interactif" à la p. [396](#)) ;
- non interactif (cf. section "Sauvegarde et restauration des données en mode non interactif" à la p. [398](#)).

Sauvegarde et restauration des données en mode interactif

► *Pour créer une copie de sauvegarde des données du Serveur d'administration en mode interactif, procédez comme suit :*

1. Lancez l'utilitaire klbackup situé dans le dossier d'installation Kaspersky Security Center.

L'Assistant de sauvegarde et de restauration des données se lance.

2. Dans la première fenêtre de l'Assistant, sélectionnez l'option **Réaliser la copie de sauvegarde des données du serveur d'administration**.

Si vous cochez la case **Exécuter la copie de sauvegarde et la restauration uniquement pour le certificat de Serveur d'administration**, seul le certificat de Serveur d'administration sera sauvegardé.

Cliquez sur **Suivant**.

3. Dans la fenêtre suivante de l'Assistant, indiquez le mot de passe et le dossier de destination pour la copie de sauvegarde. Cliquez sur **Suivant** pour exécuter la copie de sauvegarde.

► *Pour restaurer les données du Serveur d'administration en mode interactif, procédez comme suit :*

1. Désinstallez le Serveur d'administration, puis installez-le à nouveau.
2. Lancez l'utilitaire klbackup situé dans le dossier d'installation Kaspersky Security Center.

Finalement, l'Assistant de sauvegarde et de restauration des données se lancera.

L'utilitaire klbackup doit être lancé sous le même compte utilisateur que celui utilisé pour installer le Serveur d'administration.

3. Dans la première fenêtre de l'Assistant, sélectionnez l'option **Rétablir les données du Serveur d'administration**.

En cochant la case **Exécuter la copie de sauvegarde et la restauration uniquement pour le certificat de Serveur d'administration**, seulement le certificat de Serveur d'administration sera restauré.

Cliquez sur **Suivant**.

4. Dans la fenêtre de l'assistant **Paramètres de restauration** :
 - Indiquez le dossier qui contient une copie de sauvegarde du Serveur d'administration.
 - Indiquez le mot de passe saisi lors de la sauvegarde des données.
5. Cliquez sur le bouton **Suivant** pour restaurer les données.

Lors de la restauration des données, le même mot de passe que celui utilisé pour la sauvegarde doit être indiqué. Si le mot de passe est incorrect, les données ne seront pas restaurées. Si le chemin d'accès au dossier partagé a changé après la sauvegarde, vous devez vérifier le fonctionnement des tâches qui utilisent les données restaurées (restauration, installation à distance) une fois que les données auront été restaurées. Le cas échéant, les paramètres de ces tâches doivent être modifiés.

Lors de la restauration des données au départ du fichier de sauvegarde, personne ne peut utiliser le dossier partagé du Serveur d'administration. Le compte utilisateur sous lequel l'utilitaire kbackup est lancé doit avoir un accès complet au dossier partagé.

Sauvegarde et restauration des données en mode non interactif

- *Pour créer une copie de sauvegarde des données ou pour restaurer les données du Serveur d'administration en mode non interactif,*

dans la ligne de commande de l'appareil où le Serveur d'administration est installé, lancez l'utilitaire kbackup avec l'ensemble de clés nécessaire.

Syntaxe de l'utilitaire :

```
kbackup [-logfile LOGFILE] -path BACKUP_PATH  
[-use_ts][[-restore] -savecert PASSWORD
```

Si le mot de passe n'est pas saisi dans la ligne de commande de l'utilitaire kbackup, l'utilitaire demandera son entrée interactivement.

Description des paramètres :

- `-logfile LOGFILE` - enregistre un rapport sur la copie ou la restauration des données du Serveur d'administration ;
- `-path BACKUP_PATH` - enregistre les données dans le dossier BACKUP_PATH/les utilise pour la restauration à partir du dossier BACKUP_PATH (paramètre obligatoire) ;

Le compte utilisateur du serveur de base de données et l'outil kbackup doivent posséder les droits pour modifier les données dans le dossier BACKUP_PATH.

- `-use_ts` : lors de l'enregistrement des données, copier les informations dans le sous-dossier `BACKUP_PATH` dossier avec un nom représentant la date et l'heure système au format `klbackup AAAA-MM-JJ # HH-MM-SS`. Si aucune clé n'est indiquée, les données seront enregistrées à la racine du dossier `BACKUP_PATH`.

Si vous essayez de sauvegarder des données dans le dossier dans lequel il existe déjà une copie de sauvegarde, un message d'erreur apparaît. Aucune mise à jour des données ne se produit.

L'utilisation du paramètre `-use_ts` permet de gérer les archives de données du Serveur d'administration. Par exemple, si le dossier `C:\KLBackups` a été spécifié en utilisant la clé `-path`, alors les données sur l'état du Serveur d'administration datant du 19 juin 2006, à 11 heures 30 et 18 secondes, seront enregistrées dans le dossier `klbackup 2006-06-19 # 11-30-18`.

- `-restore` : restaurer les données du Serveur d'administration. La restauration des données se fera en fonction des informations conservées dans le dossier `BACKUP_PATH`. Si la clé n'est pas utilisée, la copie de sauvegarde des données se fera dans le dossier `BACKUP_PATH`.
- `-savecert PASSWORD` : la fonction Enregistrer/Restaurer le Certificat du Serveur d'administration utilise le mot de passe spécifié par le paramètre `PASSWORD` pour chiffrer ou déchiffrer le certificat.

Lors de la restauration des données, le même mot de passe que celui utilisé pour la sauvegarde doit être indiqué. Si le mot de passe est incorrect, les données ne seront pas restaurées. Si le chemin d'accès au dossier partagé a changé après la sauvegarde, vous devez vérifier le fonctionnement des tâches qui utilisent les données restaurées (restauration, installation à distance) une fois que les données auront été restaurées. Le cas échéant, les paramètres de ces tâches doivent être modifiés.

Lors de la restauration des données au départ du fichier de sauvegarde, personne ne peut utiliser le dossier partagé du Serveur d'administration. Le compte utilisateur sous lequel l'utilitaire `klbackup` est lancé doit avoir un accès complet au dossier partagé.

Déplacement du Serveur d'administration sur un autre appareil

► *Pour déplacer le Serveur d'administration sur un autre appareil sans modification de la base de données du Serveur d'administration, procédez comme suit :*

1. Créez une copie de sauvegarde des données du Serveur d'administration.
2. Installez le Serveur d'administration sur l'appareil sélectionné.

Pour simplifier le transfert des groupes d'administration, il est souhaitable que l'adresse du nouveau Serveur d'administration coïncide avec l'adresse de l'ancien Serveur. L'adresse (nom de l'appareil dans le réseau Windows ou adresse IP) est définie dans les paramètres de connexion de l'Agent d'administration au Serveur.

3. Sur le nouveau Serveur d'administration, restaurez les données du Serveur au départ de la copie de sauvegarde.
4. Si l'adresse (le nom de l'appareil dans le réseau Windows ou l'adresse IP) du nouveau Serveur d'administration ne coïncide pas avec l'adresse du Serveur précédent, créez sur le Serveur précédent la tâche de modification du Serveur d'administration pour le groupe **Appareils administrés** pour connecter les appareils clients au nouveau Serveur.

Si les adresses correspondent, la tâche de changement de Serveur n'est pas nécessaire. La connexion s'effectuera selon les paramètres définis pour l'adresse du Serveur.

5. Supprimez le Serveur d'administration précédent.

► *Pour déplacer le Serveur d'administration sur un autre appareil avec modification de la base de données du Serveur d'administration, procédez comme suit :*

1. Créez une copie de sauvegarde des données du Serveur d'administration.
2. Installez un nouveau serveur SQL.

Pour un transfert correct des données sur un nouveau serveur SQL, celui-ci doit avoir les mêmes fusionnements que le serveur SQL précédent.

3. Installez le nouveau Serveur d'administration. Le nom de la base de données du Serveur précédent et du nouveau doit correspondre.

Pour simplifier le transfert des groupes d'administration, il est souhaitable que l'adresse du nouveau Serveur d'administration coïncide avec l'adresse de l'ancien Serveur. L'adresse (nom de l'appareil dans le réseau Windows ou adresse IP) est définie dans les paramètres de connexion de l'Agent d'administration au Serveur.

