KASPERSKY lab

Manuel de l'administrateur de Kaspersky Secure Mail Gateway

Version de l'application: 1.1 Service Pack 1

Cher utilisateur,

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

Date d'édition : 24/04/2017

http://www.kaspersky.com/fr

http://www.kaspersky.com/fr

Table des matières

Présentation du manuel

Ce document constitue le manuel de l'administrateur de Kaspersky Secure Mail Gateway.
Le manuel de l'administrateur s'adresse aux spécialistes qui assurent l'installation et l'administration de Kaspersky Secure Mail Gateway, ainsi qu'aux spécialistes qui assurent l'assistance technique pour les organisations qui utilisent Kaspersky Secure Mail Gateway.

Dans ce manuel, vous trouverez des informations sur la configuration et l'utilisation de Kaspersky Secure Mail Gateway.

Vous pourrez également dans ce manuel connaître les sources d'information sur l'application et les moyens de bénéficier d'une assistance technique.

Dans cette section

Dans ce manuel

Le manuel contient les rubriques suivantes :

Sources d'informations sur l'application (à la page 24)

Cette section décrit les différentes sources d'informations sur l'application.

Kaspersky Secure Mail Gateway (à la page 27)

Cette section contient une bref survol de Kaspersky Secure Mail Gateway et de ses fonctions. Vous en saurez plus sur les modes de fonctionnement de Kaspersky Secure Mail Gateway, ainsi que sur les configurations logicielle et matérielle.

Interface de Kaspersky Secure Mail Gateway (à la page 37)

Cette section contient la description de l'interface de l'application.

Licence de l'application (à la page 39)

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

État de protection du serveur de messagerie (à la page 56)

Cette section contient des informations sur la procédure de vérification du niveau de la protection du serveur de messagerie et sur la détection des problèmes de protection.

Participation à Kaspersky Security Network et utilisation du Kaspersky Private Security Network (à la page 57)

Cette section contient les informations sur la participation à Kaspersky Security Network et sur l'utilisation de Kaspersky Private Security Network.

Déploiement de l'image de la machine virtuelle dans l'hyperviseur VMware ESXi™ (à la page 61)

Cette section contient les explications étape par étape du déploiement de l'image de la machine virtuelle de l'application dans l'hyperviseur VMware ESXi.

Déploiement de l'image de la machine virtuelle de l'application dans l'hyperviseur Microsoft® Hyper-V® (à la page 66)

Cette section contient des informations sur le déploiement de l'image de la machine virtuelle de l'application dans l'hyperviseur Microsoft Hyper-V.

Configuration initiale de l'application (à la page 72)

Cette section explique les différentes étapes de la configuration initiale de Kaspersky Secure Mail Gateway à réaliser après le déploiement de l'image de la machine virtuelle de Kaspersky Secure Mail Gateway.

Lancement de la machine virtuelle de l'application (à la page 100)

Cette section contient les explications relatives au lancement de la machine virtuelle Kaspersky Secure Mail Gateway.

Modification de la configuration de la machine virtuelle (à la page 101)

Ce paragraphe contient des informations sur la manière de modifier la configuration de la machine virtuelle dans l'hyperviseur que vous utilisez.

Prise en main de l'interface Web de l'application (à la page 104)

Cette section présente la prise en main de l'interface Web de l'application.

Intégration de Kaspersky Secure Mail Gateway dans l'infrastructure de messagerie de l'entreprise (à la page 105)

Cette section explique l'intégration de Kaspersky Secure Mail Gateway à l'infrastructure de messagerie de l'entreprise.

Surveillance de Kaspersky Secure Mail Gateway (à la page 124)

Cette section contient des informations sur la surveillance du trafic de messagerie, des dernières menaces détectées et des ressources système.

Application des règles de traitement des messages (à la page 128)

Cette section contient des informations sur les règles de traitement des messages, la configuration de leurs paramètres et la configuration des paramètres de Kaspersky Secure Mail Gateway pour chacune des règles.

Domaines et configuration du routage des emails (à la page 146)

Cette section explique comment créer la table de transport, configurer le routage des emails, configurer la sécurité TLS pour les messages entrants et sortants et ajouter des signature DKIM aux messages électroniques.

Signature DKIM aux messages sortants (à la page 164)

Cette section contient des informations sur l'ajout d'une signature DKIM aux messages sortants.

Utilisation du protocole TLS avec Kaspersky Secure Mail Gateway (à la page 167)

Cette section fournit des informations sur l'utilisation du protocole TLS avec Kaspersky Secure Mail Gateway et sur la configuration des paramètres d'utilisation de ce protocole.

Sauvegarde (à la page 174)

Cette section contient des informations sur la sauvegarde et sur son fonctionnement.

File d'attente des messages de Kaspersky Secure Mail Gateway (à la page 185)

Cette section contient les explications relatives à la file d'attente des messages de Kaspersky Secure Mail Gateway.

Rapports sur le fonctionnement de Kaspersky Secure Mail Gateway (à la page 195)

Cette section explique comment créer et consulter les rapports sur le fonctionnement de Kaspersky Secure Mail Gateway.

Paramètres généraux de Kaspersky Secure Mail Gateway (à la page 210)

Cette section contient des informations sur les paramètres généraux de l'application.

Configuration des paramètres du MTA (à la page 224)

Cette section contient des informations sur la configuration des principaux paramètres du MTA.

Mise à jour de Kaspersky Secure Mail Gateway via l'interface Web (à la page 233)

Cette section explique comment réaliser la mise à jour de Kaspersky Secure Mail Gateway via l'interface Web.

Mise à jour des bases de données de Kaspersky Secure Mail Gateway (à la page 238)

Cette section contient des informations sur la mise à jour des bases antivirus et des bases des modules Anti-Spam et Anti-Phishing.

Authentification des expéditeurs de messages (à la page 247)

Cette section contient des informations sur les technologies d'authentification des expéditeurs de messages intégrées à Kaspersky Secure Mail Gateway et sur la configuration des paramètres de l'authentification des expéditeurs de messages.

Protection antivirus des messages (à la page 266)

Cette section contient des informations sur la protection antivirus des messages et la configuration des paramètres de cette protection.

Protection des messages contre le courrier indésirable (à la page 284)

Cette section contient des informations sur la protection contre le courrier indésirable et la configuration des paramètres de cette protection.

Quarantaine de l'Anti-spam (à la page 301)

Cette section contient des informations sur la quarantaine de l'Anti-spam.

Protection des messages contre le de phishing (à la page 304)

Cette section contient des informations sur la protection des messages contre les tentatives de phishing et sur la configuration des paramètres de cette protection.

Filtrage du contenu des messages (à la page 313)

Cette section contient des informations sur le filtrage de contenu des messages et la configuration des paramètres de cette protection.

Protection KATA et intégration de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform (à la page 324)

Cette section fournit des informations sur la protection offerte par Kaspersky Anti Targeted Attack Platform et sur l'intégration de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform.

Listes noires et blanches d'adresses (à la page 338)

Cette section contient des informations sur les listes noires et blanches d'adresses email qu'il est possible de créer et de modifier dans Kaspersky Secure Mail Gateway.

Connexion au serveur LDAP (à la page 346)

Cette section contient des informations sur la connexion de Kaspersky Secure Mail Gateway au serveur LDAP et sur la configuration des paramètres et des filtres de connexion au serveur LDAP.

Utilisation de l'application via le protocole SNMP (à la page 359)

Cette section contient des informations sur l'utilisation de l'application via le protocole SNMP ainsi que sur la configuration des interruptions pour les événements survenus pendant l'utilisation de Kaspersky Secure Mail Gateway.

Messages de notification de Kaspersky Secure Mail Gateway (à la page 363)

Cette section contient des informations sur les messages de notification de Kaspersky Secure Mail Gateway et sur la configuration de leurs paramètres.

Remarques et avertissements de Kaspersky Secure Mail Gateway (à la page 371)

Cette section contient des informations sur les remarques et avertissements de Kaspersky Secure Mail Gateway et sur la configuration de leurs paramètres.

Journal des événements de Kaspersky Secure Mail Gateway (à la page 379)

Cette section contient des informations sur le journal des événements de l'application et la configuration des paramètres du journal.

Informations sur le système pour le Support Technique (à la page 386)

Cette section explique comment créer l'archive qui contient les informations relatives à Kaspersky Secure Mail Gateway pour les besoins du Support technique de Kaspersky Lab.

Journal d'audit de Kaspersky Secure Mail Gateway (à la page 389)

Cette section contient des informations sur l'utilisation du journal d'audit de Kaspersky Secure Mail Gateway.

Configuration de la date et de l'heure de Kaspersky Secure Mail Gateway (à la page 397)

Cette section explique comment configurer la date et l'heure dans l'application.

Enregistrement des données des utilisateurs (à la page 399)

Cette section contient des informations relatives aux données des utilisateurs de l'application, à l'utilisation de ces données par l'application et aux utilisateurs qui ont accès à ces données.

Contacter le Support technique (à la page 403)

Cette section contient des informations sur les modes et les conditions d'obtention de l'assistance technique.

Glossaire

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

AO Kaspersky Lab (à la page 413)

Cette section contient des informations sur AO Kaspersky Lab.

Informations sur le code tiers (à la page 415)

Cette section contient des informations sur le code tiers utilisé dans l'application.

Avis de marque déposée

Cette section cite les marques commerciales d'autres propriétaires cités dans le document.

Index

Cette section permet de trouver rapidement les informations souhaitées dans le document.

Conventions

Le présent document respecte des conventions (cf. tableau ci-dessous).

Tableau 1. Conventions

Exemple de texte	Description de la convention
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. Les remarques contiennent des informations complémentaires ou d'aide.
Exemple : …	Les exemples sont présentés en groupes sur un fond bleu sous le titre "Exemple".

Exemple de texte	Description de la convention
La *mise à jour*, c'est... L'événement *Les bases sont dépassées* survient.	Les éléments de sens suivants sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison des touches **ALT**+**F4**.	Les noms des touches du clavier sont en caractères gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Ces touches doivent être enfoncées simultanément.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères gras.
► *Pour planifier une tâche, procédez comme suit :*	Les phrases d'introduction des instructions sont en italique et "fléchées".
Dans la ligne de commande, saisissez le texte `help` Les informations suivantes s'affichent : Indiquez la date au format `JJ:MM:AA`.	Les types de texte suivants apparaissent dans un style spécial : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir à l'aide du clavier.
<Nom d'utilisateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable, sans les chevrons.

Sources d'informations sur l'application

Cette section décrit les différentes 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

Vous pouvez utiliser les sources suivantes pour rechercher des informations sur Kaspersky Secure Mail Gateway :

- Page de Kaspersky Secure Mail Gateway sur le site Internet de Kaspersky Lab ;
- Page de Kaspersky Secure Mail Gateway sur le site Internet du Support Technique (base de connaissances) ;
- Aide électronique ;
- Documentation.

Si vous ne trouvez pas la solution à votre problème, contactez le Support technique de Kaspersky Lab (cf. section "Contacter le Support technique" à la page 403).

La consultation des sources d'informations sur les site Internet requiert une connexion Internet.

Page de Kaspersky Secure Mail Gateway sur le site Internet de Kaspersky Lab

À la page de Kaspersky Secure Mail Gateway (https://www.kaspersky.fr/small-to-medium-business-security/mail-security-appliance), vous pouvez recevoir des informations générales sur l'application, ses possibilités et ses particularités de fonctionnement.

La page de Kaspersky Secure Mail Gateway contient un lien vers le magasin en ligne. Ce lien permet d'acheter l'application ou de renouveler le droit d'utilisation de celle-ci.

Page Kaspersky Secure Mail Gateway dans la Base de connaissances

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

À la page de Kaspersky Secure Mail Gateway dans la Base des connaissances (http://support.kaspersky.com/fr/ksmg), vous trouverez des articles contenant des informations utiles, des recommandations et des réponses aux questions souvent posées sur l'acquisition, l'installation et l'utilisation de l'application.

Les articles de la Base des connaissances peuvent répondre aux questions en rapport non seulement avec Kaspersky Secure Mail Gateway, mais aussi avec d'autres applications de Kaspersky Lab. Les articles de la Base de connaissances peuvent également présenter les actualités du Support Technique.

Aide électronique de Kaspersky Secure Mail Gateway (aide de l'interface Web)

L'interface Web permet d'administrer Kaspersky Secure Mail Gateway via un navigateur Internet. L'aide contient des informations sur les modalités d'administration de la protection, la configuration des paramètres de l'application et l'exécution des tâches principales de l'utilisateur via l'interface Web de Kaspersky Secure Mail Gateway (ci-après "l'interface Web").

Documentation

Le kit de distribution de l'application contient le Manuel de l'administrateur de Kaspersky Secure Mail Gateway qui vous aide à installer l'application et à réaliser la configuration initiale de ses paramètres.

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 sur notre forum (http://forum.kaspersky.fr).

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

Kaspersky Secure Mail Gateway

Cette section contient des informations sur Kaspersky Secure Mail Gateway.

Dans cette section

Présentation de Kaspersky Secure Mail Gateway

La résolution de Kaspersky Secure Mail Gateway vous permet de déployer une passerelle de messagerie virtuelle et de l'intégrer à l'infrastructure de messagerie existante de votre entreprise. La passerelle de messagerie virtuelle est dotée : d'un système d'exploitation, d'un serveur de messagerie et d'un logiciel antivirus de Kaspersky Lab.

Kaspersky Secure Mail Gateway protège le courrier entrant et sortant contre les objets malveillant et le courrier indésirable. Il opère le filtrage du contenu des messages et, dans le cadre de l'intégration à l'application Kaspersky Anti Targeted Attack Platform (ci-après "KATA"), il protège le courrier contre les intrusions contre l'infrastructure informatiques de l'organisation.

Kaspersky Secure Mail Gateway peut :

- Rechercher dans les messages électroniques entrants et sortants la présence de spam, de phishing et d'applications malveillantes, sans oublier, dans le cadre de l'intégration avec

KATA, rechercher dans les messages la présence d'indicateurs d'attaques ciblées et les intrusions dans l'infrastructure informatique de l'organisation.

Pour réagir en temps voulu aux menaces dont les informations n'ont pas été intégrées aux bases antivirus, les modules de protection de Kaspersky Secure Mail Gateway peuvent utiliser les informations provenant de Kaspersky Security Network.

- S'intégrer à l'application Kaspersky Private Security Network (ci-après KPSN) pour les organisations qui ne peuvent pas participer au Kaspersky Security Network (KSN).

  Après l'intégration à KPSN, Kaspersky Secure Mail Gateway peut utiliser les bases de données de réputation de KSN sans envoyer de données au-delà du périmètre de l'organisation.

  > Si vous avez des questions sur l'achat de l'application Kaspersky Private Security Network, contactez les experts chez nos partenaires dans votre région (https://www.kaspersky.fr/partners/distribution).

- S'intégrer à l'application Kaspersky Anti Targeted Attack Platform pour détecter des menaces telles que les attaques "0jour", les attaques ciblées et les attaques ciblées complexes advanced persistent threats (ci-après "APT").

  Une fois intégré à KATA, Kaspersky Secure Mail Gateway peut envoyer des copies des messages à KATA pour analyse. Sur la base des résultats du contrôle KATA Kaspersky Secure Mail Gateway peut bloquer certains messages.

  > Si vous avez de questions sur l'achat de l'application Kaspersky Anti Targeted Attack Platform (https://www.kaspersky.fr/enterprise-security/anti-targeted-attacks), contactez les commerciaux de Kaspersky Lab (https://www.kaspersky.fr/enterprise-security/anti-targeted-attacks).

- Détecter et bloquer le courrier indésirable, le courrier potentiellement indésirable, les diffusions massives (y compris les diffusions marketing), supprimer des messages, placer des copies des messages dans la Sauvegarde.

- Détecter, bloquer et réparer les messages électroniques infectés et les pièces jointes infectées, supprimer les messages et les pièces jointes, placer les copies des messages dans la Sauvegarde.
- Détecter et bloquer les messages contenant les macros dans la pièce jointe (par exemple, ces fichiers de formats Microsoft Office avec des macros), supprimer les messages ou les pièces jointes, placer des copies des messages dans la Sauvegarde.
- Détecter et bloquer les messages contenant des objets cryptés, supprimer les messages ou les pièces jointes, placer des copies des messages dans la Sauvegarde.
- Détecter et bloquer les messages contenant des archives, reconnaître les types de fichiers à l'intérieur des archives (par exemple, les fichiers du format ZIP, RAR, TGZ, 7z, QZIP), bloquer les fichiers distincts à l'intérieur des archives.
- Détecter et bloquer le phishing ou les liens vers des sites Internet malveillants, supprimer les messages, placer des copies des messages dans la Sauvegarde.
- Exécuter le filtrage de contenu des messages selon le nom, la taille et le type de pièce jointe (Kaspersky Secure Mail Gateway permet de réaliser les opérations suivantes : définir le format véritable et le type de la pièce jointe, indépendamment de son extension) ; supprimer les messages contenant des pièces jointes du format défini ou portant un nom précis ou les messages dont la taille dépasse la valeur admise ; placer des copies des messages dans la Sauvegarde.
- Détecter et bloquer les messages contenant des indicateurs d'attaques ciblées et d'intrusions dans l'infrastructure informatique de l'organisation (en cas d'intégration à KATA), supprimer le message, placer des copies des messages dans la Sauvegarde.
- Enregistrer les copies de sauvegarde des messages dans la Sauvegarde sur la base des résultats de leur traitement par les modules Antivirus, Anti-spam, Anti-phishing, ainsi que le filtrage de contenu et l'analyse des messages KATA.
- Conserver les messages de la Sauvegarde dans un fichier et les transmettre à leurs destinataires.
- Placer les messages la quarantaine de l'Anti-spam et la quarantaine KATA, administrer la quarantaine de l'Anti-spam et la quarantaine KATA dans l'interface Web.

- Traiter les messages électroniques selon les règles définies pour des groupes d'expéditeurs et de destinataires.
- Indiquer, dans les règles de filtrage des messages électroniques, les utilisateurs et les groupes d'utilisateurs de Microsoft Active Directory® et generic LDAP afin de pouvoir acheminer les messages pour des comptes utilisateur individuel et des groupes d'utilisateurs.
- Notifier l'expéditeur, les destinataires et l'administrateur de la détection de messages contenant des objets infectés, protégés par un mot de passe ou inaccessibles à l'analyse.
- Envoyer des notifications aux utilisateurs sur les résultats de l'analyse de leurs messages par les modules de l'application. Les notifications peuvent contenir la liste des derniers messages dans la Sauvegarde. Il est possible de configurer la planification de l'envoi des notifications.
- Mettre à jour les bases de l'application depuis les serveurs de mises à jour de Kaspersky Lab et les ressources utilisateurs (serveurs HTTP et FTP), sur programmation ou à la demande.
- Recevoir les statistiques de fonctionnement de l'application via le protocole SNMP, activer et désactiver l'envoi d'interruptions SNMP.
- Définir des paramètres et gérer le fonctionnement de l'application via l'interface Web.
- Expédier et recevoir des messages sur le canal protégé TLS/SSL ;
- Authentifier les expéditeurs des messages à l'aide des technologies SPF, DKIM et DMARC.
- Signer les messages électroniques sortants à l'aide de la technologie DKIM.
- Ajouter des remarques aux messages entrants et sortants.
- Ajouter aux messages entrants des avertissements concernant les pièces jointes dangereuses.
- Recevoir des informations sur les utilisateurs de différents domaines et proposer aux utilisateurs d'accéder à une Sauvegarde personnalisée.
- Ajouter, modifier ou supprimer des informations relatives aux domaines (dont les domaines locaux de l'organisation) et aux adresses email, configurer les paramètres de Kaspersky

Secure Mail Gateway pour ces domaines et adresses de messagerie ainsi que l'acheminement des emails.

- Vous pouvez configurer le mode de chiffrement TLS pour les cas où Kaspersky Secure Mail Gateway accepte des messages d'un autre serveur (en tant que serveur) ou les transmet à un serveur (en tant que client). Il est possible également de configurer les paramètres TLS pour des domaines distincts.
- Surveiller l'état du trafic de messagerie et de l'utilisation des ressources du système, consulter la liste des dernières menaces détectées dans l'interface Web de l'application.
- Surveiller le fonctionnement de l'application via Kaspersky Security Center version 10 SP2.
- Consulter le journal des événements de l'application et le charger sur le disque dur.
- Mettre à jour le système via l'interface Web de Kaspersky Secure Mail Gateway.
- Configurer rapidement MTA à l'aide de l'Assistant de configuration rapide.
- Mettre à jour, modifier et supprimer les clés de chiffrement DKIM et TLS.
- Créer et consulter les rapports sur les résultats du traitement des messages électroniques.
- Consulter le journal d'audit dans l'interface Web de l'application.
- Créer une archive contenant les informations au fonctionnement de Kaspersky Secure Mail Gateway en vue de l'envoyer au Support technique de Kaspersky Lab.

Kaspersky Secure Mail Gateway est diffusé sous la forme de modèles de machines virtuelles OVA (Open Virtual Appliance) ou d'archive ZIP comportant l'image de la machine virtuelle destinée à être déployée dans l'hyperviseur Microsoft Hyper-V.

Le déploiement de l'image entraîne la création d'une machine virtuelle dotée du système d'exploitation préinstallé CentOS 6.8, d'un serveur de messagerie et de l'application Kaspersky Security for Linux® Mail Server (ci-après "Kaspersky Security"). Une fois le déploiement terminé, vous pouvez configurer la machine virtuelle à l'aide de l'Assistant de configuration initiale.

Distribution

Vous pouvez acheter l'application dans la boutique en ligne de Kaspersky Lab (par exemple, http://www.kaspersky.com/fr, section **Boutique**) ou sur le site d'un partenaire.

> Ces éléments peuvent varier en fonction du pays où l'application est commercialisée.

Si vous achetez Kaspersky Secure Mail Gateway via la boutique en ligne, vous devrez télécharger l'application depuis le site Internet. Les informations indispensables à l'activation de l'application vous seront envoyées par courrier électronique après le paiement.

Configurations logicielles et matérielles

Configuration logicielle requise pour le déploiement de l'image de machine virtuelle de Kaspersky Secure Mail Gateway

L'image de la machine virtuelle de Kaspersky Secure Mail Gateway peut être déployée sur les hyperviseurs suivants :

- VMware ESXi 5.5 Update 2.
- VMware ESXi 6.0.
- Microsoft Hyper-V Server 2012 R2.

Configuration matérielle requise pour le déploiement de l'image de machine virtuelle de Kaspersky Secure Mail Gateway

Les ressources sélectionnées pour le déploiement de l'image de la machine virtuelle de Kaspersky Secure Mail Gateway doivent satisfaire aux exigences suivantes :

- adaptateur réseau E1000 ;
- espace disque disponible de 100 Go minimum ;
- au moins 4 Go de mémoire vive ;
- processeur quatre cœurs.

Configuration logicielle requise pour l'utilisation de Kaspersky Secure Mail Gateway via l'interface Web

L'un des navigateurs suivants doit être installé sur l'ordinateur pour que l'interface Web puisse fonctionner :

- Mozilla™ Firefox™ version 38.0.5 (39) ou ultérieure ;
- Internet Explorer® version 11 ou ultérieure ;
- Google Chrome™ version 43 ou ultérieure.

Modes de fonctionnement de Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway peut fonctionner en mode normal, en mode de trafic limité ou en mode certifié.

En mode normal, Kaspersky Secure Mail Gateway peut accéder à Internet et il peut se connecter aux serveurs suivants situés au-delà de l'infrastructure informatique de votre organisation :

- Serveurs de mise à jour des bases KSN (cf. section "A propos de la participation au Kaspersky Security Network et de l'utilisation de Kaspersky Private Security Network" à la page 57).
- Serveurs DNS (cf. Section" Connexion au serveur DNS pour l'authentification des expéditeurs" à la page 250).
- Serveurs de mise à jour des bases de Kaspersky Secure Mail Gateway (cf. section "À propos des sources de mises à jour" à la page 239).

En mode de trafic limité (cf. section "*Restriction du trafic de Kaspersky Secure Mail Gateway*" à la page 34), Kaspersky Secure Mail Gateway interdit l'accès Internet et la connexion aux serveurs situés en dehors de l'infrastructure informatique de votre organisation.

En mode de trafic limité, les paramètres des modules de Kaspersky Secure Mail Gateway qui requièrent un accès Internet prennent les valeurs suivantes par défaut :

- Utilisation de KSN désactivée (cf. section "Configuration de la participation au Kaspersky Security Network" à la page 58).

- L'authentification SPF (cf. section "Activation et désactivation de l'authentification SPF des expéditeurs" à la page 251) DKIM (cf. section "Activation et désactivation de l'authentification DKIM des expéditeurs" à la page 251) et DMARC des expéditeurs de messages (cf. section "Activation et désactivation de l'authentification DMARC des expéditeurs" à la page 252) est désactivée et la connexion aux serveurs DNS (cf. section "Connexion au serveur DNS pour l'authentification des expéditeurs" à la page 250) est interdite.

- Le service Enforced Anti-Spam Updates (cf. section "Configuration des paramètres du module Anti-Spam" à la page 288) est désactivé dans les paramètres du module Anti-Spam.

- En guise de source des mises à jour de la base de données, Kaspersky Secure Mail Gateway utilise Kaspersky Security Center ou une source locale de mise à jour de la base de données de Kaspersky Secure Mail Gateway (cf. section "À propos des sources de mises à jour" à la page 239).

En mode certifié (cf. section "*Etape 3. Sélection du mode de fonctionnement de l'application*" à la page 76) Kaspersky Secure Mail Gateway ne peut pas accéder à Internet et il ne peut pas se connecter aux serveurs situés au-delà de l'infrastructure informatique de votre organisation.
De plus, lorsque Kaspersky Secure Mail Gateway fonctionne en mode certifié, l'administrateur n'est pas en mesure de consulter le journal des événements depuis le menu de l'administrateur de Kaspersky Secure Mail Gateway.

Vous pouvez sélectionner le mode de fonctionnement certifié de Kaspersky Secure Mail Gateway lors du déploiement de l'image de la machine virtuelle de Kaspersky Secure Mail Gateway.

Restriction du trafic de Kaspersky Secure Mail Gateway

► *Pour faire passer Kaspersky Secure Mail Gateway au mode de* trafic limité*, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Utilisation de KSN / KPSN** du groupe **Services externes** pour ouvrir la fenêtre **Utilisation de KSN / KPSN**.

3. Sélectionnez **Ne pas utiliser KSN / KPSN**.

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

   La fenêtre **Utilisation de KSN / KPSN** se ferme.

5. Cliquez sur le lien **Autoriser la connexion au serveur DNS** du groupe **Services externes** pour ouvrir la fenêtre **Services externes**.

6. Dans la liste à droite du nom du paramètre **Autoriser la connexion au serveur DNS** , choisissez **Non**.

7. Cliquez sur le bouton **Appliquer**.

   La fenêtre **Services externes** se ferme.

8. Cliquez sur n'importe lequel des liens suivants **Utiliser KSN**, **Utiliser le service Enforced Anti-spam Updates**, **Utiliser le filtrage par réputation** ou **Temps maximal de l'analyse** du groupe **Anti-spam** pour ouvrir la fenêtre **Paramètres du module Anti-spam**.

9. Dans la liste déroulante **Utiliser le service Enforced Anti-spam Updates** du groupe **Services externes**, choisissez l'option **Non**.

10. Cliquez sur le bouton **Appliquer**.

    La fenêtre **Paramètres du module Anti-spam** se ferme.

11. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Mise à jour des bases** dans l'arborescence de la console de gestion.

12. Cliquez sur le lien **Source des mises à jour** du groupe **Paramètres de mise à jour des bases de données de l'application** pour ouvrir la fenêtre **Paramètres de mise à jour des bases de données de l'application**.

13. Dans le groupe des paramètres **Source des mises à jour**, choisissez **Kaspersky Security Center**.

14. Décochez la case **En cas d'indisponibilité, utiliser les serveurs de Kaspersky Lab**.
15. Cliquez sur le bouton **OK**.

    La fenêtre **Paramètres de mise à jour des bases de données de l'application** se ferme.

Kaspersky Secure Mail Gateway commence à fonctionner en mode de trafic limité.

Interface de Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway s'utilise à partir d'une interface Web.

La fenêtre principale de l'interface Web contient les éléments suivants :

- Arborescence de la console de gestion dans la partie gauche de la fenêtre ;
- Espace de travail dans la partie droite de la fenêtre.

Arborescence de la console de gestion de Kaspersky Secure Mail Gateway

L'arborescence de la console de gestion affiche les différentes sections de Kaspersky Secure Mail Gateway et les subdivisions de ses composants fonctionnels.

L'arborescence de la console de gestion de Kaspersky Secure Mail Gateway présente les sections suivantes :

- **Surveillance** : section contenant les données de surveillance de Kaspersky Secure Mail Gateway.
- **Règles** : section contenant les règles de traitement des messages.
- **Domaines** : section dans laquelle vous pouvez ajouter, modifier ou supprimer des informations relatives aux domaines et aux adresses email, configurer les paramètres de Kaspersky Secure Mail Gateway pour ces domaines et adresses email.
- **Clés de chiffrement** : section dans laquelle vous pouvez ajouter, modifier ou supprimer des clés de chiffrement DKIM et TLS.
- **Sauvegarde** : section contenant des informations sur la sauvegarde des messages et le filtre de recherche des messages dans celle-ci.
- **File d'attente des messages** : section contenant les informations sur la file d'attente des messages de l'agent de messagerie MTA et le filtre de recherche de messages dans la file d'attente.

- **Rapports** : section contenant les rapports sur le fonctionnement du serveur de messagerie.
- **Paramètres** : section permettant de configurer les paramètres de Kaspersky Secure Mail Gateway.
- **Configuration rapide du MTA** : assistant de configuration des paramètres principaux de MTA, le module qui permet d'intégrer rapidement Kaspersky Secure Mail Gateway à l'infrastructure de messagerie de votre organisation au premier lancement de l'interface Web de Kaspersky Secure Mail Gateway et de redéfinir les paramètres du MTA lors des utilisations suivantes de l'interface Web de Kaspersky Secure Mail Gateway.

  Après avoir suivi toutes les étapes de l'Assistant **Configuration rapide du MTA**, Kaspersky Secure Mail Gateway élimine toutes les valeurs des paramètres du MTA et les remplace par les valeurs que vous avez définies dans l'Assistant de configuration rapide du MTA.

Espace de travail de la fenêtre de l'interface Web de Kaspersky Secure Mail Gateway

L'espace de travail contient les informations relatives aux sections que vous sélectionnez dans la console de gestion, ainsi que les éléments de gestion vous permettant de modifier les paramètres de l'application.

Les sections à utiliser pour travailler sur les paramètres de Kaspersky Secure Mail Gateway sont regroupées dans les **Groupes de paramètres** de l'espace de travail, dans la fenêtre principale des paramètres.

Licence de l'application

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

Dans cette section

A propos du contrat de licence

Le *Contrat de licence Utilisateur final* est un accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions d'utilisation de l'application que vous avez achetée.

Lisez attentivement le Contrat de licence Utilisateur final 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 de Kaspersky Secure Mail Gateway ;
- En lisant le document license.txt. Ce document est repris dans la distribution de l'application.

Vous acceptez les conditions du contrat de licence Utilisateur final, en confirmant votre accord avec le texte du contrat de licence Utilisateur final lors de l'installation de l'application. Si vous n'êtes pas d'accord avec les termes du Contrat de Licence Utilisateur Final, 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 accorde le droit d'obtenir les types de service suivants :

- Utilisation de l'application conformément aux conditions du Contrat de licence ;
- Support technique.

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

Les types de licence suivants sont proposés :

- *Evaluation* : licence gratuite qui permet de découvrir les fonctionnalités de l'application.

La durée de validité de la licence d'évaluation est courte. Une fois que la licence d'évaluation de Kaspersky Secure Mail Gateway arrive à échéance, toutes les fonctions de l'application sont désactivées. Pour continuer à utiliser l'application, il faut acheter une licence commerciale.

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

- *Commerciale* : licence payante délivrée lors de l'achat de l'application.

  A l'expiration de la durée de validité de la licence commerciale, l'application continue à fonctionner, mais ses fonctionnalités sont limitées (par exemple, la mise à jour de la base de données de Kaspersky Secure Mail Gateway n'est pas disponible). Pour pouvoir continuer à bénéficier de toutes les fonctionnalités de Kaspersky Secure Mail Gateway, vous devez renouveler la licence commerciale.

Il est conseillé de renouveler la licence avant son expiration afin de garantir une protection maximale contre toutes les menaces informatiques.

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 octroyée ;
- Restrictions associées au nombre d'unités concernées par la licence (par exemple, le nombre de périphériques sur lesquels l'application peut être utilisée avec la licence) ;
- Début de validité de la licence ;
- Date d'expiration de la licence ou de l'abonnement ou durée de validité de la licence ;
- Type de licence.

A propos de la clé

La *clé* est une séquence de bits qui permet d'activer, puis d'utiliser l'application conformément aux conditions du Contrat de licence utilisateur final. La clé est générée par les experts de Kaspersky Lab.

Vous pouvez ajouter une clé à l'application d'une des manières suivantes : appliquer un *fichier clé* ou saisir un *code d'activation*.

La clé apparaît dans l'interface de l'application sous la forme d'une séquence de caractères alphanumériques unique une fois que vous l'avez ajoutée à l'application.

Une clé peut être bloquée par Kaspersky Lab en cas de non-respect des conditions du Contrat de Licence Utilisateur Final. Si la clé est bloquée, il faudra ajouter une autre clé pour utiliser l'application.

Une clé peut être active ou complémentaire.

La *clé active* est une clé utilisée au moment actuel pour faire fonctionner l'application. Une clé pour une licence d'évaluation ou une licence commerciale peut être ajoutée en tant que clé active. L'application ne peut compter qu'une seule clé active.

Une *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 complémentaire devient automatiquement active lorsque la durée de validité de la licence associée à la clé active expire. La clé additionnelle ne peut être ajoutée qu'en cas de présence d'une clé active.

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

> La clé additionnelle ne peut être ajoutée qu'en cas de présence d'une clé active.

Les types de clé proposés pour Kaspersky Secure Mail Gateway sont les suivants :

- *Clé totalement fonctionnelle*. Suite à l'ajout de cette clé, toutes les fonctionnalités de l'application sont opérationnelles et l'analyse du spam et du phishing et la recherche de virus et autres programmes dangereux sont actives.

- *Clé pour la protection anti-virus*. Suite à l'ajout de la clé, l'application lance l'analyse contre les virus et autres programmes dangereux. Par contre, l'analyse contre les spams n'a pas lieu. L'état attribué au message par l'application dans le cadre de l'analyse contre les spams contient des informations sur les fonctionnalités réduites.

- *Clé pour la protection contre le courrier indésirable et le phishing*. Suite à l'ajout de la clé, l'application réalise l'analyse contre les spams et le phishing. L'analyse contre les virus et autres programmes dangereux n'a pas lieux. L'état attribué au message par l'application dans le cadre de l'analyse contre les virus contient des informations sur les fonctionnalités réduites.

Le type de la clé additionnelle doit correspondre au type de la clé active ajoutée antérieurement. Si le type de clé additionnelle ne correspond pas au type de la clé active ajoutée antérieurement, son activation modifiera les fonctionnalités utilisables de l'application.

Les bases Antivirus et les bases Anti-Spam sont mises à jour indépendamment du type de clé.

A propos du fichier clé

Le *fichier clé* est un fichier portant l'extension .key qui vous est remis par Kaspersky Lab. Le fichier clé permet d'ajouter une clé pour activer l'application.

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

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.

En cas de suppression accidentelle du fichier clé, vous pouvez le récupérer. Vous aurez besoin du fichier clé pour ouvrir un Kaspersky CompanyAccount par exemple.

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

- Contactez le Support technique (http://support.kaspersky.fr).

- Obtenir le fichier clé sur le site Internet de Kaspersky Lab (https://activation.kaspersky.com/fr/) sur la base du code d'activation.

A propos du code d'activation

Le *code d'activation* est une séquence unique de vingt caractères alphanumériques latins. Vous saisissez le code d'activation pour ajouter la clé qui va activer Kaspersky Secure Mail Gateway. Vous recevez le code d'activation à l'adresse électronique que vous avez indiquée après l'achat de Kaspersky Secure Mail Gateway ou après la commande d'une version d'évaluation de Kaspersky Secure Mail Gateway.

Pour activer l'application à l'aide de ce code, il faut compter sur un accès Internet pour établir la connexion avec les serveurs d'activation de Kaspersky Lab.

En cas de perte du code d'activation après l'activation de l'application, vous pouvez le récupérer. Le code d'activation peut être utile pour s'inscrire, par exemple sur Kaspersky CompanyAccount. Pour récupérer le code d'activation, il faut contacter le Support Technique de Kaspersky Lab (cf. section "Mode d'obtention de l'assistance technique" à la page 403).

A propos de l'abonnement

L'abonnement à Kaspersky Secure Mail Gateway est une sollicitude d'utilisation de l'application selon des paramètres définis (date d'expiration de l'abonnement, quantité d'appareils protégés).

L'abonnement peut être limité (par exemple, pour un an) ou illimité (sans date d'expiration). Pour pouvoir continuer à utiliser Kaspersky Secure Mail Gateway à l'échéance de l'abonnement, il faut renouveler ce dernier. L'abonnement illimité se renouvelle automatiquement à condition d'avoir réalisé le paiement préalable en temps utiles.

Un abonnement limité peut bénéficier d'une période de renouvellement à tarif préférentiel au cours de laquelle l'application conserve toute ses fonctions.

Pour utiliser Kaspersky Secure Mail Gateway selon un abonnement, il faut appliquer un code d'activation. Quand le code d'activation a été appliqué, la clé active est installée. Celle-ci définit la licence d'utilisation de l'application selon un abonnement. Il est possible d'installer une clé

additionnelle uniquement à l'aide d'un code d'activation et non pas à l'aide d'un fichier clé ou d'un abonnement.

> Les codes d'activation acquis selon un abonnement ne peuvent pas être utilisés pour activer des versions précédentes de Kaspersky Secure Mail Gateway.

A propos de l'approvisionnement des données

Le fonctionnement de l'application repose sur des données dont l'envoi et le traitement doivent être approuvés par l'administrateur de Kaspersky Secure Mail Gateway.

Vous pouvez prendre connaissance des données en question et de leurs conditions d'utilisation ainsi qu'autoriser le traitement des données dans les contrats suivants entre votre organisation et Kaspersky Lab :

- Dans le Contrat de Licence Utilisateur Final (par exemple, lors de l'installation de l'application ou lors de la mise à jour du système dans la section **Paramètres**, sous-section **Mise à jour du système** de la fenêtre principale de l'interface Internet de l'application).

  Conformément aux dispositions du Contrat de Licence Utilisateur Final que vous avez accepté, vous êtes prêt à envoyer automatiquement à Kaspersky Lab les informations reprises au point Envoi des informations dans le Contrat de Licence Utilisateur Final (cf. section "A propos du Contrat de Licence Utilisateur Final" à la page 40). Ces informations permettent d'améliorer le niveau de protection du serveur de messagerie.

- Dans le Règlement de KSN (cf. section "Configuration de la participation au Kaspersky Security Network" à la page 58).

  Si vous participez au Kaspersky Security Network, vous envoyez automatiquement à Kaspersky Lab les informations obtenues suite à l'utilisation de l'application sur l'ordinateur. La liste des données transmises est indiquée dans le Règlement de KSN (cf. section "Configuration de la participation au Kaspersky Security Network" à la page 58).

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. Ces statistiques générales se créent automatiquement à partir des informations reçues et ne contiennent aucune donnée personnelle ou ni aucune autre donnée confidentielle. Les informations obtenues sont supprimées au fur et à mesure de leur accumulation (une fois par an). Les statistiques générales sont conservées pour une durée indéterminée.

Les données utilisateurs peuvent être contenues dans les modules suivants de Kaspersky Secure Mail Gateway :

- File d'attente de messages (nom des fichiers, adresses électroniques des expéditeurs et des destinataires des messages, textes des messages).
- Sauvegarde (noms des fichiers, adresses email des expéditeurs et des destinataires, textes des messages).
- Rapports sur le fonctionnement de l'application (noms de fichier, adresses électroniques des expéditeurs et des destinataires).
- Journal des événements de l'application (adresses électroniques des expéditeurs et des destinataires, noms des pièces jointes, adresses IP des ordinateurs des expéditeurs).
- Fichiers de trace (noms des fichiers, chemins d'accès aux fichiers, noms des serveurs proxy, données des comptes utilisateur, adresses IP des ordinateurs connectés aux sources des mises à jour des bases de données de l'application, noms et adresses IP des sources des mises à jour, informations sur les fichiers téléchargés et la vitesse du téléchargement).
- Fichiers contenant les paramètres de connexion au serveur LDAP et au serveur proxy (données des comptes utilisateurs des utilisateurs du serveur LDAP et du serveur proxy).

Lors de la connexion de l'application aux serveurs DNS, SURBL ou DNSBL, Kaspersky Secure Mail Gateway utilise les adresses IP et les noms de domaine FQDN qui contactent ces serveurs.

L'utilisation de l'application depuis la console de gestion de Kaspersky Secure Mail Gateway en mode Assistance technique avec les autorisations du compte utilisateur de superutilisateur permet

de gérer les paramètres du vidage. Le vidage est créé en cas d'échec de l'application et peut être utile pour analyser les causes de l'échec. Le vidage peut reprendre n'importe quelles données, dont des extraits des messages et des fichiers analysés.

L'administrateur du réseau local de l'organisation est responsable de l'accès à ces informations.

La création d'un vidage est désactivée par défaut dans Kaspersky Secure Mail Gateway.

Les données de la file d'attente des messages électroniques traités par Kaspersky Secure Mail Gateway en ce moment ainsi que les comptes utilisateur des utilisateurs du serveur LDAP et du serveur proxy sont conservées en clair dans Kaspersky Secure Mail Gateway.

Ces données sont accessibles via la console de gestion de Kaspersky Secure Mail Gateway en mode de Support Technique avec les autorisations de superutilisateur.

Il incombe à l'administrateur de Kaspersky Secure Mail Gateway de garantir la sécurité de ces données.

L'administrateur de Kaspersky Secure Mail Gateway est responsable de l'accès à ces informations.

Les données relatives aux événements et aux processus de fonctionnement de Kaspersky Secure Mail Gateway sont consignées et enregistrées dans les journaux suivants de Kaspersky Secure Mail Gateway :

- journal des événements ;
- journal de trace.

Consultation des informations relatives à la licence et aux clés ajoutées

► *Pour consulter des informations relatives à la licence et aux clés ajoutées :*

Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Licence** dans l'arborescence de la console de gestion.

Le groupe **Clé active** de l'espace de travail affiche les informations suivantes sur les clés :

- Suite de caractères alphanumériques composant la clé ;
- État de la clé ;
- Type de licence ;
- Nombre d'utilisateurs ;
- Date d'activation de l'application ;
- Date de fin de validité de la clé ;
- Nombre de jours avant la date de fin de validité de la clé.

Mise à jour des informations relatives à la licence et aux clés ajoutées

► *Pour mettre à jour les informations relatives à la licence et aux clés ajoutées, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Licence** dans l'arborescence de la console de gestion.
2. Cliquez sur le bouton **Actualiser** dans le coin supérieur droit de la fenêtre.

Les informations relatives à la licence et aux clés ajoutées sont mises à jour.

Ajout d'un fichier clé

► *Pour ajouter un fichier clé, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Licence** dans l'arborescence de la console de gestion.
2. Cliquez sur le bouton **Ajouter un fichier clé**.

   La fenêtre **Ajout d'une clé** s'ouvre.
3. Cliquez sur le bouton **Parcourir**.

   La fenêtre de sélection des fichiers s'ouvre.
4. Sélectionnez le fichier clé à ajouter.
5. Cliquez sur le bouton **OK**.

Une clé qui a été ajoutée peut avoir l'état *actif* ou *complémentaire.* La première clé ajoutée devient automatiquement une clé active. Vous pouvez utiliser l'application juste après l'ajout de la clé active.

Vous pouvez ajouter la clé additionnelle après l'ajout de la clé active. La clé additionnelle passera automatiquement à l'état actif après l'expiration de la licence. Ainsi, la protection ne sera pas interrompue entre la fin de la validité de la licence et la date de renouvellement de la licence.

> Vous pouvez également activer l'application à l'aide d'un code d'activation (cf. section "Ajout d'un code d'activation" à la page 49). Il est recommandé d'activer l'application à l'aide d'un fichier clé.

Ajout d'un code d'activation

► *Pour ajouter un code d'activation, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Licence** dans l'arborescence de la console de gestion.
2. Cliquez sur le bouton **Ajouter un code d'activation**.

La fenêtre **Activer à l'aide d'un code** s'ouvre.

3. Saisissez dans le champ **Code d'activation** le code d'activation de l'application au format XXXXX-XXXXX-XXXXX-XXXXX, où X représente des lettres de l'alphabet latin (A-Z, excepté O et I (i majuscule)) ou des chiffres (0-9).

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

Le code d'activation est envoyé aux serveurs de Kaspersky Lab pour vérification.

Si le code introduit est incorrect, la fenêtre **Activer à l'aide d'un code** affiche le message de circonstance. Vous pouvez répéter la tentative de saisie du code d'activation dans la même fenêtre.

Si le code introduit est correct, les conditions du Contrat de licence utilisateur final conformes au code d'activation saisi s'affichent. La fenêtre **Activer à l'aide d'un code** se ferme.

Vous pouvez également activer l'application à l'aide d'un fichier clé (cf. section "Ajout d'un fichier clé" à la page 49). Il est recommandé d'activer l'application à l'aide d'un fichier clé.

Suppression de la clé

► *Pour supprimer la clé, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Licence** dans l'arborescence de la console de gestion.

2. Dans l'espace de travail de la fenêtre, cochez la case en regard de la clé à supprimer.

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

   La fenêtre **Suppression de la clé** s'ouvre.

4. Cliquez sur le bouton **Oui**.

La clé sélectionnée sera supprimée.

Si vous avez ajouté une clé additionnelle pour Kaspersky Secure Mail Gateway, en cas de suppression de la clé active cette clé additionnelle passe automatiquement à l'état actif.

Si vous supprimez la clé active et la clé additionnelle, vous ne pourrez pas utiliser les fonctionnalités de l'application auxquelles votre licence vous donne accès.

Modes de fonctionnement de Kaspersky Secure Mail Gateway conformément à la licence

Kaspersky Secure Mail Gateway peut fonctionner selon différents modes, conformément à la licence :

Sans licence

Kaspersky Secure Mail Gateway fonctionne dans ce mode dès l'installation de l'application et le lancement de l'interface Web jusqu'à ce que vous ajoutiez la clé active (cf. section "Ajout d'un fichier clé" à la page 49).

En mode **Sans licence**, Kaspersky Secure Mail Gateway n'analyse pas le contenu des messages électroniques.

Licence d'évaluation

Dans ce mode, Kaspersky Secure Mail Gateway analyse les messages électroniques et met à jour la base de données.

Après l'expiration de la clé de la licence d'évaluation, Kaspersky Secure Mail Gateway n'analyse plus les messages électroniques et ne met plus à jour la base de données.

Pour continuer à utiliser Kaspersky Secure Mail Gateway, il faut installer une clé de licence commerciale.

Licence commerciale

Dans ce mode, Kaspersky Secure Mail Gateway analyse les messages électroniques et met à jour la base de données.

Après l'expiration de la clé de la licence commerciale, Kaspersky Secure Mail Gateway continue d'analyser les messages électroniques, mais la mise à jour des bases de données est suspendue.

Pour rétablir la mise à jour des bases de données, il faut installer une nouvelle clé de licence commerciale ou renouveler la validité de la clé de licence commerciale.

Kaspersky Secure Mail Gateway peut être utilisé avec une licence commerciale d'un des types suivants :

- *Clé totalement fonctionnelle*. Suite à l'ajout de cette clé, toutes les fonctionnalités de l'application sont opérationnelles et l'analyse du spam et du phishing et la recherche de virus et autres programmes dangereux sont actives.
- *Clé pour la protection anti-virus*. Suite à l'ajout de la clé, l'application lance l'analyse contre les virus et autres programmes dangereux. Par contre, l'analyse contre les spams n'a pas lieu. L'état attribué au message par l'application dans le cadre de l'analyse contre les spams contient des informations sur les fonctionnalités réduites.
- *Clé pour la protection contre le courrier indésirable et le phishing*. Suite à l'ajout de la clé, l'application réalise l'analyse contre les spams et le phishing. L'analyse contre les virus et autres programmes dangereux n'a pas lieux. L'état attribué au message par l'application dans le cadre de l'analyse contre les virus contient des informations sur les fonctionnalités réduites.

Liste noire des clés

La clé peut être ajoutée à une liste noire pour plusieurs raisons. Si cela se produit, Kaspersky Secure Mail Gateway n'analyse plus les messages électroniques, mais les tentatives de mise à jour des bases de données sont maintenues, au cas où la clé serait retirée de la liste noire.

Dès que la clé est retirée de la liste noire, Kaspersky Secure Mail Gateway reprend l'analyse des messages électroniques conformément à la licence active.

Après la désactivation de l'analyse des messages électroniques, l'agent de messagerie MTA continue de fonctionner dans Kaspersky Secure Mail Gateway, tout comme la connexion au serveur LDAP, le journal des événements, les rapports sur le fonctionnement de Kaspersky Secure Mail Gateway. La gestion de l'ensemble des paramètres de Kaspersky Secure Mail Gateway est également disponible, à l'exception des paramètres de la protection, via l'interface Internet.

Notification de l'expiration prochaine de la licence

Après chaque mise à jour des bases, l'application vérifie la validité de la licence. Lorsqu'il reste jusqu'à l'expiration de la licence le nombre de jours indiqué dans le paramètre **Envoyer une notification**, l'application commence à envoyer des notifications aux adresses électroniques de l'administrateur de Kaspersky Secure Mail Gateway que vous avez indiquées (cf. section "Configuration des adresses électroniques de l'administrateur" à la page 212).

Par défaut, l'envoi de notifications concernant l'expiration de la licence commence 30 jours avant la date d'expiration.

Ces notifications sont envoyées une fois par jour.

L'envoi est interrompu dans les cas suivants :

- Vous avez ajouté une clé de licence dont le délai de validité est supérieur à celui de la clé active et à la valeur du paramètre **Envoyer une notification**.
- La licence a expiré. Dans ce cas, une notification est envoyée pour signaler l'expiration du délai de validité.

► *Pour configurer la date de début de l'envoi des notifications ou modifier l'en-tête ou le texte de la notification d'expiration de la licence, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Notifications** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe quel lien du groupe **La licence arrive bientôt à échéance** pour ouvrir la fenêtre **Paramètres de notification**.

3. Dans le champ **Objet** , saisissez l'en-tête de la notification d'expiration de la licence.

4. Dans le champ **Texte du message** , saisissez le texte de la notification d'expiration de la licence.

5. Dans la liste **Envoyer une notification**, indiquez à partir de combien de jours avant l'expiration vous souhaitez recevoir des notifications.

6. Cliquez sur le bouton **Enregistrer**.

   La fenêtre **Paramètres de notification** se ferme.

► *Pour activer ou désactiver l'envoi de notifications concernant l'expiration de la licence, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Notifications** dans l'arborescence de la console de gestion.

2. Dans le groupe **La licence arrive bientôt à échéance**, exécutez l'une des actions suivantes :

   - Activez le commutateur en regard du groupe de paramètres **La licence arrive bientôt à échéance** pour activer l'envoi de notifications concernant l'expiration de la licence.

   - Désactivez le commutateur en regard du groupe de paramètres **La licence arrive bientôt à échéance** pour désactiver l'envoi de notifications concernant l'expiration de la licence.

Aucune notification n'est envoyée si l'application possède une clé additionnelle. La clé additionnelle devient automatiquement la clé active à l'expiration de la clé active en cours.

Si le délai de validité de la clé additionnelle s'achève avant le début de l'envoi des notifications, la première notification est envoyée au moment du remplacement de la clé active par la clé additionnelle.