4. Sur le nouveau Serveur d'administration, restaurez les données du Serveur précédent au départ de la copie de sauvegarde.
5. Si l'adresse (le nom de l'appareil dans le réseau Windows ou l'adresse IP) du nouveau Serveur d'administration ne coïncide pas avec l'adresse du Serveur précédent, créez sur le Serveur précédent la tâche de modification du Serveur d'administration pour le groupe **Appareils administrés** pour connecter les appareils clients au nouveau Serveur.
6. Si les adresses correspondent, la tâche de changement de Serveur n'est pas nécessaire. La connexion s'effectuera selon les paramètres définis pour l'adresse du Serveur.
7. Supprimez le Serveur d'administration précédent.

Sauvegarde et restauration des données en mode interactif

La maintenance de la base de données du Serveur d'administration permet de réduire le volume de celle-ci, d'augmenter la productivité et la fiabilité de fonctionnement de l'application. Il est recommandé de procéder à la maintenance de la base de données du Serveur d'administration au moins une fois par semaine.

La maintenance de la base de données du Serveur d'administration s'effectue à l'aide de la tâche correspondante. Pendant la maintenance de la base de données, l'application procède comme suit :

- elle recherche les erreurs dans la base de données ;
- elle réorganise les indices de la base de données ;

- elle met à jour les statistiques de la base de données ;
- elle comprime la base de données (si nécessaire).

La tâche de maintenance de la base de données du Serveur d'administration ne prend pas en charge MySQL. Si MySQL est utilisé comme SGBD, l'administrateur doit procéder à la maintenance de la base de données de manière autonome.

► *Pour créer une tâche de copie de maintenance de la base de données du Serveur d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le nœud du Serveur d'administration pour lequel une tâche de maintenance de la base de données doit être créée.
2. Sélectionnez le dossier **Tâches**.
3. Dans l'espace de travail du dossier **Tâches**, cliquez sur le bouton **Créer une tâche**.

Ceci permet de lancer l'Assistant de création de tâche.
4. Dans la fenêtre de l'assistant **Sélection du type de tâche**, sélectionnez le type de tâche **Maintenance des bases de données** et cliquez sur **Suivant**.
5. Si, pendant la maintenance, la base de données du Serveur d'administration doit être comprimée, dans la fenêtre de l'assistant **Paramètres**, cochez la case **Rétrécir la base de données**.
6. Suivez les étapes ultérieures de l'assistant.

La tâche créée est affichée dans la liste de tâches de l'espace de travail du dossier **Tâches**. Pour un seul Serveur d'administration, une seule tâche de maintenance des bases peut être effectuée. Si une tâche de maintenance des bases pour le Serveur d'administration est déjà créée, aucune autre ne peut être créée.

Installation de l'application à l'aide des stratégies de groupe Active Directory

Kaspersky Security Center permet d'installer les applications de Kaspersky Lab à l'aide des stratégies de groupe Active Directory.

L'installation des applications à l'aide des stratégies de groupe Active Directory est possibles uniquement lors de l'utilisation des paquets d'installation incluant l'Agent d'administration.

► *Pour installer l'application à l'aide des stratégies de groupe Active Directory, procédez comme suit :*

1. Lancez le processus de création de la tâche de groupe d'installation à distance ou de la tâche d'installation à distance pour un ensemble d'appareils.
2. Dans la fenêtre de l'Assistant de création de la tâche **Paramètres**, cochez la case **Réparer l'installation du paquet d'installation dans les stratégies de groupe d'Active Directory**.
3. Lancez la tâche créée d'installation à distance ou attendez son lancement programmé.

Finalement, le mécanisme suivant de l'installation à distance sera lancé :

1. Après le lancement de la tâche dans chaque domaine comprenant les appareils clients de l'ensemble, les objets suivants seront créés :
 - la stratégie de groupe avec le nom **Kaspersky_AK{GUID}** ;
 - le groupe de sécurité **Kaspersky_AK{GUID}** lié avec la stratégie de groupe. Ce groupe de sécurité contient les appareils clients sur lesquels la tâche se diffuse. La composition du groupe de sécurité détermine la zone d'action de la stratégie de groupe.
2. L'installation des applications sur les appareils clients s'opère directement depuis le dossier réseau partagé de l'application Share. Avec cela, dans le dossier d'installation Kaspersky Security Center un dossier secondaire joint sera créé. Ce dossier contient le fichier avec extension mst pour l'application à installer.
3. Lors de l'ajout de nouveaux appareils dans la zone d'action d'une tâche, ils seront ajoutés au groupe de protection après le lancement suivant d'une tâche. Si dans la programmation d'une tâche, la case **Lancer les tâches non exécutées** est cochée, les appareils seront immédiatement ajoutés au groupe de protection.
4. Lors de la suppression des appareils depuis la zone d'action d'une tâche, leur suppression depuis le groupe de sécurité se passera lors du prochain lancement d'une tâche.
5. Lors de la suppression d'une tâche depuis Active Directory, la stratégie sera supprimée, ainsi que le lien sur cette stratégie et le groupe de protection lié avec une tâche.

Si vous voulez utiliser un autre schéma d'installation via Active Directory, vous pouvez manuellement configurer les paramètres d'installation. Cela peut être utile, par exemple, dans les cas suivants :

- quand l'administrateur de protection antivirus ne possède pas les privilèges d'apporter les modifications de certains domaines dans Active Directory ;
- s'il est nécessaire de placer le distributif d'origine sur une ressource de réseau à part ;
- pour raccorder une stratégie de groupe à des sous-divisions concrètes Active Directory.

Les options suivantes d'utilisation d'un autre schéma d'installation via Active Directory sont disponibles :

- Si l'installation doit se passer directement depuis le dossier partagé de Kaspersky Security Center, dans les propriétés d'une stratégie de groupe d'Active Directory il est nécessaire d'indiquer le fichier avec extension msi, situé dans le dossier joint exec dans le dossier du paquet d'installation de l'application requise.
- Si le paquet d'installation doit être placé dans une autre ressource de réseau, il faut y copier tout le contenu du dossier exec, puisque, excepté le fichier avec extension msi, ce dossier contient les fichiers de configuration formés au moment de création du paquet d'installation. Pour que la clé soit installée avec l'application, il faut aussi copier le fichier clé dans ce dossier.

Particularités d'utilisation de l'interface d'administration

Dans cette section

Comment faire revenir la fenêtre des propriétés	405
Comment se déplacer dans l'arborescence de la console	406
Comment ouvrir la fenêtre des propriétés de l'objet dans la zone de travail	406
Comment sélectionner le groupe des objets dans la zone de travail	406
Comment modifier l'ensemble des colonnes dans la zone de travail	407

Comment faire revenir la fenêtre des propriétés

De temps en temps la fenêtre ouverte des propriétés de l'objet disparaît de l'écran. Ceci est dû au fait qu'elle est superposée par la fenêtre principale de l'application (cette situation est une particularité de fonctionnement de la Microsoft Management Console).

- *Pour passer à la fenêtre des propriétés de l'objet,*
cliquez une combinaison des touches **ALT+TAB**.

Comment se déplacer dans l'arborescence de la console

Pour se déplacer dans l'arborescence de la console vous pouvez utiliser les touches suivantes, situées dans la barre d'outils :

-  : passage à un pas en arrière ;
-  : passage à un pas en avant ;
-  : passage à un niveau plus haut.

Aussi vous pouvez utiliser une chaîne de navigation, située dans l'espace de travail en haut à droite. La chaîne de navigation contient le chemin complet vers ce dossier de l'arborescence de la console où vous êtes situés en ce moment. Tous les éléments de la chaîne, à part le dernier, sont les liens vers les objets de l'arborescence de la console.

Comment ouvrir la fenêtre des propriétés de l'objet dans l'espace de travail

Les propriétés de la plupart des objets de la Console d'administration peuvent être modifiées dans la fenêtre des propriétés de l'objet.

- *Pour ouvrir la fenêtre des propriétés de l'objet situé dans l'espace de travail, exécutez une des actions suivantes :*
 - dans le menu contextuel de l'objet, sélectionnez l'option **Propriétés** ;
 - sélectionnez l'objet et cliquez une combinaison des touches **ALT+ENTER**.

Comment sélectionner le groupe des objets dans l'espace de travail

Vous pouvez sélectionner le groupe des objets dans l'espace de travail. La sélection du groupe des objets peut être utilisée, par exemple, pour créer un ensemble d'appareils et former ensuite les tâches qui y sont liées.

► *Pour sélectionner la plage des objets, procédez comme suit :*

1. Sélectionnez le premier objet et appuyez sur la touche **SHIFT**.
2. En appuyant sur la touche **SHIFT**, sélectionnez le dernier objet de la plage.

La plage sera sélectionnée.

► *Pour unir les objets séparés dans le groupe, procédez comme suit :*

1. Sélectionnez le premier objet dans le groupe et appuyez sur la touche **CTRL**.
2. En appuyant sur la touche **CTRL**, sélectionnez les autres objets du groupe.

Les objets seront unis dans le groupe.

Comment modifier l'ensemble des colonnes dans l'espace de travail

La Console d'administration permet de modifier l'ensemble des colonnes, reflétées dans l'espace de travail.

► *Afin de modifier l'ensemble des colonnes dans l'espace de travail, procédez comme suit :*

1. Sélectionnez l'objet de l'arborescence de la console, pour lequel vous voulez modifier l'ensemble des colonnes.
2. Dans le menu de la Console d'administration sélectionnez l'option **Affichage** → **Ajouter ou supprimer des colonnes**.
3. Dans la fenêtre ouverte créez l'ensemble des colonnes à refléter.

Aide

Cette section reprend dans les tableaux le récapitulatif sur le menu contextuel des objets de la Console d'administration, ainsi que sur les états d'objets de l'arborescence de la console et de l'espace de travail.

Dans cette section

Utilisation de l'agent de mises à jour en guise de passerelles	408
Utilisation des masques dans les variables chaînes.....	409
Commandes du menu contextuel.....	409
A propos du gestionnaire des connexions	415
Autorisations de l'utilisateur pour la gestion des appareils mobiles via Exchange ActiveSync .	416
A propos de l'administrateur du Serveur virtuel.....	418
Liste des appareils administrés. Valeur des colonnes	419
Etats des appareils, des tâches et des stratégies	423
Icônes des états des fichiers dans la Console d'administration.....	425
Utilisation des expressions régulières dans la ligne de recherche.....	427

Utilisation de l'agent de mises à jour en guise de passerelles

Si le Serveur d'administration se trouve en dehors de la zone démilitarisée (DMZ), les Agents d'administration qui sont dans la zone de confiance perdent la possibilité de se connecter avec le Serveur.

Pour établir une connexion entre le Serveur d'administration et les Agents d'administration, il est possible d'utiliser comme passerelle un agent de mises à jour. L'Agent de mises à jour offre au Serveur d'administration un port pour établir une connexion. Au lancement, le Serveur

d'administration se connecte avec l'agent de mises à jour et n'interrompt pas la connexion avec ce dernier tout au long de son fonctionnement.

Une fois qu'il a reçu le signal du Serveur d'administration, l'Agent de mises à jour envoie un signal UDP aux Agents d'administration pour la connexion au Serveur d'Administration. Une fois que les Agents d'administration ont reçu le signal, ils se connectent à l'Agent de mises à jour qui transmet les informations entre eux et le Serveur d'administration.

Utilisation des masques dans les variables chaînes

Pour les variables de chaînes, il est permis d'utiliser les masques. Pour créer les masques, vous pouvez utiliser les expressions régulières suivantes :

- * – n'importe quelle ligne d'une longueur de 0 ou plus de symboles ;
- ? – un n'importe quel symbole ;
- [<intervalle>] : n'importe quel symbole de la plage indiquée ou de la multitude.

Par exemple : [0–9] – n'importe quel chiffre ; [abcdef] – un des caractères a, b, c, d, e, f.

Commandes du menu contextuel

Cette section contient la liste des objets de la Console d'administration et l'ensemble d'options du menu contextuel y correspondant (cf. tableau ci-après).

Tableau 6. *Éléments du menu contextuel des entrées de la Console d'administration*

Objet	Option du menu	Désignation de l'option du menu
Points généraux du menu contextuel	Recherche	Ouvrir la fenêtre de recherche d'appareils.
	Actualiser	Actualiser l'affichage de l'objet sélectionné.

Objet	Option du menu	Désignation de l'option du menu
	Exporter la liste	Exporter la liste courante dans le fichier.
	Propriétés	Ouvrir la fenêtre des propriétés de l'objet sélectionné.
	Affichage → Ajouter ou supprimer des colonnes	Ajouter ou supprimer des colonnes dans le tableau d'objets dans l'espace de travail.
	Affichage → Grandes icônes	Afficher les objets dans l'espace de travail comme des grandes icônes.
	Affichage → Petites icônes	Afficher les objets dans l'espace de travail comme des petites icônes.
	Affichage → Liste	Afficher les objets dans l'espace de travail comme une liste.
	Affichage → Tableau	Afficher les objets dans l'espace de travail comme un tableau.
	Affichage → Personnaliser	Configurer l'affichage des éléments de la console de gestion.

Objet	Option du menu	Désignation de l'option du menu
Kaspersky Security Center	Créer → Serveur d'administration	Ajouter un Serveur d'administration à l'arborescence de la console.
<Nom du Serveur d'administration>	Se connecter au Serveur d'administration	Se connecter au Serveur d'administration.
	Se déconnecter du Serveur d'administration	Se déconnecter du Serveur d'administration.
Appareils administrés	Installer une application	Exécuter l'Assistant de l'installation à distance de l'application.
	Affichage → Configuration de l'interface	Configurer l'affichage des éléments de l'interface.
	Supprimer	Supprimer le Serveur d'administration de l'arborescence de la console.
	Installer une application	Lancer l'Assistant de l'installation à distance pour le groupe d'administration.
	RAZ compteur de virus	Mettre à zéro les compteurs de virus pour les appareils qui font partie du groupe d'administration.
	Activité virale	Créer le rapport d'activité virale des appareils, qui font partie du groupe d'administration.

Objet	Option du menu	Désignation de l'option du menu
	Créer → Groupe	Créer le groupe d'administration.
	Toutes les tâches → Créer une structure de groupes	Créer la structure des groupes d'administration sur la base de la structure des domaines ou d'Active Directory.
	Toutes les tâches → Afficher un message	Lancer l'Assistant de création du message pour les utilisateurs des appareils qui font partie du groupe d'administration.
Appareils administrés → Serveurs d'administration	Créer → Serveur d'administration secondaire	Lancer l'Assistant d'ajout du Serveur d'administration secondaire.
	Créer → Serveur d'administration virtuel	Lancer l'Assistant d'ajout du Serveur d'administration virtuel.
Sélections d'appareils	Créer → Nouvelle sélection	Créer un ensemble d'appareils.
	Toutes les tâches → Importer	Importer une sélection depuis un fichier.

Objet	Option du menu	Désignation de l'option du menu
Administration des applications → Catégories d'applications	Créer → Catégorie	Créer une catégorie d'applications.
Administration des applications → Registre des applications	Filtre	Configurer le filtre pour la liste des applications.
	Applications contrôlées	Configurer la publication des événements sur l'installation des applications.
	Supprimer les applications non installées	Supprimer de la liste les informations sur les applications qui ne sont pas déjà installées sur les appareils de réseau.
Administration des applications → Mises à jour du logiciel	Accepter les Contrats de Licence des mises à jour	Accepter le Contrat de Licence Utilisateur Final des mises à jour du logiciel.
Administration des applications → Licence pour les logiciels de Kaspersky Lab	Ajouter une clé	Ajouter une clé dans le stockage du Serveur d'administration.
	Activer l'application	Lancer l'Assistant de création de la tâche d'activation de l'application.
	Rapport de clés	Créer et afficher le rapport de clés sur les appareils clients.

Objet	Option du menu	Désignation de l'option du menu
Administration des applications → Compte des licences tierces	Créer → Groupe des applications sous licence	Créer un groupe des applications sous licence.
Administration des appareils mobiles → Appareils mobiles	Créer → Appareil mobile	Connecter le nouvel appareil mobile de l'utilisateur.
Administration des appareils mobiles → Certificats	Créer → Certificat	Créer un certificat.
	Créer → Appareil mobile	Connecter le nouvel appareil mobile de l'utilisateur.
Installation à distance → Paquets d'installation	Afficher les versions actuelles des applications	Afficher la liste des versions actuelles des applications Kaspersky Lab exposées sur les serveurs Web.
	Créer → Paquet d'installation	Créer un paquet d'installation.
	Toutes les tâches → Mettre à jour les bases	Actualiser les bases des applications dans les paquets d'installation.
	Toutes les tâches → Afficher la liste générale des paquets autonomes	Consulter la liste des paquets d'installation autonomes créés pour les paquets d'installation.