Achat d'une licence

Kaspersky Secure Mail Gateway fait partie des suites complexes développées par Kaspersky Lab pour garantir la sécurité et pour administrer le système :

- Kaspersky TOTAL Security for Business (https://www.kaspersky.fr/small-to-medium-business-security/total).
- Kaspersky Security for Mail Servers (https://www.kaspersky.fr/small-to-medium-business-security/mail-server).

Afin de choisir la suite la mieux adaptée à votre entreprise, consultez les experts chez les partenaires de Kaspersky Lab. Les coordonnées et les adresses des partenaires sont fournies dans la section https://www.kaspersky.fr/partners/distribution du site de Kaspersky Lab https://www.kaspersky.fr/partners/distribution .

Etat de protection du serveur de messagerie

La section **Surveillance** de la fenêtre principale de l'interface Internet de Kaspersky Secure Mail Gateway dans la partie droite de l'espace de travail affiche les informations suivantes sur l'état de la protection du serveur de messagerie :

- État de fonctionnement du module Anti-spam, actualité des bases du module Anti-spam, nombre de messages dans la quarantaine de l'Anti-spam ;
- État de fonctionnement du module Antivirus, actualité des bases du module Antivirus ;
- État de la connexion avec le serveur avec le composant KATA, nombre de messages dans la quarantaine KATA (si vous utilisez l'application Kaspersky Anti Targeted Attack Platform) ;
- État du fonctionnement du module Anti-phishing, actualité des bases du module Anti-phishing ;
- État de la connexion au Kaspersky Security Network ou Kaspersky Private Security Network (si vous utilisez la solution Kaspersky Private Security Network) ;
- Informations sur la dernière mise à jour des bases de données de l'application ;
- État de la connexion aux serveurs LDAP ;
- Durée de validité de la licence et avertissement sur l'expiration prochaine de la licence, si c'est le cas ;
- Informations sur l'état de l'envoi et de la réception de messages par l'agent de messagerie MTA.

Si vous avez activé l'application, les modules Anti-Spam, Anti-Virus et Anti-Phishing sont activés par défaut. L'envoi et la réception de messages sont activés pour l'agent de messagerie MTA.

Participation à Kaspersky Security Network et utilisation du Kaspersky Private Security Network

Cette section contient les informations sur la participation à Kaspersky Security Network et sur l'utilisation de Kaspersky Private Security Network.

Dans cette section

A propos de la participation à Kaspersky Security Network et de l'utilisation du Kaspersky Private Security Network

Pour renforcer l'efficacité de la protection de l'ordinateur de l'utilisateur, Kaspersky Secure Mail Gateway utilise les données obtenues auprès d'utilisateurs du monde entier. Le réseau *Kaspersky Security Network* permet d'obtenir ces données.

Kaspersky Security Network (KSN) est un ensemble de services cloud qui permet d'accéder à la base de connaissances de Kaspersky Lab sur la réputation des fichiers, des sites et des applications. Grâce aux données de Kaspersky Security Network, Kaspersky Secure Mail Gateway peut réagir plus rapidement aux objets dont les informations ne figurent pas encore dans les bases de l'application. L'efficacité de certains modules est améliorée et la probabilité de faux positifs est réduite.

La participation au Kaspersky Security Network permet à Kaspersky Lab d'obtenir efficacement des informations sur les types et les sources d'objets dont les informations ne figurent pas encore dans les bases antivirus de l'application, de développer des moyens de neutralisation et de réduire le nombre de faux positifs de l'application.

Dans le cadre de la participation au Kaspersky Security Network, certaines statistiques obtenues pendant le fonctionnement de Kaspersky Secure Mail Gateway sont envoyées automatiquement à Kaspersky Lab. Ainsi, des fichiers (ou des parties de ceux) qui pourraient être utilisés par des individus malintentionnés pour nuire l'ordinateur ou aux données, peuvent être envoyés à Kaspersky Lab pour une analyse complémentaire.

Les données personnelles de l'utilisateur ne sont ni recueillies, ni traitées, ni enregistrées. Les données que Kaspersky Secure Mail Gateway transmet au Kaspersky Security Network sont décrites dans les conditions de KSN.

La participation au Kaspersky Security Network est volontaire. La décision de participer ou non à Kaspersky Security Network est prise lors de l'installation de Kaspersky Secure Mail Gateway. Il est toutefois possible de la modifier à tout moment.

Si vous ne voulez pas participer à KSN, vous pouvez utiliser Kaspersky Private Security Network (ci-après KPSN) qui est une solution qui permet aux utilisateurs d'accéder aux bases de réputation de Kaspersky Security Network et à d'autres données statistiques sans envoyer de données à Kaspersky Security Network depuis leurs ordinateurs.

Si vous avez des questions sur l'achat de l'application Kaspersky Private Security Network, contactez les experts chez nos partenaires dans votre région (https://www.kaspersky.fr/partners/distribution).

Configuration de la participation au Kaspersky Security Network

► *Pour configurer la participation au Kaspersky Security Network, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Utilisation de KSN / KPSN** du groupe **Services externes** pour ouvrir la fenêtre **Utilisation de KSN / KPSN**.

3. Dans la liste des actions, sélectionnez **Utiliser KSN**.

4. Lisez la Déclaration de Kaspersky Security Network et sélectionnez l'une des options suivantes :

   - **J'accepte** si vous souhaitez participer au Kaspersky Security Network.
   - **Je n'accepte pas** si vous ne souhaitez pas participer au Kaspersky Security Network.

5. Cliquez sur le bouton **Appliquer**.

   La fenêtre **Utilisation de KSN / KPSN** se ferme.

6. Cliquez sur le lien **Attendre la réponse KSN** du groupe **Services externes** pour ouvrir la fenêtre **Services externes**.

7. Indiquez dans le champ **Attendre la réponse KSN** la durée maximale d'attente de la réponse de KSN en secondes. Cette valeur peut être comprise entre 1 et 300 secondes.

   Valeur par défaut : 10 s.

8. Cliquez sur le bouton **Appliquer**.

La participation au Kaspersky Security Network est configurée.

Configuration de l'utilisation de Kaspersky Private Security Network

► *Pour configurer l'utilisation de Kaspersky Private Security Network, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Utilisation de KSN / KPSN** du groupe **Services externes** pour ouvrir la fenêtre **Utilisation de KSN / KPSN**.

3. Dans la liste des actions, choisissez **Utiliser KPSN**.
4. Sur ligne **Charger le fichier de configuration de KPSN** , cliquez sur le bouton **Parcourir**.

   La fenêtre de sélection des fichiers s'ouvre.
5. Sélectionnez le fichier de configuration de KPSN que vous souhaitez ajouter.

   Le fichier de configuration de KPSN doit être au format d'une archive ZIP.
6. Cliquez sur le bouton **OK**.

   La fenêtre de sélection de fichiers se ferme.
7. Cliquez sur le lien **Attendre la réponse KSN** du groupe **Services externes** pour ouvrir la fenêtre **Services externes**.
8. Indiquez dans le champ **Attendre la réponse KSN** la durée maximale d'attente de la réponse de KSN en secondes. Cette valeur peut être comprise entre 1 et 300 secondes.

   Valeur par défaut : 10 s.
9. Cliquez sur le bouton **Appliquer**.

La configuration de l'utilisation de Kaspersky Private Security Network est terminée.

Déploiement de l'image de la machine virtuelle de l'application dans l'hyperviseur VMware ESXi

Cette section contient les explications étape par étape du déploiement de l'image de la machine virtuelle de l'application dans l'hyperviseur VMware ESXi.

Dans cette section

Préparation du déploiement

Avant de déployer l'image de la machine virtuelle de l'application, assurez-vous que la version de VMware ESXi et des ressources matérielles correspondent à la configuration matérielle et logicielle requise (cf. section "Configurations logicielles et matérielles" à la page 32).

Etape 1. Sélection de l'image de machine virtuelle

L'image de la machine virtuelle de l'application est diffusée dans le paquet au format OVF.

► *Pour déployer l'image à partir du paquet OVF, procédez comme suit :*

1. Lancez l'application VMware vSphere™ Client.
2. Dans le menu **File**, sélectionnez l'option **Deploy OVF Template**.

   L'Assistant de déploiement démarre et la fenêtre **Deploy OVF Template** s'ouvre.
3. Dans la fenêtre **Deploy OVF Template**, indiquez le fichier doté d'une extension OVA qui contient l'image de la machine virtuelle.
4. Cliquez sur le bouton **Next**.

Vous passez à l'étape suivante de l'Assistant de déploiement.

Etape 2. Affichage des renseignements sur l'image de machine virtuelle

► *Pour afficher les renseignements concernant l'image de machine virtuelle de l'application, procédez comme suit :*

1. Lisez les renseignements concernant l'image de la machine virtuelle sélectionnée à l'étape précédente.
2. Cliquez sur le bouton **Next**.

Vous passez à l'étape suivante de l'Assistant de déploiement.

Etape 3. Consultation du Contrat de licence

Pour poursuivre le déploiement, vous devez accepter les conditions du Contrat de licence. Dans le cas contraire, le déploiement n'a pas lieu.

► *Pour accepter les conditions du Contrat de licence, procédez comme suit :*

1. Dans la fenêtre **Deploy OVF Template** cliquez sur le bouton **Accept**.
2. Cliquez sur le bouton **Next**.

Vous passez à l'étape suivante de l'Assistant de déploiement.

Etape 4. Configuration du nom de la machine virtuelle

► *Pour attribuer un nom à la machine virtuelle, procédez comme suit :*

1. Saisissez le nom de la machine virtuelle dans le champ **Name** (cf. ill. ci-dessous).

   > Le nom doit être unique parmi les machines virtuelles utilisées.

2. Cliquez sur le bouton **Next**.

Vous passez à l'étape suivante de l'Assistant de déploiement.

Etape 5. Sélection du magasin de données de la machine virtuelle

► *Pour sélectionner le magasin de données de l'hôte VMware ESXi (`destination storage`) sur lequel seront stockés les fichiers de la machine virtuelle de l'application, procédez comme suit :*

1. Choisissez le magasin de données dans la liste.

2. Cliquez sur le bouton **Next**.

Vous passez à l'étape suivante de l'Assistant de déploiement.

Etape 6. Sélection du type d'hébergement des fichiers de la machine virtuelle

► *Pour sélectionner le type d'hébergement des fichiers de la machine virtuelle de l'application dans le magasin de données de l'hôte VMware ESXi, procédez comme suit :*

1. Sélectionnez une des options suivantes de la liste :

   - **Thick Provision Lazy Zeroed**. Le volume d'espace disque indiqué est immédiatement réservé aux fichiers de la machine virtuelle. Les blocs de données du volume sélectionné sont remplacés par les données de la machine virtuelle pendant leur traitement.

   - **Thick Provision Eager Zeroed**. Le volume d'espace disque indiqué est immédiatement réservé aux fichiers de la machine virtuelle. Les blocs de données sont libérés sur l'espace disque.

   - **Thin Provision**. Un volume d'espace disque minimal est réservé aux fichiers de la machine virtuelle. Ce volume augmente en cas de besoin.

     > Il est recommandé d'utiliser l'une des options de Thick Provisioning.

2. Cliquez sur le bouton **Next**.

Vous passez à l'étape suivante de l'Assistant de déploiement.

Etape 7. Lancement et fin du déploiement de l'image de machine virtuelle

► *Pour lancer le déploiement de l'image de machine virtuelle et vérifier que l'opération s'est déroulée correctement, procédez comme suit :*

1. Vérifiez les paramètres de la machine virtuelle configurés aux étapes précédentes.
2. Cochez la case **Power on after deployment**, si vous souhaitez que la machine virtuelle se mette en route automatiquement après le déploiement.
3. Si tous les paramètres sont corrects, cliquez sur le bouton **Finish**.

   Le déploiement de l'image de la machine virtuelle démarre.
4. Cochez la case **Close this dialog when completed** si vous souhaitez que la fenêtre de progression du déploiement se ferme automatiquement à la fin du déploiement de l'image de machine virtuelle.
5. Une fois le déploiement terminé, cliquez sur le bouton **Close**.

Après le déploiement de l'image de la machine virtuelle, passez à la configuration initiale de la machine virtuelle (cf. page 72).

Déploiement de l'image de la machine virtuelle dans l'hyperviseur Microsoft Hyper-V

Cette section contient les explications étape par étape du déploiement de l'image de la machine virtuelle de Kaspersky Secure Mail Gateway dans l'hyperviseur Microsoft Hyper-V.

Dans cette section

Préparation du déploiement

L'image de la machine virtuelle Kaspersky Secure Mail Gateway destinée au déploiement dans l'hyperviseur Microsoft Hyper-V est diffusé sous forme d'archive au format ZIP.

Avant de déployer l'image de la machine virtuelle de Kaspersky Secure Mail Gateway, procédez comme suit :

1. Confirmez que la version Microsoft Hyper-V et les ressources matérielles sélectionnées pour la machine virtuelle correspondent à la configuration matérielle et logicielle requise (cf. section "Configuration matérielle et logicielle" à la page 32).

2. Téléchargez l'archive avec l'image de la machine virtuelle sur le site Internet de Kaspersky Lab.

3. Décompressez l'archive avec l'image de la machine virtuelle sur le disque dur de votre ordinateur.

Etape 1. Sélection de l'image de machine virtuelle

► *Pour sélectionner l'image de la machine virtuelle à déployer dans l'hyperviseur Microsoft Hyper-V, procédez comme suit :*

1. Lancez l'application Microsoft Hyper-V Manager.

2. Dans le menu **Actions** dans la partie droite de la fenêtre, sélectionnez l'option **Import Virtual Machine**.

   La fenêtre **Import Virtual Machine** s'ouvre.

3. Dans la partie gauche de la fenêtre, choisissez la section **Select Virtual Machine**.

4. Dans la partie droite de la fenêtre, sélectionnez l'image de la machine virtuelle, que vous voulez déployer.

5. Cliquez sur le bouton **Next**.

Vous passez à l'étape suivante de l'assistant.

Etape 2. Sélection du mode d'importation de la machine virtuelle

Dans l'hyperviseur Microsoft Hyper-V, il y a divers modes d'importation des machines virtuelles. Pour une bonne installation et un bon fonctionnement de Kaspersky Secure Mail Gateway, il est recommandé de créer une nouvelle machine virtuelle.

► *Pour créer une nouvelle machine virtuelle dans l'hyperviseur Microsoft Hyper-V, procédez comme suit :*

1. Dans la partie gauche de la fenêtre **Import Virtual Machine** , sélectionnez la section **Choose Import Type**.

2. Dans la partie droite de la fenêtre, sélectionnez le mode d'importation de la machine virtuelle **Copy the virtual machine (create a new unique ID)**.

3. Cliquez sur le bouton **Next**.

Vous passez à l'étape suivante de l'assistant.

Etape 3. Sélection des répertoires pour la conservation des données de la machine virtuelle

► *Pour sélectionner le répertoire d'hébergement des données de la machine virtuelle de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Dans la partie gauche de la fenêtre **Import Virtual Machine** , choisissez la section **Choose Destination**.

   Dans la partie droite de la fenêtre s'affiche le répertoire d'hébergement des données de la machine virtuelle défini par défaut par l'hyperviseur.

2. Si vous voulez modifier manuellement les répertoires d'hébergement des données de la machine virtuelle, procédez comme suit :

   a. Cochez la case **Store the virtual machine in a different location**.

b. Dans le champ **Virtual machine configuration folder**, saisissez le répertoire d'hébergement des fichiers de configuration de la machine virtuelle.

c. Dans le champ **Checkpoint store** saisissez le répertoire d'hébergement des instantanés de la machine virtuelle.

d. Dans le champ **Smart Paging folder**, saisissez le répertoire d'hébergement des fichiers d'échange de la machine virtuelle.

3. Si vous voulez choisir les répertoires d'hébergement des données de la machine virtuelle, procédez comme suit pour chaque répertoire :

   a. Cliquez sur le bouton **Parcourir** situé à droite de chaque répertoire.

   La fenêtre de sélection des dossiers du système d'exploitation que vous utilisez s'ouvre.

   b. Sélectionnez le dossier que vous voulez utiliser comme répertoire d'hébergement des données de la machine virtuelle.

   c. Appuyez sur le bouton **Ouvrir** dans la fenêtre de sélection des dossiers du système d'exploitation.

   La fenêtre de sélection de dossiers se ferme. Les répertoires d'hébergement des données de la machine virtuelle seront établis.

4. Cliquez sur le bouton **Next**.

Vous passez à l'étape suivante de l'assistant.

Etape 4. Sélection du répertoire pour l'hébergement des disques durs virtuels

► *Pour sélectionner le répertoire d'hébergement des disques durs virtuels de la machine virtuelle de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Dans la partie gauche de la fenêtre **Import Virtual Machine** , choisissez la section **Choose Storage Folders**.

Dans la partie droite de la fenêtre s'affiche le répertoire d'hébergement des disques durs virtuels de la machine virtuelle défini par défaut par l'hyperviseur.

2. Si vous voulez modifier manuellement le répertoire d'hébergement des disques durs virtuels de la machine virtuelle, dans le champ **Location** , saisissez le répertoire d'hébergement des disques durs virtuels.

3. Si vous voulez sélectionner le répertoire d'hébergement des disques durs virtuels de la machine virtuelle, procédez comme suit :

    a. A droite du champ **Location**, cliquez sur le bouton **Parcourir**.

    La fenêtre de sélection des dossiers du système d'exploitation que vous utilisez s'ouvre.

    b. Sélectionnez le dossier que vous voulez utiliser comme répertoire d'hébergement des disques durs virtuels de la machine virtuelle.

    c. Appuyez sur le bouton **Ouvrir** dans la fenêtre de sélection des dossiers du système d'exploitation.

    La fenêtre de sélection de dossiers se ferme. Le répertoire d'hébergement des disques durs virtuels de la machine virtuelle sera établi.

4. Cliquez sur le bouton **Next**.

Vous passez à l'étape suivante de l'assistant.

Etape 5. Connexion à l'interface de réseau de la machine virtuelle

► *Pour se connecter à l'interface de réseau de la machine virtuelle de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Dans la partie gauche de la fenêtre **Import Virtual Machine** , choisissez la section **Connect Network**.

    Dans la partie droite de la fenêtre s'affiche le nom de l'interface de réseau utilisée lors de la création du paquet d'installation de l'application.

2. Si des interfaces de réseau avec d'autres noms sont utilisées dans votre hyperviseur, dans la liste **Connection**, sélectionnez l'interface de réseau à laquelle vous voulez vous connecter.

3. Cliquez sur le bouton **Next**.

Vous passez à l'étape suivante de l'assistant.

Etape 6. Affichage des renseignements sur l'image de machine virtuelle

► *Pour afficher les renseignements concernant l'image de machine virtuelle de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Dans la partie gauche de la fenêtre **Import Virtual Machine** , choisissez la section **Summary**.

   Dans la partie droite de la fenêtre s'affichent les informations sur l'image de la machine virtuelle.

2. Cliquez sur le bouton **Finish**.

Le déploiement de l'image de la machine virtuelle de Kaspersky Secure Mail Gateway se termine.

Après le déploiement de l'image de la machine virtuelle, accédez à la configuration initiale de la machine virtuelle (cf. section "Configuration initiale de l'application" à la page 72).

Configuration initiale de l'application

Après le déploiement de l'image de la machine virtuelle de l'application, procédez à sa configuration initiale.

La configuration initiale d'une machine virtuelle se déroule en plusieurs étapes. L'assistant de configuration initiale de l'application démarre automatiquement lorsque la machine virtuelle est mise en route la première fois.

Dans cette section

Préparation de la configuration initiale de la machine virtuelle dans l'hyperviseur VMware ESXi

► *Pour lancer la configuration initiale de la machine virtuelle de l'application dans l'hyperviseur VMware ESXi, procédez comme suit :*

1. Lancez l'application VMware vSphere Client.
2. Sélectionnez la machine virtuelle Kaspersky Secure Mail Gateway dans la liste des machines virtuelles affichée dans la partie gauche de la fenêtre principale de l'application.
3. Démarrez la machine virtuelle en cliquant sur le bouton  dans la barre de gestion de la fenêtre principale de l'application.
4. Ouvrez la console VMware vSphere Client en cliquant sur l'onglet **Console** dans la partie droite de la fenêtre principale de l'application et suivez les étapes de l'Assistant de configuration initiale.

Préparation de la configuration initiale de la machine virtuelle dans l'hyperviseur Microsoft Hyper-V

► *Pour lancer la configuration initiale de la machine virtuelle de Kaspersky Secure Mail Gateway dans l'hyperviseur Microsoft Hyper-V, procédez comme suit :*

1. Lancez l'application Microsoft Hyper-V Manager.
2. Dans la section **Virtual Machines** sélectionnez la machine virtuelle pour laquelle vous souhaitez procéder à la configuration initiale.
3. Démarrez la machine virtuelle en cliquant sur le bouton  dans la barre de gestion de la fenêtre principale de l'application.

La console de gestion de la machine virtuelle de Kaspersky Secure Mail Gateway démarre.

4. Suivez les instructions de l'Assistant de configuration initiale de l'application.

Etape 1. Choix de la langue d'affichage du Contrat de licence

► *Pour paramétrer la langue dans laquelle s'affichera le Contrat de licence de l'application et les dispositions de Kaspersky Security Network, procédez comme suit :*

1. Choisissez la langue dans la liste.

   Les langues disponibles dépendent des paquets de localisation compris dans votre distribution de Kaspersky Secure Mail Gateway.

2. Appuyez sur la touche **Enter**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 2. Consultation du Contrat de licence

Cette étape est celle où vous acceptez ou rejetez les dispositions du Contrat de Licence Utilisateur Final de l'application. Pour vous déplacer d'une ligne à l'autre, servez-vous des touches curseur.

► *Pour accepter ou refuser les conditions du Contrat de licence, procédez comme suit :*

1. Sélectionnez l'une des options suivantes :

   - **I do not accept the agreement** pour refuser les conditions du Contrat de licence ;
   - **I accept the agreement** pour accepter les conditions du Contrat de licence.

2. Appuyez sur la touche **Enter**.

Si vous avez rejeté les conditions du Contrat de Licence Utilisateur Final, la configuration initiale de l'application s'achève. L'Assistant de configuration initiale vous invite à arrêter la machine virtuelle.

Si vous avez accepté les conditions du Contrat de Licence Utilisateur Final, l'Assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 3. Sélection du mode de fonctionnement de l'application

Cette étape correspond à la sélection du mode de fonctionnement de l'application au sein de l'infrastructure IT de votre organisation.

Kaspersky Secure Mail Gateway peut fonctionner en mode normal ou en mode certifié.

En mode normal, l'application peut accéder à Internet et peut se connecter aux serveurs suivants situés en-dehors de l'infrastructure informatique de votre organisation :

- Les serveurs de mise à jour des bases KSN (cf. section "A propos de la participation au Kaspersky Security Network" à la page 57) ;
- Les serveurs DNS (cf. section "Connexion au serveur DNS pour l'authentification des expéditeurs" à la page 250);
- Les serveurs de mise à jour des bases de l'application (cf. section "A propos des sources des mises à jour" à la page 239).

En mode certifié, l'application ne peut pas accéder à Internet et ne peut pas se connecter aux serveurs situés en-dehors l'infrastructure informatique de votre organisation. En outre quand l'application fonctionne en mode certifié, l'administrateur n'est pas en mesure de consulter le journal des événements au départ du menu de l'administrateur de l'application.

En mode certifié, les paramètres des modules de l'application qui requièrent un accès Internet prennent les valeurs suivantes par défaut :

- Utilisation de KSN désactivée (cf. section "Configuration de la participation au Kaspersky Security Network" à la page 58).
- L'authentification SPF (cf. section "Activation et désactivation de l'authentification SPF des expéditeurs" à la page 251) DKIM (cf. section "Activation et désactivation de l'authentification DKIM des expéditeurs" à la page 251) et DMARC des expéditeurs de messages (cf. section "Activation et désactivation de l'authentification DMARC des expéditeurs" à la

page 252) est désactivée et la connexion aux serveurs DNS (cf. section "Connexion au serveur DNS pour l'authentification des expéditeurs" à la page 250) est interdite.

- Le paramètre Enforced Anti-Spam Updates (cf. section "Configuration des paramètres du module Anti-spam" à la page 288) est désactivé dans les paramètres du module Anti-spam.
- En guise de source des mises à jour de la base de l'application, vous avez le choix entre Kaspersky Security Center ou une source locale de mise à jour de la base de données de Kaspersky Secure Mail Gateway (cf. section "A propos des sources des mises à jour" à la page 239).

► *Pour choisir le mode de fonctionnement de l'application, procédez comme suit :*

1. Choisissez une des options suivantes pour le transfert de l'application vers le mode certifié :
   - **No**, si vous ne voulez pas transférer l'application vers le mode certifié et si vous voulez que l'application fonctionne en mode normal.
   - **Yes** si vous souhaitez transférer l'application vers le mode certifié.
2. Appuyez sur la touche **Enter**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 4. Configuration de la participation au Kaspersky Security Network

Si vous avez choisi le mode normal de fonctionnement de l'application (cf. page 76), l'Assistant de configuration initiale de l'application vous offre l'option de participer ou non au Kaspersky Security Network (KSN).

Kaspersky Security Network (KSN) est un ensemble de services cloud qui permet d'accéder à la base de connaissances de Kaspersky Lab sur la réputation des fichiers, des sites et des applications. Grâce aux données de Kaspersky Security Network, Kaspersky Secure Mail Gateway peut réagir plus rapidement aux menaces dont les informations ne figurent pas encore

dans les bases de l'application. L'efficacité de certains modules est améliorée et la probabilité de faux positifs est réduite.

L'implication des utilisateurs dans le Kaspersky Security Network permet à Kaspersky Lab de recueillir efficacement des informations sur les types et les sources des nouvelles menaces, de développer des moyens de neutralisation et de réduire le nombre de faux positifs. De plus, la participation au Kaspersky Security Network vous donne accès aux données sur la réputation des applications et des sites Internet.

Si vous participez à Kaspersky Security Network, vous enverrez des statistiques sur le fonctionnement de Kaspersky Secure Mail Gateway à Kaspersky Lab. Cet envoi est automatique.

Les données personnelles de l'utilisateur ne sont ni recueillies, ni traitées, ni enregistrées.

La participation au Kaspersky Security Network est volontaire. Vous prenez cette décision pendant la configuration initiale de l'application, mais vous pouvez changer d'avis à tout moment.

Le texte de la Déclaration de Kaspersky Security Network s'affiche sur l'écran de la console de la machine virtuelle. Pour vous déplacer d'une ligne à l'autre, servez-vous des touches curseur.
Le texte des dispositions de Kaspersky Security Network est affiché dans la langue sélectionnée à l'étape 1 (cf. section "Etape 1. Choix de la langue d'affichage du Contrat de licence" à la page 75).

► *Pour accepter ou refuser de participer au Kaspersky Security Network, procédez comme suit :*

1. Sélectionnez l'une des options suivantes :
   - **I do not agree to participate in Kaspersky Security Network** pour refuser de participer au Kaspersky Security Network ;
   - **I agree to participate in Kaspersky Security Network** pour accepter de participer au Kaspersky Security Network.
2. Appuyez sur la touche **Enter**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 5. Sélection de la langue de saisie pour l'utilisation de l'application

► *Pour configurer la langue dans laquelle vous utiliserez l'application, procédez comme suit :*

1. Choisissez la langue de saisie dans la liste.

2. Cliquez sur le bouton **OK**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 6. Réglage du fuseau horaire

► *Pour régler le fuseau horaire dans Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sélectionnez un pays dans la liste qui s'affiche sur l'écran de la console.

2. Appuyez sur la touche **Enter**.

   La liste des fuseaux horaires disponibles dans le pays sélectionné apparaît.

3. Sélectionnez le fuseau horaire pertinent.

4. Appuyez sur la touche **Enter**.

   La fenêtre de la confirmation du choix de fuseau horaire s'ouvre.

5. Si le fuseau horaire sélectionné est correct, cliquez sur le bouton **Yes**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 7. Définition du nom d'hôte (myhostname)

► *Pour indiquer le nom d'hôte de l'application à utiliser avec les serveurs DNS (`myhostname`), procédez comme suit :*

1. Dans le champ **hostname**, saisissez le nom de domaine complet du serveur de l'application.

   Indiquez le nom du serveur au format FQDN (par exemple, host.domain.com ou host.domain.subdomain.com).

2. Cliquez sur le bouton **Ok**.

   Après avoir défini le nom d'hôte de l'application, la machine virtuelle tente de récupérer automatiquement les paramètres réseau à l'aide du serveur DHCP et de charger les bases de l'application.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 8. Configuration de l'interface réseau

Cette étape correspond à la configuration des paramètres de l'interface réseau de l'application : activez ou désactivez l'interface réseau, désignez l'adresse IP ainsi que le masque de réseau.

Dans cette section

Activation et désactivation de l'interface réseau

Pour configurer l'application, il faut activer au moins une interface réseau. Vous devrez peut-être désactiver une interface réseau si vous en utilisez plusieurs et si vous voulez désactiver temporairement l'une d'elles.

► *Pour désactiver une interface réseau, procédez comme suit :*

1. Sélectionnez le paramètre **Enabled**.
2. Appuyez sur la touche **Enter**.

   Le paramètre **Enabled** prend la valeur **no**.
3. Passez à la définition de l'adresse IP et du masque réseau (cf. section "Définition de l'adresse IP et du masque de réseau avec le serveur DHCP" à la page 81 ou "Définition de l'adresse IP et du masque de réseau statiques" à la page 82), pour terminer la configuration de l'interface réseau.

► *Pour activer une interface réseau, procédez comme suit :*

1. Vérifiez que le paramètre **Enabled** a pour valeur **yes**.

   Par défaut, l'interface réseau est activée.
2. Passez à la définition de l'adresse IP et du masque réseau (cf. section "Définition de l'adresse IP et du masque de réseau avec le serveur DHCP" à la page 81 ou "Définition de l'adresse IP et du masque de réseau statiques" à la page 82), pour terminer la configuration de l'interface réseau.

Définition de l'adresse IP et du masque de réseau avec le serveur DHCP

► *Pour définir l'adresse IP et le masque de réseau avec le serveur DHCP, procédez comme suit :*

1. Confirmez que le paramètre **Use DHCP** a la valeur **yes**.

> Vous devrez peut-être passer par le serveur DHCP pour définir l'adresse IP et le masque de réseau si vous configurez l'application en mode de test.

Par défaut, la définition de l'adresse IP et du masque de réseau passe par le serveur DHCP.

2. Sélectionnez **Continue**.
3. Appuyez sur la touche **Enter**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Définition de l'adresse IP statique et du masque de réseau

► *Pour définir l'adresse IP et le masque de réseau statiques, procédez comme suit :*

1. Sélectionnez le paramètre **Use DHCP**.

> Il est recommandé de définir une adresse IP et un masque de réseau statiques si vous configurez l'application en mode opérationnel.

2. Appuyez sur la touche **Enter**.

   La fenêtre de configuration des paramètres statiques définis pour l'interface réseau s'ouvre.

3. Cliquez sur le bouton **Yes**.

   La fenêtre de saisie de l'adresse IP statique et du masque de réseau s'ouvre.

4. Dans le champ **Address**, saisissez l'adresse IP que vous voulez attribuer à Kaspersky Secure Mail Gateway.
5. Dans le champ **Netmask**, saisissez le masque du réseau sur lequel vous utilisez l'application.
6. Cliquez sur le bouton **Ok**.

L'Assistant de configuration initiale de l'application revient à la fenêtre de configuration de l'interface réseau.

7. Vérifiez les paramètres réseau définis.
8. Sélectionnez **Continue**.
9. Appuyez sur la touche **Enter**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 9. Configuration des itinéraires réseau

A cette étape, vous définissez une adresse de passerelle pour configurer l'itinéraire réseau. Vous pouvez également ajouter, supprimer ou modifier des itinéraires réseau statiques supplémentaires à ce stade.

Dans cette section

Définition de l'adresse de la passerelle avec le serveur DHCP

► *Pour définir l'adresse de la passerelle avec le serveur DHCP, procédez comme suit :*

1. Confirmez que le paramètre **Gateway** de la liste **Default route** possède la valeur **dhcp**.

> Vous devrez peut-être passer par le serveur DHCP pour définir l'adresse de la passerelle si vous configurez l'application en mode de test.

Par défaut, la définition de l'adresse de la passerelle passe par le serveur DHCP.

2. Sélectionnez **Continue**.
3. Appuyez sur la touche **Enter**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Définition de l'adresse statique de la passerelle

► *Pour définir une adresse de passerelle statique, procédez comme suit :*

1. Dans la liste **Default route**, choisissez le paramètre **Gateway**.
2. Appuyez sur la touche **Enter**.
3. Si à l'étape antérieure de la configuration initiale de Kaspersky Secure Mail Gateway (cf. section "Etape 8. Configuration de l'interface réseau" à la page 80) vous aviez choisi l'utilisation du serveur DHCP pour configurer l'interface réseau, cliquez sur le bouton **Yes** dans la fenêtre de confirmation de la définition de l'adresse statique de la passerelle qui s'ouvre.

   La fenêtre de saisie de l'adresse statique de la passerelle s'ouvre.
4. Dans le champ **Gateway**, saisissez l'adresse de la passerelle.
5. Cliquez sur le bouton **Ok**.

   L'Assistant de configuration initiale de l'application revient à la fenêtre de la configuration des itinéraires réseaux.
6. Vérifiez les paramètres de l'itinéraire réseau configuré.

> Si vous voulez modifier, supprimer ou ajouter des itinéraires statiques supplémentaires, passez à la configuration des itinéraires réseaux statiques supplémentaires (cf. section "Ajout d'un itinéraire statique supplémentaire" à la page 85).

7. Sélectionnez **Continue**.
8. Appuyez sur la touche **Enter**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Ajout d'un itinéraire statique supplémentaire

► *Pour ajouter un itinéraire statique supplémentaire, procédez comme suit :*

1. Choisissez le paramètre **Edit static routes**.
2. Appuyez sur la touche **Enter**.

   La fenêtre de sélection de l'action à effectuer concernant les itinéraires statiques supplémentaires s'ouvre.
3. Sélectionnez **New route**.
4. Appuyez sur la touche **Enter**.

   La fenêtre de saisie des paramètres de l'itinéraire statique s'ouvre.
5. Dans le champ **Address**, saisissez l'adresse IP de l'itinéraire statique.
6. Dans le champ **Netmask**, saisissez le masque de réseau de l'itinéraire statique.
7. Dans le champ **Gateway**, saisissez l'adresse de la passerelle.
8. Cliquez sur le bouton **Ok**.

   La fenêtre de sélection de l'interface réseau sur laquelle vous souhaitez configurer l'itinéraire statique s'ouvre.

9. Sélectionnez l'interface réseau désirée.
10. Appuyez sur la touche **Enter**.

    La fenêtre contenant la liste des itinéraires statiques complémentaires s'ouvre.
11. Sélectionnez **Go back**.
12. Appuyez sur la touche **Enter**.

    L'Assistant de configuration initiale de l'application revient à la fenêtre de la configuration des itinéraires réseaux.
13. Vérifiez les paramètres de l'itinéraire réseau configuré.
14. Sélectionnez **Continue**.
15. Appuyez sur la touche **Enter**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Modification d'un itinéraire statique supplémentaire

► *Pour modifier un itinéraire statique supplémentaire, procédez comme suit :*

1. Choisissez le paramètre **Edit static routes**.
2. Appuyez sur la touche **Enter**.

   La fenêtre contenant la liste des itinéraires statiques complémentaires s'ouvre.
3. Sélectionnez l'itinéraire statique supplémentaire à modifier.
4. Appuyez sur la touche **Enter**.
5. La fenêtre de saisie des paramètres de l'itinéraire statique s'ouvre.
6. Pour modifier l'adresse IP de l'itinéraire statique, saisissez les modifications dans le champ **Address**.

7. Pour modifier le masque de réseau de l'itinéraire statique, saisissez les modifications dans le champ **Netmask**.
8. Pour modifier l'adresse de la passerelle, saisissez les modifications dans le champ **Gateway**.
9. Cliquez sur le bouton **Ok**.

   La fenêtre de sélection de l'interface réseau sur laquelle vous souhaitez configurer l'itinéraire statique s'ouvre.
10. Sélectionnez l'interface réseau désirée.
11. Appuyez sur la touche **Enter**.

    La fenêtre contenant la liste des itinéraires statiques complémentaires s'ouvre.
12. Sélectionnez **Go back**.
13. Appuyez sur la touche **Enter**.

    L'Assistant de configuration initiale de l'application revient à la fenêtre de la configuration des itinéraires réseaux.
14. Vérifiez les paramètres de l'itinéraire réseau configuré.
15. Sélectionnez **Continue**.
16. Appuyez sur la touche **Enter**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Suppression d'un itinéraire statique supplémentaire

► *Pour supprimer un itinéraire statique supplémentaire, procédez comme suit :*

1. Choisissez le paramètre **Edit static routes**.
2. Appuyez sur la touche **Enter**.

La fenêtre contenant la liste des itinéraires statiques complémentaires s'ouvre.

3. Sélectionnez **Delete routes**.
4. Appuyez sur la touche **Enter**.

   La fenêtre de sélection de la route statique à supprimer s'ouvre.

5. Sélectionnez l'itinéraire que vous voulez supprimer.
6. Cliquez sur le bouton **Delete**.

   L'assistant de configuration initiale de l'application revient à la fenêtre contenant la liste des itinéraires statiques supplémentaires restants ou, si vous avez supprimé tous les itinéraires supplémentaires, la fenêtre de sélection de l'action à effectuer sur les itinéraires s'ouvre (cf. ill. ci-dessous).

7. Sélectionnez **Go back**.
8. Appuyez sur la touche **Enter**.

   L'Assistant de configuration initiale de l'application revient à la fenêtre de la configuration des itinéraires réseaux.

9. Vérifiez les paramètres de l'itinéraire réseau configuré.
10. Sélectionnez **Continue**.
11. Appuyez sur la touche **Enter**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 10. Configuration des paramètres DNS

A cette étape, vous configurez les paramètres DNS pour l'utilisation de la machine virtuelle Kaspersky Secure Mail Gateway.

Dans cette section

Définition des adresses DNS avec le serveur DHCP

► *Pour définir une adresse DNS avec le serveur DHCP, procédez comme suit :*

1. Sélectionnez le nom de votre interface réseau (par exemple, **eth0**) dans la fenêtre de sélection du serveur DHCP pour définir les adresses DNS.

   Vous devrez peut-être passer par le serveur DHCP pour définir les adresses DNS si vous configurez l'application en mode de test.

2. Appuyez sur la touche **Enter**.

   La fenêtre de configuration des paramètres DNS à l'aide du serveur DHCP s'ouvre.

3. Vérifiez que les paramètres **Search list**, **Primary DNS** et **Secondary DNS** ont pour valeur **dhcp**.

4. Sélectionnez **Continue**.

5. Appuyez sur la touche **Enter**.

   La fenêtre des paramètres réseau de Kaspersky Secure Mail Gateway s'ouvre.

6. Sélectionnez **Continue**.

7. Appuyez sur la touche **Enter**.

L'Assistant de configuration initiale de l'application redémarre la machine virtuelle avec les nouvelles valeurs des paramètres et passe à l'étape suivante.

Définition des adresses DNS statiques

► *Pour définir les adresses DNS statiques, procédez comme suit :*

1. Sélectionnez **no** dans la fenêtre de configuration de l'utilisation du serveur DHCP pour attribuer les adresses DNS.

   > Il est recommandé de définir des adresses de DNS statiques si vous configurez l'application en mode opérationnel.

2. Appuyez sur la touche **Enter**.

   La fenêtre de saisie des adresses DNS statiques s'ouvre.

3. Dans le champ **Search list**, saisissez le suffixe DNS que vous voulez utiliser pour Kaspersky Secure Mail Gateway.

4. Dans le champ **Primary**, saisissez l'adresse IP du serveur DNS primaire au format IPv4.

5. Dans le champ **Secondary**, saisissez l'adresse IP du serveur DNS secondaire au format IPv4.

6. Cliquez sur le bouton **Ok**.

   La fenêtre de configuration des paramètres DNS statiques s'ouvre.

7. Vérifiez les paramètres de DNS configurés.

8. Sélectionnez **Continue**.

9. Appuyez sur la touche **Enter**.

   La fenêtre des paramètres réseau de Kaspersky Secure Mail Gateway s'ouvre.

10. Sélectionnez **Continue**.

11. Appuyez sur la touche **Enter**.

L'Assistant de configuration initiale de l'application redémarre la machine virtuelle avec les nouvelles valeurs des paramètres et passe à l'étape suivante.

Etape 11. Définition du mot de passe d'administration de l'interface Web

► *Pour définir le mot de passe d'administration permettant d'accéder à l'interface Web (compte `Administrator`), procédez comme suit :*

1. Dans le champ **Test input**, saisissez n'importe quels caractères et vérifiez la disposition du clavier.

2. Dans le champ **Password**, saisissez le mot de passe d'administrateur permettant d'accéder à l'interface Web de Kaspersky Secure Mail Gateway (cf. section "Prise en main de l'interface Web de l'application" à la page 104).

   Le mot de passe doit uniquement contenir :

   - 8 caractères minimum ;
   - Uniquement des caractères ASCII ;
   - Au moins une majuscule ;
   - Au moins une minuscule ;
   - Au moins un chiffre.

3. Dans le champ **Confirm password**, répétez le mot de passe.

4. Cliquez sur le bouton **Ok**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 12. Définition du mot de passe d'administration pour utiliser la console

L'administrateur de Kaspersky Secure Mail Gateway détient les droits de gestion de la machine virtuelle. Il peut arrêter et redémarrer la machine virtuelle ou modifier ses paramètres

réseau sur la console de gestion. L'administration de Kaspersky Secure Mail Gateway s'effectue à partir du compte admin, qui est associé à un mot de passe d'administration distinct.

► *Pour définir le mot de passe de l'administrateur permettant d'utiliser l'application sur la console de gestion (compte utilisateur `admin`), procédez comme suit :*

1. Dans le champ **Test input**, saisissez n'importe quels caractères et vérifiez la disposition du clavier.
2. Dans le champ **Password**, saisissez le mot de passe de l'administrateur pour l'administration des paramètres de l'application.

   Le mot de passe doit uniquement contenir :

   - 8 caractères minimum ;
   - Uniquement des caractères ASCII ;
   - Au moins une majuscule ;
   - Au moins une minuscule ;
   - Au moins un chiffre.
3. Dans le champ **Confirm password**, répétez le mot de passe.
4. Cliquez sur le bouton **Ok**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 13. Définition des adresses électroniques de l'administrateur du serveur de messagerie

► *Pour définir les adresses électroniques de l'administrateur du serveur de messagerie de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Dans le champ **admins' emails**, saisissez les adresses email de l'administrateur de l'application. Vous pouvez saisir plusieurs adresses en les séparant par des virgules.

2. Cliquez sur le bouton **OK**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 14. Configuration de la connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center

Cette étape permet de configurer la connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center à l'aide de l'Assistant de configuration de la connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center.

L'application Kaspersky Security Center est conçue pour centraliser les principales tâches d'administration concernant la gestion et la surveillance de Kaspersky Secure Mail Gateway.

Kaspersky Security Center tient lieu de *Serveur d'administration*.

L'*agent d'administration* (`nagent`) fait partie de la composition de l'application.

Kaspersky Security Center permet à l'administrateur d'effectuer les opérations de gestion de l'application suivantes :

- Ajout des clés active et additionnelle ;
- Lancement de la tâche de mise à jour des bases de données de l'application ;
- Affichage des informations sur l'état de la protection de l'application ;
- Lancement et arrêt de l'application.

Dans cette section

Activation de l'agent d'administration

Pour configurer la connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center, l'agent d'administration doit être activé.

L'agent d'administration est désactivé par défaut.

► *Pour activer l'agent d'administration, réalisez les opérations suivantes dans la fenêtre de l'Assistant de configuration de la connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center :*

1. Sélectionnez le paramètre **Enabled**.
2. Vérifiez que le paramètre **Enabled** a pour valeur **yes**.
3. Si le paramètre **Enabled** a la valeur **no**, appuyez sur la touche **Retour**.

Poursuivez la configuration de la connexion dans la fenêtre de l'Assistant de configuration de connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center.

Saisie de l'adresse du serveur d'administration

► *Pour saisir l'adresse du serveur d'administration de Kaspersky Security Center, exécutez les opérations suivantes dans la fenêtre de l'Assistant de configuration de connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center :*

1. Sélectionnez le paramètre **Address**.
2. Appuyez sur la touche **Enter**.

   La fenêtre de saisie de l'adresse du serveur d'administration s'ouvre.
3. Saisissez le nom DNS ou l'adresse IP du Serveur d'administration de Kaspersky Security Center.
4. Cliquez sur le bouton **Ok**.

Poursuivez la procédure de configuration de la connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center.

Saisie du numéro de port de connexion au serveur d'administration

► *Pour saisir le numéro du port de connexion au serveur d'administration de Kaspersky Security Center, exécutez les opérations suivantes dans la fenêtre de l'Assistant de configuration de connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center :*

1. Sélectionnez le paramètre **Port**.
2. Appuyez sur la touche **Enter**.

   La fenêtre de saisie du port de connexion au serveur d'administration s'ouvre.
3. Saisissez le numéro du port de connexion au serveur d'administration ou utilisez le port par défaut (13000).
4. Cliquez sur le bouton **Ok**.

Poursuivez la configuration de la connexion dans la fenêtre de l'Assistant de configuration de connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center.

Utilisation de la connexion SSL lors du transfert de données

Vous pouvez activer l'utilisation d'une connexion SSL lors du transfert de données sur le serveur d'administration de Kaspersky Security Center.

L'utilisation du protocole SSL lors du transfert de données sur le serveur d'administration de Kaspersky Security Center est activée par défaut.

► *Pour activer l'utilisation de la connexion SSL, réalisez les opérations suivantes dans la fenêtre de l'Assistant de configuration de connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center:*

1. Sélectionnez le paramètre **Use SSL**.
2. Confirmez que le paramètre **Use SSL** a la valeur **yes**.
3. Si le paramètre **Use SSL** a la valeur **no**, appuyez sur la touche **Retour**.

Poursuivez la configuration de la connexion dans la fenêtre de l'Assistant de configuration de connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center.

Utilisation de la passerelle lors de la connexion au serveur d'administration

Vous pouvez choisir un des modes d'utilisation de la passerelle lors de la connexion de Kaspersky Secure Mail Gateway au serveur d'administration Kaspersky Security Center :

- Désactiver l'utilisation de la passerelle ;
- Activer l'utilisation de la passerelle ;
- Activer l'utilisation de l'agent d'administration en tant que passerelle.

Par défaut, l'utilisation de la passerelle lors de la connexion au serveur d'administration est désactivée. La connexion à Kaspersky Security Center est établie directement.

► *Pour désactiver l'utilisation de la passerelle lors de la connexion de l'application au Serveur d'administration, réalisez les opérations suivantes dans la fenêtre de l'Assistant de configuration de connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center :*

1. Sélectionnez le paramètre **Gw mode**.
2. Confirmez que le paramètre **Gw mode** possède la valeur **don't use**.
3. Si le paramètre **Gw mode** possède n'importe quelle autre valeur, appuyez sur la touche **Retour** jusqu'à ce que le paramètre **Gw mode** affiche la valeur **don't use**.

► *Pour activer l'utilisation de la passerelle lors de la connexion de l'application au Serveur d'administration, réalisez les opérations suivantes dans la fenêtre de l'Assistant de configuration de connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center :*

1. Sélectionnez le paramètre **Gw mode**.
2. Appuyez sur la touche **Retour** jusqu'à ce que le paramètre **Gw mode** prenne la valeur **use gateway**.
3. Sélectionnez le paramètre **Gateway**.
4. Appuyez sur la touche **Enter**.

   La fenêtre de saisie de l'adresse de la passerelle s'ouvre.
5. Saisissez le nom DNS ou l'adresse IP de la passerelle que vous souhaitez utiliser lors de la connexion au serveur d'administration Kaspersky Security Center.
6. Cliquez sur le bouton **Ok**.

► *Pour activer l'utilisation de l'agent d'administration en tant que passerelle lors de la connexion de l'application au Serveur d'administration, réalisez les opérations suivantes dans la fenêtre de l'Assistant de configuration de connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center :*

1. Sélectionnez le paramètre **Gw mode**.
2. Appuyez sur la touche **Retour** jusqu'à ce que le paramètre **Gw mode** prenne la valeur **act as gateway**.

Passez à la vérification de la connexion de l'application à Kaspersky Security Center dans la fenêtre de l'Assistant de configuration de la connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center

Etape 15. Vérification de la connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center

► *Pour vérifier la connexion de l'application à Kaspersky Security Center, réalisez les opérations suivantes dans la fenêtre de l'Assistant de configuration de la connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center :*

1. Sélectionnez le paramètre **Check Status**.
2. Appuyez sur la touche **Enter**.
3. Si vous aviez modifié les paramètres de la connexion de l'application à Kaspersky Security Center lors de la configuration de ladite connexion (cf. section "Etape14. Configuration de la connexion de Kaspersky Secure Mail Gateway à Kaspersky Security Center" à la page 93), cliquez sur le bouton **Yes** dans la fenêtre de confirmation de l'enregistrement des modifications qui s'ouvre.

   La fenêtre de confirmation de l'enregistrement des modifications des paramètres de modifications à Kaspersky Security Center se ferme.

   Le paramètre **Check Status** prend un valeur qui correspond à l'état de la connexion de l'application à Kaspersky Security Center.

   Par exemple, si la connexion de l'application à Kaspersky Security Center a été établie, le paramètre **Check Status** prend la valeur **OK**.
4. Sélectionnez **Continue**.
5. Appuyez sur la touche **Enter**.

L'assistant de configuration initiale de l'application passe à l'étape suivante.

Etape 16. Affichage des paramètres de connexion à l'interface Web

Si la connexion réseau est établie, la configuration initiale de Kaspersky Secure Mail Gateway se termine avec cette étape. Une fenêtre affichant les paramètres de connexion à l'interface Web s'ouvre.

Notez l'adresse IP indiquée dans le champ **IP address information**, puis cliquez sur le bouton **OK**.

La configuration initiale de Kaspersky Secure Mail Gateway est terminée.

Si votre réseau n'utilise pas de serveur DHCP, Kaspersky Secure Mail Gateway ne peut pas recevoir automatiquement les paramètres de connexion à l'interface Web de l'application et l'adresse IP de connexion à l'interface Web n'apparaît pas dans la fenêtre **IP address information**. Dans ce cas, vous pouvez configurer les paramètres de connexion à l'interface Internet de l'application manuellement via le menu de l'administrateur de Kaspersky Secure Mail Gateway.

Lancement de la machine virtuelle de l'application

Après la configuration initiale (cf. section "Configuration initiale de l'application" à la page 72), la machine virtuelle Kaspersky Secure Mail Gateway démarre automatiquement. Pour garantir l'interaction avec l'infrastructure de messagerie existante, il faut également configurer le serveur de messagerie, préinstallé sur la machine virtuelle Kaspersky Secure Mail Gateway.

Vous pouvez recevoir des informations sur le fonctionnement de Kaspersky Secure Mail Gateway, mais aussi configurer les règles de traitement des messages et les paramètres de protection depuis l'interface Web (cf. page 104).

Vous pouvez configurer aussi les paramètres et gérer le travail de la machine virtuelle à partir du menu de l'administrateur dans la console de gestion de l'application.

Modification de la configuration de la machine virtuelle

Vous pouvez modifier la configuration des machines virtuelles dans les hyperviseurs VMware ESXi et Microsoft Hyper-V. Par exemple, vous pouvez ajouter ou supprimer des disques durs virtuels, ajouter ou supprimer des adaptateurs réseau virtuels ou modifier le volume de la mémoire vive virtuelle.

Dans cette section

Modification de la configuration de la machine virtuelle dans l'hyperviseur VMware ESXi

► *Pour modifier la configuration de la machine virtuelle dans l'hyperviseur VMware ESXi, procédez comme suit :*

1. Lancez l'application VMware vSphere Client.
2. Dans la liste des machines virtuelles dans la partie gauche de la fenêtre principale de l'application, sélectionnez la machine virtuelle dont vous voulez modifier la configuration.
3. Ouvrez le menu d'un clic droit de la souris.
4. Sélectionnez l'option de menu **Edit Settings**.

   La fenêtre **Virtual Machine Properties** s'ouvre.

5. Sélectionnez l'onglet avec le groupe des paramètres de configuration de la machine virtuelle que vous voulez modifier.
6. Sélectionnez les paramètres de configuration de la machine virtuelle que vous voulez modifier.
7. Dans la partie droite de la fenêtre, procédez aux modifications de la configuration de la machine virtuelle.

Pour plus d'informations sur la modification de la configuration de la machine virtuelle dans l'hyperviseur VMware ESXi, consultez la documentation de l'hyperviseur VMware ESXi.

Modification de la configuration de la machine virtuelle de l'hyperviseur Microsoft Hyper-V

► *Pour modifier la configuration de la machine virtuelle dans l'hyperviseur Microsoft Hyper-V, procédez comme suit :*

1. Lancez l'application Microsoft Hyper-V Manager.
2. Dans la section **Virtual Machines** sélectionnez la machine virtuelle dont vous souhaitez modifier la configuration.
3. Dans le menu **Actions**, dans la partie droite de la fenêtre, sélectionnez l'option **Settings**.

   La fenêtre **Settings** s'ouvre.
4. Dans la partie gauche de la fenêtre, sélectionnez les paramètres de configuration de la machine virtuelle que vous voulez modifier.
5. Dans la partie droite de la fenêtre, procédez aux modifications de la configuration de la machine virtuelle.

Pour en savoir plus sur la modification de la configuration de la machine virtuelle dans l'hyperviseur Microsoft Hyper-V, consultez la documentation de l'hyperviseur Microsoft Hyper-V.

Désactivation de la synchronisation de l'heure de la machine virtuelle et de l'hôte

La synchronisation de l'heure permet de garantir la correspondance permanente entre l'heure du système d'exploitation invité et celle de l'hôte à l'aide des outils de l'hyperviseur. Si la synchronisation de l'heure est activée, l'heure du système d'exploitation invité est toujours synchronisée avec celle de l'hôte.

Si vous voulez utiliser le protocole de temps du réseau (*Network Time Protocol*), il est conseillé de désactiver la synchronisation du temps au niveau de l'hyperviseur :

- Pour configurer un hyperviseur ESXi, consultez la documentation de VMware ESXi https://pubs.vmware.com/vsphere-50/index.jsp?topic=/com.vmware.vmtools.install.doc/GUID-C0D8326A-B6E7-4E61-8470-6C173FDDF656.html;
- Pour configurer un hyperviseur Hyper-V, consultez la documentation de Microsoft https://technet.microsoft.com/en-gb/library/dn798346(v=ws.11).aspx.

Prise en main de l'interface Web de l'application

Une fois l'installation et la configuration initiale terminées (cf. section "Configuration initiale de l'application" à la page 72), vous pouvez commencer à utiliser l'interface Web de Kaspersky Secure Mail Gateway.

► *Pour commencer à travailler dans l'interface Web de l'application, procédez comme suit :*

1. Saisissez l'adresse suivante dans votre navigateur :

   `https://<IP-address-of-deployed-appliance>/ksmg`, en utilisant l'adresse IP reçue lors de l'installation de l'application.

   Une page Web d'autorisation d'accès à l'interface Web s'ouvre et demande le nom d'utilisateur et le mot de passe d'administration de l'interface Web.

2. Dans le champ **Nom d'utilisateur**, saisissez `Administrator`

3. Saisissez dans le champ **Mot de passe** le mot de passe défini lors de l'installation de l'application.

4. Cliquez sur le bouton **Entrer**.

La page principale de l'interface Web de Kaspersky Secure Mail Gateway s'ouvre.

Intégration de Kaspersky Secure Mail Gateway dans l'infrastructure de messagerie de l'entreprise

Kaspersky Secure Mail Gateway s'intègre à la structure de messagerie existante de l'organisation et ne fonctionne pas en tant que système de messagerie autonome. Par exemple, Kaspersky Secure Mail Gateway ne remet pas les messages électroniques aux destinataires et ne gère pas les comptes des utilisateurs.

Pour ce faire, vous pouvez utiliser une des méthodes suivantes :

- Directe.
- Via la passerelle frontière sur laquelle la vérification SMTP des adresses email des destinataires est activée.

  Avant de configurer l'intégration de Kaspersky Secure Mail Gateway via une passerelle frontière, vous devez préciser si la vérification SMTP des adresses email des destinataires est activée sur la passerelle frontière à laquelle Kaspersky Secure Mail Gateway enverra les messages en provenance des domaines internes.

- Via la passerelle frontière sur laquelle la vérification SMTP des adresses email des destinataires est désactivée.

Vous pouvez configurer les paramètres principaux de l'intégration de Kaspersky Secure Mail Gateway à l'infrastructure de messagerie de l'organisation à l'aide de l'Assistant de configuration rapide du MTA ou réaliser manuellement les opérations d'intégration de Kaspersky Secure Mail Gateway à l'infrastructure de messagerie dans l'interface Web.

Après avoir suivi toutes les étapes de l'Assistant **Configuration rapide du MTA**, Kaspersky Secure Mail Gateway élimine toutes les valeurs des paramètres du MTA et les remplace par les valeurs que vous avez définies dans l'Assistant de configuration rapide du MTA.

Dans cette section

Intégration directe

L'*intégration directe* est une forme d'intégration dans le cadre de laquelle Kaspersky Secure Mail Gateway recevra les messages électroniques directement depuis Internet et les redirigera vers les serveurs de messagerie internes. Il acceptera également les messages en provenance des serveurs de messagerie internes et les diffusera sur Internet.

► *Pour configurer l'intégration de Kaspersky Secure Mail Gateway dans l'infrastructure de messagerie de votre organisation, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Configuration rapide du MTA** dans l'arborescence de la console de gestion.

2. Dans le groupe **Intégration de Kaspersky Secure Mail Gateway à l'infrastructure de messagerie**, sélectionnez **Intégration directe**.

3. Cliquez sur le lien **Commencer l'intégration** pour ouvrir l'Assistant.

Dans cette section

Etape 1. Ajout de domaines locaux (relay_domains)

Cette étape permet d'ajouter les domaines locaux de votre organisation pour lesquels Kaspersky Secure Mail Gateway acceptera les messages électroniques depuis l'extérieur. Kaspersky Secure Mail Gateway acceptera les messages uniquement pour les domaines que vous avez renseignés. Les messages destinés à d'autres domaines seront ignorés.

Si aucun domaine local n'est indiqué, Kaspersky Secure Mail Gateway n'acceptera pas les messages pour vos serveurs de messagerie internes.

► *Pour ajouter des domaines locaux de votre organisation, procédez comme suit :*

1. Cliquez sur le lien **Ajouter un domaine** pour ouvrir la fenêtre **Ajout d'un domaine**.
2. Le champ **Saisissez le nom du domaine** accueille le nom du domaine pour lequel Kaspersky Secure Mail Gateway acceptera les messages.

   Saisissez les noms de domaine au format FQDN.
3. Cliquez sur le bouton **OK**.
4. La fenêtre **Ajout d'un domaine** se ferme.

Les noms de domaine sont saisis un à un. Répétez l'opération autant de fois que nécessaire pour ajouter les autres nom de domaine à la liste.

Cliquez sur le lien **Enregistrer et passer à la configuration du routage des emails** pour passer à l'étape suivante de l'Assistant.

Etape 2. Configuration du routage des emails (transport_map)

Cette étape correspond à la configuration du routage des emails.

Kaspersky Secure Mail Gateway utilise par défaut les paramètres de votre serveur DNS pour le routage des emails. Vous pouvez configurer le routage des emails manuellement. Pour cela, il faut créer une table de transport. Saisissez-y les noms des domaines pour lesquels les messages électroniques sont prévus, puis saisissez les adresses IP ou les noms FQDN des domaines vers lesquels Kaspersky Secure Mail Gateway va rediriger les messages destinés à ces domaines.

Exemple :

Si vous voulez que les messages destinés au domaine exemple.com soient redirigés à l'adresse 1.1.1.0:25, vous devez exécuter les actions suivantes :

1. ajouter le domaine exemple.com à la table de transport ;
2. indiquer l'adresse IP 1.1.1.0 et le numéro de port 25 pour le routage des messages destinés au domaine example.com.

► *Pour configurer le routage des emails, procédez comme suit :*

1. Cliquez sur le lien **Ajouter un enregistrement à la table de transport** pour ouvrir la fenêtre **Routage des emails**.
2. Le champ **Saisissez le nom du domaine** accueille le nom du domaine auquel sont destinés les messages électroniques.

   Saisissez les noms de domaine au format FQDN.

3. Saisissez dans le champ **Saisissez l'adresse de destination des messages (IPv4, nom de domaine FQDN)** l'adresse IP ou le nom de domaine du serveur auquel vous souhaitez configurer le routage des emails.

   Vous pouvez saisir une adresse IPv4 (par exemple, 192.0.0.1 ou 192.0.0.0/16), un nom de domaine ou un nom FQDN.

4. Sélectionnez le numéro du port dans le champ **Indiquez le numéro du port de connexion avec l'adresse de destination** .

   Valeur par défaut : 25.

5. Sélectionnez l'une des options suivantes :

   - **Ne pas activer la recherche des enregistrements MX**.
   - **Activer la recherche des enregistrements MX (pour les noms de domaine ou FQDN)**.

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

7. La fenêtre **Routage des emails** se ferme.

> Les enregistrements de la table de transport sont ajoutés un à un. Répétez les opérations d'ajout d'enregistrements à la table de transport autant de fois que cela sera nécessaire.

Cliquez sur le lien **Enregistrer et passer à l'ajout de réseaux de confiance et de noeuds du réseau** pour passer à l'étape suivante de l'assistant.

Etape 3. Ajout de réseaux de confiance et de nœuds du réseau (mynetworks)

Cette étape permet de créer la liste des réseaux de confiance et des nœuds du réseau autorisés à transférer les messages électroniques via Kaspersky Secure Mail Gateway.

En règle générale, il s'agit des réseaux internes et des nœuds de réseau de votre organisation.

Par exemple, vous pouvez indiquer l'adresse IP des serveurs Microsoft Exchange utilisés dans votre entreprise.

Si aucun réseau de confiance n'est renseigné, Kaspersky Secure Mail Gateway n'acceptera pas les messages en provenance des serveurs de messagerie uniques et ne les renverra pas au-delà des limites du réseau de votre organisation.

► *Pour ajouter une liste de réseaux de confiance et de nœud du réseau, procédez comme suit :*

1. Cliquez sur le lien **Ajoutez un réseau de confiance ou un noeud du réseau** pour ouvrir la fenêtre **Ajout d'un réseau de confiance**.

2. Saisissez l'adresse du réseau ou du sous-réseau dans le champ **Saisissez l'adresse de destination des messages (IPv4, nom de domaine FQDN)** .

   Vous pouvez saisir une adresse IPv4 (par exemple, 192.0.0.1 ou 192.0.0.0/16), un nom de domaine ou un nom FQDN. .

3. Cliquez sur le bouton **OK**.

4. La fenêtre **Ajout d'un réseau de confiance** se ferme.

   Les adresses sont ajoutées une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses.

Cliquez sur le lien **Enregistrer et passer à la fin de l'intégration** pour passer à l'étape suivante de l'assistant.

Voir également

Etape 4. Fin de l'intégration directe de Kaspersky Secure Mail Gateway

Cette étape permet de consulter les valeurs des paramètres de l'intégration de Kaspersky Secure Mail Gateway dans l'infrastructure de messagerie de l'organisation et de confirmer celles-ci.

Une fois l'intégration dans l'infrastructure de messagerie de l'entreprise terminée, Kaspersky Secure Mail Gateway est automatiquement configuré avec les paramètres suivants :

- L'Authentification SPF des expéditeurs est activée.
- La vérification SMTP des adresses email des destinataires est activée (à la page 230).

Après avoir suivi toutes les étapes de l'Assistant **Configuration rapide du MTA**, Kaspersky Secure Mail Gateway élimine toutes les valeurs des paramètres du MTA et les remplace par les valeurs que vous avez définies dans l'Assistant de configuration rapide du MTA.

Intégration via la passerelle frontière (vérification SMTP des adresses des destinataires activée)

Intégration via la passerelle frontière sur laquelle la vérification SMTP des adresses email des destinataires est activée est un type d'intégration où Kaspersky Secure Mail Gateway reçoit les

messages depuis la passerelle frontière et les transmet aux serveurs de messagerie internes, mais où il reçoit également les messages des serveurs de messagerie internes qu'il transmet à la passerelle frontière. La vérification SMTP des adresses email des destinataires est activée sur la passerelle frontière.

La vérification SMTP des adresses email des destinataires est utilisée par les systèmes de messagerie pour éviter la réception de messages envoyés à des adresses qui n'existent pas.

► *Pour configurer l'intégration de Kaspersky Secure Mail Gateway à l'infrastructure de messagerie de l'organisation* à l'aide d'une passerelle frontière sur laquelle la vérification SMTP des adresses email des destinataires est activée*, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Configuration rapide du MTA** dans l'arborescence de la console de gestion.
2. Dans le groupe **Intégration de Kaspersky Secure Mail Gateway à l'infrastructure de messagerie**, sélectionnez **Intégration via une passerelle frontière**.
3. Cliquez sur le lien **Commencer l'intégration** pour passer à la section **Vérification SMTP des adresses email des destinataires sur la passerelle frontière**.
4. Sélectionnez **La vérification SMTP des adresses email des destinataires est activée sur la passerelle frontière**.
5. Cliquez sur le lien **Passer à l'ajout de domaines locaux**pour ouvrir l'Assistant.

Dans cette section

Etape 1. Ajout de domaines locaux (relay_domains)

Cette étape permet d'ajouter les domaines locaux de votre organisation pour lesquels Kaspersky Secure Mail Gateway acceptera les messages électroniques depuis l'extérieur. Kaspersky Secure Mail Gateway acceptera les messages uniquement pour les domaines que vous avez renseignés. Les messages destinés à d'autres domaines seront ignorés.

Si aucun domaine local n'est indiqué, Kaspersky Secure Mail Gateway n'acceptera pas les messages pour vos serveurs de messagerie internes.

► *Pour ajouter des domaines locaux de votre organisation, procédez comme suit :*

1. Cliquez sur le lien **Ajouter un domaine** pour ouvrir la fenêtre **Ajout d'un domaine**.
2. Le champ **Saisissez le nom du domaine** accueille le nom du domaine pour lequel Kaspersky Secure Mail Gateway acceptera les messages.

   Saisissez les noms de domaine au format FQDN.
3. Cliquez sur le bouton **OK**.
4. La fenêtre **Ajout d'un domaine** se ferme.

   Les noms de domaine sont saisis un à un. Répétez l'opération autant de fois que nécessaire pour ajouter les autres nom de domaine à la liste.

Cliquez sur le lien **Enregistrer et passer à la configuration du routage des emails** pour passer à l'étape suivante de l'Assistant.

Etape 2. Configuration du routage des emails (transport_map)

Cette étape correspond à la configuration du routage des emails.

Kaspersky Secure Mail Gateway utilise par défaut les paramètres de votre serveur DNS pour le routage des emails. Vous pouvez configurer le routage des emails manuellement. Pour cela, il faut créer une table de transport. Saisissez-y les noms des domaines pour lesquels les messages électroniques sont prévus, puis saisissez les adresses IP ou les noms FQDN des domaines vers lesquels Kaspersky Secure Mail Gateway va rediriger les messages destinés à ces domaines.

Exemple :

Si vous voulez que les messages destinés au domaine exemple.com soient redirigés à l'adresse 1.1.1.0:25, vous devez exécuter les actions suivantes :

1. ajouter le domaine exemple.com à la table de transport ;
2. indiquer l'adresse IP 1.1.1.0 et le numéro de port 25 pour le routage des messages destinés au domaine example.com.

► *Pour configurer le routage des emails, procédez comme suit :*

1. Cliquez sur le lien **Ajouter un enregistrement à la table de transport** pour ouvrir la fenêtre **Routage des emails**.
2. Le champ **Saisissez le nom du domaine** accueille le nom du domaine auquel sont destinés les messages électroniques.

   Saisissez les noms de domaine au format FQDN.
3. Saisissez dans le champ **Saisissez l'adresse de destination des messages (IPv4, nom de domaine FQDN)** l'adresse IP ou le nom de domaine du serveur auquel vous souhaitez configurer le routage des emails.

   Vous pouvez saisir une adresse IPv4 (par exemple, 192.0.0.1 ou 192.0.0.0/16), un nom de domaine ou un nom FQDN.
4. Sélectionnez le numéro du port dans le champ **Indiquez le numéro du port de connexion avec l'adresse de destination** .

   Valeur par défaut : 25.
5. Sélectionnez l'une des options suivantes :

- **Ne pas activer la recherche des enregistrements MX**.
- **Activer la recherche des enregistrements MX (pour les noms de domaine ou FQDN)**.

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

   La fenêtre **Routage des emails** se ferme.

> Les enregistrements de la table de transport sont ajoutés un à un. Répétez les opérations d'ajout d'enregistrements à la table de transport autant de fois que cela sera nécessaire.

Cliquez sur le lien **Enregistrer et passer à la saisie de l'adresse de la passerelle frontière** pour passer à l'étape suivante de l'assistant.

Etape 3. Saisie de l'adresse de la passerelle frontière (relayhost)

Cette étape correspond à la saisie de l'adresse de votre passerelle frontière. Kaspersky Secure Mail Gateway renverra tous les messages à cette adresse.

Par exemple : 192.0.2.1 ou domaine.com.

Si vous avez configuré le routage des emails pour des domaines distincts, Kaspersky Secure Mail Gateway redirigera les messages électroniques vers les adresses indiquées pour chaque domaine.

► *Pour saisir l'adresse de la passerelle frontière, procédez comme suit :*

1. Dans le champ prévu à cet effet, saisissez l'adresse IP ou le nom de domaine de la passerelle frontière.

   Vous pouvez saisir une adresse IPv4 (par exemple, 192.0.0.1 ou 192.0.0.0/16), un nom de domaine ou un nom FQDN.

2. Sélectionnez l'une des options suivantes :

   - **Ne pas activer la recherche des enregistrements MX**.

- **Activer la recherche des enregistrements MX (pour les noms de domaine ou FQDN)**.

Cliquez sur le lien **Enregistrer et passer à l'ajout de réseaux de confiance et de noeuds du réseau** pour passer à l'étape suivante de l'Assistant.

Etape 4. Ajout de réseaux de confiance et de nœuds du réseau (mynetworks)

Cette étape permet de créer la liste des réseaux de confiance et des nœuds du réseau autorisés à transférer les messages électroniques via Kaspersky Secure Mail Gateway.

En règle générale, il s'agit des réseaux internes et des nœuds de réseau de votre organisation.

Par exemple, vous pouvez indiquer l'adresse IP des serveurs Microsoft Exchange utilisés dans votre entreprise.

Si aucun réseau de confiance n'est renseigné, Kaspersky Secure Mail Gateway n'acceptera pas les messages en provenance des serveurs de messagerie uniques et ne les renverra pas au-delà des limites du réseau de votre organisation.

► *Pour ajouter une liste de réseaux de confiance et de nœud du réseau, procédez comme suit :*

1. Cliquez sur le lien **Ajoutez un réseau de confiance ou un noeud du réseau** pour ouvrir la fenêtre **Ajout d'un réseau de confiance**.

2. Le champ **Ajoutez l'adresse du réseau ou du noeud du réseau** accueille le nom du domaine auquel sont destinés les messages électroniques.

   Saisissez les noms de domaine au format FQDN.

3. Cliquez sur le bouton **OK**.

4. La fenêtre **Ajout d'un réseau de confiance** se ferme.

Les adresses sont ajoutées une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses.

Cliquez sur le lien **Enregistrer et passer à la fin de l'intégration** pour passer à l'étape suivante de l'assistant.

Etape 5. Fin de l'intégration via la passerelle frontière (vérification SMTP activée)

Cette étape permet de consulter les valeurs des paramètres de l'intégration de Kaspersky Secure Mail Gateway dans l'infrastructure de messagerie de l'organisation et de confirmer celles-ci.

Une fois l'intégration dans l'infrastructure de messagerie de l'entreprise terminée, Kaspersky Secure Mail Gateway est automatiquement configuré avec les paramètres suivants :

- L'Authentification SPF des expéditeurs est désactivée.

  N'activez pas l'authentification SPF des expéditeurs de messages : c'est la passerelle frontière qui expédie les messages que reçoit Kaspersky Secure Mail Gateway.

- L'Authentification DMARC des domaines à partir desquels Kaspersky Secure Mail Gateway reçoit des messages est désactivée (cf. section "Activation et désactivation de l'authentification DMARC des expéditeurs" à la page 252).

  N'activez pas l'authentification DMARC des domaines, car Kaspersky Secure Mail Gateway reçoit les messages de la passerelle intermédiaire.

- La vérification SMTP des adresses email des destinataires est activée (à la page 230).

  Ne désactivez pas la vérification SMTP des adresses email des destinataires car cette vérification est activée sur la passerelle frontière.

Après avoir suivi toutes les étapes de l'Assistant **Configuration rapide du MTA**, Kaspersky Secure Mail Gateway élimine toutes les valeurs des paramètres du MTA et les remplace par les valeurs que vous avez définies dans l'Assistant de configuration rapide du MTA.

Intégration via la passerelle frontière (vérification SMTP des adresses des destinataires désactivée)

Intégration via la passerelle frontière sur laquelle la vérification SMTP des adresses email des destinataires est désactivée est un type d'intégration où Kaspersky Secure Mail Gateway reçoit les messages depuis la passerelle frontière et les transmet aux serveurs de messagerie internes, mais où il reçoit également les messages des serveurs de messagerie internes qu'il transmet à la passerelle frontière. La vérification SMTP des adresses email des destinataires est désactivée sur la passerelle frontière.

La vérification SMTP des adresses email des destinataires est utilisée par les systèmes de messagerie pour éviter la réception de messages envoyés à des adresses qui n'existent pas.

► *Pour configurer l'intégration de Kaspersky Secure Mail Gateway à l'infrastructure de messagerie de l'organisation* à l'aide d'une passerelle frontière sur laquelle la vérification SMTP des adresses email des destinataires est désactivée*, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Configuration rapide du MTA** dans l'arborescence de la console de gestion.
2. Dans le groupe **Intégration de Kaspersky Secure Mail Gateway à l'infrastructure de messagerie**, sélectionnez **Intégration via une passerelle frontière**.
3. Cliquez sur le lien **Commencer l'intégration** pour passer à la section **Vérification SMTP des adresses email des destinataires sur la passerelle frontière**.
4. Sélectionnez **La vérification SMTP des adresses email des destinataires est désactivée sur la passerelle frontière**.
5. Cliquez sur le lien **Passer à la configuration du routage des emails** pour ouvrir l'Assistant.

Dans cette section

Etape 1. Configuration du routage des emails (transport_map)

Cette étape correspond à la configuration du routage des emails.

Kaspersky Secure Mail Gateway utilise par défaut les paramètres de votre serveur DNS pour le routage des emails. Vous pouvez configurer le routage des emails manuellement. Pour cela, il faut créer une table de transport. Saisissez-y les noms des domaines pour lesquels les messages électroniques sont prévus, puis saisissez les adresses IP ou les noms FQDN des domaines vers lesquels Kaspersky Secure Mail Gateway va rediriger les messages destinés à ces domaines.

Exemple :

Si vous voulez que les messages destinés au domaine exemple.com soient redirigés à l'adresse 1.1.1.0:25, vous devez exécuter les actions suivantes :

1. ajouter le domaine exemple.com à la table de transport ;
2. indiquer l'adresse IP 1.1.1.0 et le numéro de port 25 pour le routage des messages destinés au domaine example.com.

► *Pour configurer le routage des emails, procédez comme suit :*

1. Cliquez sur le lien **Ajouter un enregistrement à la table de transport** pour ouvrir la fenêtre **Routage des emails**.

2. Le champ **Saisissez le nom du domaine** accueille le nom du domaine auquel sont destinés les messages électroniques.

   Saisissez les noms de domaine au format FQDN.

3. Saisissez dans le champ **Saisissez l'adresse de destination des messages (IPv4, nom de domaine FQDN)** l'adresse IP ou le nom de domaine du serveur auquel vous souhaitez configurer le routage des emails.

   Vous pouvez saisir une adresse IPv4 (par exemple, 192.0.0.1 ou 192.0.0.0/16), un nom de domaine ou un nom FQDN.

4. Sélectionnez le numéro du port dans le champ **Indiquez le numéro du port de connexion avec l'adresse de destination** .

   Valeur par défaut : 25.

5. Sélectionnez l'une des options suivantes :

   - **Ne pas activer la recherche des enregistrements MX**.
   - **Activer la recherche des enregistrements MX (pour les noms de domaine ou FQDN)**.

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

   La fenêtre **Routage des emails** se ferme.

> Les enregistrements de la table de transport sont ajoutés un à un. Répétez les opérations d'ajout d'enregistrements à la table de transport autant de fois que cela sera nécessaire.

Cliquez sur le lien **Enregistrer et passer à la saisie de l'adresse de la passerelle frontière** pour passer à l'étape suivante de l'assistant.

Etape 2. Saisie de l'adresse de la passerelle frontière (relayhost)

Cette étape correspond à la saisie de l'adresse de votre passerelle frontière. Kaspersky Secure Mail Gateway renverra tous les messages à cette adresse.

Par exemple : 192.0.2.1 ou domaine.com.

Si vous avez configuré le routage des emails pour des domaines distincts, Kaspersky Secure Mail Gateway redirigera les messages électroniques vers les adresses indiquées pour chaque domaine.

► *Pour saisir l'adresse de la passerelle frontière, procédez comme suit :*

1. Dans le champ prévu à cet effet, saisissez l'adresse IP ou le nom de domaine de la passerelle frontière.

   Vous pouvez saisir une adresse IPv4 (par exemple, 192.0.0.1 ou 192.0.0.0/16), un nom de domaine ou un nom FQDN.

2. Sélectionnez l'une des options suivantes :

   - **Ne pas activer la recherche des enregistrements MX**.
   - **Activer la recherche des enregistrements MX (pour les noms de domaine ou FQDN)**.

Cliquez sur le lien **Enregistrer et passer à l'ajout de réseaux de confiance et de noeuds du réseau** pour passer à l'étape suivante de l'Assistant.

Etape 3. Ajout de réseaux de confiance et de nœuds du réseau (mynetworks)

Cette étape permet de créer la liste des réseaux de confiance et des nœuds du réseau autorisés à transférer les messages électroniques via Kaspersky Secure Mail Gateway.

En règle générale, il s'agit des réseaux internes et des nœuds de réseau de votre organisation.

Par exemple, vous pouvez indiquer l'adresse IP des serveurs Microsoft Exchange utilisés dans votre entreprise.

Si aucun réseau de confiance n'est renseigné, Kaspersky Secure Mail Gateway n'acceptera pas les messages en provenance des serveurs de messagerie uniques et ne les renverra pas au-delà des limites du réseau de votre organisation.

► *Pour ajouter une liste de réseaux de confiance et de nœud du réseau, procédez comme suit :*

1. Cliquez sur le lien **Ajoutez un réseau de confiance ou un noeud du réseau** pour ouvrir la fenêtre **Ajout d'un réseau de confiance**.

2. Le champ **Ajoutez l'adresse du réseau ou du noeud du réseau** accueille le nom du domaine auquel sont destinés les messages électroniques.

   Saisissez les noms de domaine au format FQDN.

3. Cliquez sur le bouton **OK**.

   La fenêtre **Ajout d'un réseau de confiance** se ferme.

   Les adresses sont ajoutées une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses.

Cliquez sur le lien **Enregistrer et passer à la fin de l'intégration** pour passer à l'étape suivante de l'assistant.

Etape 4. Fin de l'intégration via la passerelle frontière (vérification SMTP désactivée)

Cette étape permet de consulter les valeurs des paramètres de l'intégration de Kaspersky Secure Mail Gateway dans l'infrastructure de messagerie de l'organisation et de confirmer celles-ci.

Une fois l'intégration dans l'infrastructure de messagerie de l'entreprise terminée, Kaspersky Secure Mail Gateway est automatiquement configuré avec les paramètres suivants :

- L'Authentification SPF des expéditeurs est désactivée.

N'activez pas l'authentification SPF des expéditeurs de messages : c'est la passerelle frontière qui expédie les messages que reçoit Kaspersky Secure Mail Gateway.

- L'Authentification DMARC des domaines à partir desquels Kaspersky Secure Mail Gateway reçoit des messages est désactivée (cf. section "Activation et désactivation de l'authentification DMARC des expéditeurs" à la page 252).

N'activez pas l'authentification DMARC des domaines, car Kaspersky Secure Mail Gateway reçoit les messages de la passerelle intermédiaire.

- La vérification SMTP des adresses email des destinataires est désactivée (à la page 230).

N'activez pas la vérification SMTP des adresses email des destinataires car cette vérification est désactivée sur la passerelle frontière.

Après avoir suivi toutes les étapes de l'Assistant **Configuration rapide du MTA**, Kaspersky Secure Mail Gateway élimine toutes les valeurs des paramètres du MTA et les remplace par les valeurs que vous avez définies dans l'Assistant de configuration rapide du MTA.

Surveillance de Kaspersky Secure Mail Gateway

Cette section contient des informations sur la surveillance du trafic de messagerie, des dernières menaces détectées et des ressources système.

Dans cette section

Surveillance du trafic de la messagerie

Pour évaluer l'état du trafic de la messagerie dans Kaspersky Secure Mail Gateway, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Surveillance** dans l'arborescence de la console de gestion.
2. Sélectionnez l'onglet **Trafic de la messagerie** de l'espace de travail.
3. Sélectionnez une des périodes d'affichage des informations sur le trafic.

   Vous pouvez consulter les informations relatives au trafic de la messagerie pour les périodes suivantes : **heure**, **jour**, **semaine** ou **30 jours**.
4. Sélectionnez un mode d'affichage graphique des informations.

Vous pouvez consulter les diagrammes des messages détectés **par nombre** ou **par volume**.

5. Notez les états de messages (par exemple, **Propres**, **Menaces**, **Courriers indésirables** ou tous les messages), pour lesquels vous souhaitez consulter les informations.

L'espace de travail affiche les diagrammes du trafic de la messagerie pour la période sélectionnée.

Surveillance des dernières menaces détectées

Pour consulter la liste des dernières menaces détectées, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Surveillance** dans l'arborescence de la console de gestion.

2. Sélectionnez l'onglet **Dernières menaces détectées** de l'espace de travail.

La liste **Derniers objets infectés détectés** s'affiche. Elle reprend les 5 derniers objets détectés.

Surveillance de l'utilisation des ressources système

► *Pour évaluer l'état de l'utilisation des ressources système, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Surveillance** dans l'arborescence de la console de gestion.

2. Sélectionnez l'onglet **Ressources système** de l'espace de travail.

3. Cochez les types de données que vous souhaitez voir apparaître dans le diagramme de charge du système (vous pouvez choisir **Processeur**, **RAM**, **Fichier d'échange** ou toutes les options).

4. Cochez les types de données que vous souhaitez voir apparaître dans le diagramme de charge des interfaces réseau (vous pouvez choisir **Transmission**, **Réception** ou toutes les options).

L'espace de travail affiche les diagrammes **Système** et **Interfaces réseau** contenant les données sélectionnées.

Surveillance de l'état des services et du fonctionnement de l'agent de messagerie MTA

La section **Surveillance** de la fenêtre principale de l'interface Internet de Kaspersky Secure Mail Gateway dans la partie droite de l'espace de travail affiche les informations suivantes :

- État de fonctionnement du module Anti-spam, actualité des bases du module Anti-spam, nombre de messages dans la quarantaine de l'Anti-spam ;
- État de fonctionnement du module Antivirus, actualité des bases du module Antivirus ;
- État de la connexion avec le serveur avec le composant KATA, nombre de messages dans la quarantaine KATA (si vous utilisez l'application Kaspersky Anti Targeted Attack Platform) ;
- État du fonctionnement du module Anti-phishing, actualité des bases du module Anti-phishing ;
- État de la connexion au Kaspersky Security Network ou Kaspersky Private Security Network (si vous utilisez la solution Kaspersky Private Security Network) ;
- Informations sur la dernière mise à jour des bases de données de l'application ;
- État de la connexion aux serveurs LDAP ;
- Durée de validité de la licence et avertissement sur l'expiration prochaine de la licence, si c'est le cas ;
- Informations sur l'état de l'envoi et de la réception de messages par l'agent de messagerie MTA.

Si vous avez activé l'application, les modules Anti-Spam, Anti-Virus et Anti-Phishing sont activés par défaut. L'envoi et la réception de messages sont activés pour l'agent de messagerie MTA.

Voir également

Surveillance de Kaspersky Secure Mail Gateway..... 124

Application des règles de traitement des messages

La *règle de traitement des messages* (ci-après, la "règle") est une sélection de paires d'adresses d'expéditeur et de destinataire dont les messages électroniques sont traités par Kaspersky Secure Mail Gateway selon des paramètres de même valeur. L'appartenance d'un message électronique à une règle est définie par la présence dans celle-ci de l'adresse de l'expéditeur et de l'adresse du destinataire.

Par défaut, l'application prévoit les règles prédéfinies suivantes pour le traitement des messages :

- **WhiteList** : traitement des messages depuis la liste blanche globale des adresses ;
- **BlackList** : traitement des messages depuis la liste noire globale des adresses ;
- **Default** : traitement des messages selon les paramètres prédéfinis par Kaspersky Lab.

Dans le cadre du traitement du message électronique, Kaspersky Secure Mail Gateway examine la combinaison d'adresses *expéditeur-destinataire* de chaque règle, en commençant par la règle qui affiche la priorité la plus importante (1). Si aucune équivalence n'est détectée, Kaspersky Secure Mail Gateway vérifie la combinaison d'adresses de la règle suivante par ordre de priorité (2). Dès qu'une combinaison d'adresses expéditeur-destinataire a été trouvée dans une règle quelconque, le message est traité conformément aux paramètres de traitement définis dans la règle.

Si aucune règle ne contient la combinaison expéditeur-destinataire, le message est traité selon les paramètres définis pour la règle prédéfinie **Default**.

Vous pouvez définir des paramètres personnalisés de traitement des messages électroniques pour chacune des règles.

Dans cette section

Création d'une règle de traitement de messages

► *Pour créer une règle de traitement de messages, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.
2. Cliquez sur le bouton **Créer** situé dans la partie supérieure de l'espace de travail.

   Une nouvelle règle de traitement des messages s'ouvre.
3. Sélectionnez le groupe **Paramètres généraux des règles**.
4. Saisissez dans le champ **Nom de la règle (obligatoire)** le nom de la nouvelle règle.

   Le nom de la règle doit être unique dans la liste des règles de Kaspersky Secure Mail Gateway.
5. Saisissez une description dans le champ **Description de la règle** .
6. Dans le groupe de paramètres **Mode de fonctionnement de la règle** , sélectionnez l'une des options de traitement suivantes :

   - **Utiliser les paramètres des modules d'analyse** pour que le traitement des messages correspondant à la règle s'effectue selon les paramètres des modules Anti-Virus,

Anti-Spam et Anti-Phishing et selon les paramètres du filtrage de contenu qui sont définis pour cette règle.

Dans la partie inférieure de l'espace de travail apparaissent les groupes de paramètres suivants (s'ils étaient masqués), qui vous permettent de configurer les paramètres de Kaspersky Secure Mail Gateway pour cette règle :

- **Anti-spam** (cf. section "**Activation et désactivation de l'analyse antispam des messages pour une règle**" à la page 287).
- **Antivirus** (cf. section "**Activation et désactivation de la recherche de virus pour une règle**" à la page. 272).
- **Protection KATA** (cf. section "**Activation et désactivation de la protection KATA pour une règle**" à la page 334).
- **Anti-phishing** (cf. section "**Activation et désactivation de l'analyse anti-phishing pour une règle**" à la page 306).
- **Filtrage de contenu** (cf. section "**Activation et désactivation du filtrage du contenu des messages pour une règle**" à la page 316).
- **Notifications** (cf. section "**Configuration des notifications sur les événements d'analyse des messages pour une règle**" à la page 367).
- **Avertissement concernant un message** (cf. section "**Ajout d'une remarque aux événements d'analyse des messages pour une règle**" à la page 376).
- **Avertissement concernant un message dangereux** (cf. section "**Ajout d'un avertissement concernant un message dangereux pour une règle**" à la page 377).
- **Authentification des expéditeurs de messages** (cf. section "**Activation et désactivation de l'authentification des expéditeurs pour une règle**" à la page 253).

- **Rejeter sans analyse** si vous voulez que l'application refuse les messages sans les analyser lors du traitement des messages correspondant à cette règle.

- **Supprimer sans prévenir l'expéditeur** si vous voulez que l'application supprimer les messages sans prévenir l'utilisateur lors du traitement des messages conformément à cette règle.

- **Ignorer sans analyse** si vous voulez que l'application livre les messages à leurs destinataires sans les analyser lors du traitement des messages conformément à cette règle.

  Dans la partie inférieure de l'espace de travail s'affiche le groupe **Avertissement concernant un message** (cf. section "**Ajout d'une remarque aux événements d'analyse des messages pour une règle**" à la page 376) dans lequel vous pouvez configurer les remarques concernant les messages traités conformément à cette règle.

7. Cliquez sur le bouton **Créer** situé dans la partie inférieure de l'espace de travail.

La règle sera créée et ajoutée à la liste des règles dans le groupe **Règles**.

Pour que la règle soit utilisée par Kaspersky Secure Mail Gateway, vous devez configurer la liste des expéditeurs de messages (cf. section "Ajout d'adresses électroniques" à la page 133) et la liste des destinataires des messages pour cette règle.

Vous pouvez créer aussi une règle en copiant une règle existante et en modifiant ses paramètres (cf. section "Création d'une copie d'une règle de traitement des messages" à la page 131).

Par défaut, la règle disposera d'une priorité inférieure à celle des règles créées auparavant. Vous pouvez modifier la priorité d'une règle.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145). La nouvelle règle est désactivée par défaut et n'intervient pas dans le fonctionnement de l'application.

Création d'une copie d'une règle de traitement des messages

► *Pour créer une copie d'une règle de traitement des messages, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Cochez la case en regard au nom de la règle à copier.
3. Cliquez sur le bouton **Copier** situé dans la partie supérieure de l'espace de travail.
4. Dans le groupe **Paramètres généraux des règles**, modifiez le nom de la règle dans le champ **Nom de la règle (obligatoire)** .

   Le nom de la règle doit être unique dans la liste des règles de Kaspersky Secure Mail Gateway.
5. Cliquez sur le bouton **Créer** situé dans la partie inférieure de l'espace de travail.

Une copie de la règle sera créée et ajoutée à la liste des règles dans le groupe **Règles**.

Vous pouvez modifier la description, les paramètres de la règle et les paramètres de Kaspersky Secure Mail Gateway pour cette règle (cf. section "Création d'une règle de traitement des messages" à la page 129).

Par défaut, la règle disposera d'une priorité inférieure à celle des règles créées auparavant.. Vous pouvez modifier la priorité d'une règle.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145). La nouvelle règle est désactivée par défaut et n'intervient pas dans le fonctionnement de l'application.

Configuration des listes d'expéditeurs et de destinataires des messages pour une règle

Pour que la règle soit appliquée lors de l'utilisation de Kaspersky Secure Mail Gateway, vous devez configurer les listes des expéditeurs et des destinataires de messages pour cette règle.

Pour configurer la liste des expéditeurs et des destinataires de messages, procédez comme suit :

- Créer des listes d'expéditeurs et de destinataires. Vous pouvez ajouter à la liste des adresses IP d'expéditeurs de messages, des adresses électroniques et des comptes utilisateurs LDAP d'expéditeurs et de destinataires de messages.
- Copier les adresses des listes d'expéditeurs et de destinataires vers le presse-papiers et coller les adresses du presse-papiers dans les listes d'expéditeurs et de destinataires des messages.
- Supprimer des adresses des listes d'expéditeurs et de destinataires. Vous pouvez supprimer des adresses des listes, nettoyer les listes d'expéditeurs et de destinataires, ainsi que supprimer des comptes utilisateurs LDAP (cf. Section "Ajout de comptes utilisateurs LDAP" à la page 136) des listes **Liste des comptes LDAP d'expéditeurs** et **Liste des comptes LDAP de destinataires** à l'étape intermédiaire de configuration des listes des expéditeurs et des destinataires des messages.

Dans cette section

Ajout d'adresses électroniques

► *Pour ajouter des adresses électroniques à la liste des expéditeurs et des destinataires de messages, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des noms de règles, cliquez sur la règle pour laquelle vous souhaitez modifier les listes d'expéditeurs et de destinataires de messages.

3. Sélectionnez le groupe **Paramètres généraux des règles**.

4. Sélectionnez la liste à laquelle vous souhaitez ajouter des adresses électroniques :

   - **Expéditeurs** pour ajouter des adresses électroniques à la liste des expéditeurs de messages.
   - **Destinataires** pour ajouter des adresses électroniques à la liste des destinataires de messages.

5. Cliquez sur l'icône correspondant au type d'adresse (expéditeur ou destinataire) sous le nom de la liste et sélectionnez **Adresses emails** dans le menu contextuel.

6. Dans le champ à droite de l'icône **Adresses emails**, saisissez l'adresse désirée.

   Les adresses électroniques sont saisies une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses électroniques.

   Vous pouvez utiliser les caractères "*" et "?" pour créer des masques d'adresses ainsi que des expressions régulières en utilisant le préfixe "re:".

   Les expressions régulières ne respectent pas la casse.

7. Cliquez sur le bouton **Ajouter** situé à droite du champ.

   L'adresse email ajoutée apparaît dans la liste que vous avez sélectionnée avec l'icône **Adresses emails**.

8. Pour annuler la dernière opération, cliquez sur le lien **Annuler la dernière opération** situé sous la liste désirée.

9. Lorsque vous avez ajouté à la liste toutes les adresses électroniques souhaitées, cliquez sur le bouton **Appliquer** dans la partie inférieure de l'espace de travail.

Les modifications des listes d'expéditeurs et de destinataires des messages sont enregistrées dans la règle de traitement des messages que vous êtes en train de configurer.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Ajout d'adresses IP

Vous pouvez ajouter des adresses IP uniquement à la liste des expéditeurs de messages. L'ajout d'adresses IP à la liste des destinataires de message n'est pas prise en charge.

► *Pour ajouter des adresses IP à une liste d'expéditeurs de messages, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.
2. Dans la liste des noms de règles, cliquez sur la règle pour laquelle vous souhaitez modifier les listes d'expéditeurs et de destinataires de messages.
3. Sélectionnez le groupe **Paramètres généraux des règles**.
4. Dans le groupe **Expéditeurs**, cliquez sur l'icône correspondant au type d'adresse d'expéditeur, puis choisissez l'option **Adresses IP** dans le menu contextuel du bouton.
5. Dans le champ à droite de l'icône **Adresses IP**, saisissez l'adresse IP d'un expéditeur de messages.

   Les adresses IP sont ajoutées une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses IP.

   Vous pouvez saisir des adresses IPv4 (par exemple, 192.0.0.1 ou 192.0.0.0/16) et IPv6 (par exemple, 2607:f0d0:1002:51::4) ou des masques de sous-réseau en notation CIDR (par exemple, fc00::/7).
6. Cliquez sur le bouton **Ajouter** situé à droite du champ.

L'adresse IP ajoutée apparaît dans la liste des expéditeurs de messages, avec l'icône **Adresses IP**.

7. Pour annuler la dernière opération, cliquez sur le lien **Annuler la dernière opération** situé sous la liste des expéditeurs de messages.

8. Lorsque vous avez ajouté à la liste toutes les adresses IP souhaitées, cliquez sur le bouton **Appliquer** dans la partie inférieure de l'espace de travail.

Les modifications des listes d'expéditeurs et de destinataires des messages sont enregistrées dans la règle de traitement des messages que vous êtes en train de configurer.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Ajout de comptes utilisateurs LDAP

► *Pour ajouter des comptes utilisateurs LDAP à la liste des expéditeurs et des destinataires de messages, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des noms de règles, cliquez sur la règle pour laquelle vous souhaitez modifier les listes d'expéditeurs et de destinataires de messages.

3. Sélectionnez le groupe **Paramètres généraux des règles**.

4. Sélectionnez la liste à laquelle vous souhaitez ajouter des comptes utilisateurs LDAP :

   - **Expéditeurs** pour ajouter des comptes utilisateurs LDAP à la liste des expéditeurs de messages.

   - **Destinataires** pour ajouter des comptes utilisateurs LDAP à la liste des destinataires de messages.

5. Cliquez sur l'icône correspondant au type d'adresse (expéditeur ou destinataire) sous le nom de la liste et sélectionnez **Comptes LDAP** dans le menu contextuel.

6. Cliquez sur le bouton **Rechercher** situé à droite du champ.

   La fenêtre qui s'ouvre dépend de la liste à laquelle vous ajoutez des comptes utilisateurs LDAP :

   - **Configuration de la liste des expéditeurs pour la règle ** si vous ajoutez des comptes utilisateurs LDAP à la liste des expéditeurs de messages ;
   - **Configuration de la liste des destinataires pour la règle ** si vous ajoutez des comptes utilisateurs LDAP à la liste des destinataires de messages.

7. Dans la fenêtre qui s'ouvre, saisissez dans le champ **Compte LDAP de l'expéditeur** ou **Compte LDAP du destinataire** la chaîne de recherche des comptes utilisateurs dans le service d'annuaire externe.

8. Cliquez sur le bouton **Rechercher** situé à droite du champ.

   La liste des comptes utilisateurs trouvés s'affiche dans le champ situé sous le bouton **Rechercher**.

9. Sélectionnez les comptes utilisateurs LDAP à ajouter à la liste des expéditeurs ou des destinataires de messages.

   Vous pouvez sélectionner plusieurs comptes LDAP.

10. Cliquez sur le bouton **Ajouter à la liste** sous la liste.

    Les comptes utilisateurs sélectionnés apparaissent dans la liste :

    - **Liste des comptes LDAP d'expéditeurs** si vous ajoutez des comptes utilisateurs LDAP à la liste des expéditeurs de messages ;
    - **Liste des comptes LDAP de destinataires** si vous ajoutez des comptes utilisateurs LDAP à la liste des destinataires de messages.

11. Cliquez sur le bouton **OK**, dans la partie inférieure de la fenêtre :

    - **Configuration de la liste des expéditeurs pour la règle ** si vous ajoutez des comptes utilisateurs LDAP à la liste des expéditeurs de messages ;

- **Configuration de la liste des destinataires pour la règle ** si vous ajoutez des comptes utilisateurs LDAP à la liste des destinataires de messages.

La fenêtre sur laquelle vous avez ajouté des comptes utilisateurs LDAP se referme.

Les comptes utilisateurs LDAP que vous avez ajoutés apparaissent dans la liste des adresses avec l'icône **Comptes LDAP**.

12. Pour annuler la dernière opération, cliquez sur le lien **Annuler la dernière opération** situé sous la liste des adresses.

13. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Les modifications des listes d'expéditeurs et de destinataires des messages sont enregistrées dans la règle de traitement des messages que vous êtes en train de configurer.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Suppression de comptes utilisateurs LDAP des listes de comptes utilisateurs LDAP

Vous pouvez supprimer des comptes utilisateurs LDAP des listes d'expéditeurs et de destinataires de messages (cf. section "Suppression d'adresses" à la page 143) dans les règles de traitement des messages, mais aussi des listes de comptes utilisateurs LDAP dans les fenêtres **Configuration de la liste des expéditeurs pour la règle ** et **Configuration de la liste des destinataires pour la règle ** lors du processus de configuration des listes d'expéditeurs et de destinataires des messages pour une règle.

► *Pour supprimer des comptes utilisateurs LDAP des listes de comptes utilisateurs LDAP, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des noms de règles, cliquez sur la règle pour laquelle vous souhaitez modifier les listes d'expéditeurs et de destinataires de messages.

3. Sélectionnez le groupe **Paramètres généraux des règles**.
4. Sélectionnez la liste dont vous souhaitez modifier les comptes utilisateurs LDAP :
   - **Expéditeurs** pour modifier les comptes utilisateurs LDAP des expéditeurs de messages.
   - **Destinataires** pour modifier les comptes utilisateurs LDAP des destinataires de messages.
5. Cliquez sur l'icône correspondant au type d'adresse (expéditeur ou destinataire) sous le nom de la liste et sélectionnez **Comptes LDAP** dans le menu contextuel.
6. Cliquez sur le bouton **Rechercher** situé à droite du champ.

   La fenêtre qui s'ouvre dépend de la liste dont vous souhaitez modifier les comptes utilisateurs LDAP :

   - **Configuration de la liste des expéditeurs pour la règle** si vous exécutez des actions sur les comptes utilisateurs LDAP dans la liste des expéditeurs de messages.
   - **Configuration de la liste des destinataires pour la règle** si vous exécutez des actions sur les comptes utilisateurs LDAP dans la liste des destinataires de messages.
7. Sélectionnez dans la partie inférieure de la fenêtre les comptes utilisateurs LDAP à supprimer :
   - **Liste des comptes LDAP d'expéditeurs** si vous supprimez des comptes utilisateurs LDAP de la liste des expéditeurs de messages.
   - **Liste des comptes LDAP de destinataires** si vous supprimez des comptes utilisateurs LDAP de la liste des destinataires de messages.

   Vous pouvez sélectionner plusieurs comptes LDAP.
8. Cliquez sur le bouton **Supprimer de la liste** sous la liste.

   Les comptes utilisateurs sélectionnés sont supprimés de vos listes.
9. Cliquez sur le bouton **OK**, dans la partie inférieure de la fenêtre :

- **Configuration de la liste des expéditeurs pour la règle** si vous supprimez des comptes utilisateurs LDAP de la liste des expéditeurs de messages.
- **Configuration de la liste des destinataires pour la règle** si vous supprimez des comptes utilisateurs LDAP de la liste des destinataires de messages.

La fenêtre sur laquelle vous avez supprimé des comptes utilisateurs LDAP se referme.

Les comptes utilisateurs LDAP supprimés sont également supprimés de la liste des adresses d'expéditeurs et de destinataires des messages de votre règle.

10. Pour annuler la dernière opération, cliquez sur le lien **Annuler la dernière opération** situé sous la liste des adresses.
11. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Les modifications de la liste des expéditeurs et des destinataires de messages sont enregistrées dans la règle de traitement des messages que vous êtes en train de configurer.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Copie et insertion d'adresses

► *Pour copier les adresses d'une liste d'expéditeurs et de destinataires dans une règle de traitement de messages, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.
2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle dont vous souhaitez utiliser les listes d'expéditeurs ou de destinataires de messages.
3. Sélectionnez le groupe **Paramètres généraux des règles**.
4. Sélectionnez la liste dont vous souhaitez copier les adresses dans le presse-papiers :
   - **Expéditeurs** pour copier les adresses de la liste des expéditeurs de messages.

- **Destinataires** pour copier les adresses de la liste des destinataires de messages.

5. Cliquez sur le lien **Exporter** sous la liste sélectionnée pour ouvrir la fenêtre **Exportation des enregistrements dans le presse-papiers**.

6. Dans la liste **Sélectionnez le type**, sélectionnez le type des adresses à copier :

   - **Adresses emails** pour copier des adresses électroniques.

   - **Adresses IP** pour copier des adresses IP (liste d'expéditeurs de messages uniquement).

   - **Comptes LDAP**, pour copier des comptes utilisateurs LDAP.

   La liste des adresses correspondant au type sélectionné s'affiche sous la liste des types d'adresses.