Objet	Option du menu	Désignation de l'option du menu
Sondage du réseau → Domaines	Toutes les tâches → Activité des appareils	Configurer les paramètres de la réaction du Serveur d'administration à la recherche d'activité d'appareils dans le réseau.
Sondage du réseau → Plages IP	Créer → Plage IP	Créer une plage IP.
Stockages → Mises à jour et correctifs du logiciel Kaspersky Lab	Télécharger les mises à jour	Lancer la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration.
	Paramètres de téléchargement des mises à jour	Configurer les paramètres de la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration.
	Rapport de versions de base	Créer et importer le rapport de versions des bases.
	Toutes les tâches → Purger le stockage des mises à jour	Purger le stockage des mises à jour sur le Serveur d'administration.
Stockages → Matériel	Créer → Appareil	Créer un périphérique réseau.

A propos du gestionnaire des connexions

La fenêtre des propriétés de la stratégie de l'Agent d'administration dans la section **Réseau** dans la section jointe **Gestionnaire de connexions** permet de définir les intervalles temporaires auxquels l'Agent d'administration transmettra les données sur le Serveur d'administration.

Se connecter en cas de nécessité. Si cette option a été sélectionnée, la connexion s'établira quand l'Agent d'administration devra transférer les données sur le Serveur d'administration.

Se connecter aux intervalles indiqués. Si cette option a été sélectionnée, la connexion de l'Agent d'administration au Serveur d'administration est effectuée dans les intervalles indiqués. Plusieurs périodes de connexions peuvent être ajoutées.

Autorisations de l'utilisateur pour l'administration des appareils mobiles via Exchange ActiveSync

Pour administrer les appareils mobiles qui fonctionnent selon le protocole Exchange ActiveSync avec un serveur Microsoft Exchange Server 2010 ou Microsoft Exchange Server 2013, l'utilisateur doit appartenir à un groupe autorisé à réaliser les commandlets suivants :

- Get-CASMailbox
- Set-CASMailbox
- Remove-ActiveSyncDevice
- Clear-ActiveSyncDevice
- Get-ActiveSyncDeviceStatistics
- Get-AcceptedDomain
- Set-AdServerSettings

- Get-ActiveSyncMailboxPolicy
- New-ActiveSyncMailboxPolicy
- Set-ActiveSyncMailboxPolicy
- Remove-ActiveSyncMailboxPolicy

Pour administrer les appareils mobiles qui fonctionnent selon le protocole Exchange ActiveSync avec un serveur Microsoft Exchange Server 2007, l'utilisateur doit posséder des autorisations d'administration. Dans le cas contraire, il faut exécuter les commandlets pour définir les autorisations d'administration de l'utilisateur (cf. tableau ci-dessous).

Tableau 7. Autorisations d'administration pour la gestion des appareils mobiles Exchange ActiveSync sous Microsoft Exchange Server 2007

Accès	Objet	Commandlet
Complet	Branche "CN=Mobile Mailbox Policies,CN=Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	Add-ADPermission -User <nom d'utilisateur ou du groupe> -Identity "CN=Mobile Mailbox Policies,CN=<nom de l'organisation>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<nom du domaine>" -InheritanceType All -AccessRight GenericAll
Lecture	Branche "CN= Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC= yourdomain"	Add-ADPermission -User <nom d'utilisateur ou de groupe> -Identity "CN=<nom de l'organisation>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<nom du domaine>" -InheritanceType All -AccessRight GenericRead

Accès	Objet	Commandlet
Lecture et écriture	Propriétés msExchMobileMailboxPolicyLink et msExchOmaAdminWirelessEnable pour les objets dans Active Directory	<pre>Add-ADPermission -User <nom d'utilisateur ou de groupe> -Identity "DC=<nom de domaine>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable</pre>
Complet	Stockage des boîtes aux lettres ms-Exch-Store-Admin pour mailboxstorages	<pre>Get-MailboxDatabase Add-ADPermission -User <nom d'utilisateur ou de groupe> -ExtendedRights ms-Exch-Store-Admin</pre>

Pour obtenir des informations détaillées sur l'utilisation des commandlet dans la console Exchange Management Shell, consultez le site Internet du support technique Microsoft Exchange Server [http://technet.microsoft.com/en-us/library/bb123778\(v=exchg.150\).aspx](http://technet.microsoft.com/en-us/library/bb123778(v=exchg.150).aspx).

A propos de l'administrateur du Serveur virtuel

L'administrateur du réseau de l'entreprise sous le Serveur virtuel va lancer Kaspersky Security Center 10 Web Console pour consulter les informations sur l'état de la protection antivirus du réseau sous le nom du compte utilisateur indiqué dans cette fenêtre.

Dans le cas de besoin, il est possible de créer plusieurs comptes utilisateur d'administrateurs du Serveur virtuel.

L'administrateur du Serveur d'administration virtuel est un utilisateur interne de Kaspersky Security Center. Les informations sur les utilisateurs internes ne sont pas transmises au système d'exploitation. Kaspersky Security Center effectue l'authentification des utilisateurs internes.

Liste des appareils administrés. Valeur des colonnes

Le tableau ci-dessous reprend les noms et les descriptions des colonnes de la liste des appareils administrés.

Tableau 8. Valeur des colonnes de la liste des appareils administrés

Nom de la colonne	Valeur
Nom	Nom NetBios de l'appareil client. Une description des icônes de nom d'appareil est fournie dans l'appendice (cf. section "États des appareils, des tâches et des stratégies" à la page 423).
Type de S.E.	Type de système d'exploitation de l'appareil client.
Domaine Windows	Nom du domaine Windows auquel appartient l'appareil client.
Agent installé	Résultat de l'installation de l'Agent d'administration sur l'appareil client.
L'Agent fonctionne	Résultat du fonctionnement de l'Agent d'administration.
Protection en temps réel	L'application de protection est installée (<i>Oui, Non</i>).
Connexion au Serveur	Temps écoulé depuis la connexion de l'appareil client au Serveur d'administration.

Nom de la colonne	Valeur
Heure de dernière mise à jour	Temps écoulé depuis la dernière mise à jour du Serveur d'administration Kaspersky Security Center.
Etat	Etat actuel de l'appareil client (<i>OK, Critique ou Avertissement</i>).
Description de l'état	<p>Causes de la modification de l'état de l'appareil client en <i>Critique</i> ou <i>Avertissement</i>.</p> <p>L'état de l'appareil devient <i>Avertissement</i> ou <i>Critique</i> pour les raisons suivantes :</p> <ul style="list-style-type: none"> • application de protection non installée ; • détection d'un volume important de virus ; • niveau de protection en temps réel différent du niveau défini par l'administrateur ; • l'analyse antivirus n'a pas été réalisée depuis longtemps ; • les bases sont obsolètes ; • connexion non établie depuis longtemps ; • présence d'objets non traités ; • redémarrage requis ; • applications incompatibles installées ; • vulnérabilités détectées dans les applications ; • la recherche de mises à jour Windows n'a pas été réalisée depuis longtemps ; • état déterminé du chiffrement des données ; • les paramètres de l'appareil mobile ne correspondent pas à la stratégie ; • présence d'incidents non traités ; • expiration prochaine de la licence. <p>L'état de l'appareil devient uniquement <i>Critique</i> pour les raisons suivantes :</p> <ul style="list-style-type: none"> • durée de validité de la licence écoulée ;

Nom de la colonne	Valeur
	<ul style="list-style-type: none"> • perte de la connexion à l'appareil client ; • protection désactivée ; • application de protection non lancée. <p>Les applications administrées de Kaspersky Lab installées sur les appareils clients peuvent compléter la liste de descriptions des états. Kaspersky Security Center peut recevoir la description de l'état de l'appareil client de la part des applications administrées Kaspersky Lab installées sur cet appareil. Si l'état attribué à l'appareil par les applications administrées ne coïncide pas avec l'état attribué par Kaspersky Security Center, dans la Console d'administration s'affiche l'état le plus critique pour la sécurité de l'appareil. Par exemple, si une des applications administrées a attribué à l'appareil l'état <i>Critique</i>, et que Kaspersky Security Center a attribué l'état <i>Avertissement</i>, dans la Console d'administration pour l'appareil s'affichent l'état <i>Critique</i> et la description de l'état attribué par l'application administrée.</p>
Mise à jour d'information	Temps écoulé depuis la dernière synchronisation réussie de l'appareil client avec le Serveur d'administration.
Nom du domaine DNS	Nom du domaine DNS de l'appareil client.
Domaine DNS	Suffixe DNS principal.
Adresse IP	Adresse IP de l'appareil client. Il est conseillé d'utiliser une adresse IPv4.
Visible	Période de visibilité de l'appareil client dans le réseau.
Analyse à la demande	Date et heure de la dernière analyse de l'appareil client effectuée à l'aide de l'application de protection à la demande de l'utilisateur.
Virus détectés	Nombre de virus trouvés.