7. Sélectionnez les adresses à copier.

8. Copiez-les dans le presse-papiers.

9. Dans la partie inférieure de la fenêtre **Exportation des enregistrements dans le presse-papiers**, cliquez sur le bouton **Annuler**.

   La fenêtre **Exportation des enregistrements dans le presse-papiers** se ferme.

► *Pour coller les adresses du presse-papiers dans la liste d'expéditeurs ou de destinataires d'une règle de traitement des messages, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des noms de règles, cliquez sur la règle pour laquelle vous souhaitez modifier les listes d'expéditeurs et de destinataires de messages.

3. Sélectionnez le groupe **Paramètres généraux des règles**.

4. Sélectionnez la liste à laquelle vous souhaitez ajouter les adresses du presse-papiers :

   - **Expéditeurs** pour coller les adresses du presse-papiers dans la liste des expéditeurs de messages.

- **Destinataires** pour coller les adresses du presse-papiers dans la liste des destinataires de messages.

5. Cliquez sur le lien **Importer** sous la liste sélectionnée pour ouvrir la fenêtre **Importation des enregistrements depuis le presse-papiers**.

6. Dans la liste **Sélectionnez le type**, sélectionnez le type des adresses qui seront collées à partir du presse-papiers :

   - **Adresses emails** pour coller des adresses électroniques.
   - **Adresses IP** pour coller des adresses IP (liste d'expéditeurs de messages uniquement).
   - **Comptes LDAP** pour coller des comptes utilisateurs LDAP.

7. Collez les adresses provenant du presse-papiers dans le champ situé sous la liste des types d'adresses.

8. Dans la partie inférieure de la fenêtre **Exportation des enregistrements dans le presse-papiers**, cliquez sur le bouton **Importer**.

   La fenêtre **Importation des enregistrements depuis le presse-papiers** se ferme.

   Les adresses que vous avez ajoutées apparaissent dans la liste des expéditeurs ou des destinataires de messages avec l'icône correspondant à leur type d'adresse.

9. Pour annuler la dernière opération, cliquez sur le lien **Annuler la dernière opération** situé sous la liste des expéditeurs ou des destinataires de messages.

10. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Les modifications des listes d'expéditeurs et de destinataires des messages sont enregistrées dans la règle de traitement des messages que vous êtes en train de configurer.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Suppression d'adresses

Vous pouvez supprimer des adresses de vos listes d'expéditeurs et de destinataires, mais aussi effacer les listes d'expéditeurs et de destinataires d'une règle de traitement des messages.

► *Pour supprimer les adresses d'une liste d'expéditeurs ou de destinataires, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.
2. Dans la liste des noms de règles, cliquez sur la règle pour laquelle vous souhaitez modifier les listes d'expéditeurs et de destinataires de messages.
3. Sélectionnez le groupe **Paramètres généraux des règles**.
4. Sélectionnez la liste contenant les adresses à supprimer :
   - **Expéditeurs** pour supprimer des adresses de la liste des expéditeurs de messages.
   - **Destinataires** pour supprimer des adresses de la liste des destinataires de messages.
5. Sélectionnez l'adresse à supprimer de la liste.
6. Cliquez sur l'icône de suppression à droite de l'adresse à supprimer.

   L'adresse est supprimée de la liste des expéditeurs ou des destinataires de messages.
7. Pour annuler la dernière opération, cliquez sur le lien **Annuler la dernière opération** situé sous la liste des expéditeurs ou des destinataires de messages.
8. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Les modifications des listes d'expéditeurs et de destinataires des messages sont enregistrées dans la règle de traitement des messages que vous êtes en train de configurer.

► *Pour effacer une liste d'expéditeurs ou de destinataires de messages, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des noms de règles, cliquez sur la règle pour laquelle vous souhaitez modifier les listes d'expéditeurs et de destinataires de messages.
3. Sélectionnez le groupe **Paramètres généraux des règles**.
4. Sélectionnez la liste dont vous souhaitez supprimer toutes les adresses :
   - **Expéditeurs** pour effacer la liste des expéditeurs de messages.
   - **Destinataires** pour effacer la liste des destinataires de messages.
5. Cliquez sur le lien situé sous la liste choisie pour ouvrir la fenêtre de confirmation de l'opération :
   - **Purger la liste des expéditeurs** pour effacer la liste des expéditeurs de messages.
   - **Purger la liste des destinataires** pour effacer la liste des destinataires de messages.
6. Cliquez sur le bouton **Oui**.

   La fenêtre de confirmation de l'opération se ferme.

   Toutes les adresses sont supprimées de la liste des expéditeurs ou des destinataires de messages.
7. Pour annuler la dernière opération, cliquez sur le lien **Annuler la dernière opération** situé sous la liste des expéditeurs ou des destinataires de messages.
8. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Les modifications des listes d'expéditeurs et de destinataires des messages sont enregistrées dans la règle de traitement des messages que vous êtes en train de configurer.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Suppression des règles de traitement des messages

► *Pour supprimer une règle de traitement des messages, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.
2. Cochez la case en regard du nom de la ou des règles à supprimer.
3. Cliquez sur le bouton **Supprimer** situé dans la partie supérieure de l'espace de travail.

Les règles de traitement de messages que vous avez sélectionnées sont supprimées.

Activation et désactivation d'une règle de traitement de messages

► *Pour activer ou désactiver une règle de traitement de messages, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.
2. Exécutez une des actions suivantes :
   - Activez le commutateur en regard du nom de la règle à activer.
   - Désactivez le commutateur en regard du nom de la règle à désactiver.

Domaine et configuration du routage des emails

Cette section explique comment ajouter des domaines et des adresses email à la table de transport, configurer le routage des emails pour ces domaines, supprimer des domaines de la liste, configurer les modes de sécurité TLS pour les messages électroniques entrants et sortants et ajouter une signature DKIM aux messages.

Kaspersky Secure Mail Gateway utilise par défaut les paramètres de votre serveur DNS pour le routage des emails. Vous pouvez configurer le routage des emails manuellement. Pour cela, il faut créer une table de transport. Saisissez-y les noms des domaines pour lesquels les messages électroniques sont prévus, puis saisissez les adresses IP ou les noms FQDN des domaines vers lesquels Kaspersky Secure Mail Gateway va rediriger les messages destinés à ces domaines.

Exemple :

Si vous voulez que les messages destinés au domaine exemple.com soient redirigés à l'adresse 1.1.1.0:25, vous devez exécuter les actions suivantes :

1. ajouter le domaine exemple.com à la table de transport ;
2. indiquer l'adresse IP 1.1.1.0 et le numéro de port 25 pour le routage des messages destinés au domaine example.com.

Cette section décrit également la configuration du routage des emails pour les domaines locaux (relay_domains).

Les *domaines locaux* (relay_domains) représentent les domaines de votre organisation pour lesquels Kaspersky Secure Mail Gateway accepte les messages électroniques depuis l'extérieur. Kaspersky Secure Mail Gateway acceptera les messages uniquement pour les domaines que vous avez renseignés. Les messages destinés à d'autres domaines seront ignorés.

Si aucun domaine local n'est indiqué, Kaspersky Secure Mail Gateway n'acceptera pas les messages pour vos serveurs de messagerie internes.

Dans cette section

Ajout d'un enregistrement à la table de transport et configuration du routage des emails (transport_map)

► *Pour ajouter un enregistrement à la table de transport et configurer le routage des emails, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Domaines** dans l'arborescence de la console de gestion.

2. Cliquez sur le bouton **Ajouter**.

   La fenêtre de création d'un enregistrement s'ouvre.

3. Choisissez dans le groupe de paramètres **Type d'enregistrement** un des types d'enregistrement suivants :

   - **Domaine** si vous souhaitez ajouter un domaine à la table de transport.
   - **Sous-domaines de ce domaine** si vous souhaitez ajouter un sous-domaine à la table de transport.
   - **Adresse email** si vous souhaitez ajouter un adresse email à la table de transport.

4. Saisissez dans le champ **Domaine / Adresse email** le nom du domaine ou les noms des sous-domaines au format FQDN ou l'adresse email.

5. Cochez la case en regard du nom du paramètre **Domaine local** si vous voulez ajouter un domaine local (cf. section "Ajout d'un domaine local (relay_domain)" à la page 150).

6. Dans le groupe de paramètres **Routage des emails**, activez le commutateur en regard du nom du paramètre **Configurer le routage du courrier**.

7. Sélectionnez le protocole de transmission des emails dans le groupe de paramètre **Protocole** .

   - **SMTP** si vous voulez configurer la transmission des emails selon le protocole SMTP.
   - **LMTP** si vous voulez configurer la transmission des emails selon le protocole LMTP.

8. Saisissez dans le champ **Adresse de destination et numéro de port** l'adresse IP ou le nom de domaine du serveur auquel vous souhaitez configurer le routage des emails.

   Vous pouvez saisir des adresses IPv4 (par exemple, 192.0.0.1 ou 192.0.0.0/16), un masque de sous-réseau en notation CIDR (par exemple, fc00::/7), un nom de domaine ou un nom de domaine complet (FQDN).

9. Activez ou désactivez la recherche d'enregistrements MX dans le groupe **Recherche d'enregistrements MX**. Sélectionnez l'une des options suivantes :

   - **Désactivée** si vous voulez désactiver la recherche d'enregistrements MX.
   - **Activée** si vous voulez activer la recherche d'enregistrements MX.

10. Si vous ajoutez un domaine ou un sous-domaine, sélectionnez une des options suivantes dans le groupe de paramètres **Mode de chiffrement TLS pour tous les messages sortants du serveur de messagerie** :

    - **Utiliser le mode de chiffrement TLS défini pour tous les messages sortants du serveur de messagerie** si vous souhaitez utiliser pour ce domaine le mode de chiffrement TLS de la connexion défini pour tous les messages sortants du serveur de messagerie.
    - **Modifier le mode de chiffrement TLS des messages pour ce domaine** si vous souhaitez configurer un autre mode de chiffrement TLS de la connexion pour ce domaine.

11. Si vous avez opté pour la modification du mode de chiffrement TLS pour ce domaine, choisissez le mode de chiffrement TLS que vous souhaitez appliquer dans la liste **Modifier le mode de chiffrement TLS des messages pour ce domaine**.

12. Si vous souhaitez ajouter une signature DKIM aux messages en provenance d'adresses de ce domaine, réalisez les opérations suivantes dans le groupe de paramètres **Signature DKIM des messages provenant des adresses du domaine** :

    a. Cliquez sur le bouton **Ajouter**.

    La fenêtre **Création d'une signature DKIM pour le domaine** s'ouvre.

b. Saisissez le nom que vous souhaitez donner à la signature DKIM dans le champ **Sélecteur**.

c. La liste **Nom de la clé** permet de choisir la clé DKIM sur la base de laquelle la signature DKIM sera ajoutée aux messages.

d. Cliquez sur le bouton **OK**.

La fenêtre **Création d'une signature DKIM pour le domaine** se ferme.

13. Cliquez sur le bouton **Ajouter**, dans la partie inférieure de la fenêtre.

L'enregistrement ajouté apparaît dans la table de transport.

Ajout d'un domaine local (relay_domains)

► *Pour ajouter un domaine local de votre organisation, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Domaines** dans l'arborescence de la console de gestion.

2. Cliquez sur le bouton **Ajouter**.

   La fenêtre de création d'un enregistrement s'ouvre.

3. Sélectionnez dans le groupe de paramètres **Type d'enregistrement** le type de d'enregistrement **Domaine**.

4. Saisissez le nom du domaine pour lequel Kaspersky Secure Mail Gateway acceptera les messages depuis l'extérieur dans le champ **Domaine / Adresse email**.

   Saisissez le nom de domaine au format FQDN.

5. Cochez la case en regard du paramètre **Domaine local**.

Kaspersky Secure Mail Gateway acceptera les messages uniquement pour les domaines que vous avez renseignés. Les messages destinés à d'autres domaines seront ignorés.

6. Dans le groupe de paramètres **Routage des emails**, activez le commutateur en regard du nom du paramètre **Configurer le routage du courrier**.

7. Sélectionnez le protocole de transmission des emails dans le groupe de paramètre **Protocole**.

   - **SMTP** si vous voulez configurer la transmission des emails selon le protocole SMTP.
   - **LMTP** si vous voulez configurer la transmission des emails selon le protocole LMTP.

8. Saisissez dans le champ **Adresse de destination et numéro de port** l'adresse IP ou le nom de domaine du serveur auquel vous souhaitez configurer le routage des emails.

   Vous pouvez saisir des adresses IPv4 (par exemple, 192.0.0.1 ou 192.0.0.0/16), un masque de sous-réseau en notation CIDR (par exemple, fc00::/7), un nom de domaine ou un nom de domaine complet (FQDN).

9. Activez ou désactivez la recherche d'enregistrements MX dans le groupe **Recherche d'enregistrements MX**. Sélectionnez l'une des options suivantes :

   - **Désactivée** si vous voulez désactiver la recherche d'enregistrements MX.
   - **Activée** si vous voulez activer la recherche d'enregistrements MX.

10. Dans le groupe de paramètres **Mode de chiffrement TLS pour tous les messages sortants du serveur de messagerie**, sélectionnez une des options suivantes :

    - **Utiliser le mode de chiffrement TLS défini pour tous les messages sortants du serveur de messagerie** si vous souhaitez utiliser pour ce domaine le mode de chiffrement TLS de la connexion défini pour tous les messages sortants du serveur de messagerie.
    - **Modifier le mode de chiffrement TLS des messages pour ce domaine** si vous souhaitez configurer un autre mode de chiffrement TLS de la connexion pour ce domaine.

11. Si vous avez opté pour la configuration d'un autre mode de chiffrement TLS pour ce domaine, choisissez le mode de chiffrement TLS que vous souhaitez appliquer dans la liste **Modifier le mode de chiffrement TLS des messages pour ce domaine**.

12. Si vous souhaitez ajouter une signature DKIM aux messages en provenance d'adresses de ce domaine, réalisez les opérations suivantes dans le groupe de paramètres **Signature DKIM des messages provenant des adresses du domaine** :

    a. Cliquez sur le bouton **Ajouter**.

    La fenêtre **Création d'une signature DKIM pour le domaine** s'ouvre.

    b. Saisissez le nom que vous souhaitez donner à la signature DKIM dans le champ **Sélecteur**.

    c. La liste **Nom de la clé** permet de choisir la clé DKIM sur la base de laquelle la signature DKIM sera ajoutée aux messages.

    d. Cliquez sur le bouton **OK**.

    La fenêtre **Création d'une signature DKIM pour le domaine** se ferme.

13. Cliquez sur le bouton **Ajouter**, dans la partie inférieure de la fenêtre.

Le domaine pour lequel Kaspersky Secure Mail Gateway acceptera les messages apparaît dans la liste des domaines.

Suppression d'un enregistrement de la table de transport

► *Pour supprimer un enregistrement de la table de transport, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Domaines** dans l'arborescence de la console de gestion.

2. Dans la liste des domaines, cochez la case en regard de chacun des enregistrements que vous souhaitez supprimer de la table de transport.

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

La fenêtre de confirmation de l'opération **Suppression** s'ouvre.

4. Cliquez sur le bouton **Oui**.

L'enregistrement est supprimé de la table de transport.

Modification du routage des emails pour le domaine (transport_map)

► *Pour modifier le routage des emails pour un domaine, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Domaines** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien portant le nom du domaine dans la table de transport et développez les paramètres de routage des emails pour ce domaine.

3. Sélectionnez le protocole de transmission des emails dans le groupe de paramètre **Protocole** .

   - **SMTP** si vous voulez configurer la transmission des emails selon le protocole SMTP.

   - **LMTP** si vous voulez configurer la transmission des emails selon le protocole LMTP.

4. Saisissez dans le champ **Adresse de destination et numéro de port** l'adresse IP ou le nom de domaine du serveur auquel vous souhaitez configurer le routage des emails.

   Vous pouvez saisir des adresses IPv4 (par exemple, 192.0.0.1 ou 192.0.0.0/16), un masque de sous-réseau en notation CIDR (par exemple, fc00::/7), un nom de domaine ou un nom de domaine complet (FQDN).

5. Activez ou désactivez la recherche d'enregistrements MX dans le groupe **Recherche d'enregistrements MX**. Sélectionnez l'une des options suivantes :

   - **Désactivée** si vous voulez désactiver la recherche d'enregistrements MX.

   - **Activée** si vous voulez activer la recherche d'enregistrements MX.

6. Saisissez l'adresse IP du serveur vers lequel vous souhaitez configurer le routage du courrier dans le champ **Adresse de destination et numéro de port** .

   Vous pouvez saisir une adresse IPv4 (par exemple, 192.0.0.1 ou 192.0.0.0/16), un nom de domaine ou un nom FQDN.

7. Cliquez sur le bouton **OK**, dans la partie inférieure de la fenêtre.

Le routage des emails est modifié pour le domaine.

Présentation de l'utilisation du protocole TLS avec Kaspersky Secure Mail Gateway

Le *protocole TLS* (*Transport Layer Security*, sécurité de la couche de transport) est un protocole de chiffrement de la connexion entre deux serveurs. Il garantit un transfert sécurisé des données entre les nœuds du réseau Internet.

Une *session avec utilisation du protocole TLS* (ci-après, une session TLS) recouvre la succession d'événements suivants :

1. Le serveur d'où sont envoyés les messages électroniques (*client*) établit une connexion avec le serveur auquel ces messages sont envoyés (*Serveur*).
2. Les serveurs commencent à interagir via le protocole SMTP.
3. Le client envoie la commande `STARTTLS` au serveur et lui propose d'utiliser TLS dans le cadre de l'interaction SMTP.
4. Si le serveur est compatible avec TLS, il répond à la commande `Ready to start TLS` et envoie le certificat du serveur au client.
5. Le client reçoit le certificat et si ses paramètres possèdent les valeurs adéquates, il vérifie l'authenticité du certificat du serveur.
6. Le client et le serveur activent le mode de chiffrement des données.
7. Les serveurs échangent les données.

8. La session se termine.

Vous pouvez configurer le mode de sécurité TLS pour les cas où Kaspersky Secure Mail Gateway accepte des messages d'un autre serveur (en tant que serveur (cf. section "Configuration de la sécurité TLS pour les messages électroniques entrants" à la page 155)) ou les transmet à un autre serveur (en tant que client (cf. section "Configuration de la sécurité TLS pour les messages électroniques sortants" à la page 157)) et configurer les paramètres TLS pour des domaines et groupes de domaines distincts (cf. section "Domaines et configuration du routage des emails" à la page 146) qui utilisent la même adresse IP.

Configuration de la sécurité TLS pour les messages électroniques entrants

► *Pour configurer le mode de sécurité TLS dans le cas où Kaspersky Secure Mail Gateway accepte des messages d'un autre serveur (agit en tant que Serveur), procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Domaines** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe quel lien pour ouvrir la fenêtre **Paramètres TLS**.

3. Le groupe de paramètres **Mode de sécurité TLS du serveur** permet de sélectionner un des modes d'utilisation du chiffrement TLS de la connexion entre Kaspersky Secure Mail Gateway et le serveur qui envoie les messages électroniques :

   - **Ne pas utiliser le chiffrement TLS**, si vous ne souhaitez pas utiliser le chiffrement TLS pour la connexion avec le serveur qui envoie les messages électroniques.

     Dans ce cas, Kaspersky Secure Mail Gateway accepte tous les messages en clair.

   - **Proposer le chiffrement TLS** si vous souhaitez que Kaspersky Secure Mail Gateway propose au serveur qui envoie les messages électroniques d'utiliser le chiffrement TLS de la connexion.

     Dans ce cas, Kaspersky Secure Mail Gateway utilise la commande `STARTTLS` pour proposer au serveur qui envoie les messages électroniques d'utiliser le chiffrement TLS, mais il accepte les messages quelle que soit la réponse du serveur.

- **Exiger le chiffrement TLS** si vous souhaitez que Kaspersky Secure Mail Gateway exige du serveur qui envoie les messages électroniques qu'il utilise le chiffrement TLS de la connexion.

  Dans ce cas, le serveur qui envoie les messages électroniques (client) utilise la commande `STARTTLS` pour suggérer à Kaspersky Secure Mail Gateway d'utiliser le chiffrement TLS. Kaspersky Secure Mail Gateway répond par la commande `Ready to start TLS`et envoie au client le certificat du Serveur et il exige également que le client vérifie l'authenticité du certificat du serveur. Après que le client a vérifié l'authenticité du certificat du serveur, la connexion TLS chiffrée est établie.

4. Sélectionnez, dans le groupe de paramètres **Fourniture du certificat TLS du serveur**, le certificat TLS du serveur que Kaspersky Secure Mail Gateway enverra au client en vue de l'authentifier au début de chaque session TLS.

   > Vous pouvez créer ou importer un certificat TLS dans la section **Clés de chiffrement**, sous-section **TLS** de la fenêtre principale de l'interface Internet de Kaspersky Secure Mail Gateway.

5. Dans le groupe de paramètres **Demande de certificat TLS client**, sélectionnez dans le menu déroulant une des options suivantes :

   - **Ne pas demander** si vous ne souhaitez pas que Kaspersky Secure Mail Gateway demande le certificat TLS du client.
   - **Demander** si vous souhaitez que Kaspersky Secure Mail Gateway demande le certificat TLS du client, mais puisse transmettre les messages quel que soit le résultat de l'analyse du certificat.
   - **Exiger** si vous souhaitez que Kaspersky Secure Mail Gateway exige le certificat TLS du client et ne transmette pas les messages si le nom sur le certificat est incorrect ou si le certificat TLS du client n'est pas valide.

     > Choisissez les options **Demander** ou **Exiger** uniquement si vous êtes certains que les clients pris en charge par votre serveur de messagerie peuvent proposer un certificat TLS vérifiable.

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

Configuration de la sécurité TLS pour les messages électroniques sortants

► *Pour configurer le mode de sécurité TLS dans le cas où Kaspersky Secure Mail Gateway redirige des messages vers un autre serveur (agit en tant que client), procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Domaines** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe quel lien pour ouvrir la fenêtre **Paramètres TLS**.

3. Le groupe de paramètres **Mode de sécurité TLS du client** permet de sélectionner un des modes de chiffrement TLS de la connexion entre Kaspersky Secure Mail Gateway et le serveur qui reçoit les messages électroniques :

   - **Ne pas utiliser le chiffrement TLS** si vous ne souhaitez pas utiliser le chiffrement TLS pour la connexion avec le serveur qui reçoit les messages électroniques.

     Dans ce cas, Kaspersky Secure Mail Gateway redirige tous les messages en clair.

   - **Vérifier la possibilité d'un chiffrement TLS** si vous souhaitez que Kaspersky Secure Mail Gateway tente d'ouvrir une session TLS avec le serveur de messagerie de réception et transfère les messages en clair si ce serveur ne prend pas TLS en charge.

   - **Exiger le chiffrement TLS et ne pas vérifier le certificat** si vous souhaitez que Kaspersky Secure Mail Gateway redirige des messages uniquement si le serveur de messagerie de réception prend TLS en charge, quelle que soit la validité du certificat TLS.

   - **Exiger le chiffrement TLS et vérifier le certificat** si vous souhaitez que Kaspersky Secure Mail Gateway redirige les messages uniquement si le serveur de messagerie de réception prend TLS en charge, si son certificat TLS est valide et si le nom du certificat correspond au nom de domaine du serveur.

Kaspersky Secure Mail Gateway ne transfèrera pas les messages si ces conditions ne sont pas respectées.

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

Présentation de la signature DKIM des messages sortants

La signature DKIM des messages sortants est une signature numérique ajoutée aux messages envoyés depuis des adresses email d'un domaine défini afin de pouvoir identifier les utilisateurs sur la base du domaine de l'organisation.

La technologie DomainKeys Identified Mail (DKIM) regroupe plusieurs méthodes de lutte contre le phishing et le courrier indésirable en vue d'améliorer la qualité du classement et de l'identification des emails légitimes. Au lieu de recourir à l'adresse IP pour déterminer l'expéditeur du message, la technologie DKIM lui ajoute une signature numérique associée au nom du domaine de l'organisation.

Activation et désactivation de l'ajout d'une signature DKIM aux messages sortants

► *Pour activer ou désactiver l'ajout d'une signature DKIM aux messages sortants, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Domaines** dans l'arborescence de la console de gestion.

2. Dans la partie supérieure de l'espace de travail, cliquez sur le lien **Signature DKIM** pour ouvrir la fenêtre **Paramètres DKIM**.

3. Sélectionnez l'une des options suivantes dans le menu déroulant **Signature DKIM** :

   - **Activée**, si vous souhaitez activer l'ajout d'une signature DKIM aux messages sortants.

- **Désactivée**, si vous souhaitez désactiver l'ajout d'une signature DKIM aux messages sortants.

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

La fenêtre **Paramètres DKIM** se ferme.

Préparatifs pour l'ajout d'une signature DKIM aux messages sortants

Vous pouvez configurer l'ajout d'une signature DKIM aux messages dans l'interface Web de Kaspersky Secure Mail Gateway.

La configuration de l'ajout d'une signature DKIM aux messages se déroule selon les étapes suivantes ;

1. Activation de l'ajout d'une signature DKIM aux messages sortants.
2. Création et importation d'une clé DKIM.
3. Ajout d'une signature DKIM aux messages envoyés depuis des adresses email d'un domaine déterminé

Pour que le serveur de messagerie distant puisse vérifier la signature DKIM ajoutée aux messages sortant, il faut obtenir la signature DNS de la clé DKIM publique dans l'interface Web de Kaspersky Secure Mail Gateway et l'ajouter aux paramètres de votre serveur DNS.

► *Pour obtenir la signature DNS de la clé DKIM ouverte, réalisez les opérations suivantes dans l'interface Web de Kaspersky Secure Mail Gateway :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Domaines** dans l'arborescence de la console de gestion.
2. Si le paramètre **Désactivée** a la valeur Désactivé. dans l'espace de travail, procédez comme suit :
    a. cliquez sur le lien **Signature DKIM** pour ouvrir la fenêtre **Paramètres DKIM**.
    b. Dans la liste déroulante **Signature DKIM**, choisissez **Activée**.

c. Cliquez sur le bouton **OK**.

La fenêtre **Paramètres DKIM** se ferme.

3. Dans la liste de domaines, cliquez sur le nom du domaine pour les adresses duquel vous souhaitez configurer l'ajout d'une signature DKIM aux messages sortants pour ouvrir la fenêtre des modifications d'un enregistrement.

4. Cliquez sur le bouton **Ajouter** dans le groupe de paramètres **Signature DKIM des messages provenant des adresses du domaine**.

   La fenêtre **Création d'une signature DKIM pour le domaine** s'ouvre.

5. Saisissez le nom que vous souhaitez donner à la signature DKIM dans le champ **Sélecteur**.

6. La liste **Nom de la clé** permet de choisir la clé DKIM sur la base de laquelle la signature DKIM sera ajoutée aux messages.

7. Cliquez sur le bouton **OK**.

   La fenêtre **Création d'une signature DKIM pour le domaine** se ferme.

Dans le champ **Enregistrement DNS** du groupe de paramètres **Signature DKIM des messages provenant des adresses du domaine**, l'enregistrement DNS de la clé DKIM ouverte pour le domaine défini s'affiche.

► *Pour ajouter la clé DKIM publique aux paramètres de votre serveur DNS, procédez comme suit :*

1. Ouvrez une session en tant qu'administrateur sur votre serveur DNS.

2. Trouvez la page qui contient les informations relatives à la mise à jour des signatures DNS de ce domaine contenant les adresses pour lesquelles vous souhaitez configurer l'ajout d'une signature DKIM pour les messages sortants.

   Par exemple, cette page peut être intitulée "Administration DNS", "Administration du serveur de noms" ou "Paramètres complémentaires".

3. Trouvez les signatures au format TXT pour ce domaine contenant les adresses pour lesquelles vous souhaitez configurer l'ajout d'une signature DKIM pour le courrier sortant.

4. Dans la liste des signatures au format TXT, ajoutez la signature DNS de la clé DKIM ouverte pour le domaine en question de la manière suivante :

   ```
   <sélectionneur>._domainkey.<nom de domaine pour lequel vous souhaitez ajouter une clé DKIM publique>. IN TXT ( "v=<version DKIM>; k=rsa; s=email" "p=<signature DNS de la clé DKIM publique>" )
   ```

Exemple d'enregistrement DNS d'une clé DKIM publique :

```
mail._domainkey.example.com IN TXT ( "v=DKIM1; k=rsa; s=email; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtyb09IeTJtIxTEohP/wa8eZ
OuiFJxL3pjk+1R81ajQyTb4J8Dj23RbjOKCZGFdyJfj7MUUL9MpvAo6OL9KrfaF8ehR7Mb
Hhaix1qPDfSP5a97vl9/6KR2TKJfi+0dQ/pMLJMbnXfdWeoDoDBUK0++B8HHCnSpLTxsH/
YDOtjKaHFxbU6DMEICTiVBWR+yeWopdWi9kPNT5SJ5H" )
```

> Pour en savoir plus sur la fonction des paramètres de la signature DNS d'une clé DKIM ouverte, consultez le document RFC 5617.

5. Enregistrez les modifications.

> La syntaxe de l'exemple de signature DNS illustre l'ajout aux paramètres d'un serveur DNS BIND. La syntaxe d'une signature DNS ajoutée à d'autres serveurs DNS peut légèrement différer de l'exemple fourni.

Ajout d'une signature DKIM aux messages en provenance d'adresses d'un domaine déterminé

Avant d'ajouter une signature DKIM aux messages en provenance d'adresses d'un domaine déterminé, il faut créer ou importer une clé DKIM.

► *Pour ajouter une signature DKIM aux messages envoyés depuis une adresse email d'un domaine déterminé, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Domaines** dans l'arborescence de la console de gestion.
2. Si le paramètre **Désactivée** a la valeur Désactivé. dans l'espace de travail, procédez comme suit :
   a. cliquez sur le lien **Signature DKIM** pour ouvrir la fenêtre **Paramètres DKIM**.
   b. Dans la liste déroulante **Signature DKIM**, choisissez **Activée**.
   c. Cliquez sur le bouton **OK**.

   La fenêtre **Paramètres DKIM** se ferme.
3. Sélectionnez dans la liste le domaine pour lequel vous souhaitez ajouter une signature DKIM aux messages sortants.
4. Cliquez sur le bouton **Ajouter** dans le groupe de paramètres **Signature DKIM des messages provenant des adresses du domaine**.
5. La fenêtre **Création d'une signature DKIM pour le domaine** s'ouvre.
6. Saisissez le nom que vous souhaitez donner à la signature DKIM dans le champ **Sélecteur**.
7. La liste **Nom de la clé** permet de choisir la clé DKIM sur la base de laquelle la signature DKIM sera ajoutée aux messages.
8. Cliquez sur le bouton **OK**.

La fenêtre **Création d'une signature DKIM pour le domaine** se ferme.

Une fois que vous avez configuré l'ajout d'une signature DKIM aux messages dans l'interface Web de Kaspersky Secure Mail Gateway et pour que le serveur de messagerie distant puisse contrôler cette signature DKIM, vous devez ajouter la clé DKIM publique aux paramètres de votre serveur DNS (cf. section "Préparatifs pour l'ajout d'une signature DKIM aux messages sortants" à la page 159).

Signature DKIM des messages sortants

Cette section contient des informations sur l'ajout d'une signature DKIM aux messages sortants.

Dans cette section

Création d'une clé DKIM

► *Pour créer une clé DKIM, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Clés de chiffrement** puis la sous-section **DKIM** dans l'arborescence de la console de gestion.
2. Cliquez sur le bouton **Créer** situé dans la partie supérieure de l'espace de travail.

   Le champ **Nom de la clé** s'affiche.
3. Le champ **Nom de la clé** accueille le nom de la clé DKIM à trouver lors de l'ajout de la signature DKIM des messages.
4. Cliquez sur le bouton **OK**.

La clé DKIM que vous avez créée apparaît dans la liste des clés DKIM dans l'espace de travail de la fenêtre principale de l'interface Internet de l'application.

Importation d'une clé DKIM depuis un fichier

► *Pour importer une clé DKIM depuis un fichier, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Clés de chiffrement** puis la sous-section **DKIM** dans l'arborescence de la console de gestion.
2. Cliquez sur le bouton **Importer** situé dans la partie supérieure de l'espace de travail.
3. Saisissez dans le champ **Nom de la clé** qui s'affiche le nom que vous souhaitez donner à la clé DKIM à importer.
4. Cliquez sur le bouton **Parcourir** à droite du champ **Sélectionnez le fichier de la clé DKIM**.

   La fenêtre de sélection de fichiers de votre navigateur s'ouvre.
5. Choisissez le fichier de la clé DKIM que vous souhaitez importer, puis cliquez sur le bouton **Ouvrir** de votre navigateur.

   > Le fichier doit contenir une clé RSA au format PEM d'une longueur de 2 048 ou 4 096 bits.

   La fenêtre de sélection de fichiers se ferme.
6. Cliquez sur le bouton **OK**.

La clé DKIM apparaît dans la liste des clés DKIM dans l'espace de travail de la fenêtre principale de l'interface Internet de l'application.

Suppression d'une clé DKIM

► *Pour supprimer la clé DKIM, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Clés de chiffrement** puis la sous-section **DKIM** dans l'arborescence de la console de gestion.

2. Dans la liste des clés DKIM, cochez la case en regard du ou des clés que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer** situé dans la partie supérieure de l'espace de travail.

   La fenêtre de confirmation de l'opération **Suppression des éléments sélectionnés** s'ouvre.
4. Cliquez sur le bouton **Oui**.

   La fenêtre **Suppression des éléments sélectionnés** se ferme.

La clé DKIM sélectionnée sera supprimée.

Utilisation du protocole TLS avec Kaspersky Secure Mail Gateway

Cette section fournit des informations sur l'utilisation du protocole TLS avec Kaspersky Secure Mail Gateway et sur la configuration des paramètres d'utilisation de ce protocole.

Dans cette section

Création du certificat TLS

► *Pour créer un certificat TLS, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Clés de chiffrement** puis la sous-section **TLS** dans l'arborescence de la console de gestion.

2. Cliquez sur le bouton **Créer** situé dans la partie supérieure de l'espace de travail.

3. Saisissez le nom du certificat TLS à envoyer au client SMTP pour authentification au début de chaque session TLS dans le champ **Nom du certificat TLS**.

   Le certificat TLS du serveur est offert si Kaspersky Secure Mail Gateway remplit une fonction de serveur de messagerie (il reçoit des messages).

   Le nom du certificat TLS ne peut être vide.

4. Saisissez l'Etat ou la province de votre organisation dans le champ **Etat (province)** .
5. Saisissez la ville de votre organisation dans le champ **Ville** .
6. Saisissez le code de deux lettres du pays où se trouve votre organisation dans le champ **Code du pays**.

   Par exemple, saisissez RU pour la Russie ou US pour les Etats-Unis.
7. Saisissez dans le champ **Nom de l'organisation** le nom de votre organisation.
8. Saisissez le nom de la division de l'organisation pour laquelle vous créez un certificat TLS dans le champ **Nom de la division de l'organisation**.
9. Saisissez l'adresse électronique de l'administrateur de Kaspersky Secure Mail Gateway dans le champ **Adresse email**.
10. Cliquez sur le bouton **OK**.

Le certificat TLS que vous avez créé apparaît dans la liste des certificats TLS dans l'espace de travail de la fenêtre principale de l'interface Internet de l'application.

Suppression du certificat TLS

► *Pour supprimer un certificat TLS, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Clés de chiffrement** puis la sous-section **TLS** dans l'arborescence de la console de gestion.
2. Dans la liste des certificats TLS, cochez la case en regard du ou des certificats que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer** situé dans la partie supérieure de l'espace de travail.

   La fenêtre de confirmation de l'opération **Suppression des éléments sélectionnés** s'ouvre.
4. Cliquez sur le bouton **Oui**.

   La fenêtre **Suppression des éléments sélectionnés** se ferme.

Le certificat TLS sera supprimé.

Préparation de l'importation du certificat TLS auto-signé

Un certificat TLS auto-signé prévu pour l'importation dans Kaspersky Secure Mail Gateway doit remplir les conditions suivantes :

- Le fichier du certificat doit posséder un nom unique dans la liste des certificats utilisés par Kaspersky Secure Mail Gateway.
- Le fichier de certificat et le fichier de clé privée doivent être au format PEM.
- La clé doit avoir une longueur de 1 024 bits minimum.

L'exemple fourni illustre les préparatifs de l'importation d'un certificat TLS auto-signé de serveur server_cert.pem, dont la clé privée se trouve dans le fichier key.pem.

► *Pour préparer un certificat TLS auto-signé en vue de l'importation dans Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Dans le fichier de clé privée, supprimez le mot de passe d'accès au certificat, le cas échéant. Saisissez pour ce faire la commande :

   ```
   # openssl rsa -in <nom du fichier de clé privée>.pem -out <nom du fichier de clé privée après la suppression du mot de passe>.pem
   ```

   Par exemple, vous pouvez exécuter la commande suivante :

   ```
   # openssl rsa -in key.pem -out key-nopass.pem
   ```

2. Unifiez la clé privée et le certificat du serveur dans un fichier. Saisissez pour ce faire la commande :

   ```
   % cat <nom du fichier de clé privée après la suppression du mot de passe>.pem <nom de certificat du serveur>.pem <nom du certificat de serveur après l'unification des fichiers>.pem
   ```

Par exemple, vous pouvez exécuter la commande suivante :

```
% cat key-nopass.pem server_cert.pem > cert.pem
```

Le certificat TLS auto-signé (par exemple, cert.pem) est prêt à être importé dans Kaspersky Secure Mail Gateway.

Préparatifs pour l'importation d'un certificat TLS signé par une autorité de certification

Un certificat TLS signé par une autorité de certification (certificat AC) et prévu pour une importation dans Kaspersky Secure Mail Gateway doit remplir les conditions suivantes :

- Le fichier du certificat doit posséder un nom unique dans la liste des certificats utilisés par Kaspersky Secure Mail Gateway.
- Les fichiers du certificat serveur, des certificats AC intermédiaire et racine ainsi que le fichier de la clé privée doivent être au format PEM.
- La clé doit avoir une longueur de 1 024 bits minimum.
- Il doit contenir la *chaîne de certification* complète, le chemin depuis le certificat du serveur jusqu'au certificat AC racine.

  Lors de la réception du certificat AC, il faudra peut-être utilisé un certificat intermédiaire en plus du certificat de serveur.
- Les certificats doivent apparaître dans la chaîne dans l'ordre suivant : tout d'abord le certificat du serveur, puis les certificats AC intermédiaires.
- Les certificats intermédiaires ne peuvent pas être absents de la chaîne de certification.
- La chaîne de certification ne peut pas contenir de certificats qui ne sont pas liés à la certification actuelle.

L'exemple fourni illustre les préparatifs de l'importation d'un certificat TLS de serveur signé par une autorité de certification server_cert.pem, dont la clé privée se trouve dans le fichier key.pem. Le nom du certificat intermédiaire est intermediate CA, et le nom du certificat racine est CA.

► *Pour préparer un certificat TLS signé par une autorité de certification en vue de l'importation dans Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Dans le fichier du certificat TLS, supprimez le mot de passe d'accès au certificat, le cas échéant. Saisissez pour ce faire la commande :

   ```
   # openssl rsa -in <nom du fichier de clé privée>.pem -out <nom du fichier de clé privée après la suppression du mot de passe>.pem
   ```

   Par exemple, vous pouvez exécuter la commande suivante :

   ```
   # openssl rsa -in key.pem -out key-nopass.pem
   ```

2. Exécutez une des actions suivantes :

   - Si vous ne pensez pas que les clients auxquels le serveur va envoyer ce certificat possèdent leur copie des certificats AC racine et intermédiaires, unifiez la clé privée, le certificat de serveur, le certificat intermédiaire et le certificat AC racine dans un fichier. Saisissez pour ce faire la commande :

     ```
     % cat <nom du fichier de clé privée après la suppression du mot de passe>.pem <nom du certificat du serveur>.pem <nom du certificat AC intermédiaire>.pem <nom du certificat AC racine>.pem <nom du certificat TLS après l'unification des fichiers>.pem
     ```

     Par exemple, vous pouvez exécuter la commande suivante :

     ```
     % cat key-nopass.pem server_cert.pem intermediate_CA.pem root_CA.pem > cert.pem
     ```

   - Si vous êtes certains que les clients auxquels le serveur va envoyer ce certificat possèdent leur copie des certificats AC racine et intermédiaires, unifiez la clé privée et le certificat de serveur dans un fichier. Saisissez pour ce faire la commande :

```
% cat <nom du fichier de clé privée après la suppression du mot de passe>.pem <nom de certificat du serveur>.pem <nom du certificat de serveur après l'unification des fichiers>.pem
```

Par exemple, vous pouvez exécuter la commande suivante :

```
% cat key-nopass.pem server_cert.pem > cert.pem
```

Le certificat TLS, signé par une autorité de certification (par exemple, cert.pem) est prêt à être importé dans Kaspersky Secure Mail Gateway.

Importation du certificat TLS depuis un fichier

Avant d'importer des certificats TLS dans l'interface Web de Kaspersky Secure Mail Gateway, il faut les préparer.

Vous pouvez préparer l'importation des certificats de type suivant :

- certificat TLS auto-signé (cf. section "Préparatifs pour l'importation du certificat TLS auto-signé" à la page 169) ;
- certificat TLS signé par une autorité de certification (ci-après désigné aussi certificat CA) (cf. section "Préparatifs pour l'importation d'un certificat TLS signé par une autorité de certification" à la page 170).

Les certificats auto-signés sont utilisés généralement pour tester et déboguer les connexions avec chiffrement SSL et TLS. Il est conseillé d'utiliser sur des serveurs publics des certificats signés par une autorité de certification (certificats AC).

► *Pour importer un certificat TLS, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Clés de chiffrement** puis la sous-section **TLS** dans l'arborescence de la console de gestion.
2. Cliquez sur le bouton **Importer** situé dans la partie supérieure de l'espace de travail.
3. Le champ **Nom du certificat TLS** accueille le nom que vous souhaitez attribuer au certificat TLS à importer.

4. Cliquez sur le bouton **Parcourir** situé à droite du champ **Sélectionnez le fichier du certificat TLS**.

   La fenêtre de sélection de fichiers de votre navigateur s'ouvre.

5. Sélectionnez le fichier du certificat TLS que vous souhaitez importer, puis cliquez sur le bouton **Ouvrir** de votre navigateur.

   > Le fichier du certificat (cf. section "Préparatifs pour l'importation du certificat TLS auto-signé" à la page 169, "Préparatifs pour l'importation d'un certificat TLS signé par une autorité de certification" à la page 170) doit contenir le certificat TLSet la clé TLS privée avec l'extension pem. La clé privée ne peut être chiffrée ou protégée par un mot de passe.

   La fenêtre de sélection de fichiers se ferme.

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

Le certificat TLS apparaît dans la liste des certificats TLS dans l'espace de travail de la fenêtre principale de l'interface Internet de l'application.

La Sauvegarde

La *Sauvegarde* est un endroit prévu pour la copie des messages que Kaspersky Secure Mail Gateway conserve pendant le traitement. Les copies des messages y sont conservées sous forme chiffrée et pour cette raison, elles ne menacent pas la sécurité de votre ordinateur.

Kaspersky Secure Mail Gateway place dans la Sauvegarde les copies des messages :

- Auxquels le module Antivirus a attribué un des états d'analyse (cf. section "A propos des états de la recherche de virus dans les messages" à la page 271) et avant l'exécution sur ceux-ci des actions (cf. section "Configuration des actions à exécuter sur les messages lors de la recherche de virus" à la page 276) ;

- Auxquels le module Anti-spam a attribué un des états d'analyse (cf. section "A propos des états de l'analyse antispam" à la page 286) et avant l'exécution sur ceux-ci des actions (cf. section "Configuration des actions à exécuter sur les messages lors de l'analyse contre les spams" à la page 295) ;

- Auxquels le module Anti-phishing a attribué un des états d'analyse (cf. section "A propos des états de l'analyse anti-phishing" à la page 305) et avant l'exécution sur ceux-ci des actions (cf. section "Configuration des actions à exécuter sur les messages lors de l'analyse anti-phishing" à la page 309) ;

- Auxquels le Filtrage du contenu a attribué un des états d'analyse (cf. section "A propos des états du filtrage de contenu des messages" à la page 314) et avant l'exécution sur ceux-ci des actions (cf. section "Configuration des actions à exécuter sur les messages lors du filtrage de contenu" à la page 319) ;

- Dont les adresses des expéditeurs figurent dans la liste noire d'adresses personnelle (cf. section "Configuration des paramètres de la liste noire d'adresses personnelle" à la page 340) et avant l'exécution sur ceux-ci des actions prévues.

Les copies des messages sont placées dans la Sauvegarde avec leurs pièces jointes.

Par défaut, la taille maximale de la Sauvegarde est de 7,32 Go. Lorsque la taille de la Sauvegarde dépasse la valeur de seuil définie par défaut, l'application commence à supprimer les copies de messages les plus anciennes de la Sauvegarde. Lorsque la taille de la Sauvegarde redevient

inférieure à la valeur de seuil définie par défaut, l'application arrête de supprimer les copies de message de la Sauvegarde.

Dans cette section

Configuration des paramètres de la sauvegarde

► *Pour configurer les paramètres de la Sauvegarde, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Sauvegarde** dans l'arborescence de la console de gestion.
2. Cliquez sur n'importe quel lien pour ouvrir la fenêtre **Paramètres de la Sauvegarde**.
3. Dans le champ **Taille maximale de la Sauvegarde**, indiquez le volume maximal que peut occuper la sauvegarde sur le disque dur.

   Il est recommandé d'indiquer une valeur supérieure à 100 Mo.
4. Dans le champ **Seuil d'espace disponible pour l'envoi du message**, indiquez le seuil d'espace libre dans la sauvegarde à partir duquel l'application enverra des notifications à l'administrateur de Kaspersky Secure Mail Gateway.

5. Sélectionnez l'une des options suivantes dans la liste **Autoriser la remise des messages infectés** :

   - **Oui** si vous voulez autoriser l'envoi (cf. section "Remise des messages de la Sauvegarde aux destinataires" à la page 181) des messages infectés de la Sauvegarde aux destinataires.

   - **Non** si vous voulez interdire l'envoi (cf. section "Remise des messages de la Sauvegarde aux destinataires" à la page 181) aux destinataires des messages infectés se trouvant dans la Sauvegarde.

   > Ce paramètre est appliqué pour le compte utilisateur HelpDesk (cf. section "Configuration des paramètres du compte utilisateur HelpDesk" à la page 214). L'utilisateur sous le compte utilisateur Administrator peut remettre les messages de la Sauvegarde (cf. section "Remise des messages de la Sauvegarde aux destinataires" à la page 181) aux destinataires quelle que soit la valeur du paramètre **Autoriser la remise des messages infectés** .

6. Sélectionnez l'une des options suivantes dans la liste **Traitement des messages en cas d'indisponibilité de la Sauvegarde** :

   - **Poursuivre le traitement** si vous souhaitez que le traitement des messages continue indépendamment des possibilités d'accès à la sauvegarde ;

   - **Signaler l'erreur temporaire du serveur** si vous souhaitez qu'une notification soit envoyée signaler l'indisponibilité temporaire de la Sauvegarde.

   - **Rejeter les messages** si vous souhaitez que les messages soient refusés quand la sauvegarde est indisponible.

7. Saisissez l'objet de la notification dans le champ **Objet de la notification d'envoi du message dans la pièce jointe**. Par exemple, Message delivery from Backup.

8. Saisissez le texte de la notification dans le champ **Corps de la notification d'envoi du message dans la pièce jointe**. Par exemple, vous pouvez rédiger un avertissement qui rappelle qu'un message remis depuis la Sauvegarde peut être dangereux et contenir des virus.

9. Cliquez sur le bouton **OK**.

   La fenêtre **Paramètres de la Sauvegarde** se ferme.

Recherche des copies de messages dans la Sauvegarde

► *Pour trouver les copies de messages dans la Sauvegarde, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Sauvegarde** dans l'arborescence de la console de gestion.

2. Dans l'espace de travail, sous les boutons **Envoyer**, **Consulter**, **Supprimer** et **Enregistrer**, cliquez sur n'importe quel lien pour ouvrir la fenêtre **Filtre de recherche**.

3. Saisissez dans le champ **De** le texte à chercher dans les adresses électroniques des destinataires des messages.

   > Vous pouvez saisir une adresse email (telle que example-email@example.com), un nom de domaine (tel que example.com) ou des caractères apparaissant dans une adresse électronique (tels que exa).

4. Saisissez dans le champ **A** le texte à chercher dans les adresses électroniques des destinataires des messages.

5. Saisissez dans le champ **Objet** le texte à chercher dans les en-têtes des messages.

6. Saisissez dans le champ **ID du message** le texte à chercher dans l'identifiant des messages sur le serveur de messagerie.

7. Sélectionnez dans la liste **ID de la Règle** l'identifiant de la règle selon laquelle les messages ont été traités.

8. Dans la liste **ID**, sélectionnez l'identificateur du message dans la Sauvegarde.

9. Sélectionnez dans la liste **Intervalle** l'intervalle qui s'est écoulé entre le traitement du message et le placement de sa copie dans la Sauvegarde.

Vous pouvez sélectionner l'un des intervalles suivants :

- **Heure**.
- **Jour**.
- **Semaine**.
- **2 semaines**.
- **Mois**.
- **3 mois**.
- **Année**.
- **Personnalisé**.

10. Si vous avez sélectionné l'intervalle **Personnalisé**, procédez comme suit :

    a. Indiquez dans les champs **début** la date et l'heure de début de l'intervalle de la recherche.

    b. Indiquez dans les champs **fin** la date et l'heure de fin de l'intervalle de la recherche.

11. Dans le groupe de paramètres **Type d'analyse**, cochez les cases en regard des modules de Kaspersky Secure Mail Gateway à l'origine du placement des messages dans la Sauvegarde sur la base des résultats de l'analyse.

    Vous pouvez sélectionner un ou plusieurs modules :

- **Anti-spam**.
- **Antivirus**.
- **Filtrage de contenu**.
- **Anti-phishing**.
- **Liste noire d'adresses personnelles**.
- **Authentification**.

- **Protection KATA**.

12. Dans le groupe de paramètres **Taille du message (Ko)**, indiquez une restriction des recherches en fonction de la taille des messages en kilo-octets.

    Vous pouvez sélectionner l'une des restrictions suivantes :

    - **Inférieur ou égal à** la taille indiquée en kilo-octets.
    - **Supérieur ou égal à** la taille indiquée en kilo-octets.

13. Cliquez sur le bouton **OK**.

Les copies de messages correspondant aux paramètres de la recherche s'affichent dans la liste des copies de messages, dans la section **Sauvegarde**.

Affichage des informations relatives au message dans la Sauvegarde

► *Pour voir les informations relatives au message dans la Sauvegarde, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Sauvegarde** dans l'arborescence de la console de gestion.

2. Dans la liste des copies des messages de la Sauvegarde, dans la partie inférieure de l'espace de travail, sélectionnez une des actions suivantes :

    - Sur la ligne d'information correspondant au message à consulter, cliquez sur un des liens **De**, **A** ou **Objet**.
    - Sur la ligne d'information correspondant au message à consulter, cochez la case et cliquez sur le bouton **Consulter**.

    La copie du message s'ouvre et affiche les informations suivantes :

    - **ID**.
    - **Objet**.

- **Message traité selon la règle**.
- **ID de la Règle**.
- **De**.
- **A**.
- **Copie**.
- **Copie cachée**.
- **Résultat de l'analyse** avec la liste des modules d'analyse **Anti-spam** , **Antivirus** , **Filtrage du contenu** , **Anti-phishing** , **Authentification** et **Protection KATA** .
- **Motif du placement dans la Sauvegarde**.
- **Action**.
- **Heure de placement dans la Sauvegarde**.
- **ID du message sur le serveur de messagerie**.
- **Taille du message**.
- **Heure d'envoi**.
- **Heure de réception**.
- **Pièces jointes**.
- **Virus**.
- **Date de publication des bases antivirus**.
- **Date de publication des bases de l'Anti-spam**.

3. Pour revenir à la liste des copies des messages de la Sauvegarde, cliquez sur le bouton **Liste des messages** dans la partie supérieure de l'espace de travail.

Remise des messages de la Sauvegarde aux destinataires

Si vous estimez qu'un message de la Sauvegarde ne présente pas de danger, vous pouvez le remettre à ses destinataires.

Vous pouvez remettre le message depuis la Sauvegarde après l'avoir consulté (cf. section "Consultation des informations relatives aux messages dans la Sauvegarde" à la page 179) ou après avoir sélectionné les messages que vous voulez envoyer dans la liste des copies de messages de la Sauvegarde (un ou plusieurs messages).

La remise de messages infectés peut compromettre la sécurité des ordinateurs des destinataires.

Avant de remettre un message infecté à un destinataire, assurez-vous que la remise de messages infectés est autorisée dans les paramètres de la Sauvegarde (cf. section "Configuration des paramètres de la Sauvegarde" à la page 175) (pour les comptes utilisateur personnels et le compte utilisateur HelpDesk).

► *Pour livrer un message de la Sauvegarde à ses destinataires, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Sauvegarde** dans l'arborescence de la console de gestion.

2. Dans la liste des copies des messages de la Sauvegarde, située dans la partie inférieure de l'espace de travail, cochez les cases sur les lignes d'information correspondant aux messages à envoyer.

3. Si vous souhaitez consulter les informations sur un message, cliquez sur le bouton **Consulter** dans la partie inférieure de l'espace de travail, sur la ligne contenant les informations sur le message que vous souhaitez consulter.

   La copie du message s'affiche.

4. Cliquez sur le bouton **Envoyer** dans la partie supérieure de l'espace de travail.

   La fenêtre **Envoyer le message** s'ouvre.

5. Cochez la case en regard du paramètre **Remettre le message en tant que pièce jointe** si vous voulez remettre le message en tant que pièce jointe.

6. Cochez la case en regard du paramètre **A l'adresse email des destinataires dans l'en-tête du message** pour envoyer le message à l'adresse électronique de ses destinataires d'origine.

7. Cochez la case en regard du paramètre **A d'autres adresses emails** pour envoyer le message à d'autres adresses électroniques.

8. Si vous avez opté pour la remise d'un message à des adresses email additionnelles, saisissez dans le champ **A d'autres adresses emails** situé sous le paramètre les adresses email auxquelles vous souhaitez envoyer le message.

9. Cliquez sur le bouton **OK**.

   La fenêtre **Envoyer le message** se ferme.

   Le message est placé dans la file d'attente des envois.

10. Pour revenir à la liste des copies des messages de la Sauvegarde, cliquez sur le bouton **Liste des messages** dans la partie supérieure de l'espace de travail.

    Dans la liste des copies des messages de la Sauvegarde, l'entrée **Le message a été placé dans la file d'attente pour envoi** s'affiche.

11. Pour masquer la notification **Le message a été placé dans la file d'attente pour envoi**, cliquez sur le lien **Cacher** à droite de la ligne de la notification.

Enregistrement d'un message de la sauvegarde dans un fichier

Si vous estimez qu'un message de la Sauvegarde ne présente pas de danger, vous pouvez l'enregistrer dans un fichier sur le disque dur.

Vous pouvez enregistrer le message depuis la Sauvegarde après l'avoir consulté (cf. section "Consultation des informations relatives aux messages dans la Sauvegarde" à la page 179)

ou après avoir marqué le message que vous voulez enregistrer dans la liste des copies de messages de la Sauvegarde.

L'enregistrement de messages infectés sur un disque dur peut compromettre la sécurité de l'ordinateur.

► *Pour enregistrer un message de la Sauvegarde, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Sauvegarde** dans l'arborescence de la console de gestion.

2. Dans la liste des copies des messages de la Sauvegarde, située dans la partie inférieure de l'espace de travail, cochez la case sur la ligne d'information correspondant au message à enregistrer.

3. Si vous souhaitez consulter les informations sur un message, cliquez sur le bouton **Consulter** dans la partie inférieure de l'espace de travail, sur la ligne contenant les informations sur le message que vous souhaitez consulter.

   La copie du message s'affiche.

4. Cliquez sur le bouton **Enregistrer** dans la partie supérieure de l'espace de travail.

   Le message est enregistré sur le disque dur de l'ordinateur dans le répertoire qui a été désigné comme répertoire de téléchargement des fichiers Internet dans les paramètres du navigateur que vous utilisez avec Kaspersky Secure Mail Gateway.

   Par exemple, si vous avez un système d'exploitation Microsoft Windows® et que le répertoire Downloads est indiqué dans les paramètres de votre navigateur comme répertoire de téléchargement des fichiers Internet, le message est enregistré dans le dossier Downloads sur le disque dur de votre ordinateur.

5. Pour revenir à la liste des copies des messages de la Sauvegarde, cliquez sur le bouton **Liste des messages** dans la partie supérieure de l'espace de travail.

Suppression des copies de messages de la Sauvegarde

Vous pouvez supprimer une copie d'un message depuis la Sauvegarde après l'avoir consulté (cf. section "Consultation des informations relatives aux messages dans la Sauvegarde" à la page 179) ou après avoir sélectionné les messages que vous voulez supprimer dans la liste des copies de messages de la Sauvegarde (un ou plusieurs messages).

► *Pour supprimer un ou plusieurs messages de la Sauvegarde, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Sauvegarde** dans l'arborescence de la console de gestion.

2. Dans la liste des copies des messages de la Sauvegarde, située dans la partie inférieure de l'espace de travail, cochez les cases sur les lignes d'information correspondant aux messages à supprimer.

3. Si vous souhaitez consulter les informations sur un message, cliquez sur le bouton **Consulter** dans la partie inférieure de l'espace de travail, sur la ligne contenant les informations sur le message que vous souhaitez consulter.

   La copie du message s'affiche.

4. Cliquez sur le bouton **Supprimer** dans la partie supérieure de l'espace de travail.

5. La fenêtre **Suppression de messages** s'ouvre.

6. Cliquez sur le bouton **Supprimer** dans la fenêtre **Suppression de messages**.

   La copie du message est supprimée de la Sauvegarde.

7. Pour revenir à la liste des copies des messages de la Sauvegarde, cliquez sur le bouton **Liste des messages** dans la partie supérieure de l'espace de travail.

   Dans la liste des copies des messages de la Sauvegarde, l'enregistrement **Le message marqué a été supprimé** s'affiche.

8. Pour masquer la notification **Le message marqué a été supprimé**, cliquez sur le lien **Cacher** à droite de la ligne de la notification.

File d'attente de messages de Kaspersky Secure Mail Gateway

Cette section fournit des informations sur l'utilisation des files d'attente de messages de Kaspersky Secure Mail Gateway ainsi que sur la marche à suivre pour trier et filtrer les messages dans les files d'attente de messages, dans la quarantaine KATA et la quarantaine de l'Anti-Spam. Elle explique également comment rechercher des événements dans plusieurs colonnes du tableau selon les utilisateurs que vous avez choisis.

Dans cette section

Activation et désactivation de l'envoi et de la réception de messages

► *Pour activer l'envoi et la réception de messages par l'agent de messagerie de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **File d'attente des messages** dans l'arborescence de la console de gestion.

2. la partie supérieure de l'espace de travail, exécutez l'une des opérations suivantes :

   - Activez le commutateur en regard du nom du paramètre **Envoi de messages** si vous voulez autoriser l'envoi de messages via l'agent de messagerie de Kaspersky Secure Mail Gateway.

   - Désactivez le commutateur à côté du nom du paramètre **Envoi de messages** si vous voulez interdire l'envoi des messages par l'agent postal Kaspersky Secure Mail Gateway.

     Si dans les paramètres avancés du MTA (cf. section "Configuration des paramètres étendus du MTA" à la page 226) le paramètre `Refuser les messages destinés à des adresses qui n'ont pas été vérifiées (reject_unverified_recipient)` est sélectionné, la réception des messages est également désactivée.

   - Activez le commutateur en regard du nom du paramètre **Réception de messages** si vous voulez autoriser la réception des messages par l'agent de messagerie de Kaspersky Secure Mail Gateway.

   - Désactivez le commutateur en regard du nom du paramètre **Réception de messages** si vous voulez interdire la réception des messages par l'agent de messagerie de Kaspersky Secure Mail Gateway.

Attention ! Ces paramètres déterminent l'envoi et la réception de messages par l'agent de messagerie de Kaspersky Secure Mail Gateway.

Consultation des informations sur la file d'attente de messages, la quarantaine KATA et la quarantaine de l'Anti-Spam

► *Pour consulter les informations sur la file d'attente de messages de la quarantaine KATA et de la quarantaine de l'Anti-spam,*

sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **File d'attente des messages** dans l'arborescence de la console de gestion.

Les informations suivantes s'affichent :

- **Quarantaine KATA (taille)**. Taille de la quarantaine KATA et pourcentage d'utilisation de celle-ci par rapport au volume maximal défini dans les paramètres de la protection KATA (cf. section "Protection KATA et intégration de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform" à la page 324).
- **Quarantaine KATA (messages)**. Quantité actuelle de messages dans la quarantaine KATA.
- **Vérifiés dans KATA (messages)**. Quantité de messages analysés dans KATA au cours de la dernière heure.
- **Délai d'attente de KATA écoulé (messages)**. Quantité de messages dont la durée d'attente de l'analyse dans KATA a expiré au cours de la dernière heure. La durée d'attente maximale de l'analyse dans KATA est définie dans les paramètres de la protection KATA (cf. section "Protection KATA et intégration de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform" à la page 324).
- **Quarantaine de l'Anti-spam (taille)**. Taille de la quarantaine de l'Anti-spam et pourcentage d'utilisation de celle-ci par rapport au volume maximal autorisé d'après les paramètres de la quarantaine de l'Anti-spam (cf. section "Quarantaine de l'Anti-spam" à la page 301)
- **Quarantaine de l'Anti-spam (messages)**. Quantité actuelle de messages dans la quarantaine de l'Anti-spam.
- **File d'attente MTA (messages)**. Quantité total de messages actuellement dans la file d'attente.

Tri des messages de la file d'attente

► Pour trier *les messages dans la file d'attente*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **File d'attente des messages** dans l'arborescence de la console de gestion.

   Le tableau des messages de la file d'attente de messages de la quarantaine KATA ou de la quarantaine de l'Anti-spam s'ouvre.

2. Cliquez sur le bouton à gauche du nom de la colonne selon laquelle vous souhaitez trier les messages. Vous pouvez trier les messages selon un des paramètres suivants :

   - **ID du message dans la file d'attente** : ID des messages de la file d'attente.
   - **De** : adresse de l'expéditeur des messages.
   - **A** : adresse du destinataire des messages.
   - **Taille** : taille des messages.
   - **Reçu** : heure d'entrée des messages dans la file d'attente.
   - **Erreur** : erreur d'analyse des messages.

► *Pour modifier l'ordre du tri des messages dans la file d'attente,*

cliquez sur le bouton ou à gauche du nom de la colonne du tableau dont vous souhaitez changer l'ordre.

Filtrage et recherche de message selon le nom de la file d'attente

► Pour filtrer ou trouver des messages en fonction du *nom de la file d'attente*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **File d'attente des messages** dans l'arborescence de la console de gestion.

2. Cliquez sur lien **File d'attente** pour développer la liste des noms de files d'attente.
3. Cochez les cases en regard des noms des files d'attente dans lesquelles vous souhaitez trouver les messages. Vous pouvez choisir un ou plusieurs des files d'attente suivantes :
   - **Deferred**.
   - **Active**.
   - **Inbound (Files d'attente Maildrop et Incoming)**.
   - **Hold**.
   - **Quarantaine de l'Anti-spam**.
   - **Quarantaine KATA**.
4. Cliquez sur le bouton **Appliquer**.

Dans l'espace de travail de la section **File d'attente des messages** de la fenêtre de l'interface Web de Kaspersky Secure Mail Gateway, la liste des messages composée d'après les critères de filtrage s'affiche.

Si aucun filtre n'avait été défini, la liste reprend tous les messages de la file d'attente.

Filtrage et recherche de message selon l'ID du message dans la file d'attente

► Pour filtrer ou trouver des messages selon *ID du message dans la file d'attente*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **File d'attente des messages** dans l'arborescence de la console de gestion.
2. Cliquez sur le lien **ID du message dans la file d'attente** pour ouvrir la fenêtre de la configuration du filtrage des messages.

3. Saisissez dans le champ **ID** quelques caractères ou tous les caractères de l'ID du message dans la file d'attente.

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

Dans l'espace de travail de la section **File d'attente des messages** de la fenêtre de l'interface Web de Kaspersky Secure Mail Gateway, la liste des messages composée d'après les critères de filtrage s'affiche.

Si aucun filtre n'avait été défini, la liste reprend tous les messages de la file d'attente.

Filtrage et recherche des messages selon l'adresse de l'expéditeur des messages

► Pour filtrer ou trouver des messages en fonction de *l'adresse de l'expéditeur du message*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **File d'attente des messages** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **De** pour ouvrir la fenêtre de la configuration du filtrage des messages.

3. Saisissez dans le champ **De** quelques caractères ou tous les caractères de l'adresse de l'expéditeur du message.

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

Dans l'espace de travail de la section **File d'attente des messages** de la fenêtre de l'interface Web de Kaspersky Secure Mail Gateway, la liste des messages composée d'après les critères de filtrage s'affiche.

Si aucun filtre n'avait été défini, la liste reprend tous les messages de la file d'attente.

Filtrage et recherche des messages selon l'adresse du destinataire des messages

► Pour filtrer ou trouver des messages en fonction de *l'adresse du destinataire du message*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **File d'attente des messages** dans l'arborescence de la console de gestion.
2. Cliquez sur le lien **A** pour ouvrir la fenêtre de la configuration du filtrage des messages.
3. Saisissez dans le champ **A** quelques caractères ou tous les caractères de l'adresse du destinataire du message.
4. Cliquez sur le bouton **Appliquer**.

Dans l'espace de travail de la section **File d'attente des messages** de la fenêtre de l'interface Web de Kaspersky Secure Mail Gateway, la liste des messages composée d'après les critères de filtrage s'affiche.

Si aucun filtre n'avait été défini, la liste reprend tous les messages de la file d'attente.

Filtrage et recherche des messages selon l'heure d'arrivée du message dans la file d'attente

► Pour filtrer ou trouver des messages selon *l'heure d'entrée du message dans la file d'attente*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **File d'attente des messages** dans l'arborescence de la console de gestion.
2. Cliquez sur le lien **Reçu** pour développer la liste des intervalles de recherche de messages.
3. Sélectionnez un des intervalles suivants :

- **Dernière heure**.
- **Dernier jour**.
- **Dernière semaine**.
- **Personnalisé**.

4. Si vous avez choisi l'intervalle défini par l'utilisateur pour la recherche des messages, procédez comme suit :

    a. Dans le calendrier qui s'ouvre, indiquez la date de début et la date de fin de la période d'entrée des messages dans la file d'attente.

    b. Cliquez sur le bouton **Appliquer**.

    Le calendrier se referme.

Dans l'espace de travail de la section **File d'attente des messages** de la fenêtre de l'interface Web de Kaspersky Secure Mail Gateway, la liste des messages composée d'après les critères de filtrage s'affiche.

Si aucun filtre n'avait été défini, la liste reprend tous les messages de la file d'attente.

Envoi forcé et suppression de messages de la file d'attente

Pour forcer l'envoi ou la suppression de messages de la file d'attente de l'agent MTA, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **File d'attente des messages** dans l'arborescence de la console de gestion.
2. Consultez la liste des messages de la file d'attente dans l'espace de travail.
3. A gauche du nom du type de file d'attente, cochez la case en regard des messages que vous souhaitez traiter.

4. Cliquez sur l'un des boutons suivants dans la barre d'outil de la partie supérieure de l'espace de travail :

   - **Envoyer** si vous souhaitez forcer l'envoi des messages sélectionnés.
   - **Tout envoyer** si vous souhaitez forcer l'envoi de tous les messages.

Les tentatives fréquentes au sein d'une file d'attente d'envoyer des messages qui ne peuvent être remis ont un impact négatif sur la vitesse d'envoi des autres messages.

   - **Supprimer** si vous souhaitez supprimer les messages sélectionnés.
   - **Tout supprimer** si vous souhaitez supprimer tous les messages.

La suppression de tous les messages de la file d'attente est définitive et porte sur toutes les données de la file d'attente, y compris les messages reçus, mais non encore traités.

Lors de l'envoi forcé des messages de la file d'attente **Quarantaine KATA**, les messages sont de toute façon analysés dans Kaspersky Anti Targeted Attack Platform mais Kaspersky Secure Mail Gateway n'attend pas le résultat de l'analyse de ceux-ci. Ces messages n'apparaissent pas dans la file d'attente d'analyse.

Voir également

Rapports sur le fonctionnement de Kaspersky Secure Mail Gateway

Cette section fournit des informations sur les rapports et explique comment créer et consulter les rapports sur le fonctionnement du serveur de messagerie.

Vous pouvez configurer les types de rapports suivants sur le fonctionnement du serveur de messagerie :

- **Quotidiens**.
- **Hebdomadaires**.
- **Mensuels**.
- **Personnalisé**.

Dans cette section

Contenu des rapports sur le fonctionnement de Kaspersky Secure Mail Gateway

Il est possible d'obtenir des informations sur les résultats du fonctionnement de Kaspersky Secure Mail Gateway pendant une période déterminée grâce aux rapports de Kaspersky Secure Mail Gateway.

Ces rapports contiennent les informations suivantes sur le fonctionnement de Kaspersky Secure Mail Gateway :

1. Rapport global sur les détections. Le rapport sur les résultats du fonctionnement des modules de Kaspersky Secure Mail Gateway reprend le nombre et le volume de messages répartis selon les catégories suivantes :

- Détectés dans KATA.
- Détectés par le module Antivirus.
- Détectés par le module Anti-phishing.
- Détectés par le module Anti-spam.
- Violations de l'authentification des expéditeurs.
- Traités par le module du filtrage du contenu.
- Propres.
- Non analysés.
- Total des messages.

2. Rapport total sur les actions exécutées par Kaspersky Secure Mail Gateway sur les messages. Affiche la quantité et le volume de messages comptés selon les paramètres suivants :

   - Messages remis, y compris les types suivants :
     - Propres.
     - Désinfectés.
     - Avec pièces jointes supprimées.
     - Ignorés.
     - Non analysés.
   - Messages non remis, y compris les types suivants :
     - Supprimés.
     - Rejeter.
     - Reportés.
   - Total des messages.

3. Rapport sur les détections du module Antivirus. Affiche la quantité de messages analysés et non analysés par le module Antivirus pour la période définie et contient les statistiques de détection des messages des types suivants :
    - Propres.
    - Infectés.
    - Cryptés.
    - Erreurs d'analyse.
    - Les messages non vérifiés pour une ou plusieurs des raisons suivantes :
        - Exclus de l'analyse sur la base des règles de contrôle des listes noire ou blanche globales.
        - Exclus de l'analyse sur la base des règles du traitement des listes noire ou blanche personnalisées.
        - Recherche de virus désactivée pour tous les messages.
        - Recherche de virus désactivée pour la règle qui a traité le message.
        - Absence des bases antivirus.
        - Problèmes de licence.
4. Rapport sur les détections du module Anti-spam. Affiche la quantité de messages analysés et non analysés par le module Anti-spam pour la période définie et contient les statistiques de détection des messages des types suivants :
    - Courrier normal.
    - Courrier indésirable.
    - Courrier potentiellement indésirable.
    - Message d'un expéditeur douteux.
    - Diffusion massive.
    - Erreurs d'analyse.

De plus, le nombre de messages dans la quarantaine de l'Anti-spam et le nombre de message non vérifiés s'affiche.

5. Rapport sur les détections du module Anti-phishing. Affiche la quantité de messages analysés et non analysés par le module Anti-phishing pour la période définie et contient les statistiques de détection des messages des types suivants :

   - Pas de phishing.
   - Phishing.
   - Adresse Internet malveillante.
   - Erreurs d'analyse.

   De plus, le nombre de messages non analysés s'affiche.

6. Rapport sur les résultats du filtrage du contenu des messages. Reprend le nombre de messages traités selon les règles du filtrage du contenu pour la période indiquée et classés selon les catégories suivantes :

   - Messages sans violations.
   - Messages dépassant la taille autorisée.
   - Messages contenant une pièce jointe dont le nom est interdit.
   - Messages contenant une pièce jointe de type interdit.

   De plus, le nombre de messages non analysés s'affiche.

7. Rapport sur les règles de traitement des messages appliquées (cf. section "Application des règles de traitement des messages" à la page 128).

8. Rapport sur les dix sources principales de courrier indésirable. Reprend les adresses des sources et la quantité de déclenchements du module Anti-spam.

9. Rapport sur les dix adresses email qui ont reçu le plus de messages contenant du spam. Reprend les adresses email des destinataires des messages et le nombre de déclenchements du module Anti-spam.

10. Rapport sur les dix sources principales d'objets malveillants selon les conclusions du module Anti-virus. Reprend les adresses des sources et la quantité de déclenchements du module Antivirus.

11. Rapport sur les dix adresses email qui ont reçu le plus de d'objets malveillants selon les conclusions du module Antivirus. Reprend les adresses des destinataires et la quantité de déclenchements du module Antivirus.

12. Rapport sur les dix principaux objets malveillants selon les conclusions du module Antivirus. Reprend les noms des objets et le nombre de déclenchements du module Antivirus.

Consultation des rapports sur le fonctionnement de Kaspersky Secure Mail Gateway

► Pour consulter les rapports sur le fonctionnement de *Kaspersky Secure Mail Gateway*, procédez comme suit :

1. Dans l'arborescence de la console de gestion affichée dans la fenêtre principale de l'interface Web de l'application, choisissez la section **Rapports**, puis la sous-section en fonction du type de rapport que vous souhaitez consulter :

   - **Tous les rapports**, si vous souhaitez consulter tous les rapports.
   - **Quotidiens**, si vous souhaitez consulter les rapports quotidiens.
   - **Hebdomadaires**, si vous souhaitez consulter les rapports hebdomadaire.
   - **Mensuels**, si vous souhaitez consulter les rapports mensuels.
   - **Personnalisé**, si vous souhaitez consulter les rapports personnalisés.

   Une page reprenant les rapports du type que vous avez choisi s'ouvre.

2. Cliquez sur le lien **PDF** sur le lien contenant les informations relatives au rapport que vous souhaitez consulter.

Le rapport sera enregistré sur le disque dur de l'ordinateur, dans le répertoire qui a été indiqué comme répertoire de téléchargement des fichiers Internet dans les paramètres du navigateur que vous utilisez avec Kaspersky Secure Mail Gateway.

Par exemple, si vous avez un système d'exploitation Microsoft Windows et que le répertoire Downloads est indiqué dans les paramètres de votre navigateur comme répertoire de téléchargement des fichiers Internet, le message est enregistré dans le dossier Downloads sur le disque dur de votre ordinateur.

Suppression des rapports sur le fonctionnement de Kaspersky Secure Mail Gateway

► Pour supprimer un ou plusieurs rapports sur le fonctionnement de *Kaspersky Secure Mail Gateway*, procédez comme suit :

1. Dans l'arborescence de la console affichée dans la fenêtre principale de l'interface Web de l'application, choisissez la section **Rapports**, puis la sous-section en fonction du type de rapport que vous souhaitez supprimer :

   - **Tous les rapports** si vous souhaitez supprimer tous les rapports de la liste.
   - **Quotidiens** si vous souhaitez supprimer les rapports quotidiens du rapport.
   - **Hebdomadaires** si vous souhaitez supprimer les rapports hebdomadaires de la liste.
   - **Mensuels** si vous souhaitez supprimer les rapports mensuels de la liste.
   - **Personnalisé** si vous souhaitez supprimer les rapports personnalisés.

   Une page reprenant les rapports du type que vous avez choisi s'ouvre.

2. Cochez les cases en regard des lignes qui reprennent les informations relatives aux rapports que vous souhaitez supprimer.

3. Cliquez sur le bouton **Supprimer** situé dans la partie supérieure de l'espace de travail.

   La fenêtre de confirmation de l'opération **Suppression de rapports** s'ouvre.

4. Cliquez sur le bouton **Supprimer**.

   La fenêtre **Suppression de rapports** se ferme.

Les rapports que vous aurez sélectionnés seront supprimés.

Activation et désactivation de la création de rapports quotidiens

► *Pour activer ou désactiver la création de rapports quotidiens sur le fonctionnement de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Rapports** puis la sous-section **Quotidiens** dans l'arborescence de la console de gestion.

2. Dans le groupe **Création d'un rapport quotidien**, exécutez l'une des actions suivantes :

   - Activez l'interrupteur en regard du nom du groupe **Création d'un rapport quotidien** si vous souhaitez activer la création de rapports hebdomadaires sur le fonctionnement de Kaspersky Secure Mail Gateway.

   - Désactivez l'interrupteur en regard du nom du groupe **Création d'un rapport quotidien** si vous souhaitez désactiver la création de rapports hebdomadaires sur le fonctionnement de Kaspersky Secure Mail Gateway.

Configuration des paramètres du rapport quotidien

► *Pour configurer les paramètres du rapport quotidien sur le fonctionnement de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Rapports** puis la sous-section **Quotidiens** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe quel lien du groupe **Création d'un rapport quotidien** pour ouvrir la fenêtre **Paramètres du rapport quotidien**.

3. Définissez l'heure de création du rapport quotidien dans le champ **Heure de création du rapport**.

   Saisissez une heure comprise entre 00h00 et 23h59.

4. La liste **Langue du rapport** permet de choisir la langue de rédaction du rapport quotidien.

5. Choisissez le format d'affichage des dates du rapport quotidien dans le champ **Format des dates dans le rapport**.

6. Si vous souhaitez que Kaspersky Secure Mail Gateway envoie le rapport quotidien à une adresse email, cochez la case en regard du paramètre **Envoyer le rapport** et procédez comme suit :

   a. Cochez la case en regard du paramètre **Envoyer le rapport à l'administrateur** si vous souhaitez que Kaspersky Secure Mail Gateway envoie le rapport quotidien à l'adresse email de l'administrateur de Kaspersky Secure Mail Gateway.

   b. Saisissez dans le champ **Envoyer le rapport aux adresses email suivantes** l'adresse email pour laquelle vous souhaitez configurer l'envoi du rapport quotidien.

   > Les adresses électroniques sont saisies une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses électroniques.

   Vous pouvez utiliser les caractères "*" et "?" pour créer des masques d'adresses ainsi que des expressions régulières en utilisant le préfixe "re:".

   > Les expressions régulières ne respectent pas la casse.

   c. Cliquez sur le bouton  situé à droite du champ.

   La nouvelle adresse email apparaît dans la liste reprise sous le champ de saisie.

7. Cliquez sur le bouton **OK**.

   La fenêtre **Paramètres du rapport quotidien** se ferme.

Le groupe **Création d'un rapport quotidien** reprend les valeurs que vous avez attribuées aux paramètres du rapport quotidien sur le fonctionnement de Kaspersky Secure Mail Gateway.

Les rapports de fonctionnement de Kaspersky Secure Mail Gateway générés sont repris dans une liste sous le groupe **Création d'un rapport quotidien**.

Activation et désactivation de la création de rapports hebdomadaires

► *Pour activer ou désactiver la création de rapports hebdomadaires sur le fonctionnement de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Rapports** puis la sous-section **Hebdomadaires** dans l'arborescence de la console de gestion.

2. Dans le groupe **Création d'un rapport hebdomadaire**, exécutez l'une des actions suivantes :

   - Activez le commutateur en regard du nom du groupe **Création d'un rapport hebdomadaire** si vous souhaitez activer la création de rapports hebdomadaires sur le fonctionnement de Kaspersky Secure Mail Gateway.

   - Désactivez le commutateur en regard du nom du groupe **Création d'un rapport hebdomadaire** si vous souhaitez désactiver la création de rapports hebdomadaires sur le fonctionnement de Kaspersky Secure Mail Gateway.

Configuration des paramètres du rapport hebdomadaire

► *Pour configurer les paramètres du rapport hebdomadaire sur le fonctionnement de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Rapports** puis la sous-section **Hebdomadaires** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe quel lien du groupe **Création d'un rapport hebdomadaire** pour ouvrir la fenêtre **Paramètres du rapport hebdomadaire**.

3. Sélectionnez le jour de la semaine et l'heure de création du rapport hebdomadaire dans les champs **Jour et heure de création du rapport**.

   Saisissez une heure comprise entre 00h00 et 23h59.

4. La liste **Langue du rapport** permet de choisir la langue dans laquelle le rapport hebdomadaire sera rédigé.

5. Choisissez le format d'affichage des dates du rapport hebdomadaire dans le champ **Format des dates dans le rapport**.

6. Si vous souhaitez que Kaspersky Secure Mail Gateway envoie le rapport hebdomadaire à une adresse email, cochez la case en regard du paramètre **Envoyer le rapport** et procédez comme suit :

   a. Cochez la case en regard du paramètre **Envoyer le rapport à l'administrateur** si vous souhaitez que Kaspersky Secure Mail Gateway envoie le rapport hebdomadaire à l'adresse email de l'administrateur de Kaspersky Secure Mail Gateway.

   b. Saisissez dans le champ **Envoyer le rapport aux adresses email suivantes** l'adresse email pour laquelle vous souhaitez configurer l'envoi du rapport hebdomadaire.

   > Les adresses électroniques sont saisies une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses électroniques.

   Vous pouvez utiliser les caractères "*" et "?" pour créer des masques d'adresses ainsi que des expressions régulières en utilisant le préfixe "re:".

   > Les expressions régulières ne respectent pas la casse.

   c. Cliquez sur le bouton  situé à droite du champ.

   La nouvelle adresse email apparaît dans la liste reprise sous le champ de saisie.

7. Cliquez sur le bouton **OK**.

La fenêtre **Paramètres du rapport hebdomadaire** se ferme.

Le groupe **Création d'un rapport hebdomadaire** reprend les valeurs que vous avez attribuées aux paramètres du rapport hebdomadaire sur le fonctionnement de Kaspersky Secure Mail Gateway.

Les rapports de fonctionnement de Kaspersky Secure Mail Gateway générés seront affichés dans une liste sous le groupe **Création d'un rapport hebdomadaire**.

Activation et désactivation de la création de rapports mensuels

► *Pour activer ou désactiver la création de rapports mensuels sur le fonctionnement de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Rapports** puis la sous-section **Mensuels** dans l'arborescence de la console de gestion.

2. Dans le groupe **Création d'un rapport mensuel**, exécutez l'une des actions suivantes :

   - Activez le commutateur en regard du nom du groupe **Création d'un rapport mensuel** si vous souhaitez activer la création de rapports mensuels sur le fonctionnement de Kaspersky Secure Mail Gateway.

   - Désactivez le commutateur en regard du nom du groupe **Création d'un rapport mensuel** si vous souhaitez désactiver la création de rapports mensuels sur le fonctionnement de Kaspersky Secure Mail Gateway.

Configuration des paramètres du rapport mensuel

► *Pour configurer les paramètres du rapport mensuel sur le fonctionnement de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Rapports** puis la sous-section **Mensuels** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe quel lien du groupe **Création d'un rapport mensuel** pour ouvrir la fenêtre **Paramètres du rapport mensuel**.

3. Sélectionnez le jour du mois et l'heure de création du rapport mensuel dans les champs **Jour du mois et heure de création du rapport**.

   Saisissez une heure comprise entre 00h00 et 23h59.

4. La liste **Langue du rapport** permet de choisir la langue de rédaction du rapport mensuel.

5. Choisissez le format d'affichage des dates du rapport mensuel dans le champ **Format des dates dans le rapport**.

6. Si vous souhaitez que Kaspersky Secure Mail Gateway envoie le rapport mensuel à une adresse email, cochez la case en regard du paramètre **Envoyer le rapport** et procédez comme suit :

   a. Cochez la case en regard du paramètre **Envoyer le rapport à l'administrateur** si vous souhaitez que Kaspersky Secure Mail Gateway envoie le rapport mensuel à l'adresse email de l'administrateur de Kaspersky Secure Mail Gateway.

   b. Saisissez dans le champ **Envoyer le rapport aux adresses email suivantes** l'adresse email pour laquelle vous souhaitez configurer l'envoi du rapport mensuel.

   > Les adresses électroniques sont saisies une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses électroniques.

   Vous pouvez utiliser les caractères "*" et "?" pour créer des masques d'adresses ainsi que des expressions régulières en utilisant le préfixe "re:".

   > Les expressions régulières ne respectent pas la casse.

   c. Cliquez sur le bouton  situé à droite du champ.

   La nouvelle adresse email apparaît dans la liste reprise sous le champ de saisie.

7. Cliquez sur le bouton **OK**.

   La fenêtre **Paramètres du rapport mensuel** se ferme.

Le groupe **Création d'un rapport mensuel** reprend les valeurs que vous avez attribuées aux paramètres du rapport mensuel sur le fonctionnement de Kaspersky Secure Mail Gateway.

Les rapports de fonctionnement de Kaspersky Secure Mail Gateway générés seront affichés dans une liste sous le groupe **Création d'un rapport mensuel**.

Création d'un rapport personnalisé

► *Pour créer un rapport personnalisé, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Rapports** puis la sous-section **Personnalisé** dans l'arborescence de la console de gestion.

2. Cliquez sur le bouton **Créer** situé dans la partie supérieure de l'espace de travail.

   La fenêtre **Paramètres du rapport personnalisé** s'ouvre.

3. Sélectionnez dans la liste **Période couverte par le rapport** la période que sera couverte par le rapport personnalisé, puis réalisez les opérations suivantes en fonction de l'option choisie :

   - Si vous avez décidé de créer un rapport pour un jour spécifique, saisissez la date de jour en question dans le champ **Jour**.

   - Si vous avez décidé de créer un rapport pour un mois spécifique, saisissez le mois en question dans le champ **Mois**.

   - Si vous avez décidé de créer un rapport pour une année spécifique, saisissez le mois en question dans le champ **Année**.

   - Si vous avez décidé de créer un rapport pour une plage de dates spécifique, saisissez les dates de début et de fin de la plage en question dans le champ **Plage de dates**.

4. La liste **Langue du rapport** permet de choisir la langue de rédaction du rapport personnalisé.

5. Choisissez le format d'affichage des dates du rapport personnalisé dans le champ **Format des dates dans le rapport**.

6. Si vous voulez que Kaspersky Secure Mail Gateway envoie le rapport personnalisé aux adresses email, procédez comme suit :

    a. Cochez la case en regard du paramètre **Envoyer le rapport à l'administrateur** si vous souhaitez que Kaspersky Secure Mail Gateway envoie le rapport personnalisé à l'adresse email de l'administrateur de Kaspersky Secure Mail Gateway.

    b. Saisissez dans le champ **Envoyer le rapport aux adresses email suivantes** l'adresse email pour laquelle vous souhaitez configurer l'envoi du rapport personnalisé.

    > Les adresses électroniques sont saisies une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses électroniques.

    Vous pouvez utiliser les caractères "*" et "?" pour créer des masques d'adresses ainsi que des expressions régulières en utilisant le préfixe "re:".

    > Les expressions régulières ne respectent pas la casse.

    c. Cliquez sur le bouton  situé à droite du champ.

    La nouvelle adresse email apparaît dans la liste reprise sous le champ de saisie.

7. Cliquez sur le bouton **OK**.

    La fenêtre **Paramètres du rapport personnalisé** se ferme.

Les rapports sur le fonctionnement de Kaspersky Secure Mail Gateway apparaissent dans la liste de l'espace de travail situé dans la fenêtre principale de l'interface Web de l'application.

Paramètres généraux de Kaspersky Secure Mail Gateway

Cette section fournit des informations sur la configuration des paramètres généraux de Kaspersky Secure Mail Gateway.

Dans cette section

Configuration des paramètres de connexion au serveur proxy

► *Pour configurer les paramètres de connexion au serveur proxy, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe quel lien du groupe **Utiliser un serveur proxy** pour ouvrir la fenêtre **Paramètres de connexion**.

3. Dans la liste déroulante **Utiliser un serveur proxy** du groupe de paramètres **Paramètres du serveur proxy**, sélectionnez une des options suivantes :

   - **Oui** pour activer un serveur proxy avec Kaspersky Secure Mail Gateway ;
   - **Non** pour désactiver un serveur proxy avec Kaspersky Secure Mail Gateway.

4. Dans le champ **Adresse**, saisissez l'adresse du serveur proxy.

5. Dans le champ **Port**, indiquez le numéro de port du serveur proxy.

6. Dans la liste déroulante **Authentification** du groupe de paramètres **Paramètres d'authentification**, sélectionnez une des options suivantes :

   - **Pas nécessaire** si vous ne souhaitez pas utiliser l'authentification pour vous connecter au serveur proxy.
   - **Simple** si vous souhaitez utiliser l'authentification pour vous connecter au serveur proxy.

7. Si vous avez choisi l'option **Simple** pour le paramètre **Authentification**, indiquez dans les champs **Nom d'utilisateur** et **Mot de passe** le nom d'utilisateur et le mot de passe permettant de se connecter au serveur proxy.

8. Dans la liste déroulante **Ne pas utiliser pour les adresses locales** du groupe de paramètres **Paramètres de connexion au serveur proxy**, sélectionnez une des options suivantes :

- **Oui** si vous ne souhaitez pas utiliser le serveur proxy pour les adresses email internes à votre entreprise ;
- **Non** pour utiliser le serveur proxy y compris pour les adresses email internes à votre entreprise.

9. Cliquez sur le bouton **OK**.

► *Pour activer ou désactiver l'utilisation du serveur proxy, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Mise à jour des bases** dans l'arborescence de la console de gestion.
2. Dans l'espace de travail, exécutez l'une des opérations suivantes :
   - Activez le commutateur en regard du groupe de paramètres **Utiliser un serveur proxy** pour utiliser un serveur proxy avec Kaspersky Secure Mail Gateway.
   - Désactivez le commutateur en regard du groupe de paramètres **Utiliser un serveur proxy** si vous ne souhaitez pas utiliser un serveur proxy avec Kaspersky Secure Mail Gateway.

Vous pouvez activer l'utilisation du serveur proxy seulement après la configuration des paramètres de connexion au serveur proxy.

Configuration des adresses électroniques de l'administrateur

► *Pour configurer les adresses électroniques de l'administrateur en vue de l'envoi de notifications, rapports et autres messages de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Adresse de l'administrateur** du groupe **Adresses emails** pour ouvrir la fenêtre **Adresse de l'administrateur**.

3. Saisissez dans le champ **Adresses électronique auxquelles Kaspersky Secure Mail Gateway envoie les notifications, les rapports et les messages depuis l'adresse de l'application** l'adresse email de l'administrateur.

   Les adresses électroniques sont saisies une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses électroniques.

   Vous pouvez utiliser les caractères "*" et "?" pour créer des masques d'adresses ainsi que des expressions régulières en utilisant le préfixe "re:".

   Les expressions régulières ne respectent pas la casse.

4. Cliquez sur le bouton **Ajouter** situé à droite du champ.

   La liste des adresses électroniques de l'administrateur apparaît sur la fenêtre sous le bouton d'ajout.

5. Cliquez sur le bouton **OK**.

6. La fenêtre **Adresse de l'administrateur** se ferme.

Les adresses électroniques sont affichées à droite du lien **Adresse de l'administrateur** de l'espace de travail dans la fenêtre principale de l'interface Web de l'application.

Configuration des paramètres du compte utilisateur HelpDesk

Cette section fournit des informations sur le compte utilisateur HelpDesk et la configuration de ses paramètres.

Dans cette section

A propos du compte HelpDesk

Le compte utilisateur HelpDesk est prévu pour octroyer un accès restreint aux paramètres de l'application. Le compte utilisateur HelpDesk permet à l'administrateur de Kaspersky Secure Mail Gateway d'octroyer à un autre utilisateur les autorisations requises pour réaliser certaines opérations, par exemple analyser des incidents qui impliquent des messages de la Sauvegarde.

Pour obtenir un accès à Kaspersky Secure Mail Gateway sous le compte utilisateur HelpDesk, procédez comme suit :

- Activer le compte utilisateur HelpDesk (cf. section "Activation et désactivation du compte utilisateur HelpDesk" à la page 215).
- Définir le nom d'utilisateur et le mot de passe (cf. section "Modification du nom et du mot de passe du compte utilisateur HelpDesk" à la page 216).

- Saisir les identifiants définis (cf. section "Prise en main de l'interface Web de l'application" à la page 104) sur la page d'ouverture d'autorisation de l'interface Web.

Une fois l'authentification terminée et à conditions de disposer des autorisations correspondantes, l'utilisateur HelpDesk peut réaliser les opérations suivantes dans Kaspersky Secure Mail Gateway :

- Consultation des informations relatives aux messages dans la Sauvegarde.
- Remise des messages de la Sauvegarde au destinataire.

  La valeur de ce paramètre est définie dans les paramètres de la Sauvegarde (cf. section "Configuration des paramètres de la Sauvegarde" à la page 175).
- Modification des listes noire et blanche définies par l'utilisateur.
- Opérations sur les rapports :
  - Consultation des rapports prêts ;
  - Enregistrement d'un rapport prêt sur le disque dur ;
  - Création ponctuelle d'un rapport selon des paramètres définis par l'utilisateur ;
  - Création régulière de rapports quotidiens, hebdomadaires et mensuels ;
  - Suppression des rapports sélectionnés dans la liste des rapports prêts ;
  - Modification des paramètres de génération de rapports pour les périodes passées selon une planification.

Activation et désactivation du compte utilisateur HelpDesk

► *Pour activer ou désactiver le compte utilisateur HelpDesk, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Dans le groupe **Activer le compte utilisateur HelpDesk**, exécutez l'une des actions suivantes :

   - Activez le commutateur en regard du nom du groupe de paramètres **Activer le compte utilisateur HelpDesk** si vous souhaitez activer le compte utilisateur HelpDesk.
   - Désactivez le commutateur en regard du nom du groupe de paramètres **Activer le compte utilisateur HelpDesk** si vous souhaitez désactiver le compte utilisateur HelpDesk.

Modification du nom et du mot de passe du compte utilisateur HelpDesk

► *Pour modifier le nom ou le mot de passe du compte utilisateur HelpDesk, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.
2. Cliquez sur n'importe quel lien du groupe **Activer le compte utilisateur HelpDesk** pour ouvrir la fenêtre **Paramètres du compte utilisateur HelpDesk**.
3. Dans le groupe **Nom d'utilisateur et mot de passe du compte utilisateur HelpDesk**, procédez comme suit :

   - Si vous voulez modifier le nom du compte utilisateur HelpDesk, saisissez un nouveau nom dans le champ **Nom d'utilisateur**.
   - Si vous voulez modifier le mot de passe du compte utilisateur HelpDesk, définissez un nouveau mot de passe dans le champ **Mot de passe** et confirmez-le dans le champ **Confirmation du mot de passe**.

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

   La fenêtre **Paramètres du compte utilisateur HelpDesk** se ferme.

Octroi de l'accès aux listes noire et blanche de l'utilisateur pour le compte utilisateur HelpDesk

► *Pour octroyer l'accès aux listes noire et blanche de l'utilisateur pour le compte utilisateur HelpDesk, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe quel lien du groupe **Activer le compte utilisateur HelpDesk** pour ouvrir la fenêtre **Paramètres du compte utilisateur HelpDesk**.

3. Dans la liste déroulante **Autoriser l'accès aux listes de l'utilisateur** du groupe **Droits du compte utilisateur HelpDesk**, choisissez l'option **Oui**.

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

   La fenêtre **Paramètres du compte utilisateur HelpDesk** se ferme.

Octroi de l'accès aux rapports pour le compte utilisateur HelpDesk

► *Pour octroyer l'accès aux rapports pour le compte utilisateur HelpDesk, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe quel lien du groupe **Activer le compte utilisateur HelpDesk** pour ouvrir la fenêtre **Paramètres du compte utilisateur HelpDesk**.

3. Dans la liste déroulante **Autoriser l'accès au rapport** du groupe **Droits du compte utilisateur HelpDesk**, choisissez l'option **Oui**.

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

La fenêtre **Paramètres du compte utilisateur HelpDesk** se ferme.

Modification du mot de passe du compte Administrator

► *Pour modifier le mot de passe du compte utilisateur Administrator, procédez comme suit :*

1. Dans le coin inférieur gauche de la fenêtre principale de l'interface Web de l'application, cliquez sur le lien **Administrator** pour ouvrir la fenêtre **Modifier le mot de passe pour {UserName}**.
2. Saisissez dans le champ **Ancien mot de passe** le mot de passe actuel du compte Administrator.
3. Saisissez dans le champ **Nouveau mot de passe** le nouveau mot de passe du compte Administrator.
4. Saisissez dans le champ **Confirmation du nouveau mot de passe** la confirmation du nouveau mot de passe du compte Administrator.
5. Cliquez sur le bouton **Modifier le mot de passe**.

La fenêtre **Modifier le mot de passe pour {UserName}** se ferme.

Configuration des paramètres du journal des événements et du journal d'audit

Il est possible de choisir une catégorie du journal des événements et d'indiquer le niveau de consignation dans ce journal.

Les événements sont consignés par défaut dans la catégorie *Mail* du journal et ils ont le niveau *Info*.

► *Pour configurer les paramètres du journal des événements et du journal d'audit, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe quel lien du groupe de paramètres **Paramètres du journal d'événement** pour ouvrir la fenêtre **Paramètres du journal d'événement**.

3. Dans la liste **Catégorie du journal des événements**, sélectionnez la catégorie du journal des événements.

4. Sélectionnez le niveau du journal des événements dans la liste **Degré d'importance** .

5. Dans la liste **Nombre maximum d'entrées dans le journal d'audit**, sélectionnez le nombre maximal d'enregistrements dans le journal d'audit.

   Le nombre d'enregistrements dans le journal d'audit est limité par défaut à 100 000. .Une fois cette limite atteinte, il y a une rotation du journal d'audit : Kaspersky Secure Mail Gateway écrase les enregistrements les plus anciens avec les nouvelles données.

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

Configuration des paramètres des performances de l'application

► *Pour configurer les paramètres des performances de l'application, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Nombre de flux de l'analyse** du groupe de paramètres **Paramètres de performance** pour ouvrir la fenêtre **Paramètres de performance**.

3. Dans la liste **Nombre de flux de l'analyse**, choisissez le nombre de flux de messages que Kaspersky Secure Mail Gateway peut analyser simultanément.

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

Configuration de l'aspect des messages analysés

► *Pour configurer l'aspect des messages analysés, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Ajouter les en-têtes des messages** du groupe de paramètres **Paramètres des messages** pour ouvrir la fenêtre **Paramètres des messages**.

3. Sélectionnez l'une des options suivantes dans la liste **Ajouter les en-têtes des messages** :

   - **Oui** si vous souhaitez ajouter des en-têtes aux messages analysés.

   - **Non** si vous ne souhaitez pas ajouter d'en-têtes aux messages analysés.

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

Configuration du modèle de messages en cas de suppression d'une pièce jointe

► *Pour configurer le modèle des messages en cas de suppression d'une pièce jointe, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **En cas de suppression d'une pièce jointe** du groupe de paramètres **Modèles** pour ouvrir la fenêtre **Modèles**.

3. Saisissez dans le champ **En cas de suppression d'une pièce jointe, insérer le texte suivant dans le corps du message** le texte que vous voulez ajouter aux messages dans lesquels Kaspersky Secure Mail Gateway supprime les pièces jointes.

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

Exportation des paramètres de l'application

► *Pour exporter les paramètres de l'application, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Enregistrer les paramètres** du groupe de paramètres **Importation et exportation des paramètres de l'application** pour ouvrir la fenêtre **Enregistrement des paramètres de l'application**.

3. Cliquez sur le bouton **OK**.

Un fichier au format KZ est chargé sur le disque dur de l'ordinateur, dans le répertoire qui a été indiqué comme répertoire de téléchargement des fichiers Internet dans les paramètres du navigateur que vous utilisez avec Kaspersky Secure Mail Gateway. Le fichier contient tous les paramètres actifs de l'application, y compris les règles du traitement des messages avec tous les destinataires et les expéditeurs.

Importation des paramètres de l'application

► *Pour importer les paramètres de l'application, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Charger les paramètres** du groupe de paramètres **Importation et exportation des paramètres de l'application** pour ouvrir la fenêtre **Chargement des paramètres de l'application**.

3. Cliquez sur le bouton **Parcourir**.

   La fenêtre de sélection des fichiers s'ouvre.

4. Choisissez le fichier au format KZ qui contient les paramètres de l'application que vous souhaitez charger.

5. Choisissez une des options suivantes pour l'importation des paramètres de l'application :

   - **Tous les paramètres** si vous souhaitez importer tous les paramètres de l'application.
   - **Paramètres sélectionnés** si vous souhaitez choisir les paramètres à importer.

6. Si vous importez **Paramètres sélectionnés**, cochez les cases en regard des paramètres de l'application que vous souhaitez importer.

7. Cliquez sur le bouton **Suivant**.

8. Si l'importation des paramètres de l'application réussit, cliquez sur le bouton **Redémarrer l'application**.

L'application est relancée. Quelques minutes plus tard, il faut rafraîchir la fenêtre du navigateur et ouvrir une autre session.

Relancement de l'application

► *Pour relancer l'application, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Voulez-vous redémarrer l'application** du groupe de paramètres **Importation et exportation des paramètres de l'application** pour ouvrir la fenêtre **Confirmation du relancement de l'application**.

3. Cliquez sur le bouton **OK**.

L'application est relancée. Quelques minutes plus tard, il faut rafraîchir la fenêtre du navigateur et ouvrir une autre session.

Configuration du paramètre d'intégration à Kaspersky Security Center

Une fois installé, Kaspersky Secure Mail Gateway transmet les informations qui le concernent à Kaspersky Security Center. Sur la base de ces informations, Kaspersky Security Center regroupe toutes les machines virtuelles Kaspersky Secure Mail Gateway dans un cluster. Ce cluster reçoit un nom. Vous pouvez configurer ce paramètre d'intégration à Kaspersky Security Center.

► *Pour configurer le paramètre d'intégration à Kaspersky Security Center, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Paramètres généraux** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Identificateur de cluster** du groupe de paramètres **Intégration à Kaspersky Security Center** pour ouvrir la fenêtre **Intégration à Kaspersky Security Center**.

3. Saisissez dans le champ **Définissez l'identificateur de cluster de Kaspersky Security Center** l'identifiant du cluster Kaspersky Security Center. Saisissez par exemple, Kaspersky Secure Mail Gateway.

Cliquez sur le bouton **OK**.

Configuration des paramètres du MTA

Kaspersky Secure Mail Gateway s'intègre à la structure de messagerie existante de l'organisation et ne fonctionne pas en tant que système de messagerie autonome. Par exemple, Kaspersky Secure Mail Gateway ne remet pas les messages électroniques aux destinataires et ne gère pas les comptes des utilisateurs.

Vous pouvez configurer les paramètres principaux du MTA à l'aide de l'Assistant de configuration rapide du MTA ou manuellement via l'interface Web de l'application.

Cette section contient des informations sur la configuration manuelle des paramètres du MTA.

Dans cette section

Configuration des paramètres principaux du MTA

Pour configurer les paramètres principaux du MTA, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **MTA** dans l'arborescence de la console de gestion.

2. Déployez le groupe **Paramètres principaux** si ce n'est pas encore fait.

3. Cliquez sur n'importe quel lien du groupe **Paramètres principaux** pour ouvrir la fenêtre **Paramètres principaux de MTA**.

4. Si vous voulez modifier le nom de domaine Kaspersky Secure Mail Gateway (mydomain), saisissez le nouveau nom de domaine du serveur de l'application dans le champ **Nom de domaine**.

5. Si vous voulez modifier le nom de domaine complet Kaspersky Secure Mail Gateway (myhostname), saisissez dans le champ **Nom d'hôte** le nouveau nom de domaine du serveur de l'application.