Nom de la colonne	Valeur
Etat de la protection en temps réel	Etat de la protection en temps réel (<i>En cours de démarrage, En cours d'exécution, En cours d'exécution (protection maximale), En cours d'exécution (vitesse maximale), En cours d'exécution (recommandé), En cours d'exécution (avec paramètres personnalisés), Stoppée, Suspendue, Echec</i>).
Adresse IP de la connexion	Adresse IP de la connexion au Serveur d'administration Kaspersky Security Center.
Version de l'Agent d'administration	Version de l'Agent d'administration.
Version de la protection	Version de l'application de protection installée sur l'appareil client.
Version de la base	Version de la base antivirus.
Heure de l'activation	Date et heure du dernier démarrage de l'appareil client.
Redémarrage	Le redémarrage de l'appareil client est requis.
Agent de mises à jour	Nom de l'appareil qui remplit le rôle d'Agent de mises à jour pour cet appareil client.
Description	Description de l'appareil client obtenue lors du sondage du réseau.
Etat du chiffrement	Etat du chiffrement des données de l'appareil client.

Nom de la colonne	Valeur
Etat WUA	Etat du Windows Update Agent de l'appareil client. La valeur "Oui" désigne les appareils clients qui reçoivent les mises à jour via Windows Update depuis le Serveur d'administration. La valeur "Non" désigne les appareils clients qui reçoivent les mises à jour via Windows Update depuis d'autres sources.
Capacité du système d'exploitation	Capacité du système d'exploitation de l'appareil client.
Etat de protection contre les spams	Etat de protection contre les spams (<i>En cours d'exécution, En cours de démarrage, Stoppée, Suspendue, Echec, Inconnu</i>).
Etat de protection contre les fuites de données	Etat de protection contre les fuites de données (<i>En cours d'exécution, En cours de démarrage, Stoppée, Suspendue, Echec, Inconnu</i>).
Etat de protection des serveurs de collaboration	Etat du filtrage du contenu (<i>En cours d'exécution, En cours de démarrage, Stoppée, Suspendue, Echec, Inconnu</i>).
Etat de protection antivirus des serveurs de messagerie	Etat de protection antivirus des serveurs de messagerie (<i>En cours d'exécution, En cours de démarrage, Stoppée, Suspendue, Echec, Inconnu</i>).

Etats des appareils, des tâches et des stratégies

Le tableau ci-après reprend la liste des icônes qui apparaissent dans l'arborescence de la console et dans l'espace de travail de la Console d'administration à côté des noms des appareils, des tâches et des stratégies. Ces icônes définissent l'état des objets.

Tableau 9. Etats des appareils, des tâches et des stratégies

Icône	Etat
	Appareil avec un système d'exploitation pour postes de travail détecté dans le réseau mais n'appartenant à aucun groupe d'administration.
	Appareil avec un système d'exploitation pour postes de travail appartenant à un groupe d'administration et correspondant à l'état <i>OK</i> .
	Appareil avec un système d'exploitation pour postes de travail appartenant à un groupe d'administration et correspondant à l'état <i>Avertissement</i> .
	Appareil avec un système d'exploitation pour poste de travail appartenant à un groupe d'administration et correspondant à l'état <i>Critique</i> .
	Appareil avec un système d'exploitation pour postes de travail appartenant à un groupe d'administration dont la connexion au Serveur d'administration est perdue.
	Appareil avec un système d'exploitation pour serveurs détecté dans le réseau mais n'appartenant à aucun groupe d'administration.
	Appareil avec un système d'exploitation pour serveurs appartenant à un groupe d'administration et correspondant à l'état <i>OK</i> .
	Appareil avec un système d'exploitation pour serveurs appartenant à un groupe d'administration et correspondant à l'état <i>Avertissement</i> .
	Appareil avec un système d'exploitation pour serveurs appartenant à un groupe d'administration et correspondant à l'état <i>Critique</i> .
	Appareil avec un système d'exploitation pour serveurs appartenant à un groupe d'administration dont la connexion au Serveur d'administration est perdue.
	Appareil mobile détecté dans le réseau et ne faisant partie d'aucun groupe d'administration.
	Appareil mobile faisant partie d'un groupe d'administration avec l'état <i>OK</i> .

	Appareil mobile faisant partie d'un groupe d'administration avec l'état <i>Avertissement</i> .
	Appareil mobile faisant partie d'un groupe d'administration avec l'état <i>Critique</i> .
	Appareil mobile faisant partie d'un groupe d'administration et dont la connexion au Serveur d'administration a été perdue.
	Stratégie active.
	Stratégie inactive.
	Stratégie active héritée du groupe créé sur le Serveur d'administration principal.
	Stratégie active héritée depuis le groupe à un niveau supérieur de la hiérarchie.
	Tâche (de groupe, du Serveur d'administration ou pour un ensemble d'appareils) dans l'état <i>En attente d'exécution</i> ou <i>Terminée</i> .
	Tâche (de groupe, du Serveur d'administration ou pour un ensemble d'appareils) dans l'état <i>En cours d'exécution</i> .
	Tâche (de groupe, du Serveur d'administration ou pour un ensemble d'appareils) dans l'état <i>Terminée avec une erreur</i> .
	Tâche héritée du groupe créé sur le Serveur d'administration principal.
	Tâche héritée depuis le groupe à un niveau supérieur de la hiérarchie.

Icônes des états des fichiers dans la Console d'administration

Pour simplifier l'utilisation des fichiers dans la Console d'administration de Kaspersky Security Center, des icônes s'affichent en regard des noms de fichiers. Les icônes signalent les états attribués aux fichiers par les applications administrées de Kaspersky Lab sur les appareils clients. Les icônes s'affichent dans l'espace de travail des dossiers **Quarantaine**, **Sauvegarde** et **Fichiers avec traitement différé**.

Tableau 10. Correspondance des icônes aux états des fichiers

Icône	Etat
	Fichier avec l'état <i>Infecté</i> .
	Fichier avec l'état <i>Avertissement</i> ou <i>Potentiellement infecté</i> .
	Fichier avec l'état <i>Placé dans le dossier par l'utilisateur</i> .
	Fichier avec l'état <i>Faux positif</i> .
	Fichier avec l'état <i>Désinfecté</i> .
	Fichier avec l'état <i>Supprimé</i> .
	Fichier dans le dossier Quarantaine avec l'état <i>Non infecté</i> , <i>Protégé par un mot de passe</i> ou <i>L'envoi à Kaspersky Lab est requis</i> . S'il n'y a pas de description de l'état en regard de l'icône, cela signifie que l'application administrée de Kaspersky Lab sur l'appareil client a transmis à Kaspersky Security Center un état inconnu.

	<p>Fichier dans le dossier Sauvegarde avec l'état <i>Non infecté</i>, <i>Protégé par un mot de passe</i> ou <i>L'envoi à Kaspersky Lab est requis</i>. S'il n'y a pas de description de l'état en regard de l'icône, cela signifie que l'application administrée de Kaspersky Lab sur l'appareil client a transmis à Kaspersky Security Center un état inconnu.</p>
	<p>Fichier dans le dossier Fichiers avec traitement différé avec l'état <i>Non infecté</i>, <i>Protégé par un mot de passe</i> ou <i>L'envoi à Kaspersky Lab est requis</i>. S'il n'y a pas de description de l'état en regard de l'icône, cela signifie que l'application administrée de Kaspersky Lab sur l'appareil client a transmis à Kaspersky Security Center un état inconnu.</p>

Utilisation des expressions régulières dans la ligne de recherche

Vous pouvez saisir les expressions régulières suivantes dans la ligne de recherche pour rechercher des mots et des caractères particuliers :

- *. Remplace une succession d'un nombre indéterminé de caractères. Par exemple, pour rechercher les mots informatique, informaticien ou informations, saisissez `informati*` dans la ligne de recherche.
- ?. Remplace un n'importe quel caractère. Par exemple, pour rechercher les mots car ou cap, saisissez `ca?` dans la ligne de recherche.