6. Indiquez dans le champ **Taille maximale du message** la taille maximale des messages électroniques reçus ou transmis par Kaspersky Secure Mail Gateway, en-tête SMTP compris. Indiquez la taille maximale octets.

   Saisissez 0 si aucune limite n'est nécessaire.

   Valeur par défaut : 2 0971 520 octet.

7. Créez la liste des réseaux de confiance et des nœuds du réseau autorisés à transférer les messages électroniques via Kaspersky Secure Mail Gateway (mynetworks). En règle générale, il s'agit des réseaux internes et des nœuds de réseau de votre organisation. Par exemple, vous pouvez indiquer l'adresse IP des serveurs Microsoft Exchange utilisés dans votre entreprise.

   > Si aucun réseau de confiance n'est renseigné, Kaspersky Secure Mail Gateway n'acceptera pas les messages en provenance des serveurs de messagerie uniques et ne les renverra pas au-delà des limites du réseau de votre organisation.

   Exécutez les actions suivantes pour chaque adresse que vous souhaitez ajouter :

   a. Saisissez dans le champ **Réseaux de confiance** l'adresse IP du réseau ou l'adresse du sous-réseau.

   Saisissez l'adresse IP au format IPv4 ou l'adresse du sous-réseau au format CIDR

   b. Cliquez sur le bouton **Ajouter**.

L'adresse IP du réseau ou l'adresse du sous-réseau que vous avez ajoutée apparaît dans la liste des réseaux et des nœuds de réseaux de confiance.

> Les adresses IP sont saisies une à une. Répétez les actions pour l'ajout d'adresses IP ou d'adresses de sous-réseau à la liste pour tous les réseaux et nœuds de réseaux de confiance à ajouter.

8. Saisissez dans le champ **Adresse de destination des messages** l'adresse de votre passerelle frontière (relayhost). Kaspersky Secure Mail Gateway renverra tous les messages à cette adresse.

   Vous pouvez saisir une adresse IPv4 (par exemple, 192.0.0.1 ou 192.0.0.0/16), un nom de domaine ou un nom FQDN.

   Si vous avez configuré le routage des emails pour des domaines distincts (cf. section "Domaines et configuration du routage des emails" à la page 146), Kaspersky Secure Mail Gateway redirige les messages électroniques vers les adresses indiquées pour chaque domaine.

9. Sélectionnez une des valeurs suivantes dans la liste **Recherche d'enregistrements MX** :

   - **Activée** si vous voulez activer la recherche d'enregistrements MX pour les noms de domaine ou FQDN.
   - **Désactivée** si vous voulez désactiver la recherche d'enregistrements MX.

10. Cliquez sur le bouton **OK**.

La fenêtre **Paramètres principaux de MTA** se ferme.

Configuration des paramètres étendus du MTA

Pour configurer les paramètres MTA avancés, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **MTA** dans l'arborescence de la console de gestion.

2. Développez le groupe **Paramètres avancés**.

3. Cliquez sur n'importe quel lien de la partie supérieure de la liste des paramètres pour ouvrir la fenêtre **Paramètres MTA avancés**.

4. Le champ **Texte du message d'accueil du serveur SMTP** est destiné au message qui accompagne le code 220 sur le message d'accueil SMTP.

5. Le champ **Maximum de tentatives de connexion** permet de définir le nombre maximum de tentatives de connexion par minute d'un client SMTP distant au service du serveur SMTP.

   Saisissez 0 si aucune limite n'est nécessaire.

   Valeur par défaut : 0 (sans limite).

6. Le champ **Maximum de connexions simultanées** permet de définir le nombre maximum de tentatives de connexion simultanées d'un client SMTP distant au service du serveur SMTP.

   Saisissez 0 si aucune limite n'est nécessaire.

   Valeur par défaut : 50.

7. Le champ **Maximum de requêtes de livraison de messages** permet de définir le nombre maximum de requêtes par minute qu'un client SMTP envoie au serveur SMTP pour livrer un message, que le serveur de messagerie accepte ou non ces messages.

   Saisissez 0 si aucune limite n'est nécessaire.

   Valeur par défaut : 0 (sans limite).

8. Le champ **Durée maximale de la session SMTP** permet de définir la durée maximale au cours de laquelle il faut recevoir la requête d'un client SMTP distant et envoyer la réponse du serveur SMTP.

   Valeur par défaut : 30 s.

9. Le champ **Intervalle entre les connexions à une adresse de destination** permet de définir l'intervalle entre les tentatives d'établissement d'une connexion entre le gestionnaire de file d'attente du client de messagerie et l'adresse de destination des messages, quand cette adresse de destination n'est pas disponible.

Valeur par défaut : 60 s.

10. Le champ **Intervalle minimal entre les livraisons depuis la file Deferred** permet de définir l'intervalle minimal entre les tentatives d'envoi d'un message reporté dans la file d'attente Deferred.

    Valeur par défaut : 300 s.

11. Définissez dans le champ **Intervalle maximal entre les livraisons depuis la file Deferred** l'intervalle maximum entre les tentatives d'expédition d'un message placé dans la file d'attente Deferred.

    Valeur par défaut : 4000 s.

12. Le champ **Durée maximale de conservation d'un message dans la file d'attente** permet de limiter la durée de conservation dans la file d'attente d'un message qui porte depuis toujours un état d'erreur qui rend la livraison du message impossible.

    Valeur par défaut : 3 jours.

13. Définissez dans le champ **Intervalle de traitement de la file d'attente Deferred** la fréquence d'analyse de la file d'attente Deferred par le gestionnaire.

    Valeur par défaut : 1000 s.

14. Le champ **Durée maximale de conservation d'un message d'échec de livraison** permet de limiter la durée de conservation dans la file d'attente d'un message service porteur d'un état d'erreur permanent qui rend la livraison du message impossible.

    Valeur par défaut : 3 jours.

15. Le champ **Adresse de copie cachée de tous les messages** accueille l'adresse email facultative pour la réception d'un copie conforme invisible de tous les messages reçus par l'agent de messagerie MTA.

16. La liste **Vérifier le format des adresses selon la norme RFC 821** permet de configurer l'activation et la désactivation de la vérification des adresses email dans les commandes `SMTP MAIL FROM` et `RCPT TO` pour confirmer que les adresses sont encadrées par des chevrons et qu'elles ne contiennent aucune phrase ou expression RFC 822.

Cette vérification permet d'éviter la réception de messages en provenance d'applications douteuses.

Pour configurer la vérification des adresses, choisissez une des valeurs suivantes dans la liste **Vérifier le format des adresses selon la norme RFC 821** :

- **Oui**, si vous souhaitez activer l'analyse.
- **Non**, si vous ne souhaitez pas activer l'analyse.

Valeur par défaut : **Oui**.

17. Configurez le paramètre **Désactiver la vérification des destinataires SMTP VRFY** qui permet d'activer ou de désactiver la commande `SMTP VRFY`. La commande `SMTP VRFY` empêche la collecte d'adresses email par plusieurs services.

    Pour activer ou désactiver la commande `SMTP VRFY`, choisissez une des options suivantes dans la liste **Désactiver la vérification des destinataires SMTP VRFY** :

    - **Oui**, si vous souhaitez activer la commande.
    - **Non**, si vous souhaitez désactiver la commande.

    Valeur par défaut : **Oui**.

18. Le champ **Liste des commandes EHLO non signalées par le serveur SMTP** permet de cocher la case en regard des commandes `EHLO` qui ne sont pas sensibles à la case (par exemple, `pipelining`, `starttls`, `auth`) et que votre serveur SMTP n'annoncera pas dans la réponse à une requête `EHLO` en provenance d'un client SMTP externe.

    Valeurs par défaut : `silent-discard`, `dsn`, `etrn`.

19. Cliquez sur le bouton **OK**.

    La fenêtre **Paramètres MTA avancés** se ferme.

Vérification SMTP des adresses email des destinataires

Cette section contient des informations sur l'authentification SMTP des destinataires et la configuration des paramètres de cette authentification.

Dans cette section

Présentation de la vérification SMTP des adresses email des destinataires

La vérification SMTP des adresses email des destinataires consiste à confirmer l'existence des adresses email des destinataires.

Lorsque Kaspersky Secure Mail Gateway reçoit des messages pour des domaines protégés et les envoie vers le serveur de messagerie back-end, il faut empêcher que Kaspersky Secure Mail Gateway reçoive des messages envoyés à des adresses email inexistantes et cela, pour deux raisons :

- La réception de messages destinés à des adresses électroniques inexistantes charge le processeur, puisque le courrier est traité pour rien.
- Les tentatives de livraison à des adresses email inexistantes pourraient amener Kaspersky Secure Mail Gateway ou le serveur back-end à créer des notifications d'échec de livraison qui entraîneraient l'ajout de Kaspersky Secure Mail Gateway ou de votre serveur de messagerie back-end à une liste noire.

La vérification des destinataires des messages n'a pas lieu si Kaspersky Secure Mail Gateway accepte les messages en provenance d'adresses de nœuds de confiance du réseau (cf. section "Configuration des paramètres principaux du MTA" à la page 224).

Activation et désactivation de la vérification SMTP des adresses des destinataires

► *Pour activer ou désactiver la vérification SMTP des adresses des destinataires, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **MTA** dans l'arborescence de la console de gestion.

2. Développez le groupe **Paramètres avancés**.

3. Cliquez sur le lien **Refuser les messages destinés à des domaines inconnus** ou **Refuser les messages destinés à des adresses qui n'ont pas été vérifiées** pour ouvrir la fenêtre **Paramètres MTA avancés**.

   Sélectionnez une des valeurs suivantes dans la liste **Refuser les messages destinés à des domaines inconnus** :

   - **Oui**, si vous souhaitez que Kaspersky Secure Mail Gateway rejette la requête de remise d'un message si le nom de domaine `RCPT TO` ne contient pas les enregistrements MX du serveur DNS et l'adresse DNS ou si l'enregistrement MX est endommagé (par exemple, la longueur de l'adresse de l'hôte MX est nulle).

   - **Non**, si vous ne souhaitez pas que Kaspersky Secure Mail Gateway rejette la requête de remise d'un message si le nom de domaine `RCPT TO` ne contient pas les enregistrements MX du serveur DNS et l'adresse DNS ou si l'enregistrement MX est endommagé (par exemple, la longueur de l'adresse de l'hôte MX est nulle).

   Valeur par défaut : **Oui**.

4. A droite du nom du paramètre **Refuser les messages destinés à des adresses qui n'ont pas été vérifiées**, choisissez une des options suivantes :

- **Non**, si vous ne souhaitez pas refuser les messages destinés aux adresses qui n'ont pas été vérifiées.
- **Refuser si l'adresse est indisponible**, si vous voulez rejeter la demande de remise d'un message, si l'adresse `RCPT TO` est inaccessible.
- **Refuser si l'adresse ne figure pas dans la liste des adresses autorisées**, si vous souhaitez refuser la requête de remise de messages si les adresses `RCPT TO` ne figurent pas dans la liste des adresses acceptées pour cette classe de domaine.

5. Cliquez sur le bouton **OK**.

La fenêtre **Paramètres MTA avancés** se ferme.

Les vérifications SMTP des adresses email des destinataires n'ont pas lieu si Kaspersky Secure Mail Gateway accepte les messages en provenance d'adresses de nœuds de confiance du réseau (cf. section "Configuration des paramètres principaux du MTA" à la page 224).

Un trafic de messagerie dense peut augmenter la charge sur le serveur de messagerie en raison de l'envoi des notifications sur l'impossibilité de remettre des messages.

Mise à jour Kaspersky Secure Mail Gateway via l'interface Web

Cette section explique comment réaliser la mise à jour de Kaspersky Secure Mail Gateway via l'interface Web.

Dans cette section

Présentation de la mise à jour de Kaspersky Secure Mail Gateway via l'interface Web

Kaspersky Lab publie de temps à autres des paquets de mise à jour de Kaspersky Secure Mail Gateway. Il peut s'agir par exemple de paquets de mise à jour urgents qui éliminent des vulnérabilités ou des erreurs, des mises à jour qui introduisent de nouvelles fonctions ou améliorent les fonctions existantes de Kaspersky Secure Mail Gateway ou des paquets contenant de nouvelles versions linguistiques de Kaspersky Secure Mail Gateway.

Lorsque des mises à jour de Kaspersky Secure Mail Gateway ont été publiées, vous pouvez les installer via l'interface Web de Kaspersky Secure Mail Gateway.

Avant d'installer une mise à jour via l'interface Web de Kaspersky Secure Mail Gateway, vous devez télécharger la mise à jour ou la localisation au format TGZ ainsi que les instructions relatives à l'installation de cette mise à jour depuis la boutique en ligne vers votre ordinateur.

Il se peut que les services de Kaspersky Secure Mail Gateway soient suspendus pendant l'installation de la mise à jour. La mise à jour en elle-même peut durer plusieurs minutes. Une fois que la mise à jour de Kaspersky Secure Mail Gateway aura été lancée, il ne faut pas l'interrompre, ni éteindre la machine virtuelle. Après l'installation de la mise à jour, il faudra peut-être redémarrer Kaspersky Secure Mail Gateway.

Préparatifs pour la mise à jour de Kaspersky Secure Mail Gateway via l'interface Web

Avant de passer à la mise à jour de Kaspersky Secure Mail Gateway, il est vivement recommandé de réaliser une copie de sauvegarde de la machine virtuelle Kaspersky Secure Mail Gateway (instantané de la machine virtuelle dans l'hyperviseur) afin de pouvoir revenir à la version antérieure de Kaspersky Secure Mail Gateway en cas d'échec de l'installation de la nouvelle version de Kaspersky Secure Mail Gateway.

Avant la réalisation d'un instantané de la machine virtuelle Kaspersky Secure Mail Gateway, il est conseillé de désactiver l'envoi ou la réception de messages via l'agent de messagerie de Kaspersky Secure Mail Gateway (cf. section "Activation et désactivation de l'envoi et de la réception de messages" à la page 186) et de désactiver la machine virtuelle.

► *Pour prendre un instantané de la machine virtuelle Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Lancez l'application VMware vSphere Client.
2. Sélectionnez la machine virtuelle dont vous souhaitez prendre un instantané.
3. Ouvrez le menu d'un clic droit de la souris.

4. Choisissez l'option **Snapshot**, sous-option **Take Snapshot** (cf. ill. ci-dessous).

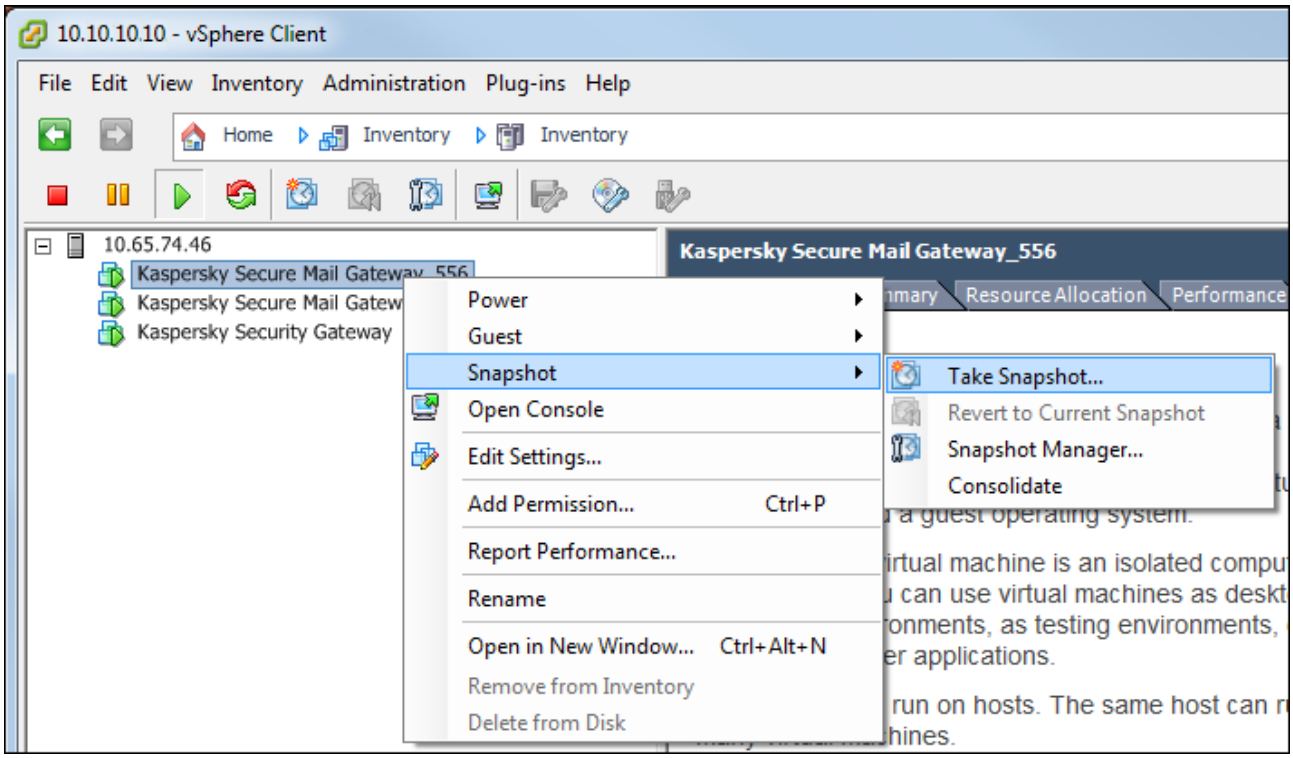

Figure 1 : Prise d'un instantané de la machine virtuelle

La fenêtre **Take Virtual Machine Snapshot** s'ouvre (cf. ill. ci-dessous).

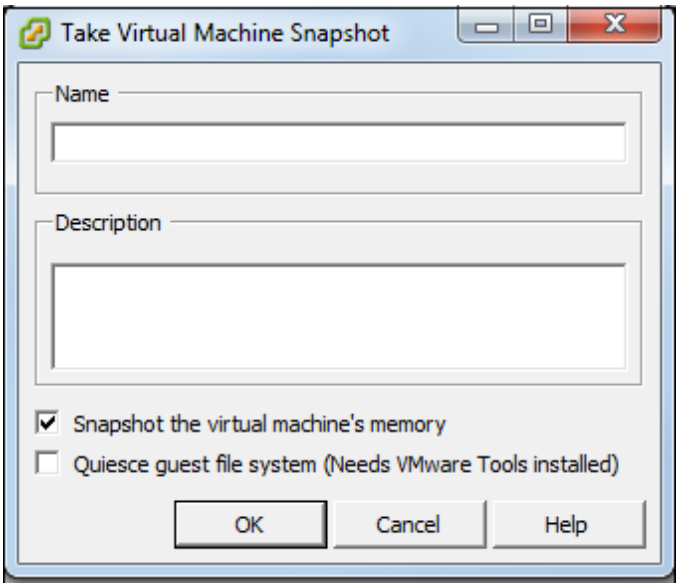

Figure 2 : Saisie des données de l'instantané de la machine virtuelle

5. Saisissez le nom de l'instantané de la machine virtuelle dans le champ **Name**.

6. Saisissez une description de l'instantané de la machine virtuelle dans le champ **Description**.

7. Cochez la case **Snapshot the virtual machine's memory**.

L'instantané de votre machine virtuelle s'affiche dans la liste des machines virtuelles de la partie gauche de la fenêtre principale de l'application.

Après que vous avez réalisé l'instantané de la machine virtuelle Kaspersky Secure Mail Gateway, il est conseillé d'activer la machine virtuelle et de lancer la mise à jour de Kaspersky Secure Mail Gateway.

Pour en savoir plus sur la manipulation des machines virtuelles dans VMware vSphere Client, consultez la documentation de VMware vSphere Client.

Réalisation de la mise à jour de Kaspersky Secure Mail Gateway via l'interface Web

► *Pour mettre à jour Kaspersky Secure Mail Gateway via l'interface Web, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Mise à jour du système** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Démarrer la mise à jour** pour ouvrir la fenêtre **Mise à jour du système**.

Cliquez sur le bouton **Parcourir** situé à droite du champ **Téléchargement du paquet de mises à jour**.

La fenêtre de sélection de fichiers de votre navigateur s'ouvre.

1. Sélectionnez le fichier de mise à jour que vous souhaitez télécharger, puis cliquez sur le bouton **Ouvrir** de votre navigateur.

La fenêtre de sélection de fichiers se ferme.

2. Cliquez sur le bouton **Suivant**.

3. Suivez les instructions de l'Assistant de mise à jour.

   Les étapes de l'Assistant de mise à jour peuvent varier en fonction du type de mise à jour téléchargée.

> Pour obtenir de plus amples informations sur l'installation de chaque type de mise à jour, consultez le manuel d'installation de cette mise à jour.

Mise à jour de la base de données de Kaspersky Secure Mail Gateway

Cette section contient des informations sur la mise à jour des bases antivirus et des bases des modules Anti-Spam et Anti-Phishing.

Dans cette section

A propos de la mise à jour des bases

Les bases des modules Antivirus, Anti-spam et Anti-phishing (ci-après, "bases") sont des fichiers contenant des définitions qui permettent de détecter du code malveillant dans les objets analysés. Ces définitions contiennent les informations sur les extraits de contrôle du code malveillant et les algorithmes de réparation des objets contenant ces menaces.

Les experts antivirus de Kaspersky Lab découvrent chaque jour une multitude de nouvelles menaces, créent les définitions qui les identifient et ajoutent ces dernières au *paquet de mises à jour des bases* (ci-après, "paquet de mises à jour"). Le paquet de mises à jour désigne un ou plusieurs fichiers contenant des enregistrements qui identifient les menaces détectées depuis la publication

du paquet de mises à jour précédent. Pour minimiser le risque d'infection du serveur de messagerie protégé, il est conseillé d'obtenir les paquets de mises à jour régulièrement.

Pendant la durée de validité de la licence, vous pouvez obtenir les paquets de mises à jour automatiquement selon une programmation ou installer les paquets de mises à jour manuellement après les avoir téléchargés depuis le site Internet de Kaspersky Lab.

Pendant l'installation, Kaspersky Secure Mail Gateway récupère les bases actuelles depuis un des serveurs de mise à jour de Kaspersky Lab. Si la mise à jour de la base de données automatique a été configurée, Kaspersky Secure Mail Gateway l'exécute selon la planification (selon une fréquence d'une fois toutes les cinq minutes).

Kaspersky Secure Mail Gateway vérifie automatiquement la présence de nouveaux paquets de mises à jour sur les serveurs de mise à jour de Kaspersky Lab selon un intervalle défini. Par défaut, si les bases de Kaspersky Secure Mail Gateway n'ont pas été mises à jour au cours des dernières 24 heures ou si les bases du module Anti-Spam ne sont pas mises à jour dans l'heure qui suit la publication des derniers paquets de mises à jour par Kaspersky Lab, Kaspersky Secure Mail Gateway consigne l'événement *Les bases sont dépassées*. Si les bases antivirus n'ont plus été mises à jour depuis une semaine ou si les bases du module Anti-Spam n'ont pas été mises à jour au cours des dernières 24 heures, Kaspersky Secure Mail Gateway consigne l'événement *Les bases sont fortement dépassées*. Vous pouvez configurer les notifications de l'administrateur pour ces événements.

A propos des sources de mises à jour

La source des mises à jour est une ressource qui contient les mises à jour des bases de données de Kaspersky Secure Mail Gateway.

Les serveurs de mise à jour de Kaspersky Lab sont la principale source des mises à jour. Il s'agit de sites Internet spéciaux où sont publiées les mises à jour des bases et des modules de l'application pour tous les produits de Kaspersky Lab. Si vous utilisez un serveur proxy pour l'accès Internet, vous devez configurer les paramètres de connexion au serveur proxy (cf. section "Configuration des paramètres de connexion au serveur proxy pour la mise à jour des bases de données" à la page 245).

Pour diminuer le trafic Internet, vous pouvez configurer la mise à jour des bases de données Kaspersky Secure Mail Gateway depuis la *source des mises à jour personnalisée (cf.*

section "Sélection de la source des mises à jour des bases" à la page 240). La source des mises à jour personnalisées peut être un serveur HTTP ou FTP que vous avez désigné, ainsi que des répertoires locaux sur votre ordinateur.

Si Kaspersky Secure Mail Gateway est administré par le Kaspersky Security Center, ce dernier peut être utilisé comme source des mises à jour.

Sélection de la source des mises à jour des bases

► *Pour sélectionner une source des mises à jour des bases, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Mise à jour des bases** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Source des mises à jour** du groupe **Paramètres de mise à jour des bases de données de l'application** pour ouvrir la fenêtre **Paramètres de mise à jour des bases de données de l'application**.

3. Dans le groupe de paramètres **Source des mises à jour**, sélectionnez la source à partir de laquelle vous souhaitez recevoir le paquet de mises à jour :

   - **Serveurs de Kaspersky Lab**.
   - **Kaspersky Security Center**.
   - Source de mises à jour personnalisée.

4. Si vous avez sélectionné une source des mises à jour personnalisée, indiquez dans le champ situé sous **Kaspersky Security Center** l'adresse Internet du paquet des mises à jour sur votre serveur FTP ou HTTP, ou le chemin d'accès complet au répertoire contenant le paquet de mises à jour.

   Vous pouvez également cocher la case **En cas d'indisponibilité, utiliser les serveurs de Kaspersky Lab** afin de recevoir le paquet de mises à jour depuis les serveurs de mise à jour de Kaspersky Lab lorsque votre source des mises à jour n'est pas disponible.

5. Cliquez sur le bouton **OK**.

Configuration de la planification et des paramètres de la mise à jour des bases de données

► *Pour configurer la planification et les paramètres de mise à jour des bases de données, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Mise à jour des bases** dans l'arborescence de la console de gestion.

2. Dans le groupe **Paramètres de mise à jour des bases de données de l'application**, cliquez sur le lien **Planification** ou **Source des mises à jour** pour ouvrir la fenêtre **Paramètres de mise à jour des bases de données de l'application**.

3. Dans le groupe de paramètres **Planification**, sélectionnez dans le menu déroulant l'une des options suivantes :

   - **Manuel** (cf. section "**Lancement manuel de la mise à jour des bases de données**" à la page 244).
   - **Une fois**.
   - **Chaque semaine**.
   - **Chaque mois**.
   - **Lancer tous les**.

4. Dans le groupe de paramètres **Planification** à droite de la liste déroulante, définissez la fréquence du lancement de la mise à jour. Vous pouvez choisir une des valeurs suivantes en fonction de la planification choisie :

   - Pour un lancement de la mise à jour des bases **Une fois**, indiquez dans les champs correspondants la date et l'heure de lancement de la mise à jour de la base de données.

- Pour un lancement de la mise à jour des bases **Chaque semaine**, indiquez dans les champs correspondants le jour de la semaine et l'heure de lancement de la mise à jour de la base de données.

  Par exemple, si les valeurs **Lundi** et **15:00** sont indiquées, la mise à jour de la base de données est lancée tous les lundis à 15 heures.

- Pour un lancement de la mise à jour de la base de données **Chaque mois**, indiquez dans les champs correspondants le jour du mois et l'heure de lancement de la mise à jour des bases.

  Par exemple, si les valeurs **20** et **15:00** sont indiquées, la mise à jour de la base de données est lancée le 20 de chaque mois à 15 heures.

- Pour un lancement de la mise à jour de la base de données **Lancer tous les**, indiquez dans les champs correspondants la fréquence de lancement de la mise à jour des bases en minutes, heures ou jours :

  - Pour définir la fréquence de lancement en minutes, sélectionnez la valeur **min** dans la liste à droite de la fenêtre, indiquez la fréquence en minutes, puis, dans le champ **commençant par**, indiquez l'heure du premier lancement de la mise à jour des bases.

    Par exemple, si la valeur **30** est indiquée pour la fréquence, avec une fréquence en **min** et la valeur **15:00** pour le champ **commençant par**, les bases seront mises à jour toutes les 30 minutes à partir de 15 heures.

  - Pour définir la fréquence de lancement en heures, sélectionnez la valeur **h** dans la liste à droite de la fenêtre, indiquez la fréquence en heures, puis, dans le champ **commençant par**, indiquez la date et l'heure du premier lancement de la mise à jour des bases.

    Par exemple, si la valeur **3** est indiquée pour la fréquence, avec une fréquence en **h** et les valeurs **25.12.2017** et **15:00** pour le champ **commençant par**, les bases seront mises à jour toutes les trois heures à partir du 25/05/2017 à 15 heures.

  - Pour définir la fréquence de lancement en jours, sélectionnez la valeur **jour** dans la liste à droite de la fenêtre, indiquez la fréquence en jours, puis, dans le champ **commençant par**, indiquez l'heure du lancement de la mise à jour des bases.

Par exemple, si la valeur **2** est indiquée pour la fréquence, avec une fréquence en **jour** et la valeur **15:00** pour le champ **commençant par**, les bases seront mises à jour tous les deux jours à 15 heures.

5. Le groupe de paramètres **Description des paramètres de mise à jour** du champ **Déconnexion aléatoire** permet de définir l'écart en minutes par rapport à la planification définie pendant lequel la mise à jour de la base de données sera lancée sur les ordinateurs afin que tous les ordinateurs ne contactent pas en même temps la source des mises à jour. Cette fonction résout les problèmes liés à la sollicitation de la source des mises à jour par un nombre élevé d'ordinateurs client lors du lancement de la mise à jour de la base de données.

6. Dans le groupe de paramètres **Description des paramètres de mise à jour**, indiquez dans le champ **Exécuter pas plus de** la durée maximale d'exécution de la mise à jour des bases (en minutes). A l'expiration de ce délai, la mise à jour sera interrompue.

7. Dans le groupe de paramètres **Description des paramètres de mise à jour**, utilisez la liste **Lancer les tâches ignorées** pour sélectionner l'ordre de lancement des tâches à exécuter si la mise à jour n'est pas terminée à l'heure prévue par la planification pour l'une des raisons suivantes :

   - l'ordinateur était indisponible (éteint ou non connecté à Internet) ;
   - l'application n'a pas été lancée.

   Quand le lancement des tâches non exécutées est activé, une tentative de lancement de la mise à jour de la base de l'application est réalisée lors du prochain lancement de l'application. En cas de mise à jour selon les modes **Manuel** et **Une fois**, la tâche de mise à jour est lancée directement après l'apparition de l'ordinateur sur le réseau local.

   Si le lancement des tâches non exécutées n'a pas été activé, les tâches de mise à jour des bases sur les postes client se lancent uniquement selon la programmation et, pour les mises à jour en mode **Manuel** ou **Une fois**, uniquement lorsque les postes sont visibles sur le réseau local.

8. Cliquez sur le bouton **OK**.

Utilisation des valeurs par défaut des paramètres de mise à jour des bases

► *Pour utiliser les valeurs par défaut des paramètres de mise à jour des bases et la planification par défaut de la mise à jour, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Mise à jour des bases** dans l'arborescence de la console de gestion.

2. Dans le groupe **Paramètres de mise à jour des bases de données de l'application**, cliquez sur le lien **Planification** pour ouvrir la fenêtre **Paramètres de mise à jour des bases de données de l'application**.

3. Dans la partie inférieure de la fenêtre **Paramètres de mise à jour des bases de données de l'application**, cliquez sur le lien **Etablir les valeurs par défaut**.

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

Lancement manuel de la mise à jour des bases

► *Pour lancer manuellement la mise à jour de la base de données, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Mise à jour des bases** dans l'arborescence de la console de gestion.

2. Dans le groupe **Paramètres de mise à jour des bases de données de l'application** de l'espace de travail, lancez la mise à jour des bases en cliquant sur le lien **Lancer la mise à jour**.

   Le lien **Lancer la mise à jour** devient **Mise à jour en cours** et l'état d'avancement de la mise à jour des bases de données s'affiche.

Configuration des paramètres de connexion au serveur proxy pour la mise à jour des bases de données

► *Pour configurer les paramètres de connexion au serveur proxy pour la mise à jour des bases de données, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Mise à jour des bases** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe quel lien du groupe **Utiliser un serveur proxy** pour ouvrir la fenêtre **Paramètres de connexion**.

3. Dans la liste déroulante **Utiliser un serveur proxy** du groupe de paramètres **Paramètres du serveur proxy**, sélectionnez une des options suivantes :

   - **Oui** – pour activer un serveur proxy avec Kaspersky Secure Mail Gateway ;
   - **Non** – pour désactiver un serveur proxy avec Kaspersky Secure Mail Gateway.

4. Dans le champ **Adresse**, saisissez l'adresse du serveur proxy.

5. Dans le champ **Port**, indiquez le numéro de port du serveur proxy.

6. Dans la liste déroulante **Authentification** du groupe de paramètres **Paramètres d'authentification**, sélectionnez une des options suivantes :

   - **Pas nécessaire**, si vous ne souhaitez pas utiliser l'authentification pour vous connecter au serveur proxy.
   - **Simple**, si vous souhaitez utiliser l'authentification pour vous connecter au serveur proxy.

7. Si vous avez choisi l'option **Simple** pour le paramètre **Authentification**, indiquez dans les champs **Nom d'utilisateur** et **Mot de passe** le nom d'utilisateur et le mot de passe permettant de se connecter au serveur proxy.

8. Dans la liste déroulante **Ne pas utiliser pour les adresses locales** du groupe de paramètres **Paramètres de connexion au serveur proxy**, sélectionnez une des options suivantes :

    - **Oui**, si vous ne souhaitez pas utiliser le serveur proxy pour les adresses email internes à votre entreprise ;
    - **Non** – pour utiliser le serveur proxy y compris pour les adresses email internes à votre entreprise.

9. Cliquez sur le bouton **OK**.

► *Pour activer ou désactiver l'utilisation du serveur proxy, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Mise à jour des bases** dans l'arborescence de la console de gestion.
2. Dans l'espace de travail, exécutez l'une des opérations suivantes :

    - Activez le commutateur en regard du groupe de paramètres **Utiliser un serveur proxy** pour utiliser un serveur proxy avec Kaspersky Secure Mail Gateway.
    - Désactivez le commutateur en regard du groupe de paramètres **Utiliser un serveur proxy**, si vous ne souhaitez pas utiliser un serveur proxy avec Kaspersky Secure Mail Gateway.

Vous pouvez activer l'utilisation du serveur proxy seulement après la configuration des paramètres de connexion au serveur proxy.

Authentification des expéditeurs des messages.

L'authentification des expéditeurs de messages vise à offrir une protection supplémentaire de l'infrastructure de messagerie de votre organisation contre le courrier indésirable et le phishing.

Kaspersky Secure Mail Gateway exploite les technologies suivantes pour authentifier les expéditeurs de messages :

- Authentification SPF (Sender Policy Framework).
- Authentification DKIM (DomainKeys Identified Mail).
- Authentification DMARC (Domain-based Message Authentication, Reporting and Conformance).

L'*authentification SPF* des expéditeurs de messages désigne la technique selon laquelle les adresses IP des expéditeurs sont comparées avec la liste des sources de messages potentielles créée par l'administrateur du serveur de messagerie.

Kaspersky Secure Mail Gateway reçoit la liste des sources de messages potentielles depuis le serveur DNS.

Activez l'authentification SPF si Kaspersky Secure Mail Gateway reçoit les messages directement d'Internet. Désactivez l'authentification SPF si Kaspersky Secure Mail Gateway reçoit les messages depuis un serveur intermédiaire interne.

L'*authentification DKIM* des expéditeurs de message désigne la vérification de la signature numérique des messages.

Chaque message reçoit une signature numérique associée au nom de domaine de l'organisation. Kaspersky Secure Mail Gateway vérifie cette signature numérique.

L'*authentification DMARC* des expéditeurs de messages permet de confirmer si le message provient bien du domaine indiqué.

Une fois que le message a subi l'authentification SPF et DKIM, le système vérifie si le domaine contenant l'adresse de l'expéditeur dans le champ De de l'en-tête du message électronique correspond aux identifiants SPF et DKIM, ainsi qu'aux états SPF et DKIM.

Pour l'authentification SPF, DKIM et DMARC des expéditeurs des messages, il faut autoriser la connexion de Kaspersky Secure Mail Gateway au serveur DNS (cf. section "Connexion au serveur DNS pour l'authentification des expéditeurs" à la page 250). Si la connexion au serveur DNS est interdite, les authentifications SPF, DKIM et DMARC des expéditeurs de messages seront désactivées.

Si Kaspersky Secure Mail Gateway découvre une violation, à l'issue des authentifications SPF, DKIM ou DMARC des expéditeurs de messages, on estime que des *violations de l'authentification des expéditeurs* ont été découvertes pendant les authentifications SPF, DKIM et DMARC.

Dans cette section

Connexion au serveur DNS pour l'authentification des expéditeurs

Pour réaliser l'authentification des expéditeurs de messages, il faut autoriser la connexion de Kaspersky Secure Mail Gateway au serveur DNS. Si la connexion au serveur DNS est interdite, les authentifications SPF, DKIM et DMARC des expéditeurs de messages seront désactivées.

Vous pouvez également définir la durée maximale d'attente de la réponse du serveur DNS à l'issue de laquelle le serveur DNS sera considéré comme inaccessible et le message sera traité par Kaspersky Secure Mail Gateway sans authentification des expéditeurs. Valeur par défaut : 10 s.

► *Pour autoriser la connexion de Kaspersky Secure Mail Gateway au serveur DNS, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.
2. Cliquez sur le lien **Autoriser la connexion au serveur DNS** du groupe **Services externes** pour ouvrir la fenêtre **Services externes**.
3. Dans la liste à droite du nom du paramètre **Autoriser la connexion au serveur DNS** , sélectionnez **Oui**.
4. Cliquez sur le bouton **Appliquer**.

► *Pour définir la durée maximale d'attente de la réponse du serveur DNS, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.
2. Cliquez sur le lien **Autoriser la connexion au serveur DNS** du groupe **Services externes** pour ouvrir la fenêtre **Services externes**.
3. Dans le champ situé à droite du paramètre **Attendre la réponse du serveur DNS**, indiquez la durée maximale d'attente de la réponse du serveur DNS en secondes.

   Valeur par défaut : 10 s.
4. Cliquez sur le bouton **Appliquer**.

Activation et désactivation de l'authentification SPF des expéditeurs

► *Pour activer ou désactiver l'authentification SPF des expéditeurs, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Activer l'authentification SPF des expéditeurs** du groupe **Services externes** pour ouvrir la fenêtre **Services externes**.

3. Dans la liste à droite du nom du paramètre **Activer l'authentification SPF des expéditeurs** , sélectionnez une des options suivantes :

   - **Oui**, si vous souhaitez activer l'authentification SPF des expéditeurs de messages.

   - **Non**, si vous souhaitez désactiver l'authentification SPF des expéditeurs.

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

Pour l'authentification SPF des expéditeurs des messages, il faut autoriser la connexion de Kaspersky Secure Mail Gateway au serveur DNS (cf. section "Connexion au serveur DNS pour l'authentification des expéditeurs" à la page 250). Si la connexion au serveur DNS est interdite, l'authentification SPF des expéditeurs de messages sera désactivée.

Activation et désactivation de l'authentification DKIM des expéditeurs

► *Pour activer ou désactiver l'authentification DKIM des expéditeurs, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Activer l'authentification DKIM des expéditeurs** du groupe **Services externes** pour ouvrir la fenêtre **Services externes**.

3. Dans la liste à droite du nom du paramètre **Activer l'authentification DKIM des expéditeurs**, sélectionnez une des options suivantes :

   - **Oui**, si vous souhaitez activer l'authentification DKIM des expéditeurs de messages.
   - **Non**, si vous souhaitez désactiver l'authentification DKIM des expéditeurs.

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

Pour l'authentification DKIM des expéditeurs des messages, il faut autoriser la connexion de Kaspersky Secure Mail Gateway au serveur DNS (cf. section "Connexion au serveur DNS pour l'authentification des expéditeurs" à la page 250). Si la connexion au serveur DNS est interdite, l'authentification DKIM des expéditeurs de messages sera désactivée.

Activation et désactivation de l'authentification DMARC des expéditeurs

► *Pour activer ou désactiver l'authentification DMARC des expéditeurs, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.
2. Cliquez sur le lien **Activer l'authentification DMARC des expéditeurs** du groupe **Services externes** pour ouvrir la fenêtre **Services externes**.
3. Dans la liste à droite du nom du paramètre **Activer l'authentification DMARC des expéditeurs**, sélectionnez une des options suivantes :

   - **Oui**, si vous souhaitez activer l'authentification DMARC des expéditeurs de messages.
   - **Non**, si vous souhaitez désactiver l'authentification DMARC des expéditeurs.

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

Pour l'authentification DMARC des expéditeurs des messages, il faut autoriser la connexion de Kaspersky Secure Mail Gateway au serveur DNS (cf. section "Connexion au serveur DNS pour l'authentification des expéditeurs" à la page 250). Si la connexion au serveur DNS est interdite, l'authentification DMARC des expéditeurs de messages sera désactivée.

Activation et désactivation de l'authentification des expéditeurs pour une règle

Vous pouvez activer ou désactiver l'authentification des expéditeurs de messages pour une ou plusieurs règles.

Avant d'activer l'authentification des expéditeurs des messages pour la règle, confirmez qu'au moins une authentification des expéditeurs des messages est activée dans les paramètres de Kaspersky Secure Mail Gateway (cf. section "Activation et désactivation de l'authentification SPF des expéditeurs" à la page 251, "Activation et désactivation de l'authentification DKIM des expéditeurs" à la page 251, "Activation et désactivation de l'authentification DMARC des expéditeurs" à la page 252).

► *Pour activer ou désactiver l'authentification des expéditeurs de messages pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez activer ou désactiver l'authentification des expéditeurs de messages.

3. Choisissez le groupe **Authentification des expéditeurs de messages**.

4. Exécutez une des actions suivantes :

   - Activez le commutateur en regard du nom du groupe de paramètres **Authentification des expéditeurs de messages**, si vous souhaitez activer l'authentification des expéditeurs.

- Désactivez le commutateur en regard du nom du groupe de paramètres **Authentification des expéditeurs de messages**, si vous souhaitez désactiver l'authentification des expéditeurs.

5. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration de la détection des erreurs TempError et PermError lors de l'authentification des expéditeurs

Si vous souhaitez que l'erreur temporaire TempError soit considérée comme une violation de l'authentification des expéditeurs, vous pouvez définir à cette fin une ou plusieurs règles.

Avant d'indiquer s'il faut considérer une erreur temporaire TempError comme une violation de l'authentification des expéditeurs, confirmez qu'au moins une authentification des expéditeurs des messages est activée dans les paramètres de Kaspersky Secure Mail Gateway (cf. section "Activation et désactivation de l'authentification SPF des expéditeurs" à la page 251, "Activation et désactivation de l'authentification DKIM des expéditeurs" à la page 251, "Activation et désactivation de l'authentification DMARC des expéditeurs" à la page 252).

► *Pour indiquer s'il faut considérer une erreur temporaire TempError comme une violation de l'authentification des expéditeurs, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien du nom de la règle dans la liste afin d'ouvrir la règle pour laquelle vous souhaitez indiquer s'il faut considérer une erreur temporaire TempError comme une violation de l'authentification des expéditeurs.

3. Choisissez le groupe **Authentification des expéditeurs de messages**.

4. Exécutez une des actions suivantes :

   - Cochez la case en regard du paramètre **Considérer les erreurs temporaires (TempError) comme des violations** si vous souhaitez que Kaspersky Secure Mail

Gateway considère les erreurs temporaires TempError comme une violation de l'authentification des expéditeurs.

- Décochez la case en regard du paramètre **Considérer les erreurs temporaires (TempError) comme des violations** si vous ne souhaitez pas que Kaspersky Secure Mail Gateway considère les erreurs temporaires TempError comme une violation de l'authentification des expéditeurs.

5. Exécutez une des actions suivantes :

   - Cochez la case en regard du paramètre **Considérer les erreurs permanentes (PermError) comme violation de l'authentification de l'expéditeur** si vous souhaitez que Kaspersky Secure Mail Gateway considère les erreurs permanentes PermError comme une violation de l'authentification des expéditeurs.

   - Décochez la case en regard du paramètre **Considérer les erreurs permanentes (PermError) comme violation de l'authentification de l'expéditeur** si vous ne souhaitez pas que Kaspersky Secure Mail Gateway considère les erreurs permanentes PermError comme une violation de l'authentification des expéditeurs.

6. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration des paramètres complémentaires de l'authentification DMARC pour la règle

Il est possible de configurer des paramètres complémentaires de l'authentification DMARC des expéditeurs pour une ou plusieurs règles.

Avant de configurer d'autres paramètres d'authentification DMARC des messages pour la règle, confirmez que l'authentification DMARC des expéditeurs des messages est activée dans les paramètres de Kaspersky Secure Mail Gateway (cf. section "Activation et désactivation de l'authentification DMARC des expéditeurs" à la page 251).

► *Pour configurer les paramètres complémentaires de l'authentification DMARC pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer des paramètres complémentaires d'authentification DMARC.

3. Choisissez le groupe **Authentification des expéditeurs de messages**.

4. Activez le commutateur en regard du groupe de paramètres **Authentification des expéditeurs de messages**, s'il est désactivé.

5. Dans le groupe de paramètres **Authentification DKIM des expéditeurs** , exécutez l'une des actions suivantes :

   - Cochez la case en regard du nom du paramètre **Considérer le résultat de l'authentification DMARC comme prioritaire**, si vous voulez que Kaspersky Secure Mail Gateway définisse la violation de l'authentification des expéditeurs des messages sur la base des résultats de l'authentification DMARC.

   - Décochez la case en regard du nom du paramètre **Considérer le résultat de l'authentification DMARC comme prioritaire**, si vous ne voulez pas que Kaspersky Secure Mail Gateway définisse la violation de l'authentification des expéditeurs des messages sur la base des résultats de l'authentification DMARC.

   Si la case est cochée, la violation de l'authentification des expéditeurs est déterminée sur la base des résultats de l'authentification DMARC. Si la case est décochée, les résultats des authentifications SPF, DKIM et DMARC sont considérés comme équivalents. Une violation de chacune de ces authentifications est considérée comme une violation de l'authentification des expéditeurs. En cas de violation simultanée de plusieurs authentifications, l'action la plus stricte est exécutée sur le message (cf. section "Configuration des actions à exécuter sur les messages lors de l'authentification DMARC, SPF ou DKIM" à la page 262) en cas de violation SPF, DKIM ou DMARC de l'authenticité de l'expéditeur.

6. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration des paramètres complémentaires de l'authentification SPF pour la règle.

Il est possible de configurer des paramètres complémentaires de l'authentification SPF des expéditeurs pour une ou plusieurs règles.

Avant de configurer d'autres paramètres d'authentification SPF des messages pour la règle, confirmez que l'authentification SPF des expéditeurs des messages est activée dans les paramètres de Kaspersky Secure Mail Gateway (cf. section "Activation et désactivation de l'authentification DMARC des expéditeurs" à la page 251).

► *Pour configurer les paramètres complémentaires de l'authentification SPF pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.
2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer des paramètres complémentaires d'authentification SPF.
3. Choisissez le groupe **Authentification des expéditeurs de messages**.
4. Activez le commutateur en regard du groupe de paramètres **Authentification des expéditeurs de messages**, s'il est désactivé.
5. Dans le groupe de paramètres **Authentification SPF des expéditeurs**, exécutez une des actions suivantes :
   - Cochez la case du paramètre **Considérer SPF softfail comme une violation**, si vous souhaitez que Kaspersky Secure Mail Gateway considère toute erreur SPF softfail détectée lors de l'authentification SPF comme une violation de l'authentification des expéditeurs.
   - Décochez la case du paramètre **Considérer SPF softfail comme une violation**, si vous ne souhaitez pas que Kaspersky Secure Mail Gateway considère toute erreur SPF

softfail détectée lors de l'authentification SPF comme une violation de l'authentification des expéditeurs.

6. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration des paramètres complémentaires de l'authentification DKIM pour la règle

Il est possible de configurer des paramètres complémentaires de l'authentification DKIM des expéditeurs pour une ou plusieurs règles.

Avant de configurer d'autres paramètres d'authentification DKIM des messages pour la règle, confirmez que l'authentification DKIM des expéditeurs des messages est activée dans les paramètres de Kaspersky Secure Mail Gateway (cf. section "Activation et désactivation de l'authentification DKIM des expéditeurs" à la page 251).

► *Pour configurer les paramètres complémentaires de l'authentification DKIM pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.
2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer des paramètres complémentaires d'authentification DKIM.
3. Choisissez le groupe **Authentification des expéditeurs de messages**.
4. Activez le commutateur en regard du groupe de paramètres **Authentification des expéditeurs de messages**, s'il est désactivé.
5. Dans le groupe de paramètres **Authentification DKIM des expéditeurs**, exécutez une des actions suivantes :
   - Cochez la case en regard du paramètre **Considérer l'absence de signature DKIM comme une violation**, si vous souhaitez que Kaspersky Secure Mail Gateway considère

l'absence de signature DKIM dans le message comme une violation de l'authentification des expéditeurs lors de l'authentification DKIM.

- Décochez la case en regard du paramètre **Considérer l'absence de signature DKIM comme une violation**, si vous ne souhaitez pas que Kaspersky Secure Mail Gateway considère l'absence de signature DKIM dans le message comme une violation de l'authentification des expéditeurs lors de l'authentification DKIM.

6. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration des tags dans l'objet des messages selon les résultats de l'authentification SPF

► *Pour configurer les tags que Kaspersky Secure Mail Gateway ajoutera à l'objet des messages à la suite de l'authentification SPF des expéditeurs, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les tags à ajouter à l'objet des messages selon les résultats de l'authentification SPF.

3. Choisissez le groupe **Authentification des expéditeurs de messages**.

4. Activez le commutateur en regard du groupe de paramètres **Authentification des expéditeurs de messages** s'il est désactivé.

5. Dans le groupe de paramètres **Authentification SPF des expéditeurs**, cliquez sur le lien à droit du nom du paramètre **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Etiquette de violation pour l'authentification SPF**.

6. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet du message en cas de violation de l'authentification SPF des expéditeurs.

7. Cliquez sur le bouton **OK**.

La fenêtre **Etiquette de violation pour l'authentification SPF** se ferme.

8. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration des tags dans l'objet des messages selon les résultats de l'authentification DKIM

► *Pour configurer les tags que Kaspersky Secure Mail Gateway ajoutera à l'objet des messages à la suite de l'authentification DKIM des expéditeurs, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les tags à ajouter à l'objet des messages selon les résultats de l'authentification DKIM.

3. Choisissez le groupe **Authentification des expéditeurs de messages**.

4. Activez le commutateur en regard du groupe de paramètres **Authentification des expéditeurs de messages**, s'il est désactivé.

5. Dans le groupe de paramètres **Authentification DKIM des expéditeurs**, cliquez sur le lien à droite du nom du paramètre **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Etiquette de violation pour l'authentification DKIM**.

6. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet du message en cas de violation de l'authentification DKIM des expéditeurs.

7. Cliquez sur le bouton **OK**.

   La fenêtre **Etiquette de violation pour l'authentification DKIM** se ferme.

8. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration des tags dans l'objet des messages selon les résultats de l'authentification DMARC

► *Pour configurer les tags que Kaspersky Secure Mail Gateway ajoutera à l'objet des messages à la suite de l'authentification DMARC des expéditeurs, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les tags à ajouter à l'objet des messages selon les résultats de l'authentification DMARC.

3. Choisissez le groupe **Authentification des expéditeurs de messages**.

4. Activez le commutateur en regard du groupe de paramètres **Authentification des expéditeurs de messages**, s'il est désactivé.

5. Dans le groupe de paramètres **En cas de détection d'une violation DMARC**, cliquez sur le lien à droite du nom du paramètre **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Etiquette de violation pour l'authentification DMARC**.

6. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet du message en cas de violation de l'authentification DMARC des expéditeurs.

7. Cliquez sur le bouton **OK**.

   La fenêtre **Etiquette de violation pour l'authentification DMARC** se ferme.

8. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration des actions à exécuter sur les messages lors de l'authentification DMARC, SPF ou DKIM

Vous pouvez configurer les actions à exécuter sur les messages lors de l'authentification DMARC, SPF et DKIM des expéditeurs pour une ou plusieurs règles.

Avant de configurer les actions à exécuter sur les messages lors de l'authentification DMARC, SPF ou DKIM, confirmez que l'authentification des expéditeurs correspondante est activée dans les paramètres de Kaspersky Secure Mail Gateway (cf. section "Activation et désactivation de l'authentification DMARC des expéditeurs" à la page 252).

► *Pour configurer les actions à exécuter sur les messages lors de l'authentification DMARC, SPF et DKIM des expéditeurs, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les actions à effectuer sur les messages lors de l'authentification DMARC.

3. Choisissez le groupe **Authentification des expéditeurs de messages**.

4. Activez le commutateur en regard du groupe de paramètres **Authentification des expéditeurs de messages**, s'il est désactivé.

5. Dans le groupe **Authentification DKIM des expéditeurs**, sélectionnez dans la liste déroulante **En cas de détection d'une violation DMARC** une des actions suivantes à exécuter sur les messages pour lesquels l'authentification DMARC a détecté une violation de l'authentification des expéditeurs :

   - **Appliquer la stratégie DMARC**.

     La stratégie DMARC est définie par l'administrateur du serveur de messagerie sur le serveur DNS.

- **Refuser le message**.
- **Supprimer le message**.
- **Ignorer**.

6. Cochez la case en regard du nom du paramètre **Placer au préalable une copie dans la Sauvegarde**, si vous souhaitez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant le traitement.
7. Dans le groupe **Authentification SPF des expéditeurs**, sélectionnez dans la liste déroulante **En cas de détection d'une violation SPF** une des actions suivantes à exécuter sur les messages pour lesquels l'authentification SPF a détecté une violation de l'authentification des expéditeurs :
   - **Refuser le message**.
   - **Supprimer le message**.
   - **Ignorer**.
8. Cochez la case en regard du nom du paramètre **Placer au préalable une copie dans la Sauvegarde**, si vous souhaitez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant le traitement.
9. Dans le groupe **Authentification DKIM des expéditeurs**, sélectionnez dans la liste déroulante **En cas de détection d'une violation DKIM** une des actions suivantes à exécuter sur les messages pour lesquels l'authentification DKIM a détecté une violation de l'authentification des expéditeurs :
   - **Refuser le message**.
   - **Supprimer le message**.
   - **Ignorer**.
10. Cochez la case en regard du nom du paramètre **Placer au préalable une copie dans la Sauvegarde**, si vous souhaitez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant le traitement.

11. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Préparatifs pour la configuration de l'authentification SPF et DMARC des expéditeurs des messages sortants

Pour que le serveur de messagerie distant puisse authentifier l'expéditeur des messages si cet expéditeur est Kaspersky Secure Mail Gateway (authentification de l'expéditeur des messages sortants), il faut ajouter les signatures SPF et DMARC dans les paramètres de votre serveur DNS.

► *Pour ajouter les signatures SPF et DMARC aux paramètres de votre serveur DNS, procédez comme suit :*

1. Ouvrez une session en tant qu'administrateur sur votre serveur DNS.

2. Trouvez la page qui contient les informations relatives à la mise à jour des signatures DNS de ce domaine contenant les adresses pour lesquelles vous souhaitez configurer l'authentification de l'expéditeur des messages sortants.

   Par exemple, cette page peut être intitulée "Administration DNS", "Administration du serveur de noms" ou "Paramètres complémentaires".

3. Trouvez les signatures au format TXT pour ce domaine contenant les adresses pour lesquelles vous souhaitez configurer l'authentification de l'expéditeur des messages sortants.

4. Dans la liste des signatures au format TXT, ajoutez la signature SPF pour le domaine en question de la manière suivante :

   ```
   <nom du domaine pour lequel vous souhaitez configurer
   l'authentification SPF de l'expéditeur des messages sortants> IN TXT
   "v=<version de SPF> +all>"
   ```

   Par exemple, vous pouvez ajouter la ligne :

   ```
   example.com IN TXT "v=spf1 +all"
   ```

> Pour en savoir plus sur la fonction des paramètres de la signature SPF, consultez le document RFC 4408.

5. Dans la liste des signatures au format TXT, ajoutez la signature DMARC pour le domaine en question de la manière suivante :

   ```
   _dmarc.<nom du domaine contenant les adresses pour lesquelles vous souhaitez configurer l'authentification DMARC de l'expéditeur des messages sortants>. IN TXT "v=<version DMARC>; p=<action que le serveur de messagerie distant exécutera sur tous les messages électroniques qui ne remplissent pas les exigences DMARC>;"
   ```

   Par exemple, vous pouvez ajouter la ligne :

   ```
   _dmarc.example.com. IN TXT "v=DMARC1; p=quarantine;"
   ```

   > Pour en savoir plus sur la fonction des paramètres de la signature DMARC, consultez la documentation de DMARC.

6. Enregistrez les modifications.

> La syntaxe des exemples de signature SPF et DMARC illustre l'ajout aux paramètres d'un serveur DNS BIND. La syntaxe d'une signature SPF ou DMARC ajoutée à d'autres serveurs DNS peut légèrement différer de l'exemple fourni.

Protection anti-virus des messages

Kaspersky Secure Mail Gateway assure la protection antivirus des messages : il recherche la présence éventuelles de virus et autres programmes présentant une menace dans les messages électroniques et répare les objets infectés à l'aide des informations de la version actuelle (la plus récente) des bases anti-virus.

Le module Anti-Virus recherche d'éventuels virus et d'autres programmes présentant une menace dans des messages. Le module Anti-Virus analyse le corps du message et les fichiers joints de tous les formats (pièces jointes) à l'aide des bases anti-virus. Il permet également d'identifier et de bloquer les pièces jointes destinées à un nombre restreint de destinataires et qui font partie d'attaques ciblées contre une vulnérabilité dans une application.

En complément de l'analyse antivirus des messages, vous pouvez activer la détection (cf. section "le Configuration des paramètres du module Anti-Virus" à la page 273) de certains programmes légitimes (cf. section "Présentation de la protection des ordinateurs contre certaines applications légales" à la page 267) par le module Anti-Virus.

Sur la base des résultats de l'analyse antivirus, le module Antivirus attribue au message un des états de la recherche de virus (cf. section "A propos des états de la recherche de virus dans les messages" à la page 271) et ajoute le tag contenant l'état au début de l'objet du message (champ Objet).

Selon l'état qui lui a été attribué, le message est soumis à l'action définie dans les paramètres de la règle de traitement applicable au message. Vous pouvez choisir les actions (cf. section "Configuration des actions à exécuter sur les messages lors de l'analyse antivirus" à la page 276) que l'application exécute sur les messages qui ont un état défini et configurer les tags (cf. section "Configuration des tags dans l'objet des messages selon les résultats de l'analyse antivirus" à la page 279) à ajouter aux messages d'après les résultats de la recherche de virus. Avant de passer au traitement, l'application conserve une copie de ce dernier dans la Sauvegarde.

Vous pouvez indiquer la taille maximale des pièces jointes analysées et définir les objets ne faisant pas l'objet d'une analyse antivirus (cf. section "Configuration des restrictions et des exclusions de l'analyse antivirus des messages" à la page 282). Il est possible d'exclure de l'analyse les pièces jointes d'un certain format ou les pièces jointes portant un nom défini.

Le module Anti-Virus est activé par défaut. Le cas échéant, vous pouvez désactiver le module Antivirus (cf. section "Activation et désactivation de la protection antivirus des messages" à la page 272) ou désactiver la recherche de virus dans les messages pour n'importe quelle règle (cf. section "Activation et désactivation de la recherche de virus pour une règle" à la page 272).

Dans cette section

Présentation de la protection des ordinateurs contre certaines applications légales

Les *applications légales* sont des applications qui peuvent être installées et utilisées sur les ordinateurs des utilisateurs et qui ont été développées pour réaliser les tâches de l'utilisateur. Il existe toutefois certaines applications légales qui sont capables de nuire aux ordinateurs de particuliers ou aux réseaux d'entreprises si elles sont utilisées par des individus malintentionnés. Un individu malintentionné qui parviendrait à prendre les commandes d'une application de ce genre sur l'ordinateur de l'utilisateur ou à en installer une pourrait exploiter certaines de ses fonctions pour compromettre la sécurité de l'ordinateur de l'utilisateur ou du réseau informatique

de l'organisation.

Parmi celles-ci, nous retrouvons les clients IRC, les numéroteurs automatiques (dialers), les programmes pour le chargement des fichiers, les dispositifs de surveillance de l'activité des systèmes informatiques, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet.

Ces types d'application sont décrits en détails dans le tableau ci-dessous.

Type	Nom	Description
Client-IRC	Client de canal IRC	Les utilisateurs installent ces applications afin de pouvoir communiquer dans les canaux IRC (Internet Relay Chats). Les individus malintentionnés les utilisent pour diffuser des programmes malveillants.
Dialer	Numéroteurs automatiques	Ils peuvent établir des connexions téléphoniques par modem à l'insu de l'utilisateur.
Downloader	Programmes de téléchargement	Ils peuvent télécharger des fichiers depuis des pages Internet en mode caché.
Monitor	Programmes de surveillance	Ils permettent de surveiller l'activité sur l'ordinateur sur lequel ils sont installés (observent les applications exécutées et les échanges de données avec les applications sur d'autres ordinateurs).
PSWTool	Récupérateur de mots de passe	Ils permettent de consulter et de récupérer les mots de passe oubliés. C'est à cette fin que les individus malintentionnés les installent à l'insu des utilisateurs.
RemoteAdmin	Programmes d'administration à distance	Ils sont souvent utilisés par les administrateurs de système ; ils permettent d'accéder à l'interface de l'ordinateur distant afin de l'observer et de l'administrer. Les individus malintentionnés les installent dans ce même but à l'insu des utilisateurs afin d'observer les ordinateurs et de les administrer. Les applications légales d'administration à distance se distinguent des chevaux de Troie d'administration à distance de type porte dérobée. Les chevaux de Troie possèdent des fonctions qui leur permettent de s'introduire dans un système et de s'y installer. Les applications légales ne possèdent pas de telles fonctions.

Type	Nom	Description
Server-FTP	Serveurs FTP	Ils remplissent les fonctions d'un serveur FTP. Les individus malintentionnés les introduisent sur les ordinateurs afin d'ouvrir un accès à distance via le protocole FTP.
Server-Proxy	Serveurs proxy	Ils remplissent les fonctions d'un serveur proxy. Les individus malintentionnés les installent sur les ordinateurs afin de pouvoir diffuser du courrier indésirable au nom de ceux-ci.
Server-Telnet	Serveurs Telnet	Ils remplissent les fonctions d'un serveur Telnet. Les individus malintentionnés les introduisent sur les ordinateurs afin d'ouvrir un accès à distance via le protocole Telnet.
Server-Web	Serveurs Internet	Ils remplissent les fonctions d'un serveur Internet. Les individus malintentionnés les introduisent sur les ordinateurs afin d'ouvrir un accès à distance via le protocole HTTP.
RiskTool	Outils pour travailler sur une machine virtuelle	Ils offrent des possibilités complémentaires lors de l'utilisation d'un ordinateur (dissimulation de fichiers ou de fenêtres d'applications actives, interruption de processus actifs).
NetTool	Outils réseau	Une fois installés sur l'ordinateur, ils permettent d'exploiter des fonctions complémentaires lors de l'utilisation d'autres ordinateurs du réseau (redémarrage, détection de ports ouverts, exécution d'applications).
Client-P2P	Clients de réseaux d'échange de fichiers	Ils permettent d'utiliser les réseaux P2P. Les individus malintentionnés peuvent les utiliser pour diffuser des programmes malveillants.

Type	Nom	Description
Client-SMTP	Clients SMTP	Ils envoient des messages électroniques en mode masqué. Les individus malintentionnés les installent sur les ordinateurs afin de pouvoir diffuser du courrier indésirable au nom de ceux-ci.
WebToolbar	Barre d'outils Internet	Ils ajoutent une barre d'outils dans l'interface d'autres applications en vue d'une utilisation de systèmes de recherche.
FraudTool	Pseudo-programmes	Ils se font passer pour d'autres programmes. Par exemple, il existe des pseudo-antivirus ; ils affichent des messages sur la découverte de programmes malveillants alors qu'en réalité ils sont incapables d'identifier ou de réparer quoi que ce soit.

A propos des états de la recherche de virus dans les messages

En fonction des résultats de l'analyse antivirus, le module Anti-Virus attribue au message l'un des états suivants :

- *Clean (message sain)* : l'objet n'est pas infecté.
- *Infected (message infecté)* : l'objet est infecté, irréparable ou la réparation de l'objet n'a pas été effectuée.
- *Disinfected (message réparé)* : l'objet a été réparé.
- *Encrypted (message crypté)* : l'analyse est impossible, car l'objet est crypté.
- *Corrupted (message corrompu)* : l'objet est endommagé ou son analyse s'est soldée par un échec.

- *Attachments with macros (pièces jointes avec les macros)* : le message contient une macro dans la pièce jointe.

Activation et désactivation de la protection antivirus des messages

► *Pour activer ou désactiver la protection antivirus des messages, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Dans le groupe **Antivirus**, exécutez l'une des actions suivantes :

   - Activez le commutateur en regard du nom du groupe de paramètres **Antivirus** pour activer la protection antivirus des messages.

   - Désactivez le commutateur en regard du nom du groupe de paramètres **Antivirus** pour désactiver la protection antivirus des messages.

Activation et désactivation de l'analyse antivirus pour une règle

Vous pouvez activer ou désactiver l'analyse contre les virus de messages pour une ou plusieurs règles. Cette analyse est activée par défaut.

Avant d'activer ou de désactiver l'analyse antivirus des messages pour une règle, confirmez que le module Antivirus de Kaspersky Secure Mail Gateway est activé (cf. section "Activation et désactivation de la protection contre les tentatives de phishing" à la page 306).

► *Pour activer ou désactiver l'analyse antivirus des messages pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez activer ou désactiver l'analyse antivirus des messages.
3. Sélectionnez le groupe **Antivirus**.
4. Exécutez une des actions suivantes :
   - Activez le commutateur en regard du nom du groupe de paramètres **Antivirus** pour activer l'analyse antivirus des messages pour la règle.
   - Désactivez le commutateur en regard du nom du groupe de paramètres **Antivirus** pour désactiver l'analyse antivirus des messages pour la règle.
5. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration des paramètres du module Anti-Virus

► *Pour configurer les paramètres du module Anti-Virus, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.
2. Cliquez sur n'importe quel lien du groupe **Antivirus** pour ouvrir la fenêtre **Paramètres du module Antivirus**.
3. Dans le groupe de paramètres **Protection et analyse heuristique**, sélectionnez une des options suivantes de la liste déroulante **Utiliser KSN** :
   - **Oui –** pour utiliser le service KSN ;
   - **Non –** pour ne pas utiliser le service KSN.
4. Dans le groupe de paramètres **Protection et analyse heuristique**, sélectionnez une des options suivantes de la liste déroulante **Utiliser l'analyse heuristique** :
   - **Oui –** pour utiliser l'analyse heuristique.
   - **Non**, si vous ne souhaitez pas utiliser l'analyse heuristique.

5. Si vous avez activé l'utilisation de l'analyse heuristique, sélectionnez le niveau d'analyse heuristique requis dans la liste **Niveau de l'analyse heuristique** du groupe de paramètres **Protection et analyse heuristique**.

6. Dans le groupe de paramètres **Protection et analyse heuristique**, sélectionnez une des options suivantes dans la liste déroulante **Je considère certaines applications légales, qui peuvent être utilisées par des individus malintentionnés, comme dangereuses pour le réseau informatique de l'entreprise** :

   - **Oui**, si vous estimez que de telles applications, utilisées par des individus malintentionnés, pourraient nuire au réseau informatique de l'entreprise.

   - **Non**, si vous n'estimez pas que de telles applications, utilisées par des individus malintentionnés, pourraient nuire au réseau informatique de l'entreprise.

   Sont considérées comme applications légales (cf. section "Présentation de la protection des ordinateurs contre certaines applications légales" à la page 267) , les utilitaires commerciaux d'administration à distance, les clients IRC, les composeurs, les applications de téléchargement de fichiers, les moniteurs d'activité des systèmes informatiques, les utilitaires de mots de passe. Les messages contenant ces applications sont traités conformément aux règles appliquées aux objets infectés.

7. Si dans la liste **Je considère certaines applications légales, qui peuvent être utilisées par des individus malintentionnés, comme dangereuses pour le réseau informatique de l'entreprise** vous avez choisi **Oui**, sélectionnez une des options suivantes dans la liste déroulante **Activer la détection de certaines applications légales** du groupe de paramètres **Protection et analyse heuristique** :

   - **Oui**, si vous souhaitez que Kaspersky Secure Mail Gateway détecte de telles applications.

   - **Non**, si vous souhaitez désactiver la détection de ces applications par Kaspersky Secure Mail Gateway.

8. Dans le groupe de paramètres **Performance**, indiquez dans le champ **Durée maximale de l'analyse** la durée maximale de l'analyse des messages à la recherche de virus (en secondes).

Si la recherche de virus dans le message n'est pas terminée dans le délai imparti, Kaspersky Secure Mail Gateway exécute les actions suivantes :

- Interruption de l'analyse du message (action **Ignorer**).
- Attribution de l'état *Clean (message sain)* au message.
- Ajout du tag `av-status="Clean"` à l'objet du message.
- Remise du message au destinataire.
- Ajout de l'enregistrement suivant au journal des événements /var/log/maillog :

```
<date et heure de l'analyse> <nom d'hôte de Kaspersky Secure Mail Gateway> : not clean: message-id = <ID du message> : relay-ip = <adresse IP de l'ordinateur du destinataire du message> : action="Skipped": rules = <ID de la règle> : size = <taille du message> : mail-from = <adresse email de l'expéditeur du message> : rcpt-to = <adresse email de l'expéditeur du message> : av-status="Clean", ap-status="Error", as-status="Error", ma-status="NotScanned, disabled by settings", cf-status="NotScanned, disabled by settings">
```

9. Dans le groupe de paramètres **Performance**, indiquez dans le champ **Niveau d'imbrication** le niveau maximal d'imbrication des messages analysés par le module Anti-Virus.
10. Cliquez sur le bouton **Appliquer**.

Utilisation des valeurs par défaut des paramètres du module Anti-Virus

► *Pour utiliser les valeurs par défaut des paramètres du module Anti-Virus, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.
2. Cliquez sur n'importe quel lien du groupe **Antivirus** pour ouvrir la fenêtre **Paramètres du module Antivirus**.

3. Dans la partie inférieure de la fenêtre **Paramètres du module Antivirus**, cliquez sur le lien **Etablir les valeurs par défaut**.

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

Configuration des actions à exécuter sur les messages lors de l'analyse antivirus

► *Pour configurer les actions de Kaspersky Secure Mail Gateway sur les messages lors de l'analyse antivirus, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les actions à effectuer sur les messages lors de l'analyse antivirus.

3. Sélectionnez le groupe **Antivirus**.

4. Activez le commutateur en regard du groupe de paramètres **Antivirus**, s'il est désactivé.

5. Dans la liste déroulante **En cas de détection d'un objet infecté** , sélectionnez une des actions suivantes à exécuter sur les messages infectés qui constituent une menace pour le réseau local de l'organisation :

   - **Réparer**.
   - **Supprimer la pièce jointe**.
   - **Supprimer le message**.
   - **Refuser le message**.
   - **Ignorer**.

   Réparer est l'action sélectionnée par défaut.

6. Si pour le paramètre **En cas de détection d'un objet infecté** vous avez choisi l'action **Réparer**, choisissez dans la liste déroulante **En cas d'échec de la désinfection** dans la

partie droite de l'espace de travail une des actions suivantes à réaliser sur les messages infectés qui n'ont pas pu être désinfectés :

- **Supprimer la pièce jointe**.
- **Supprimer le message**.
- **Refuser le message**.

Supprimer la pièce jointe est l'action sélectionnée par défaut.

7. Si vous avez choisi **Réparer**, **Supprimer la pièce jointe** ou **Supprimer le message** en guise d'action, vous pouvez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant leur traitement. Pour ce faire, cochez la case en regard du nom du paramètre **Placer au préalable une copie dans la Sauvegarde**.

   Par défaut, avant l'exécution des actions **Réparer**, **Supprimer la pièce jointe** et **Supprimer le message**, l'application place une copie des messages dans la Sauvegarde.

8. Dans le menu déroulant **En cas de détection d'erreurs d'analyse**, sélectionnez l'une des actions suivantes à exécuter sur les messages dont l'analyse a mis en évidence des erreurs :

   - **Supprimer la pièce jointe**.
   - **Supprimer le message**.
   - **Refuser le message**.
   - **Ignorer**.

   Ignorer est l'action sélectionnée par défaut.

9. Si vous avez choisi l'action **Supprimer la pièce jointe** ou **Supprimer le message**, vous pouvez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant leur traitement. Pour ce faire, cochez la case en regard du nom du paramètre **Placer au préalable une copie dans la Sauvegarde**.

   Par défaut, avant l'exécution des actions **Supprimer la pièce jointe** et **Supprimer le message**, l'application place une copie des messages dans la Sauvegarde.

10. Dans le menu déroulant **En cas de détection d'un objet chiffré**, sélectionnez une des actions suivantes à exécuter sur les messages contenant des objets cryptés :

    - **Supprimer la pièce jointe**.
    - **Supprimer le message**.
    - **Refuser le message**.
    - **Ignorer**.

    Ignorer est l'action sélectionnée par défaut.

11. Si vous avez choisi l'action **Supprimer la pièce jointe** ou **Supprimer le message**, vous pouvez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant leur traitement. Pour ce faire, cochez la case en regard du nom du paramètre **Placer au préalable une copie dans la Sauvegarde**.

    Par défaut, avant l'exécution des actions **Supprimer la pièce jointe** et **Supprimer le message**, l'application place une copie des messages dans la Sauvegarde.

12. Cochez la case **Traiter les pièces jointes avec des macros**, si vous souhaitez que l'application traite les pièces jointes avec des macros.

13. Dans le menu déroulant **En cas de détection d'une macro**, sélectionnez une des actions suivantes à exécuter sur les messages contenant des macros en pièce jointe :

    - **Supprimer la pièce jointe**.
    - **Supprimer le message**.
    - **Refuser le message**.
    - **Ignorer**.

    Supprimer la pièce jointe est l'action sélectionnée par défaut.

14. Si vous avez choisi l'action **Supprimer la pièce jointe** ou **Supprimer le message**, vous pouvez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant leur traitement. Pour ce faire, cochez la case en regard du nom du paramètre **Placer au préalable une copie dans la Sauvegarde**.

Par défaut, avant l'exécution des actions **Supprimer la pièce jointe** et **Supprimer le message**, l'application place une copie des messages dans la Sauvegarde.

15. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que l'analyse antivirus des messages pour une règle est activée (cf. section "Activation et désactivation de l'analyse antivirus pour une règle" à la page 272), et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Configuration des tags dans l'objet des messages selon les résultats de l'analyse antivirus

► *Pour configurer les tags que Kaspersky Secure Mail Gateway ajoutera à l'objet des messages à la suite de l'analyse antivirus, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les tags à ajouter à l'objet des messages selon les résultats de l'analyse antivirus.

3. Sélectionnez le groupe **Antivirus**.

4. Activez le commutateur en regard du groupe de paramètres **Antivirus**, s'il est désactivé.

5. Ajoutez un tag au champ Objet pour les messages infectés. Pour ce faire, procédez comme suit :

    a. Dans le groupe de paramètres **En cas de détection d'un objet infecté**, cliquez sur le lien à droite du nom du paramètre **Ajouter le texte suivant à l'objet du message infecté** pour ouvrir la fenêtre **Tag pour message contenant des objets malveillants**.

b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des messages infectés. Par exemple, vous pouvez ajouter le tag **Infected**.

c. Cliquez sur le bouton **OK**.

La fenêtre **Tag pour message contenant des objets malveillants** se ferme.

6. Ajoutez un tag au champ Objet pour les messages désinfectés. Pour ce faire, procédez comme suit :

a. Dans le groupe de paramètres **En cas de détection d'un objet infecté**, cliquez sur le lien à droite du nom du paramètre **Ajouter le texte suivant à l'objet du message réparé** pour ouvrir la fenêtre **Tag pour message contenant des objets réparés**.

b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des messages réparés. Par exemple, vous pouvez ajouter le tag **Cured**.

c. Cliquez sur le bouton **OK**.

La fenêtre **Tag pour message contenant des objets réparés** se ferme.

7. Ajoutez un tag dans le champ Objet des messages contenant des objets dont l'analyse s'est soldée par une erreur. Pour ce faire, procédez comme suit :

a. Dans le groupe de paramètres **En cas de détection d'erreurs d'analyse** , cliquez sur le lien à droite du nom du paramètre **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Tag pour message contenant des objets provoquant des erreurs d'analyse**.

b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des messages dont l'analyse provoque des erreurs d'analyse. Par exemple, vous pouvez ajouter le tag **Corrupted**.

c. Cliquez sur le bouton **OK**.

La fenêtre **Tag pour message contenant des objets provoquant des erreurs d'analyse** se ferme.

8. Ajoutez un tag dans le champ Objet des messages contenant des objets cryptés. Pour ce faire, procédez comme suit :

a. Dans le groupe de paramètres **En cas de détection d'un objet chiffré**, cliquez sur le lien à droite du paramètre **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Tag pour message contenant des objets chiffrés**.

b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des messages contenant des objets cryptés. Par exemple, vous pouvez ajouter le tag **Encrypted**.

c. Cliquez sur le bouton **OK**.

La fenêtre **Tag pour message contenant des objets chiffrés** se ferme.

9. Ajoutez un tag dans le champ Objet des messages contenant des macros en pièce jointe. Pour ce faire, procédez comme suit :

   a. Dans le groupe de paramètres **En cas de détection d'une macro**, cliquez sur le lien à droite du nom du paramètre **Ajouter à l'objet du message le texte** pour ouvrir fenêtre **Note pour désigner les messages dont les pièces jointes renferment des macros**.

   b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des messages contenant des macros en pièce jointe. Par exemple, vous pouvez ajouter la note **Attachments with Macros**.

   c. Cliquez sur le bouton **OK**.

   La fenêtre **Note pour désigner les messages dont les pièces jointes renferment des macros** se ferme.

10. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que l'analyse antivirus des messages pour une règle est activée (cf. section "Activation et désactivation de l'analyse antivirus pour une règle" à la page 272), et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Configuration des restrictions et des exclusions de l'analyse antivirus des messages

► *Pour configurer les restrictions et les exclusions de l'analyse antivirus des messages pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les restrictions et les exclusions de l'analyse antivirus.

3. Sélectionnez le groupe **Antivirus**.

4. Activez le commutateur en regard du groupe de paramètres **Antivirus**, s'il est désactivé.

5. Pour exclure les archives de l'analyse antivirus des messages, cochez dans le groupe de paramètres **Exclusions de l'analyse** la case **Ne pas analyser les archives**.

6. Pour exclure de l'analyse antivirus les pièces jointes d'une taille déterminée, allez dans le groupe de paramètres **Exclusions de l'analyse** et procédez comme suit :

    a. Cliquez sur lien à droite du paramètre **Ne pas analyser les objets dont la taille est supérieur à :** pour ouvrir la fenêtre **Limitation en fonction de la taille des messages**.

    b. Dans le champ situé sous le nom de la fenêtre, saisissez la taille maximale des objets à analyser, qui doit être comprise entre 0 Ko et 1048576 Ko (1 Go).

    Si la valeur est égale à 0 Ko, la taille des objets n'est pas limitée.

    c. Cliquez sur le bouton **OK**.

    La fenêtre **Limitation en fonction de la taille des messages** se ferme.

7. Pour exclure de l'analyse antivirus les pièces jointes portant un nom spécifique, allez dans le groupe de paramètres **Exclusions de l'analyse** et procédez comme suit :

a. Cliquez sur le lien à droite du paramètre **Ne pas analyser les pièces jointes selon les masques de noms** pour ouvrir la fenêtre **Limitation en fonction des masques de nom**.

b. Dans le champ situé sous le nom de la fenêtre, saisissez les masques de noms des pièces jointes à exclure de l'analyse antivirus.

Les masques peuvent contenir n'importe quel caractère. Les masques doivent être séparés par un point-virgule.

c. Cliquez sur le bouton **OK**.

La fenêtre **Limitation en fonction des masques de nom** se ferme.

8. Pour exclure de l'analyse antivirus les pièces jointes d'un format déterminé, allez dans le groupe de paramètres **Exclusions de l'analyse** et procédez comme suit :

a. Cliquez sur le lien à droite du paramètre **Ne pas analyser les objets joints sur les types de fichiers** pour ouvrir la fenêtre **Limitation en fonction du type de fichiers**.

b. Cochez les cases correspondant aux types de format des pièces jointes à exclure de l'analyse antivirus.

c. Cliquez sur le bouton **Fermer**.

La fenêtre **Limitation en fonction du type de fichiers** se ferme.

9. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que l'analyse antivirus des messages pour une règle est activée (cf. section "Activation et désactivation de la recherche de virus pour une règle" à la page 272), et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Protection contre le courrier indésirable

Kaspersky Secure Mail Gateway filtre le courrier indésirable (spam) dans le flux des messages électroniques transmis par le serveur de messagerie.

L'analyse antispam des messages est effectuée par le module Anti-Spam. Le module Anti-Spam recherche des éléments de courrier indésirable dans chacun des messages analysés. Pour cela, le module Anti-Spam, analyse d'abord les attributs du message tels que : les adresses de l'expéditeur et du destinataire, la taille du message, les titres (y compris les en-tête De et A). Ensuite le module Anti-Spam analyse le contenu du message (y compris l'en-tête Objet) et des fichiers joints.
Le module Anti-Spam est activé par défaut. S'il y a lieu, vous pouvez désactiver le module Anti-Spam (cf. section "Activation et désactivation de la protection contre le courrier indésirable" à la page 287) ou désactiver l'analyse 'analyse antispam des messages pour n'importe quelle règle (cf. section "Activation et désactivation de l'analyse antispam des messages pour une règle" à la page 287). Il est également possible de limiter la taille des messages qui seront soumis à l'analyse contre les spams.

L'application attribue au message dans lequel du courrier indésirable ou du courrier indésirable potentiel a été détecté un état défini (cf. section "A propos des états de l'analyse antispam" à la page 286) conformément au niveau de spam obtenu suite à l'analyse du message par le module Anti-Spam. Le *niveau de spam* est un nombre entier compris entre 0 et 100 obtenu par addition de points attribués au message à chaque déclenchement du module Anti-Spam.
Pour déterminer le classement du message, l'application prend également en considération les réponses des serveurs DNSBL et SURBL, la réponse du serveur UDS et celle de la technologie SPF, sans oublier les résultats du filtrage des messages selon la réputation.

Le *filtrage de la réputation* est un service dans le nuage qui utilise la technologie de définition de la réputation des messages. Les informations relatives à l'apparition des nouveaux types de spam sont plus vite disponibles dans le nuage que dans les bases du module Anti-Spam, ce qui permet d'accélérer la détection des éléments de courrier indésirable dans les messages et d'améliorer la précision de cette détection.

Selon l'état qui lui a été attribué, le message est soumis à l'action définie dans les paramètres de la règle de traitement applicable au message. Vous pouvez choisir les actions (cf.

section "Configuration des actions à exécuter sur les messages lors de l'analyse contre les spams" à la page 295), que l'application exécute sur les messages qui ont un état défini, et configurer les tags (cf. section "Configuration des tags dans l'objet des messages selon les résultats de l'analyse antispam" à la page 298) à ajouter aux messages d'après les résultats de l'analyse antispam.
Par défaut, l'application exécute l'action **Skip (Ignorer)**.

Il est possible de modifier les fonctions du module Anti-Spam en modifiant le fichier de configuration de l'Anti-Spam. Dans le fichier de configuration, vous pouvez modifier par exemple les états de l'analyse antispam (cf. section "A propos des états de l'analyse antispam" à la page 286) ou le niveau de détail de l'enregistrement des données des messages électroniques dans le journal des événements de Kaspersky Secure Mail Gateway (cf. section "Présentation du journal des événements" à la page 379).

Le fichier de configuration du module Anti-Spam est accessible via la console de gestion de Kaspersky Secure Mail Gateway en mode de Support Technique avec les autorisations de superutilisateur.

Dans cette section

A propos des états de l'analyse antispam

En fonction des résultats de l'analyse antispam, le module Anti-Spam attribue au message l'un des états suivants :

- *Clean (courrier normal)* : le message ne contient pas de courrier indésirable.
- *Spam (courrier indésirable)* : l'application a classé le message comme courrier indésirable confirmé.
- *Probable spam (courrier potentiellement indésirable)* : le message est peut-être non sollicité.
- *Blacklisted (Message d'un expéditeur douteux)* : l'adresse email de l'expéditeur fait partie de la liste globale ou personnelle des adresses (cf. section "Listes noires et blanches des adresses" à la page 338) ou l'adresse IP ou le nom DNS de l'hôte font partie de la liste noire

DNSBL (cf. section "Configuration de la liste DNSBL personnalisée du module Anti-Spam" à la page 290).

- *Massmail (diffusion massive)* : le message a été reçu dans le cadre d'un envoi de masse.
- *Error (erreur d'analyse)* : l'analyse du message s'est soldée par un échec.

Activation et désactivation de la protection contre le courrier indésirable

► *Pour activer ou désactiver la protection des messages contre le courrier indésirable, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.
2. Dans le groupe **Anti-spam**, exécutez l'une des actions suivantes :
   - Activez le commutateur en regard du nom du groupe de paramètres **Anti-spam** pour activer la protection des messages contre le courrier indésirable.
   - Désactivez le commutateur en regard du nom du groupe de paramètres **Anti-spam** pour désactiver la protection des messages contre le spam.

Activation et désactivation de l'analyse antispam des messages pour une règle

Vous pouvez activer ou désactiver l'analyse des messages contre les spams pour une ou plusieurs règles. Cette analyse est activée par défaut.

Avant d'activer ou de désactiver l'analyse antispam des messages pour une règle, confirmez que le module Anti-Spam de Kaspersky Secure Mail Gateway est activé (cf. section "Activation et désactivation de la protection contre les tentatives de phishing" à la page 306).

► *Pour activer ou désactiver l'analyse antispam des messages pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez activer ou désactiver l'analyse antispam des messages.

3. Sélectionnez le groupe **Anti-spam**.

4. Exécutez une des actions suivantes :

   - Activez le commutateur en regard du groupe de paramètres **Anti-spam** pour activer l'analyse antispam des messages pour la règle.

   - Désactivez le commutateur en regard du groupe de paramètres **Anti-spam** pour désactiver l'analyse antispam des messages pour la règle.

5. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration des paramètres du module Anti-Spam

► *Pour configurer les paramètres du module Anti-Spam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe lequel des liens suivants **Utiliser KSN**, **Utiliser le service Enforced Anti-spam Updates**, **Utiliser le filtrage par réputation** ou **Temps maximal de l'analyse** du groupe **Anti-spam** pour ouvrir la fenêtre **Paramètres du module Anti-spam**.

3. Dans la liste déroulante **Utiliser KSN** du groupe de paramètres **Services externes**, sélectionnez une des options suivantes :

   - **Oui –** pour utiliser le service KSN ;

   - **Non –** pour ne pas utiliser le service KSN.

4. Dans la liste déroulante **Utiliser le service Enforced Anti-spam Updates** du groupe de paramètres **Services externes**, sélectionnez une des options suivantes :

   - **Oui –** pour utiliser le service de mise à jour forcée des bases du module Anti-spam ;
   - **Non –** pour ne pas utiliser le service de mise à jour forcée des bases du module Anti-spam ;

5. Dans la liste déroulante **Utiliser le filtrage par réputation** du groupe de paramètres **Services externes**, sélectionnez une des options suivantes :

   - **Oui –** pour utiliser le service de filtrage de la réputation ;
   - **Non**, si vous ne souhaitez pas utiliser le service de filtrage de la réputation.

6. Dans le groupe de paramètres **Performance**, indiquez dans le champ **Temps maximal de l'analyse** la durée maximale de l'analyse antispam des messages (en secondes).

   Si la recherche de courrier indésirable n'est pas terminée dans le délai imparti, Kaspersky Secure Mail Gateway exécute les actions suivantes :

   - Interruption de l'analyse du message (action **Ignorer**).
   - Attribution de l'état *Error (erreur d'analyse)* au message.
   - Ajout de la note `as-status="Error"` à l'objet du message.
   - Remise du message au destinataire.
   - Ajout de l'enregistrement suivant au journal des événements /var/log/maillog :

     ```
     <date et heure de l'analyse> <nom d'hôte de Kaspersky Secure Mail Gateway> : not clean: message-id = <ID du message> : relay-ip = <adresse IP de l'ordinateur du destinataire du message> : action="Skipped": rules = <ID de la règle> : size = <taille du message> : mail-from = <adresse email de l'expéditeur du message> : rcpt-to = <adresse email de l'expéditeur du message> : av-status="Clean", ap-status="Error", as-status="Error", ma-status="NotScanned, disabled by settings", cf-status="NotScanned, disabled by settings">
     ```

7. Cliquez sur le bouton **Appliquer**.

Utilisation des valeurs par défaut des paramètres du module Anti-Spam

► *Pour utiliser les valeurs par défaut des paramètres du module Anti-Spam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe lequel des liens suivants **Utiliser KSN**, **Utiliser le service Enforced Anti-spam Updates**, **Utiliser le filtrage par réputation** ou **Temps maximal de l'analyse** du groupe **Anti-spam** pour ouvrir la fenêtre **Paramètres du module Anti-spam**.

3. Dans la partie inférieure de la fenêtre **Paramètres du module Anti-spam**, cliquez sur le lien **Etablir les valeurs par défaut**.

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

Configuration de la liste personnalisée DNSBL du module Anti-Spam

Vous pouvez créer *une liste de serveurs DNSBL personnalisée* pour renforcer l'efficacité de la détection du courrier indésirable. Les listes d'adresses IP qui ont été repérées par le passé dans l'objet ou le corps de messages identifiés comme indésirables et auxquelles le module Anti-Spam attribue un niveau de spam et un des états d'analyse antispam (cf. section "A propos des états de l'analyse antispam" à la page 286) sont stockées sur les serveurs DNSBL.

► *Pour créer la liste personnalisée DNSBL du module Anti-Spam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Dans le groupe **Anti-spam**, cliquez sur le lien **Liste personnalisée DNSBL** pour ouvrir la fenêtre **Liste personnalisée DNSBL**.

3. Dans le champ situé sous le nom de la fenêtre, saisissez les noms DNS ou les adresses IP à inscrire sur la liste DNSBL.

   Vous pouvez uniquement saisir les caractères a–z, A–Z, 0–9, "-" et ".", le caractère "-" ne peut pas être le dernier. Par exemple, vous pouvez ajouter à la liste le nom DNS de l'expéditeur dns-bl.example.com ou l'adresse IP 10.0.0.1 de l'expéditeur.

   Les adresses doivent être séparées par un point-virgule.

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

► *Pour consulter la liste personnalisée DNSBL du module Anti-Spam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Dans le groupe **Anti-spam**, cliquez sur le lien **Liste personnalisée DNSBL** pour ouvrir la fenêtre **Liste personnalisée DNSBL**.

3. Cliquez sur le bouton **Appliquer** ou **Annuler** quand vous aurez terminé de travailler sur la liste.

   La fenêtre **Liste personnalisée DNSBL** se ferme.

► *Pour supprimer un enregistrement de la liste personnalisée DNSBL du module Anti-Spam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Dans le groupe **Anti-spam**, cliquez sur le lien **Liste personnalisée DNSBL** pour ouvrir la fenêtre **Liste personnalisée DNSBL**.

3. Saisissez un ou plusieurs enregistrements à supprimer dans le champ qui se trouve sous le nom de la fenêtre.

4. Cliquez sur la touche **DELETE**.

5. Cliquez sur le bouton **Appliquer**.

Configuration de la liste personnalisée SURBL du module Anti-Spam

Vous pouvez créer *une liste de serveurs SURBL personnalisée* pour renforcer l'efficacité de la détection du courrier indésirable. Les listes des adresses Internet qui ont été repérées par le passé dans l'objet ou le corps de messages identifiés comme indésirables et auxquelles le module Anti-Spam attribue un niveau de spam et un des états de l'analyse antispam (cf. section "A propos des états de l'analyse antispam" à la page 286) sont stockées sur les serveurs SURBL.

► *Pour créer la liste personnalisée SURBL du module Anti-Spam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Dans le groupe **Anti-spam**, cliquez sur le lien **Liste personnalisée SURBL** pour ouvrir la fenêtre **Liste personnalisée SURBL**.

3. Dans le champ situé sous le nom de la fenêtre, saisissez les noms DNS ou les adresses IP à inscrire sur la liste SURBL.

   Vous pouvez uniquement saisir les caractères a–z, A–Z, 0–9, "-" et ".", le caractère "-" ne peut pas être le dernier. Par exemple, vous pouvez ajouter à la liste le nom DNS dns-bl.example.com ou l'adresse IP 10.0.0.1.

   Les adresses doivent être séparées par un point-virgule.

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

► *Pour consulter la liste personnalisée SURBL du module Anti-Spam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Dans le groupe **Anti-spam**, cliquez sur le lien **Liste personnalisée SURBL** pour ouvrir la fenêtre **Liste personnalisée SURBL**.

3. Cliquez sur le bouton **Appliquer** ou **Annuler** quand vous aurez terminé de travailler sur la liste.

La fenêtre **Liste personnalisée SURBL** se ferme.

► *Pour supprimer un enregistrement de la liste personnalisée SURBL du module Anti-Spam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Dans le groupe **Anti-spam**, cliquez sur le lien **Liste personnalisée SURBL** pour ouvrir la fenêtre **Liste personnalisée SURBL**.

3. Saisissez un ou plusieurs enregistrements à supprimer dans le champ qui se trouve sous le nom de la fenêtre.

4. Cliquez sur la touche **DELETE**.

5. Cliquez sur le bouton **Appliquer**.

Configuration des paramètres du module Anti-Spam pour une règle

Vous pouvez configurer les paramètres du module Anti-Spam pour une ou plusieurs règles.

► *Pour configurer les paramètres du module Anti-Spam pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les paramètres du module Anti-Spam.

3. Sélectionnez le groupe **Anti-spam**.

4. Activez le commutateur en regard du groupe de paramètres **Anti-spam** s'il est désactivé.

5. Dans le groupe de paramètres **Paramètres généraux**, cochez les cases en regard des paramètres généraux à activer :

a. **Utiliser les technologies de traitement des images**, si vous souhaitez utiliser la technologie GSG qui permet d'identifier les images contenant du texte en vue de confirmer si ce texte est indésirable. Le texte est reconnu même s'il a été modifié, transformé en image, "brouillé" ou soumis à n'importe quel autre traitement visant à masquer le rôle de l'image envoyée.

b. **Analyser les pièces jointes au format RTF** pour que le module Anti-Spam analyse les pièces jointes aux messages présentant un format RTF.

6. Dans le groupe de paramètres **Analyse à l'aide de services externes**, cochez les cases en regard des paramètres d'utilisation des services externes à activer :

   a. **Utiliser la liste DNSBL définie par l'utilisateur** (cf. section "**Configuration de la liste DNSBL personnalisée du module Anti-Spam**" à la page 290), si vous voulez que le module Anti-Spam vérifie la présence d'adresses des expéditeurs sur les serveurs DNSBL dans la liste DNSBL personnalisée.

   Vous pouvez consulter la liste DNSBL personnalisée en cliquant sur **personnalisée** dans le nom du paramètre **Utiliser la liste DNSBL définie par l'utilisateur**.

   b. **Utiliser la liste SURBL définie par l'utilisateur** (cf. section "**Configuration de la liste DNSBL personnalisée du module Anti-Spam**" à la page 292), si vous voulez que le module Anti-Spam vérifie la présence d'adresses Internet repérées dans l'objet ou le corps de messages sur les serveurs SURBL présents dans la liste SURBL personnalisée.

   Vous pouvez consulter la liste SURBL personnalisée en cliquant sur **personnalisée** dans le nom du paramètre **Utiliser la liste SURBL définie par l'utilisateur**.

7. Dans le groupe de paramètres **Augmenter le niveau de spam si**, cochez les cases en regard des langues et des polices dont l'utilisation dans un message peut augmenter le score de courrier indésirable :

   a. **Le message est rédigé en chinois**, pour que le module Anti-Spam augmente le score de courrier indésirable des messages rédigés en chinois.

   b. **Le message est rédigé en japonais**, pour que le module Anti-Spam augmente le score de courrier indésirable des messages rédigés en japonais.

c. **Le message est rédigé en coréen**, pour que le module Anti-Spam augmente le score de courrier indésirable des messages rédigés en coréen.

d. **Le message est rédigé en thaï**, pour que le module Anti-Spam augmente le score de courrier indésirable des messages rédigés en thaï.

e. **Le message est rédigé en alphabet cyrillique**, pour que le module Anti-Spam augmente le score de courrier indésirable des messages rédigés en cyrillique.

8. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que l'analyse antispam des messages pour une règle est activée et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Configuration des actions à exécuter sur les messages lors de l'analyse contre les spams

► *Pour configurer les actions de Kaspersky Secure Mail Gateway sur les messages lors de l'analyse antispam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les actions à effectuer sur les messages lors de l'analyse antispam.

3. Sélectionnez le groupe **Anti-spam**.

4. Activez le commutateur en regard du groupe de paramètres **Anti-spam** s'il est désactivé.

5. Dans le menu déroulant **En cas de détection d'un courrier indésirable**, sélectionnez une des actions suivantes à exécuter sur les messages contenant du spam :

   - **Supprimer le message**.

- **Refuser le message**.
- **Ignorer**.

6. Si vous voulez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant leur traitement, cochez la case en regard du paramètre **Placer au préalable une copie dans la Sauvegarde**.

   Avant l'exécution de l'action **Supprimer le message**, l'application place par défaut une copie des messages dans la Sauvegarde.

7. Dans le menu déroulant **En cas de détection d'un courrier potentiellement indésirable** , sélectionnez l'une des actions suivantes. Elle sera appliquée aux courriers potentiellement indésirables :

   - **Supprimer le message**.
   - **Refuser le message**.
   - **Ignorer**.

8. Si vous voulez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant leur traitement, cochez la case en regard du paramètre **Placer au préalable une copie dans la Sauvegarde**.

   Avant l'exécution de l'action **Supprimer le message**, l'application place par défaut une copie des messages dans la Sauvegarde.

9. Dans le menu déroulant **Utiliser la liste SURBL définie par l'utilisateur**, sélectionnez une des actions suivantes à effectuer sur les messages dont l'expéditeur a été détecté dans la liste DNSBL (cf. section "Configuration de la liste DNSBL personnalisée du module Anti-Spam" à la page 290) et à qui l'état est attribué (cf. section "A propos des états de l'analyse antispam" à la page 286) *Blacklisted (douteux*) :

   - **Supprimer le message**.
   - **Refuser le message**.
   - **Ignorer**.

10. Si vous voulez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant leur traitement, cochez la case en regard du paramètre **Placer au préalable une copie dans la Sauvegarde**.

    Avant l'exécution de l'action **Supprimer le message**, l'application place par défaut une copie des messages dans la Sauvegarde.

11. Dans le menu déroulant **En cas de détection d'une diffusion de masse** , sélectionnez l'une des actions suivantes. Elle sera appliquée aux messages pour lesquels une diffusion massive a été détectée :

    - **Supprimer le message**.
    - **Refuser le message**.
    - **Ignorer**.

12. Si vous voulez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant leur traitement, cochez la case en regard du paramètre **Placer au préalable une copie dans la Sauvegarde**.

    Avant l'exécution de l'action **Supprimer le message**, l'application place par défaut une copie des messages dans la Sauvegarde.

13. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

L'action **Ignorer** est choisie par défaut pour tous les messages.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que l'analyse antispam des messages pour une règle est activée et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Configuration des tags dans l'objet des messages selon les résultats de l'analyse antispam

► *Pour configurer les tags que Kaspersky Secure Mail Gateway ajoutera à l'objet des messages à la suite de l'analyse antispam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les tags à ajouter à l'objet des messages selon les résultats de l'analyse antispam.

3. Sélectionnez le groupe **Anti-spam**.

4. Activez le commutateur en regard du groupe de paramètres **Anti-spam** s'il est désactivé.

5. Ajoutez un tag dans le champ Objet des messages contenant du courrier indésirable. Pour ce faire, procédez comme suit :

    a. Dans le groupe de paramètres **En cas de détection d'un courrier indésirable**, cliquez sur le lien à droite du paramètre **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Tag pour identifier les courriers indésirables**.

    b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des courriers indésirables. Par exemple, vous pouvez ajouter le tag **Spam**.

    c. Cliquez sur le bouton **OK**.

    La fenêtre **Tag pour identifier les courriers indésirables** se ferme.

6. Ajoutez un tag dans le champ Objet des messages contenant probablement du courrier indésirable. Pour ce faire, procédez comme suit :

    a. Dans le groupe de paramètres **En cas de détection d'un courrier potentiellement indésirable**, cliquez sur le lien à droite du nom du paramètre **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Tag pour identifier les courriers potentiellement indésirables**.

b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des courriers indésirables probables. Par exemple, vous pouvez ajouter le tag **Probable spam**.

c. Cliquez sur le bouton **OK**.

La fenêtre **Tag pour identifier les courriers potentiellement indésirables** se ferme.

7. Ajoutez le tag dans le champ Objet des messages dont l'expéditeur a été détecté dans la liste DNSBL (cf. section "Configuration de la liste DNSBL personnalisée du module Anti-Spam" à la page 290) et à qui l'état a été attribué (cf. section "A propos des états de l'analyse antispam" à la page 286) *Blacklisted (peu fiable*). Pour ce faire, procédez comme suit :

   a. Dans le groupe de paramètres **Si l'adresse email de l'expéditeur du message figure dans la liste noire DNSBL**, cliquez sur le lien à droite du nom du paramètre **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Tag pour désigner les messages de la liste noire DNSBL**.

   b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des messages envoyés par des expéditeurs douteux. Par exemple, vous pouvez ajouter le tag **Blacklisted**.

   c. Cliquez sur le bouton **OK**.

   La fenêtre **Tag pour désigner les messages de la liste noire DNSBL** se ferme.

8. Ajoutez un tag dans le champ Objet des messages envoyés par diffusion massive. Pour ce faire, procédez comme suit :

   a. Dans le groupe de paramètres **En cas de détection d'une diffusion de masse**, cliquez sur le lien à droite du nom du paramètre **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Tag pour désigner les diffusions de masse**.

   b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des messages envoyés par diffusion massive. Par exemple, vous pouvez ajouter le tag **MASSMAIL**.

   c. Cliquez sur le bouton **OK**.

   La fenêtre **Tag pour désigner les diffusions de masse** se ferme.

9. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que l'analyse antispam des messages pour une règle est activée et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Quarantaine de l'Anti-spam

Les messages électronique dont l'analyse par l'Anti-spam n'a pas donné un résultat définitif sont placés temporairement dans la quarantaine de l'Anti-spam. Vous pouvez configurer les paramètres de la quarantaine de l'Anti-spam.

Dans cette section

Activation et désactivation de l'utilisation de la quarantaine de l'Anti-spam

► *Pour activer ou désactiver l'utilisation de la quarantaine de l'Anti-spam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Dans le groupe **Quarantaine de l'Anti-spam**, exécutez l'une des actions suivantes :

   - Activez le commutateur en regard du nom du groupe de paramètres **Quarantaine de l'Anti-spam** pour activer l'utilisation de la quarantaine de l'Anti-spam.

   - Désactivez le commutateur en regard du nom du groupe de paramètres **Quarantaine de l'Anti-spam** pour désactiver l'utilisation de la quarantaine de l'Anti-spam.

Configuration des paramètres de la Quarantaine de l'Anti-spam

Les messages électronique dont l'analyse par l'Anti-spam n'a pas donné un résultat définitif sont placés temporairement dans la quarantaine de l'Anti-spam. Vous pouvez configurer les paramètres de la quarantaine de l'Anti-spam.