Le texte dans la ligne de recherche ne peut pas commencer par ?.

- [`<intervalle>`]. Remplace n'importe quel symbole de la plage indiquée ou de la multitude. Par exemple, pour rechercher n'importe quel chiffre, saisissez l'expression `[0-9]` dans la ligne. Pour rechercher un des caractères a, b, c, d, e, f, saisissez l'expression `[abcdef]` dans la ligne.

Vous pouvez saisir les expressions régulières suivantes dans la ligne de recherche dans le cadre d'une recherche en texte intégral :

- Espace. Signifie la présence d'au moins un mot parmi les mots séparés par des espaces. Par exemple, pour rechercher des expressions contenant le mot `Secondaire` ou `Virtuel` (ou les deux), saisissez l'expression `Secondaire Virtuel`.
- Symbole "plus" (+), AND ou &&. Avant le mot signifie la présence obligatoire du mot dans le texte. Par exemple, pour rechercher des expressions contenant le mot `Secondaire` et le mot `Virtuel`, vous pouvez saisir une des expressions suivantes dans la ligne de recherche : `+Secondaire+Virtuel`, `Secondaire AND Virtuel`, `Secondaire && Virtuel`.
- OR ou ||. L'utilisation de cet opérateur entre deux mots indique qu'un mot ou l'autre doit figurer dans le texte. Par exemple, pour rechercher des expressions contenant le mot `Secondaire` ou le mot `Virtuel`, saisissez une des expressions suivantes dans la ligne de recherche : `Secondaire OR Virtuel`, `Secondaire || Virtuel`.
- Symbole "moins" (-). Avant le mot signifie l'absence obligatoire du mot dans le texte. Par exemple, pour rechercher une expression qui doit contenir le mot `Secondaire` mais pas le mot `Virtuel`, il faut saisir l'expression `+Secondaire-Virtuel` dans la ligne de recherche.
- "<fragment du texte>". Le fragment du texte entre guillemets doit être entièrement présent dans le texte. Par exemple, pour rechercher une expression contenant la combinaison `Serveur secondaire`, il faut saisir `"Serveur secondaire"` dans la ligne de recherche.

La recherche en texte intégral est disponible dans les groupes de filtrage suivants :

- dans le groupe de filtrage de la liste des événements selon les colonnes **Événement** et **Description** ;
- dans le groupe de filtrage des comptes utilisateur selon la colonne **Nom** ;
- dans le groupe de filtrage du registre des applications selon la colonne **Nom**, si la case **Grouper les application par noms** est décochée.

Glossaire

A

Administrateur de Kaspersky Security Center

La personne qui gère les opérations du programme grâce à un système d'administration centralisé à distance de Kaspersky Security Center.

Agent d'administration

Le module de l'application Kaspersky Security Center qui coordonne les interactions entre le Serveur d'administration et les applications Kaspersky Lab installées sur un poste spécifique du réseau (un poste de travail ou un serveur). Ce composant est un composant unique pour toutes les applications de l'entreprise pour Windows. Il existe des versions de l'Agent d'administration spécifiques aux applications Kaspersky Lab fonctionnant sur Novell®, Unix™ et Mac.

Agent d'authentification

L'interface qui permet de passer la procédure d'authentification pour accéder aux disques durs chiffrés et pour démarrer le système d'exploitation après le chiffrement du disque dur système.

Agent de mises à jour

Appareil avec un Agent d'administration installé, utilisé pour la diffusion des mises à jour, l'installation des applications à distance, la réception d'informations sur les appareils faisant partie du groupe d'administration et/ou d'un domaine multicast. Les agents de mises à jour sont conçus pour réduire la surcharge sur le Serveur d'administration lors de la diffusion des mises à jour et pour optimiser le trafic sur le réseau. Ils peuvent être désignés automatiquement par le Serveur d'administration ou manuellement par l'administrateur.

Appareil EAS

Appareil mobile qui se connecte au Serveur d'administration via le protocole Exchange ActiveSync. Le protocole Exchange ActiveSync permet de connecter et d'administrer les appareils iOS, Android et Windows Phone®.

Appareil KES

Appareil mobile qui se connecte au Serveur d'administration et est administré à l'aide de l'app mobile Kaspersky Endpoint Security for Android.

Appareil MDM iOS

Appareil mobile qui se connecte au Serveur MDM iOS via le protocole MDM iOS. Ce protocole permet de connecter et d'administrer les appareils ayant un système d'exploitation iOS.

Attaque de virus

Tentatives multiples d'infection d'un appareil par un virus.

B

Base antivirus

Base de données contenant des informations sur les menaces informatiques connues de Kaspersky Lab au moment de la publication des bases antivirus. Les entrées de la base antivirus permettent de détecter le code malveillant dans les objets analysés. Les bases antivirus sont créées par les experts de Kaspersky Lab et sont actualisées toutes les heures.

Boutique des apps

Module de l'application Kaspersky Security Center. La boutique des apps est utilisée pour l'installation d'apps sur les appareils Android des utilisateurs. Dans la boutique d'apps, on peut publier les fichiers apk des apps et les liens vers les apps dans Google Play.

C

Certificat général

Certificat conçu pour identifier l'appareil mobile de l'utilisateur.

Client du Serveur d'administration (Appareil client)

Appareil, serveur ou poste de travail sur lequel l'Agent d'administration est installé, ainsi que les applications administrées de Kaspersky Lab.

Clé active

La clé utilisée au moment actuel pour faire fonctionner l'application.

Clé complémentaire

La clé qui confirme le droit d'utilisation de l'application, mais non utilisée au moment actuel.

Console d'administration Kaspersky

Le module de l'application Kaspersky Security Center qui offre l'interface utilisateur pour les services d'administration du Serveur d'administration et de l'Agent d'administration.

D

Domaine multicast

Segment logique de réseau informatique dans lequel tous les nœuds peuvent se transmettre des données mutuellement à l'aide d'un canal multicast au niveau du modèle réseau OSI (Open Systems Interconnection Basic Reference Model).

G

Groupe d'administration

L'ensemble d'appareils regroupés selon les fonctions exécutées et les applications de Kaspersky Lab installées. Les appareils sont regroupés pour en faciliter la gestion dans son ensemble. Le groupe peut contenir d'autres groupes. Les stratégies de groupe et les tâches de groupe peuvent être créées pour chaque application installée dans le groupe.

Groupe de rôle

Le groupe des utilisateurs des appareils mobiles Exchange ActiveSync qui possèdent les mêmes privilèges d'administrateur (cf. section "Privilèges d'administrateur" à la page 424).

Groupe des applications sous licence

Le groupe des applications créé sur la base des critères définis par l'administrateur (par exemple, selon l'éditeur) pour lesquels le comptage des installations sur les appareils clients a lieu.

K

Kaspersky Security Network (KSN)

Infrastructure de services cloud et offrant l'accès à la base opérationnelle de connaissance de Kaspersky Lab sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky Lab sur les menaces, augmente l'efficacité de fonctionnement de certains modules de la protection, ainsi que diminue la possibilité des faux positifs.

M

Mise à jour disponible

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

N

Niveau d'importance du correctif

Caractéristique du correctif. Cinq niveaux d'importance existent pour les correctifs des éditeurs étrangers ou Microsoft :

- Critique.
- Elevé.
- Normal.
- Bas.
- Inconnu.

Le niveau d'importance du correctif d'un éditeur étranger ou de Microsoft est défini par le niveau de gravité le plus défavorable de la vulnérabilité corrigé par le correctif.

P

Paquet d'installation

L'ensemble de fichiers pour l'installation à distance de l'application Kaspersky Lab à l'aide du système d'administration à distance Kaspersky Security Center. Le paquet d'installation contient un ensemble de paramètres nécessaires pour installer une application et assurer son efficacité immédiatement après l'installation. Les valeurs des paramètres correspondent aux valeurs des paramètres de l'application par défaut. Le paquet d'installation est créé sur la base de fichiers .kpd et .kud inclus dans la distribution de l'application.

Privilèges d'administrateur

Le niveau des privilèges et des pouvoirs de l'utilisateur pour administrer les objets Exchange à l'intérieur de l'entreprise Exchange.

Profil

L'ensemble des paramètres de comportement des appareils mobiles Exchange ActiveSync lors de la connexion au serveur Microsoft Exchange.

Profil de configuration

La stratégie qui contient l'ensemble de paramètres et de restrictions pour l'appareil mobile MDM iOS.

Profil MDM iOS

L'ensemble des paramètres de connexion des appareils mobiles iOS au Serveur d'administration. Le profil MDM iOS est installé par l'utilisateur sur l'appareil mobile, après quoi l'appareil mobile se connecte au Serveur d'administration.

Profil provisioning

L'ensemble des paramètres pour utiliser les apps sur les appareils mobiles iOS. Le profil provisioning contient les informations sur la licence et il est lié à une app concrète.

Propriétaire de l'appareil

Le propriétaire de l'appareil est un utilisateur que l'administrateur peut contacter en cas de nécessité d'un travail quelconque avec l'appareil.

R

Restauration

Le déplacement d'un objet original depuis le dossier de quarantaine ou de sauvegarde vers l'emplacement où il était avant sa mise en quarantaine, sa désinfection ou sa suppression ou vers un dossier spécifié par l'utilisateur.

Restauration des données du Serveur d'administration

Il s'agit de la restauration des données du Serveur d'administration à l'aide d'un utilitaire de sauvegarde sur la base des informations présentes dans le dossier de sauvegarde. L'utilitaire permet de restaurer :

- la base du Serveur d'administration (stratégie, tâches, paramètres d'application, événements enregistrés sur le Serveur d'administration) ;
- les données de configuration de la structure du groupe d'administration et des appareils clients ;
- le stockage des paquets d'installation des applications pour l'installation à distance (contenu des dossiers Packages, Uninstall, Updates) ;
- le certificat de Serveur d'administration.

S

Serveur d'administration domestique

Le Serveur d'administration domestique est le Serveur d'administration qui a été indiqué lors de l'installation de l'Agent d'administration. Le Serveur d'administration domestique peut être utilisé dans les paramètres des profils de connexion de l'Agent d'administration.

Serveur d'administration virtuel

Le module de l'application Kaspersky Security Center conçu pour l'administration du système de protection du réseau de l'entreprise cliente.

Le Serveur d'administration virtuel est un cas particulier du Serveur d'administration secondaire et, par rapport au Serveur d'administration physique, possède des restrictions suivantes :

- Le Serveur d'administration virtuel peut fonctionner uniquement s'il fait partie du Serveur d'administration principal.
- Le Serveur d'administration virtuel utilise pour son fonctionnement la base de données du Serveur d'administration principal : les tâches de sauvegarde et de restauration des données, les analyses et les réceptions des mises à jour ne sont pas prises en charge sur le serveur virtuel. Ces tâches se résolvent dans le cadre du Serveur d'administration principal.
- La création des Serveurs d'administration secondaires (y compris les Serveurs virtuels) n'est pas prise en charge pour le Serveur virtuel.

Serveur des appareils mobiles

Le module de Kaspersky Security Center qui offre l'accès aux appareils mobiles et qui permet de les administrer via la Console d'administration.

Serveur des appareils mobiles Exchange ActiveSync

Module de Kaspersky Security Center qui permet de connecter les appareils mobiles Exchange ActiveSync au Serveur d'administration. Il est installé sur l'appareil client.

Serveur Internet de Kaspersky Security Center

Le module Kaspersky Security Center qui s'installe avec le Serveur d'administration. Le Serveur Internet est conçu pour transférer via réseau des paquets d'installation autonomes, des profils MDM iOS, ainsi que des fichiers du dossier partagé.

Serveur MDM iOS

Module Kaspersky Security Center installé sur l'appareil client et qui permet de connecter les appareils mobiles iOS au Serveur d'administration et de les administrer à l'aide du service Apple Push Notifications (APNs).

Sous-réseau Network Location Awareness

Le sous-réseau Network Location Awareness (NLA) est un sous-réseau d'un ensemble d'appareils indiqués manuellement. Dans le cadre de la fonctionnalité de Kaspersky Security Center, le sous-réseau NLA permet de créer manuellement un ensemble d'appareils sur lesquels l'agent de mises à jour diffusera des mises à jour.

Stratégie

La stratégie définit les paramètres de fonctionnement de l'application et l'accès à la configuration de l'application installée sur les ordinateurs du groupe d'administration. Pour chaque application, il est nécessaire de créer une stratégie. Vous pouvez créer un nombre illimité de stratégies pour les applications installées sur les ordinateurs dans chaque groupe d'administration, mais il n'est possible d'appliquer qu'une seule stratégie à la fois à chaque application.

Stratégie MDM

Ensemble de paramètres de fonctionnement de l'application utilisés pour l'administration des appareils mobiles administrés via le Kaspersky Security Center. L'administration de plusieurs types d'appareils mobiles implique des ajustements différents pour les paramètres de fonctionnement de

l'application. La stratégie contient les paramètres de la configuration complète de toutes les fonctions de l'application.

T

Tâche

Fonctions exécutées par une application de Kaspersky Lab et effectuée sous la forme de tâches, par exemple : Protection en temps réel des fichiers, Analyse complète des appareils et mise à jour des bases de données de données.

Tâche de groupe

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

Tâche locale

La tâche définie et exécutée sur un appareil client particulier.

Tâches pour l'ensemble d'appareils

La tâche définie pour un ensemble d'appareils clients parmi des groupes d'administration aléatoires et exécutée sur ces derniers.

U

Utilisateurs internes

Les comptes utilisateur des utilisateurs internes sont utilisés pour travailler avec les Serveurs d'administration virtuels. Sous le nom du compte utilisateur de l'utilisateur interne, l'administrateur du Serveur virtuel permet de lancer Kaspersky Security Center 10 Web Console pour consulter les informations sur l'état de la protection antivirus du réseau. Dans le cadre de fonctionnalité de l'application Kaspersky Security Center, les utilisateurs internes possèdent les privilèges des utilisateurs réels.

Les comptes utilisateur des utilisateurs internes sont créés et utilisés uniquement à l'intérieur de Kaspersky Security Center. Les informations sur les utilisateurs internes ne sont pas transmises au système d'exploitation. Kaspersky Security Center effectue l'authentification des utilisateurs internes.

V

Vulnérabilité

Imperfection du système d'exploitation ou du programme qui peut être utilisée par des éditeurs de programme malveillant pour pénétrer dans le système d'exploitation ou dans le programme et nuire à son intégrité. Un nombre important de vulnérabilités dans un système d'exploitation fragilise ce dernier car les virus qui s'installent dans le système d'exploitation peuvent provoquer des échecs du système d'exploitation en lui-même et des applications installées.

W

Windows Server Update Services (WSUS)

L'application utilisée pour diffuser les mises à jour des applications Microsoft sur les ordinateurs des utilisateurs dans le réseau de l'entreprise.

Z

Zone démilitarisée (DMZ)

La zone démilitarisée est un segment du réseau local où se trouvent les serveurs qui répondent aux requêtes Internet. Afin de garantir la sécurité du réseau local, l'accès à celui-ci depuis la zone démilitarisée est limité et protégé par un pare-feu.

AO Kaspersky Lab

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection informatique contre différents types de menaces, y compris les virus et les autres applications malveillantes, le courrier indésirable (spam), les attaques de réseau et les attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions logicielles pour la sécurité informatique des utilisateurs finaux (classement "IDC Worldwide Endpoint Security Revenue by Vendor"). En Russie, selon les données IDC, Kaspersky Lab est l'éditeur préféré de systèmes de protection informatique pour utilisateurs domestiques ("IDC Endpoint Tracker 2014").

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est un groupe international de sociétés avec 38 bureaux dans 33 pays du monde. La société emploie plus de 3000 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 inclut des applications pour la protection des données des ordinateurs de bureau et portables, des smartphones et d'autres appareils mobiles.

La société offre des solutions et des technologies de protection et de contrôle des postes de travail et des appareils mobiles, des machines virtuelles, des serveurs de fichiers et des serveurs Web, des passerelles de messagerie et des pare-feu. Le portefeuille de la société comprend également des produits spécialisés dans la protection contre les attaques DDoS, dans la protection des environnements sous l'administration d'un système automatisé de gestion des processus technologiques et dans la prévention de l'escroquerie financière. 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 quelle que soit sa taille 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 milliers de nouvelles menaces informatiques, développent les outils d'identification et de désinfection de ces menaces et ajoutent leurs signatures aux bases utilisées par les applications de Kaspersky Lab.

Technologies. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est pas par hasard si le noyau du logiciel de Kaspersky Anti-Virus est utilisé par de nombreux développeurs de logiciels dans leurs produits, dont : Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. 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. Par exemple, en 2014, selon les résultats des expériences et des recherches effectuées par le laboratoire antivirus autrichien qui fait autorité AV-Comparatives, Kaspersky Lab est devenu un des deux leaders en termes de nombre de certificats reçus Advanced+. En conséquence, la société s'est vu attribuer le certificat Top Rated. 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 400 millions d'utilisateurs. Elle compte également plus de 270 000 entreprises parmi ses clients.

Site de Kaspersky Lab

<http://www.kaspersky.fr>

Encyclopédie des virus :

<http://www.viruslist.com/fr>

Encyclopédie de virus :

<http://newvirus.kaspersky.fr> (pour l'analyse de fichiers et de sites suspects)

Forum de Kaspersky Lab :

<http://forum.kaspersky.fr>

Protection complémentaire avec l'utilisation de Kaspersky Security Network

Kaspersky Lab offre un niveau complémentaire de protection avec l'utilisation de Kaspersky Security Network. Ce mode de protection permet une lutte efficace contre les menaces dangereuses et les menaces du type zero-day (jour zéro). Les technologies Cloud unies avec Kaspersky Endpoint Security et les connaissances d'experts des experts de virus de Kaspersky Lab assurent une protection puissante contre les menaces les plus difficiles.

Pour plus d'informations sur la protection complémentaire dans Kaspersky Endpoint Security, visitez le site Internet de Kaspersky Lab.

Avis de marques déposées

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

Active Directory, ActiveSync, Excel, Internet Explorer, Hyper-V, Microsoft, MultiPoint, SQL Server, Tahoma, Windows, Windows Server, Windows Phone et Windows Vista sont des marques déposées de Microsoft Corporation enregistrées aux Etats-Unis et dans d'autres pays.

Adobe est une marque commerciale ou déposée d'Adobe Systems Incorporated enregistrée aux Etats-Unis et/ou dans d'autres pays.

AirPlay, AirDrop, AirPrint, App Store, Apple, FaceTime, FileVault, iBook, iBooks, iPad, iPhone, iTunes, Leopard, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger sont des marques déposées d'Apple Inc. enregistrées aux Etats-Unis et dans d'autres pays.

AMD, AMD64 sont des marques commerciales de Advanced Micro Devices, Inc.

Apache et Apache feather logo sont les marques de commerce de Apache Software Foundation.

BlackBerry appartient à Research In Motion Limited, déposée aux Etats-Unis et peut être déposée ou déposée aux autres pays.

Le nom commercial Bluetooth et le logo appartiennent à Bluetooth SIG, Inc.

Cisco, Cisco Systems, IOS sont des marques déposées de Cisco Systems, Inc. Enregistrées aux Etats-Unis et dans d'autres pays, et/ou ses sociétés affiliées.

Citrix et XenServer sont des marques commerciales de Citrix Systems, Inc. ou de ses filiales, déposées à l'office des brevets des États-Unis ou d'autres pays.

La marque Debian est une marque déposée de Software in the Public Interest, Inc.

Android, Chrome, Google, Google Play, Google Maps et Youtube sont des marques commerciales de Google, Inc.

Firefox est la marque de commerce de Mozilla Foundation.

FreeBSD est une marque commerciale déposée du fonds FreeBSD.

Oracle et Java sont des marques commerciales déposées d'Oracle Corporation ou de ses filiales.

QRadar est une marque commerciale de International Business Machines Corporation déposée dans de nombreux pays du monde.

CentOS, Fedora et Red Hat Enterprise Linux sont des marques commerciales de Red Hat Inc. déposées aux Etats-Unis et dans d'autres pays.

Linux – la marque Linus Torvalds déposée aux Etats-Unis et aux autres pays.

Novell – la marque Novell, Inc. déposée aux Etats-Unis et aux autres pays.

Symbian Foundation Ltd est le propriétaire de la marque de commerce Symbian.

SPL, Splunk sont les marques de Splunk, Inc., enregistrés dans les États-Unis et d'autres pays.

SUSE est une marque déposée de SUSE LLC enregistrée aux Etats-Unis et dans d'autres pays.

UNIX - la marque déposée aux Etats-Unis et aux autres pays, l'utilisation est sous licence de X/Open Company Limited.

VMware, VMware vSphere sont des marques commerciales de VMWare, Inc. déposée aux États-Unis ou dans d'autres pays.

Index

A

Active Directory	402
Administration	
ordinateur client.....	164
stratégies	118
Administration de l'application	118
Agents de mises à jour.....	342
Ajout	
ordinateur client.....	162
Serveur d'administration	101
Appareil mobile Exchange ActiveSync	284
Appareil mobile MDM iOS	290
Arborescence de la console	49
Assistant de conversion des stratégies et des tâches	127, 143

C

Certificat	
installation du certificat pour l'utilisateur.....	188, 274
messagerie	188, 274
partagé	188, 274

VPN.....	188, 274
Certificat du Serveur d'administration.....	101
Chiffrement.....	318
Clé.....	347
Clé	
installation.....	349
Clé	
suppression	349
Clé	
diffusion	350
Clé	
rapport	352
Clusters.....	384

E

exec.....	402
-----------	-----

G

Gestion	
clés.....	347
configuration initiale.....	75
Groupe des applications sous licence.....	227
Groupes	

structure.....	114
Groupes d'administration	78

I

Image.....	254
Importation	
stratégies	126
tâches.....	142
Installation	
Active Directory	402

L

Licence	66
Licence	
contrat de licence utilisateur final.....	65
Licence	
fichier clé	73
Licence de l'application	65, 67

M

Matrices	384
Menu contextuel	61, 409
Mise à jour	
affichage	337

analyse	334
diffusion	338, 339, 340, 342
obtention	330
Mise à jour de l'application	236

N

Notifications.....	196
--------------------	-----

O

Ordinateurs clients.....	83
--------------------------	----

Ordinateurs clients

connexion au serveur	151
----------------------------	-----

Ordinateurs clients

message à l'utilisateur	165
-------------------------------	-----

P

Plage IP

création.....	214
---------------	-----

modification.....	212, 214
-------------------	----------

Profil de stratégie.....	127, 128
--------------------------	----------

Profil de stratégie

Profil de stratégie

création	130
----------------	-----

Profil de stratégie

Profil de stratégie	
suppression	133
Protection antivirus	382

R

Rapport	
création.....	192
Rapports	
affichage	192
clés.....	352
créer	192
diffusion	193
Restriction du trafic	107
Rôle de l'utilisateur	
ajouter	278
Rôles d'utilisateurs.....	183
Rôles d'utilisateurs	
Rôle utilisateur	
ajouter	183
Rôles d'utilisateurs	
Rôle utilisateur	
désigner	184

S

Sauvegarde	
tâche	395
utilitaire	396
Sélections d'événements	
configuration	200
consultation du journal	200
création.....	201
Serveur d'administration.....	78
Serveur d'administration virtuel.....	80
Serveur des appareils mobiles Exchange ActiveSync.....	284
Sondage	
groupes Active Directory	211
plages IP.....	212
réseau Windows.....	211
Sondage du réseau	209
Statistiques.....	194
Stockages	
clés.....	347
paquets d'installation	354
registre des applications	226
Stratégie.....	85

Stratégie	
création.....	120
Stratégies	
activation	122
copie.....	125
exportation	126
importation	126
suppression	125
utilisateurs mobiles	375
Suppression	
Serveur d'administration	102
stratégie.....	125
T	
Tâche.....	85
Tâche	
ajout d'une clé.....	349
Tâches	
administration des ordinateurs clients.....	164
consultation des résultats	145
Diffusion des rapports.....	193
exécution	145
exportation	141

importation	142
locales	138
Modification du Serveur d'administration.....	163
sauvegarde	395
tâches de groupes	135

Tâches de groupe

filtre	146
héritage.....	139

U

Utilisateurs mobiles

profil	377
règles de permutation	378

V

Vulnérabilité	232
---------------------	-----