► *Pour configurer les paramètres de la quarantaine de l'Anti-Spam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Cliquez sur un des liens **Durée de conservation maximale de l'objet en quarantaine**, **Taille maximale de la quarantaine de l'Anti-spam** ou **Nombre maximal de messages dans la quarantaine de l'Anti-spam** dans le groupe de paramètres **Quarantaine de l'Anti-spam** pour ouvrir la fenêtre **Paramètres du module Anti-spam quarantaine**.

3. Indiquez dans le champ **Durée de conservation maximale du message en quarantaine** la durée maximale de conservation du message dans la quarantaine de l'Anti-Spam à l'issue de laquelle le message est remis au destinataire.

4. Indiquez dans le champ **Taille maximale de la quarantaine de l'Anti-spam** la taille maximale de la quarantaine de l'Anti-spam. Une fois ce volume atteint, les messages ne sont plus mis en quarantaine.

5. Indiquez dans le champ **Nombre maximal de message dans la quarantaine de l'Anti-spam** le nombre maximum de messages dans la quarantaine de l'Anti-spam. Une fois ce nombre dépassé, les messages ne sont plus placés en quarantaine.

6. Cliquez sur le bouton **Appliquer**.

Utilisation des valeurs par défaut des paramètres de la Quarantaine de l'Anti-spam

► *Pour utiliser les valeurs par défaut des paramètres du module Anti-Spam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Cliquez sur un des liens **Durée de conservation maximale de l'objet en Quarantaine**, **Taille maximale de la Quarantaine de l'Anti-spam** ou **Nombre maximal de messages dans la Quarantaine de l'Anti-spam** dans le groupe de paramètres **Quarantaine de l'Anti-spam** pour ouvrir la fenêtre **Paramètres du module Anti-spam Quarantaine**.

3. Dans le bas de la fenêtre **Paramètres du module Anti-spam Quarantaine**, cliquez sur le lien **Etablir les valeurs par défaut**.

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

Protection des messages contre les tentatives de phishing

Kaspersky Secure Mail Gateway filtre les messages qui transitent via le serveur de messagerie et bloque le phishing et les liens vers des ressources Internet qui contiennent des programmes malveillants. Le *phishing* désigne les messages contenant des liens vers des adresses Internet de phishing ou des images ou du texte qui incite l'utilisateur à transmettre des données confidentielles aux individus malintentionnés.

La recherche de phishing et de liens vers des ressources Internet abritant des programmes malveillants est confiée au module Anti-Phishing. Ce dernier analyse le contenu du message (y compris le champ Objet) et les pièces jointes.

Selon les résultats de l'analyse anti-phishing, l'application attribue au message un des états de l'analyse anti-phishing (cf. section "A propos des états de l'analyse anti-phishing" à la page 305) et ajoute le tag contenant l'état au début de l'objet du message (champ Objet). Vous pouvez configurer dans les paramètres de la règle le tag contenant l'état du message (cf. section "Configuration des actions à exécuter sur les messages lors de l'analyse anti-phishing" à la page 309).

En fonction de l'état attribué au message, l'application exécute sur le message l'action (cf. section "Configuration des actions à exécuter sur les messages lors de l'analyse anti-phishing" à la page 309) définie dans les paramètres de la règle d'après laquelle l'application traite le message. Vous pouvez sélectionner les actions que l'application va exécuter sur les messages qui ont un état défini. L'application exécute par défaut l'action **Skip (Ignorer)**. Les messages sont remis à l'utilisateur sans modifications.

Le module Anti-Phishing est activé par défaut. S'il y a lieu, vous pouvez désactiver le module Anti-Phishing (cf. section "Activation et désactivation de la protection contre les tentatives de phishing" à la page 306) ou désactiver l'analyse anti-phishing des messages pour n'importe quelle règle (cf. section "Activation et désactivation de l'analyse anti-phishing des messages pour une règle" à la page 306).

Dans cette section

A propos des états de l'analyse anti-phishing

En fonction des résultats de l'analyse anti-phishing, le module Anti-Phishing attribue au message l'un des états suivants :

- *Clean (pas de tentative de phishing)* : le message ne comporte pas de lien vers une adresse Internet, une image ou un texte de phishing invitant l'utilisateur à communiquer des données confidentielles à des individus malintentionnés. Il ne contient pas non plus de lien vers des ressources Web hébergeant des applications malveillantes.
- *Phishing (tentative de phishing)* : l'application a détecté dans le message une image ou un texte invitant l'utilisateur à transmettre des données confidentielles à des individus malintentionnés.
- *Malicious link (lien malveillant)* : l'application a détecté dans le message un lien vers une ressource Web hébergeant des applications malveillantes.
- *Error (erreur d'analyse)* : l'analyse du message s'est soldée par un échec.

Activation et désactivation de la protection contre les tentatives de phishing

► *Pour activer ou désactiver la protection des messages contre les tentatives de phishing, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Dans le groupe **Anti-phishing**, exécutez l'une des actions suivantes :

   - Activez le commutateur en regard du groupe de paramètres **Anti-phishing** pour activer la protection des messages contre les tentatives de phishing.

   - Désactivez le commutateur en regard du groupe de paramètres **Anti-phishing** pour désactiver la protection des messages contre les tentatives de phishing.

Activation et désactivation de l'analyse anti-phishing des messages pour une règle

Vous pouvez activer ou désactiver l'analyse des messages contre le phishing pour une ou plusieurs règles. Cette analyse est activée par défaut.

Avant d'activer ou de désactiver l'analyse anti-phishing des messages pour une règle, confirmez que le module Anti-Phishing de Kaspersky Secure Mail Gateway est activé (cf. section "Activation et désactivation de la protection contre les tentatives de phishing" à la page 306).

► *Pour activer ou désactiver l'analyse anti-phishing des messages pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.
2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez activer ou désactiver l'analyse anti-phishing des messages.
3. Sélectionnez le groupe **Anti-phishing**.
4. Exécutez une des actions suivantes :
   - Activez le commutateur en regard du groupe de paramètres **Anti-phishing** pour activer l'analyse anti-phishing des messages pour la règle.
   - Désactivez le commutateur en regard du groupe de paramètres **Anti-phishing** pour désactiver l'analyse anti-phishing des messages pour la règle.
5. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration des paramètres du module Anti-Phishing

► *Pour configurer les paramètres du module Anti-Phishing, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.
2. Cliquez sur n'importe quel lien du groupe **Anti-phishing** pour ouvrir la fenêtre **Paramètres du module Anti-phishing**.
3. Sélectionnez l'une des options suivantes dans le menu déroulant **Utiliser KSN** :
   - **Oui –** pour utiliser le service KSN ;
   - **Non –** pour ne pas utiliser le service KSN.
4. Sélectionnez l'une des options suivantes dans le menu déroulant **Utiliser l'Anti-phishing heuristique** :

- **Oui –** pour utiliser l'Anti-Phishing heuristique.
- **Non**, si vous ne souhaitez pas utiliser l'Anti-Phishing heuristique.

5. Dans le champ **Temps maximal de l'analyse**, indiquez la durée maximale de l'analyse anti-phishing des messages (en secondes).

   Si l'analyse des messages à la recherche de phishing ne se termine pas dans le délai que vous avez défini, Kaspersky Secure Mail Gateway exécute les actions suivantes :

   - Interruption de l'analyse du message (action **Ignorer**).
   - Attribution de l'état *Error (erreur d'analyse)* au message.
   - Ajout d'une note à l'objet du message `ap-status="Error"`.
   - Remise du message au destinataire.
   - Ajout de l'enregistrement suivant au journal des événements /var/log/maillog :

     ```
     <date et heure de l'analyse> <nom d'hôte de Kaspersky Secure Mail Gateway> : not clean: message-id = <ID du message> : relay-ip = <adresse IP de l'ordinateur du destinataire du message> : action="Skipped": rules = <ID de la règle> : size = <taille du message> : mail-from = <adresse email de l'expéditeur du message> : rcpt-to = <adresse email de l'expéditeur du message> : av-status="Clean", ap-status="Error", as-status="Error", ma-status="NotScanned, disabled by settings", cf-status="NotScanned, disabled by settings">
     ```

6. Cliquez sur le bouton **Appliquer**.

Utilisation des valeurs par défaut des paramètres du module Anti-Phishing

► *Pour utiliser les valeurs par défaut des paramètres du module Anti-Phishing, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Cliquez sur n'importe quel lien du groupe **Anti-phishing** pour ouvrir la fenêtre **Paramètres du module Anti-phishing**.

3. Dans la partie inférieure de la fenêtre **Paramètres du module Anti-phishing**, cliquez sur le lien **Etablir les valeurs par défaut**.

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

Configuration des actions à exécuter sur les messages lors de l'analyse anti-phishing

► *Pour configurer les actions de Kaspersky Secure Mail Gateway sur les messages lors de l'analyse anti-phishing, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les actions à effectuer sur les messages lors de l'analyse anti-phishing.

3. Sélectionnez le groupe **Anti-phishing**.

4. Activez le commutateur en regard du groupe de paramètres **Anti-phishing** s'il est désactivé.

5. Dans le menu déroulant **En cas de détection de phishing ou de liens menant à des sites Internet hébergeant des programmes malveillants**, sélectionnez l'une des

actions suivantes. Elle sera appliquée aux messages contenant une tentative de phishing ou des liens vers des ressources Web hébergeant des applications malveillantes :

- **Supprimer le message**.
- **Refuser le message**.
- **Ignorer**.

Ignorer est l'action sélectionnée par défaut.

6. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que l'analyse anti-phishing des messages pour une règle est activée (cf. section "Activation et désactivation de l'analyse anti-phishing pour une règle" à la page 306), et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Configuration des tags dans l'objet des messages selon les résultats de l'analyse anti-phishing

► *Pour configurer les tags que Kaspersky Secure Mail Gateway ajoutera à l'objet des messages à la suite de l'analyse anti-phishing, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.
2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les tags à ajouter à l'objet des messages selon les résultats de l'analyse anti-phishing.
3. Sélectionnez le groupe **Anti-phishing**.
4. Activez le commutateur en regard du groupe de paramètres **Anti-phishing** s'il est désactivé.

5. Ajoutez un tag dans le champ Objet des messages contenant du phishing. Pour ce faire, procédez comme suit :

    a. Dans le groupe de paramètres **En cas de détection de phishing ou de liens menant à des sites Internet hébergeant des programmes malveillants**, cliquez sur le lien à droite du paramètre **Ajouter le texte suivant à l'objet du message de phishing** pour ouvrir la fenêtre **Note pour identifier les messages de phishing**.

    b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des messages de phishing. Par exemple, vous pouvez ajouter le tag **Phishing**.

    c. Cliquez sur le bouton **OK**.

    La fenêtre **Note pour identifier les messages de phishing** se ferme.

6. Ajoutez un tag dans le champ Objet des messages contenant un lien vers des sites Internet hébergeant des programmes malveillants. Pour ce faire, procédez comme suit :

    a. Dans le groupe de paramètres **En cas de détection de phishing ou de liens menant à des sites Internet hébergeant des programmes malveillants**, cliquez sur le lien à droite du paramètre **Ajouter le texte suivant à l'objet du message contenant un lien vers un site Internet hébergeant des programmes malveillants** pour ouvrir la fenêtre **Tag des messages contenant un lien vers des sites Internet hébergeant des programmes malveillants**.

    b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des messages contenant un lien vers des sites Internet hébergeant des programmes malveillants. Par exemple, vous pouvez ajouter le tag **Malicious Link**.

    c. Cliquez sur le bouton **OK**.

    La fenêtre **Tag des messages contenant un lien vers des sites Internet hébergeant des programmes malveillants** se ferme.

7. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que l'analyse anti-phishing des messages pour une règle est activée (cf. section "Activation et désactivation de l'analyse anti-phishing pour une règle" à la page 306), et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Filtrage de contenu des messages

Kaspersky Secure Mail Gateway filtre le contenu des messages qui transitent via le serveur de messagerie. Vous pouvez limiter le transfert par le serveur de messagerie pour les messages qui répondent à certains paramètres.

Le filtrage de contenu des messages s'effectue en fonction de l'un des paramètres suivants :

- la taille du message ;
- les masques de noms des fichiers joints ;
- le format des fichiers joints.

Vous pouvez indiquer la taille maximale d'un message avec pièce-jointe, définir les masques des noms indésirables de pièces-jointes et indiquer les formats indésirables de pièces jointes (cf. section "Configuration des paramètres du filtrage du contenu des messages pour une règle" à la page 317).

D'après les résultats du filtrage du contenu, le module de gestion de l'analyse des messages Scan Logic attribue au message un des états du filtrage du contenu (cf. section "A propos des états du filtrage du contenu" à la page 314).

En fonction de l'état attribué au message, l'application exécute sur celui-ci l'action (cf. section "Activation et désactivation du filtrage du contenu des messages pour une règle" à la page 316) définie dans les paramètres de la règle de traitement du message. Vous pouvez sélectionner les actions que l'application va effectuer sur les messages qui ont un état approprié. L'application exécute par défaut l'action **Reject (Rejeter)** sur les messages.

Dans cette section

A propos des états du filtrage de contenu des messages

En fonction des résultats du filtrage de contenu, le module de gestion de l'analyse des messages Scan Logic attribue au message l'un des états suivants :

- *Clean (message correct)* : le message ne franchit aucune des limites définies dans les paramètres du filtrage de contenu.
- *BannedFileName (nom de pièce jointe interdit)* : le message contient une pièce jointe dont le nom est interdit.
- *BannedFileFormat (format de pièce jointe interdit)* : le message comporte une pièce jointe au format interdit.
- *SizeExceeded (message trop lourd)* : dépassement de la taille maximale autorisée pour le message.

Activation et désactivation du filtrage de contenu des messages

► *Pour activer ou désactiver* le filtrage de contenu des messages, procédez comme suit *:*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Dans le groupe **Filtrage de contenu**, exécutez l'une des actions suivantes :

   - Activez le commutateur en regard du nom du groupe **Filtrage de contenu** pour activer le filtrage de contenu des messages ;

   - Désactivez le commutateur en regard du nom du groupe **Filtrage de contenu** pour désactiver le filtrage du contenu des messages.

Définition du niveau d'imbrication maximal des archives pour le filtrage du contenu

► *Pour définir le niveau d'imbrication maximal des archives pour le filtrage de contenu*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Niveau d'imbrication** du groupe **Filtrage de contenu** pour ouvrir la fenêtre **Paramètres du module Filtrage du contenu**.

3. Indiquez dans le champ **Niveau d'imbrication** le niveau d'imbrication maximal des archives pour le filtrage de contenu.

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

Utilisation des valeurs par défaut des paramètres du module Filtrage du contenu

► *Pour utiliser les valeurs par défaut des paramètres du module Filtrage du contenu, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Niveau d'imbrication** du groupe **Filtrage de contenu** pour ouvrir la fenêtre **Paramètres du module Filtrage du contenu**.

3. Dans la partie inférieure de la fenêtre **Paramètres du module Filtrage du contenu**, cliquez sur le lien **Etablir les valeurs par défaut**.

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

Activation et désactivation du filtrage de contenu des messages pour une règle

Vous pouvez activer ou désactiver le filtrage du contenu des messages pour une ou plusieurs règles. Par défaut, le filtrage de contenu des messages est désactivé.

Avant d'activer ou de désactiver le filtrage du contenu des messages pour une règle, confirmez que le filtrage du contenu des messages dans Kaspersky Secure Mail Gateway est activé (cf. section "Activation et désactivation du filtrage du contenu des messages" à la page 315).

► *Pour activer ou désactiver le filtrage de contenu des messages pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez activer ou désactiver le filtrage de contenu des messages.

3. Sélectionnez le groupe **Filtrage de contenu**.

4. Exécutez une des actions suivantes :

   - Activez le commutateur en regard du groupe de paramètres **Filtrage de contenu** pour activer le filtrage de contenu des messages pour la règle.

   - Désactivez le commutateur en regard du groupe de paramètres **Filtrage de contenu** pour désactiver le filtrage de contenu des messages pour la règle.

5. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration des paramètres du filtrage de contenu des messages pour une règle

► *Pour configurer les paramètres du filtrage de contenu des messages pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les paramètres du filtrage de contenu des messages.

3. Sélectionnez le groupe **Filtrage de contenu**.

4. Activez le commutateur en regard du groupe de paramètres **Filtrage de contenu** s'il est désactivé.

5. Pour limiter le transfert des messages contenant des pièces jointes d'une taille prédéfinie, procédez comme suit :

   a. Dans le groupe de paramètres **Si la taille maximale du message est dépassée,** cliquez sur le lien à droite du paramètre **Taille maximale autorisée du message** pour ouvrir la fenêtre **Limitation en fonction de la taille des messages**.

b. Dans le champ situé sous le nom de la fenêtre, saisissez la taille maximale des objets, qui doit être comprise entre 0 Ko et 1048576 Ko (1 Go).

Si la valeur est égale à 0 Ko, la taille des objets n'est pas limitée.

c. Cliquez sur le bouton **OK**.

La fenêtre **Limitation en fonction de la taille des messages** se ferme.

6. Pour limiter le transfert des messages contenant des pièces jointes d'un format prédéfini, procédez comme suit :

   a. Dans le groupe de paramètres **Si le format de la pièce jointe figure dans la liste des formats interdits**, cliquez sur le lien à droite du paramètre **Formats de pièce jointe interdits** pour ouvrir la fenêtre **Limitation en fonction du type de fichiers**.

   b. Cochez les cases en regard des formats de pièces jointes pour lesquels vous souhaitez limiter le transfert des messages.

   Vous pouvez limiter le transfert de messages contenant les objets suivants :

   - fichiers exécutables (par exemple, EXE ; DLL ; OCX) ;
   - fichiers de documents (par exemple, DOC ; XLS ; PDF ; PPT) ;
   - fichiers multimédia (par exemple, AVI ; WMV ; MP3) ;
   - fichiers graphiques (par exemple, JPG ; BMP ; WMF) ;
   - archives (par exemple, ZIP ; RAR ; TGZ) ;
   - bases de données (par exemple, ACCDB ; ACCDC ; MDB) ;
   - autres fichiers (par exemple, TXT ; CHM ; HTM).

   c. Cliquez sur le bouton **Fermer**.

   La fenêtre **Limitation en fonction du type de fichiers** se ferme.

7. Pour limiter le transfert des messages contenant des pièces jointes d'un nom prédéfini, procédez comme suit :

a. Dans le groupe de paramètres **Si le nom de la pièce jointe figure dans la liste des noms interdits**, cliquez sur le lien à droite du paramètre **Noms de pièce jointe interdits** pour ouvrir la fenêtre **Limitation en fonction des masques de nom**.

b. Dans le champ situé sous le nom de la fenêtre, saisissez les masques de nom des pièces jointes pour lesquels vous souhaitez limiter le transfert des messages.

Les masques peuvent contenir n'importe quel caractère. Les masques doivent être séparés par un point-virgule.

Ainsi, vous pouvez saisir le masque de nom `*.exe` et limiter le transfert de fichiers contenant des objets joints avec l'extension exe.

c. Cliquez sur le bouton **OK**.

La fenêtre **Limitation en fonction des masques de nom** se ferme.

8. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que le filtrage du contenu des messages pour une règle est activé (cf. section "Activation et désactivation du filtrage du contenu des messages pour une règle" à la page 316), et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Configuration des actions à exécuter sur les messages lors du filtrage de contenu

► *Pour configurer les actions de Kaspersky Secure Mail Gateway sur les messages lors du filtrage de contenu, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les actions à effectuer sur les messages lors du filtrage de contenu.

3. Sélectionnez le groupe **Filtrage de contenu**.

4. Activez le commutateur en regard du groupe de paramètres **Filtrage de contenu** s'il est désactivé.

5. Dans le menu déroulant **Si la taille maximale du message est dépassée** , sélectionnez l'une des actions suivantes. Elle sera appliquée aux messages contenant des pièces jointes dont la taille dépasse la limite indiquée :

   - **Supprimer le message**.
   - **Refuser le message**.
   - **Ignorer**.

6. Si vous voulez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant leur traitement, cochez la case en regard du paramètre **Placer au préalable une copie dans la Sauvegarde**.

   Avant l'exécution de l'action **Supprimer le message**, l'application place par défaut une copie des messages dans la Sauvegarde.

7. Dans la liste déroulante **Si le format de la pièce jointe figure dans la liste des formats interdits** , sélectionnez une des actions suivantes à exécuter sur les messages contenant des objets au format interdit :

   - **Supprimer le message**.
   - **Supprimer la pièce jointe**.
   - **Refuser le message**.
   - **Ignorer**.

8. Si vous voulez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant leur traitement, cochez la case en regard du paramètre **Placer au préalable une copie dans la Sauvegarde**.

   Par défaut, avant l'exécution des actions **Supprimer la pièce jointe** et **Supprimer le message**, l'application place une copie des messages dans la Sauvegarde.

9. Dans la liste déroulante **Si le nom de la pièce jointe figure dans la liste des noms interdits** , sélectionnez une des actions suivantes à exécuter sur les messages contenant des pièces jointes portant un nom interdit :

   - **Supprimer le message**.
   - **Supprimer la pièce jointe**.
   - **Refuser le message**.
   - **Ignorer**.

10. Si vous voulez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant leur traitement, cochez la case en regard du paramètre **Placer au préalable une copie dans la Sauvegarde**.

    Par défaut, avant l'exécution des actions **Supprimer la pièce jointe** et **Supprimer le message**, l'application place une copie des messages dans la Sauvegarde.

11. Si vous voulez activer le filtrage du contenu pour les fichiers à l'intérieur des archives en pièce jointe aux messages, cochez la case en regard du nom du paramètre **Vérifier les formats et les noms des fichiers dans les archives**.

12. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

L'action **Refuser le message** est choisie par défaut pour tous les messages.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que le filtrage du contenu des messages pour une règle est activé (cf. section "Activation et désactivation du filtrage du contenu des messages pour une règle" à la page 316), et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Configuration des tags dans l'objet des messages selon les résultats de l'analyse antivirus

► *Pour configurer les tags que Kaspersky Secure Mail Gateway ajoute à l'objet des messages à la suite du filtrage du contenu, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les tags à ajouter à l'objet des messages en fonction des résultats du filtrage du contenu.

3. Sélectionnez le groupe **Filtrage de contenu**.

4. Activez le commutateur en regard du groupe de paramètres **Filtrage de contenu** s'il est désactivé.

5. Ajoutez le tag au champ Objet pour les messages qui dépassent la taille maximale autorisée. Pour ce faire, procédez comme suit :

    a. Dans le groupe de paramètres **Si la taille maximale du message est dépassée** , cliquez sur le lien à droite du nom du paramètre **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Note pour signaler un message dont la taille est supérieure à la taille admise**.

    b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des messages qui dépassent la taille maximale autorisée.

    c. Cliquez sur le bouton **OK**.

    La fenêtre **Note pour signaler un message dont la taille est supérieure à la taille admise** se ferme.

6. Ajoutez le tag au champ Objet des messages accompagnés d'une pièce jointe au format interdit. Pour ce faire, procédez comme suit :

a. Dans le groupe de paramètres **Si le format de la pièce jointe figure dans la liste des formats interdits**, cliquez sur le lien à droite du nom du paramètre **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Note pour signaler un message dont le fichier joint possède un format interdit**.

b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des messages accompagnés d'une pièce jointe au format interdit.

c. Cliquez sur le bouton **OK**.

La fenêtre **Note pour signaler un message dont le fichier joint possède un format interdit** se ferme.

7. Ajoutez le tag au champ Objet des messages accompagnés d'une pièce jointe portant un nom interdit. Pour ce faire, procédez comme suit :

   a. Dans le groupe de paramètres **Si le nom de la pièce jointe figure dans la liste des noms interdits**, cliquez sur le lien à droite du paramètre **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Note pour signaler un message dont le fichier joint porte un nom interdit**.

   b. Dans le champ situé sous le nom de la fenêtre, saisissez le texte à ajouter au début de l'objet des messages accompagnés d'une pièce jointe portant un nom interdit.

   c. Cliquez sur le bouton **OK**.

   La fenêtre **Note pour signaler un message dont le fichier joint porte un nom interdit** se ferme.

8. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que le filtrage du contenu des messages pour une règle est activé (cf. section "Activation et désactivation du filtrage du contenu des messages pour une règle" à la page 316), et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Protection KATA et intégration de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform

Vous pouvez configurer l'intégration de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform.

Kaspersky Anti Targeted Attack Platform (KATA) est une solution (ci-après, l'application) mise au point pour protéger l'infrastructure informatique de l'organisation et la détection en temps utiles de menaces telles que les attaques "0jour", les attaques ciblées et les attaques ciblées complexes de type "advanced persistent threats" (ci-après, "APT").

Suite à l'intégration, Kaspersky Secure Mail Gateway peut envoyer des messages électroniques pour analyse à Kaspersky Anti Targeted Attack Platform et recevoir le résultat de l'analyse. KATA recherche dans les messages la présence éventuelle de signes d'attaques ciblées et d'intrusion dans l'infrastructure informatique de l'organisation.

Sur la base des résultats du contrôle KATA Kaspersky Secure Mail Gateway peut bloquer certains messages.

Dans cette section

Saisie des paramètres d'intégration du côté de Kaspersky Secure Mail Gateway

► *Pour saisir les paramètres de l'intégration de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform du côté de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Dans la fenêtre principale de l'interface Web de Kaspersky Secure Mail Gateway, sélectionnez la section **Paramètres**, sous-section **Protection** de l'arborescence de la console de gestion.

2. Sélectionnez le groupe **Protection KATA**.

3. Activez le commutateur en regard du nom du groupe de paramètres **Protection KATA**.

4. Cliquez sur n'importe quel lien du groupe **Protection KATA** pour ouvrir la fenêtre **Protection KATA**.

5. Saisissez dans le champ **Adresse IPv4 de KATA Central Node** l'adresse IP du serveur Kaspersky Anti Targeted Attack Platform avec le composant Central Node.

6. Saisissez dans le champ **Port KATA Central Node** le port de connexion au serveur Kaspersky Anti Targeted Attack Platform avec le composant Central Node.

7. Saisissez dans le champ **Délai d'attente maximal de la réponse de KATA** le temps d'attente maximal du résultat de l'analyse du message par l'application Kaspersky Anti Targeted Attack Platform.

8. Saisissez dans le champ **Taille maximale de la quarantaine KATA** le volume maximal de la quarantaine de Kaspersky Anti Targeted Attack Platform. Une fois ce volume atteint, les messages ne sont plus mis en quarantaine.

9. Saisissez dans le champ **Nombre maximal de messages en quarantaine KATA** le nombre maximum de messages dans la quarantaine Kaspersky Anti Targeted Attack Platform. Une fois ce nombre dépassé, les messages ne sont plus placés en quarantaine.

10. Si vous souhaitez rétablir les valeurs par défaut des paramètres **Port KATA Central Node**, **Délai d'attente maximal de la réponse de KATA**, **Taille maximale de la quarantaine**

KATA et **Nombre maximal de messages en quarantaine KATA**, cliquez sur le lien **Etablir les valeurs par défaut** dans la partie inférieure de la fenêtre **Protection KATA**.

11. Cliquez sur le bouton **Appliquer**.

    La fenêtre **Protection KATA** se ferme.

Kaspersky Secure Mail Gateway tente d'établir une connexion avec le serveur Kaspersky Anti Targeted Attack Platform doté du composant Central Node.

Passez à la confirmation de l'intégration de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform du côté de Kaspersky Anti Targeted Attack Platform.

Confirmation de l'intégration du côté de Kaspersky Anti Targeted Attack Platform

► *Pour confirmer l'intégration de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform du côté de Kaspersky Anti Targeted Attack Platform, procédez comme suit :*

1. Entrez dans la console de gestion du serveur Kaspersky Anti Targeted Attack Platform doté du composant Central Node selon le protocole SSH ou via le terminal.

2. Sur invite du système, saisissez le nom du compte utilisateur de l'administrateur du serveur Kaspersky Anti Targeted Attack Platform doté du composant Central Node ainsi que le mot de passe de l'administrateur.

   Le menu de l'administrateur de l'application s'affiche.

3. Dans le menu de l'administrateur de l'application, choisissez l'option **Program settings**.

4. Appuyez sur la touche **ENTER**.

   La fenêtre **Select action** s'ouvre.

5. Choisissez l'action **Configure KSMG Sensor connections**.

6. Appuyez sur la touche **ENTER**.

   La fenêtre **Configure KSMG Sensor connections** s'affiche.

7. Choisissez la ligne qui contient l'adresse IP du serveur Kaspersky Secure Mail Gateway. La ligne d'une connexion non confirmée est accompagnée d'un astérisque.

8. Appuyez sur la touche **ENTER**.

   La fenêtre contenant les empreintes des clés publiques de la connexion entre Kaspersky Secure Mail Gateway et Kaspersky Anti Targeted Attack Platform s'ouvre.

9. Confirmez que la clé de Kaspersky Secure Mail Gateway correspond à l'empreinte de la clé dans l'interface Web de Kaspersky Secure Mail Gateway.

10. Choisissez **Accept KSMG Sensor**.

11. Appuyez sur la touche **ENTER**.

    Vous revenez à la fenêtre **Configure KSMG Sensor connections**. La ligne qui reprend l'adresse IP du serveur Kaspersky Secure Mail Gateway n'est pas accompagnée d'un astérisque.

L'intégration de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform du côté de Kaspersky Anti Targeted Attack Platform est confirmée.

Vérification de la connexion de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform

► *Pour vérifier la connexion de Kaspersky Secure Mail Gateway avec Kaspersky Anti Targeted Attack Platform, procédez comme suit :*

1. Dans la fenêtre principale de l'interface Web de Kaspersky Secure Mail Gateway, sélectionnez la section **Paramètres**, sous-section **Protection** de l'arborescence de la console de gestion.

2. Sélectionnez le groupe **Protection KATA**.

3. Activez le commutateur en regard du nom du groupe de paramètres **Protection KATA**.

4. Cliquez sur le lien **Etat de la connexion avec KATA** du groupe **Protection KATA** pour ouvrir la fenêtre **Etat de la connexion avec KATA**.

   L'adresse IP du serveur Kaspersky Anti Targeted Attack Platform doté du composant Central Node s'affiche en regard du paramètre **Adresse IPv4 de KATA Central Node**.

   L'état de la connexion de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform s'affiche en regard du paramètre **Etat de la connexion**.

   L'empreinte de la clé de Kaspersky Secure Mail Gateway s'affiche en regard du nom du paramètre **Empreinte de la clé publique KSMG**.

   L'empreinte de la clé de Kaspersky Anti Targeted Attack Platform s'affiche en regard du paramètre **Empreinte de la clé publique KATA**.

Si les empreintes des clés des deux serveurs et l'état de la connexion de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform **Connected** apparaissent dans la fenêtre **Etat de la connexion avec KATA**, l'intégration de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform est configurée correctement et la connexion entre les serveurs est établie.

Configuration de l'envoi des messages de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform pour analyse

► *Pour configurer l'envoi des messages électroniques de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform pour analyse, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle afin d'ouvrir la règle pour laquelle vous voulez configurer l'envoi des messages électroniques de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform pour analyse.

3. Choisissez le groupe **Protection KATA**.

4. Activez le commutateur en regard du groupe de paramètres **Protection KATA** s'il est désactivé.

5. Dans la liste déroulante **Si KATA a détecté un événement**, sélectionnez une des actions suivantes à exécuter sur les messages dans lesquels KATA détecte un événement :

   - **Supprimer le message**.
   - **Refuser le message**.
   - **Ignorer**.

6. Ajoutez un tag dans le champ Objet pour les messages dans lesquels KATA a détecté un événement. Pour ce faire, procédez comme suit :

   a. Dans le groupe de paramètres **Protection KATA**, cliquez sur le lien à droite du nom du paramètres **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Tag pour les messages avec attaque KATA détectée**.

b. Dans le champ situé sous la fenêtre, saisissez le texte à ajouter au début de l'objet des messages dans lesquels KATA a détecté des événements. Par exemple, vous pouvez ajouter le tag **KATA detect**.

c. Cliquez sur le bouton **OK**.

La fenêtre **Tag pour les messages avec attaque KATA détectée** se ferme.

7. Cochez la case en regard du nom du paramètre **Placer au préalable une copie dans la Sauvegarde** si vous souhaitez configurer l'enregistrement automatique des copies des messages dans la Sauvegarde avant le traitement.

8. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Vous avez configuré l'envoi des messages électroniques de Kaspersky Secure Mail Gateway à Kaspersky Anti Targeted Attack Platform pour analyse dans le cadre de la règle sélectionnée.

Activation et désactivation de la protection KATA

► *Pour activer ou désactiver la protection KATA, procédez comme suit :*

1. Dans la fenêtre principale de l'interface Web de Kaspersky Secure Mail Gateway, sélectionnez la section **Paramètres**, sous-section **Protection** de l'arborescence de la console de gestion.

2. Dans le groupe **Protection KATA**, exécutez l'une des actions suivantes :

   - Activez le commutateur en regard du groupe de paramètres **Protection KATA** pour activer la protection de Kaspersky Anti Targeted Attack Platform.

   - Désactivez le commutateur en regard du groupe de paramètres **Protection KATA** pour désactiver la protection de Kaspersky Anti Targeted Attack Platform.

Configuration des paramètres de la protection KATA

► *Pour configurer les paramètres de la protection KATA du côté de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Dans la fenêtre principale de l'interface Web de Kaspersky Secure Mail Gateway, sélectionnez la section **Paramètres**, sous-section **Protection** de l'arborescence de la console de gestion.

2. Sélectionnez le groupe **Protection KATA**.

3. Activez le commutateur en regard du nom du groupe de paramètres **Protection KATA**.

4. Cliquez sur n'importe quel lien du groupe **Protection KATA** pour ouvrir la fenêtre **Protection KATA**.

5. Saisissez dans le champ **Délai d'attente maximal de la réponse de KATA** le temps d'attente maximal du résultat de l'analyse du message par l'application Kaspersky Anti Targeted Attack Platform.

6. Saisissez dans le champ **Taille maximale de la quarantaine KATA** le volume maximal de la quarantaine de Kaspersky Anti Targeted Attack Platform. Quand le volume de la quarantaine est dépassé, la quarantaine n'accepte plus de copies de messages.

7. Saisissez dans le champ **Nombre maximal de messages en quarantaine KATA** le nombre maximum de messages dans la quarantaine Kaspersky Anti Targeted Attack Platform. Une fois le nombre de copies de messages dépassé, les messages ne sont plus placés en quarantaine.

8. Cliquez sur le bouton **Appliquer**.

Utilisation des valeurs par défaut des paramètres de la protection KATA

► *Pour utiliser les valeurs par défaut des paramètres du module Anti-Spam, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.
2. Cliquez sur n'importe quel lien du groupe **Protection KATA** pour ouvrir la fenêtre **Protection KATA**.
3. Dans la partie inférieure de la fenêtre **Protection KATA**, cliquez sur le lien **Etablir les valeurs par défaut**.
4. Cliquez sur le bouton **Appliquer**.

Activation et désactivation de la protection KATA pour une règle

Vous pouvez activer ou désactiver la protection KATA pour une ou plusieurs règles. La protection KATA est activée par défaut.

Avant d'activer ou de désactiver la protection KATA pour une règle, confirmez que la protection KATA est activée dans les paramètres de l'application (cf. section "Activation et désactivation de la protection KATA" à la page 332).

► *Pour activer ou désactiver la protection KATA pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.
2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez activer ou désactiver la protection KATA.
3. Choisissez le groupe **Protection KATA**.

4. Exécutez une des actions suivantes :

   - Activez le commutateur en regard du groupe de paramètres **Filtrage de contenu** pour activer la protection KATA pour la règle.

   - Désactivez le commutateur en regard du groupe de paramètres **Filtrage de contenu** pour désactiver la protection KATA pour la règle.

5. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Configuration des actions à réaliser sur les messages à l'issue de l'analyse KATA

► *Pour configurer les actions de Kaspersky Secure Mail Gateway sur les messages à l'issue de l'analyse KATA, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les actions à exécuter sur les messages à l'issue de l'analyse KATA.

3. Choisissez le groupe **Protection KATA**.

4. Activez le commutateur en regard du groupe de paramètres **Protection KATA** s'il est désactivé.

5. Dans la liste déroulante **Si KATA a détecté un événement**, sélectionnez une des actions suivantes à exécuter sur les messages dans lesquels KATA détecte un événement :

   - **Supprimer le message**.

   - **Refuser le message**.

   - **Ignorer**.

   Supprimer le message est l'action sélectionnée par défaut.

6. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que la protection KATA pour la règle est activée (cf. section "Activation et désactivation de l'analyse KATA pour une règle" à la page 334) et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Configuration des tags à ajouter à l'objet des messages en fonction des résultats de l'analyse KATA

► *Pour configurer les tags que Kaspersky Secure Mail Gateway doit ajouter à l'objet des messages en fonction des résultats de l'analyse KATA, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer les tags à ajouter à l'objet des messages en fonction des résultats de l'analyse KATA.

3. Choisissez le groupe **Protection KATA**.

4. Activez le commutateur en regard du groupe de paramètres **Protection KATA** s'il est désactivé.

5. Ajoutez un tag dans le champ Objet pour les messages dans lesquels KATA a détecté un événement. Pour ce faire, procédez comme suit :

    a. Dans le groupe de paramètres **Protection KATA**, cliquez sur le lien à droite du nom du paramètres **Ajouter à l'objet du message le texte** pour ouvrir la fenêtre **Tag pour les messages avec attaque KATA détectée**.

b. Dans le champ situé sous la fenêtre, saisissez le texte à ajouter au début de l'objet des messages dans lesquels KATA a détecté un événement. Par exemple, vous pouvez ajouter le tag **KATA detect**.

c. Cliquez sur le bouton **OK**.

La fenêtre **Tag pour les messages avec attaque KATA détectée** se ferme.

6. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que la protection KATA pour la règle est activée (cf. section "Activation et désactivation de l'analyse KATA pour une règle" à la page 334) et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Listes noires et blanches d'adresses

Cette section contient des informations sur les listes noires et blanches d'adresses email qu'il est possible de créer et de modifier dans Kaspersky Secure Mail Gateway.

Dans cette section

Présentation des listes noire et blanche d'adresses

Les listes noires et blanches d'adresses permettent de configurer avec plus de finesse la réaction du système de messagerie face aux messages qui n'appartiennent pas officiellement au courrier indésirable (par exemple, des diffusions d'informations). De plus, les listes noires d'adresses permettent de configurer le blocage des messages qui contiennent des menaces et du courrier indésirable sans attendre la mise à jour des bases de Kaspersky Secure Mail Gateway.

Il existe deux types de listes noires et blanches d'adresses :

- *Personnalisées*. Contiennent les adresses des expéditeurs de messages pour un destinataire. La liste blanche personnalisée des adresses accepte les messages sans analyse contre les spams. L'analyse anti-phishing, la recherche de virus et autres programmes dangereux, ainsi que le filtrage du contenu ont lieu.

- *Globales*. Contient les adresses des expéditeurs et des destinataires. Vous pouvez définir ces listes dans les règles de traitement des messages WhiteList et BlackList (cf. section "Application des règles de traitement des messages" à la page 128). Vous pouvez créer des règles contenant les adresses des expéditeurs et des destinataires dont les messages doivent rejeter ou accepter sans analyse. La liste blanche globale des adresses accepte les messages sans analyse contre les spams, recherche de virus ou analyse anti-phishing.

Le traitement des messages dont les adresses d'expéditeurs et de destinataires figurent dans une liste blanche ou noire d'adresses globale se déroule de la manière suivante :

- Si les adresses des expéditeurs et des destinataires des messages figurent dans la liste noire globale d'adresses, l'application rejette les messages. Le message n'arrive pas sur le serveur de messagerie Kaspersky Secure Mail Gateway.

- Si l'adresse de l'expéditeur et celle des destinataires figurent dans une liste blanche d'adresses globale, l'application transfère le message pour une analyse complémentaire, sans intervention des modules Anti-Spam, Anti-Virus et Anti-Phishing :

- Si l'adresse de l'expéditeur et celle des destinataires du message figurent simultanément dans les listes noire et blanche d'adresses globales, l'application traite le message selon la règle qui affiche la plus grande priorité.

Un message sera traité selon la règle d'une liste blanche ou noire d'adresses personnelle s'il ne tombe pas sous le coup de l'action de liste noire ou blanche d'adresses globales.

Le principe de traitement d'un message dont l'expéditeur figure dans une liste blanche ou noire d'adresse personnelle est le suivant :

- Si l'adresse de l'expéditeur du message figure dans la liste noire personnalisée et qu'une des adresses des destinataires appartient au propriétaire de la liste noire personnalisée, le message n'est pas remis à ce destinataire. En fonction de l'action sur les messages de la liste noire personnalisée qui a été choisie, le message est supprimer ou placer dans le stockage.

- Si l'adresse de l'expéditeur figure dans une liste blanche personnalisée, le message sera remis au destinataire sur la base des résultats de la recherche de virus, de l'analyse anti-phishing et du filtrage du contenu.

- Si l'adresse de l'expéditeur figure à la fois dans une liste blanche personnalisée et une liste noire personnalisée, le message sera traité conformément à la liste blanche personnalisée.

Configuration des paramètres de la liste noire personnalisée d'adresses

Pour configurer les paramètres de la liste noire personnalisée des adresses électroniques, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Protection** dans l'arborescence de la console de gestion.
2. Cliquez sur n'importe quel lien du groupe **Paramètres de la liste noire personnalisée** pour ouvrir la fenêtre **Paramètres de la liste noire**.
3. Dans la liste **Si l'adresse email de l'expéditeur figure sur la liste noire** , sélectionnez une des actions suivantes à exécuter sur les messages :
   - **Supprimer le message** si vous souhaitez supprimer les messages dont les expéditeurs figurent dans la liste noire personnalisée.
   - **Refuser le message** si vous souhaitez rejeter les messages dont les expéditeurs figurent dans la liste noire personnalisée.
4. Sélectionnez une des valeurs suivantes dans la liste **Placer le message dans la Sauvegarde** :
   - **Oui**, si vous souhaitez placer dans la Sauvegarde les messages dont les expéditeurs figurent dans la liste noire personnalisée.
   - **Non**, si vous ne souhaitez pas placer dans la Sauvegarde les messages dont les expéditeurs figurent dans la liste noire personnalisée.
5. Cliquez sur le bouton **Appliquer**.

Consultation des listes noire et blanche personnelles des adresses

Pour avoir accès aux listes noires et blanches personnelles des adresses à partir de l'interface de Web Kaspersky Secure Mail Gateway, vous devez ajouter la connexion au serveur LDAP (cf. section "Ajout de la connexion au serveur LDAP" à la page 348).

Pour utiliser les listes noires et blanches personnelles des adresses depuis l'interface Web de Kaspersky Secure Mail Gateway, vous devez vous connecter au serveur LDAP (cf. section "Connexion et déconnexion du serveur LDAP" à la page 347).

Pour consultez les listes noire et blanches personnelles d'adresses électroniques, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **LDAP** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Accès aux listes noires et blanches** dans le groupe de paramètres **Listes noires et blanches personnelles des adresses** pour ouvrir la fenêtre **Listes noires et blanches personnelles des adresses**.

3. Saisissez dans le champ **Rechercher selon le nom de l'utilisateur ou selon le nom du groupe dans le service de répertoires LDAP** la ligne de recherche des listes noir et blanche personnelles selon le nom d'utilisateur ou le nom du groupe dan le service des catalogues LDAP.

4. Cliquez sur le bouton **Rechercher** situé à droite du champ.

   La liste des enregistrements LDAP qui contiennent la chaîne de recherche que vous avez saisie apparaît sous le champ de saisie.

5. Cliquez sur l'enregistrement LDAP de l'utilisateur dont vous souhaitez consulter les listes noire et blanche personnelles des adresses.

6. Lorsque vous en avez terminé avec les listes personnelles de l'utilisateur, cliquez sur le bouton **Fermer**.

La fenêtre **Listes noires et blanches personnelles des adresses** se ferme.

Ajout d'adresses aux listes noires et blanches d'adresses personnelles

Pour avoir accès aux listes noires et blanches personnelles des adresses à partir de l'interface de Web Kaspersky Secure Mail Gateway, vous devez ajouter la connexion au serveur LDAP (cf. section "Ajout de la connexion au serveur LDAP" à la page 348).

Pour utiliser les listes noires et blanches personnelles des adresses depuis l'interface Web de Kaspersky Secure Mail Gateway, vous devez vous connecter au serveur LDAP (cf. section "Connexion et déconnexion du serveur LDAP" à la page 347).

Pour consulter les listes noires et blanches personnelles d'adresses électroniques, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **LDAP** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Accès aux listes noires et blanches** dans le groupe de paramètres **Listes noires et blanches personnelles des adresses** pour ouvrir la fenêtre **Listes noires et blanches personnelles des adresses**.

3. Saisissez dans le champ **Rechercher selon le nom de l'utilisateur ou selon le nom du groupe dans le service de répertoires LDAP** la ligne de recherche des listes noir et blanche personnelles selon le nom d'utilisateur ou le nom du groupe dan le service des catalogues LDAP.

4. Cliquez sur le bouton **Rechercher** situé à droite du champ.

La liste des enregistrements LDAP qui contiennent la chaîne de recherche que vous avez saisie apparaît sous le champ de saisie.

5. Cliquez sur l'enregistrement LDAP de l'utilisateur dans la liste noire ou blanche personnelle duquel vous souhaitez ajouter des adresses.

   Les listes noire et blanche d'adresses personnelles apparaissent dans la partie inférieure de la fenêtre.

6. Saisissez l'adresse email requise dans le champ de saisie des adresses de la liste à laquelle vous souhaitez ajouter des adresses email.

   > Les adresses électroniques sont saisies une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses électroniques.

   Vous pouvez utiliser les caractères "*" et "?" pour créer des masques d'adresses ainsi que des expressions régulières en utilisant le préfixe "re:".

   > Les expressions régulières ne respectent pas la casse.

7. Cliquez sur le bouton  situé à droite du champ.

   L'adresse email ajoutée s'affiche dans la liste que vous avez sélectionnée.

8. Lorsque vous en avez terminé avec les listes personnelles de l'utilisateur, cliquez sur le bouton **Appliquer**.

La fenêtre **Listes noires et blanches personnelles des adresses** se ferme.

Suppression des adresses des listes noire ou blanche personnelles d'adresses

Pour accéder aux listes noire et blanche d'adresses personnelles depuis l'interface Web de Kaspersky Secure Mail Gateway, il faut ajouter une connexion au serveur LDAP (cf. section "Ajout de la connexion au serveur LDAP" à la page 348) et s'y connecter (cf. section "Connexion et déconnexion du serveur LDAP" à la page 347).

Pour supprimer des adresses des listes noires et blanches personnelles des adresses, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **LDAP** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Accès aux listes noires et blanches** dans le groupe de paramètres **Listes noires et blanches personnelles des adresses** pour ouvrir la fenêtre **Listes noires et blanches personnelles des adresses**.

3. Saisissez dans le champ **Rechercher selon le nom de l'utilisateur ou selon le nom du groupe dans le service de répertoires LDAP** la ligne de recherche des listes noir et blanche personnelles selon le nom d'utilisateur ou le nom du groupe dan le service des catalogues LDAP.

4. Cliquez sur le bouton **Rechercher** situé à droite du champ.

   La liste des enregistrements LDAP qui contiennent la chaîne de recherche que vous avez saisie apparaît sous le champ de saisie.

5. Cliquez sur l'enregistrement LDAP de l'utilisateur dans les listes noire et blanche personnelles des adresses duquel vous souhaitez supprimer l'adresse.

   Les listes noire et blanche d'adresses personnelles apparaissent dans la partie inférieure de la fenêtre.

6. Sélectionnez, dans la liste d'adresses, l'adresse email que vous souhaitez supprimer.

Les adresses email sont éliminées une à une. Répétez l'opération autant de fois que nécessaire pour supprimer d'autres adresses de la liste des adresses email.

7. Cliquez sur le bouton **Supprimer**situé à droite du champ.

   L'adresse email est alors supprimée de la liste que vous aviez sélectionnée.

8. Lorsque vous en avez terminé avec les listes personnelles de l'utilisateur, cliquez sur le bouton **Appliquer**.

La fenêtre **Listes noires et blanches personnelles des adresses** se ferme.

Connexion au serveur LDAP

Cette section contient des informations sur la connexion de Kaspersky Secure Mail Gateway au serveur LDAP et sur la configuration des paramètres et des filtres de connexion au serveur LDAP.

Dans cette section

Présentation de la connexion au serveur LDAP

Kaspersky Secure Mail Gateway permet d'établir des connexions via le protocole LDAP aux serveurs de services d'annuaires externes utilisés par votre organisation.

Un *service d'annuaire* est une suite logicielle qui rassemble au même endroit les informations sur les ressources réseau (les utilisateurs, par exemple), afin de centraliser leur gestion.

LDAP (Lightweight Directory Access Protocol) est un protocole client-serveur léger permettant d'accéder à des services d'annuaire.

La connexion à un service d'annuaire externe via le protocole LDAP donne à l'administrateur de Kaspersky Secure Mail Gateway la possibilité d'exécuter les tâches suivantes :

- Ajouter des expéditeurs ou des destinataires (cf. section "Ajout de comptes utilisateurs LDAP" à la page 136) du service d'annuaire externe dans les règles de traitement des messages.
- Créer, modifier et consulter les listes noires et blanches personnelles des adresses (cf. section "Consultation des listes noires et blanches personnelles des adresses" à la page 341) des utilisateurs du réseau local de l'organisation.
- Consulter les copies des messages des utilisateurs du réseau local de l'organisation dans la Sauvegarde (cf. section "Consultation des informations relatives aux messages dans la Sauvegarde" à la page 179).

Connexion et déconnexion du serveur LDAP

► *Pour établir une connexion à un serveur LDAP ou pour l'annuler, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **LDAP** dans l'arborescence de la console de gestion.
2. Cliquez sur le lien **Connexion au serveur LDAP** pour ouvrir la fenêtre **Connexion au serveur LDAP**.

3. Sélectionnez l'une des options de connexion suivantes au serveur LDAP :

   - **Non utilisé** si vous ne souhaitez pas utiliser un serveur LDAP dans le cadre du fonctionnement de Kaspersky Secure Mail Gateway.

   - **Active Directory ou Generic LDAP** si vous souhaitez établir une connexion au serveur LDAP Microsoft ou tout autre service d'annuaire compatible LDAP (par exemple, Red Hat® Directory Server) ;

4. Si vous souhaitez limiter le délai d'attente de la réponse du serveur, cochez la case en regard de **Limiter le délai d'attente de la réponse du serveur**.

5. Si vous avez coché la case en regard du paramètre **Limiter le délai d'attente de la réponse du serveur**, indiquez dans le champ **Délai d'attente de la réponse du serveur en secondes** la durée maximale d'attente de la réponse du serveur LDAP en secondes.

   Valeur par défaut : 20 s.

6. Cliquez sur le bouton **Appliquer**.

La fenêtre **Connexion au serveur LDAP** se ferme.

Ajout d'une connexion au serveur LDAP

Vous pouvez ajouter une connexion à un ou plusieurs serveurs LDAP.

► *Pour ajouter une connexion au serveur LDAP, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **LDAP** dans l'arborescence de la console de gestion.

2. Si le paramètre **Connexion au serveur LDAP** a la valeur **Non utilisé** dans l'espace de travail, procédez comme suit :

   a. Cliquez sur le lien **Connexion au serveur LDAP** pour ouvrir la fenêtre **Connexion au serveur LDAP**.

   b. Dans la liste **Serveur LDAP**, sélectionnez **Active Directory ou Generic LDAP**.

c. Si vous souhaitez limiter le délai d'attente de la réponse du serveur, cochez la case en regard de **Limiter le délai d'attente de la réponse du serveur**.

d. Si vous avez coché la case en regard du paramètre **Limiter le délai d'attente de la réponse du serveur**, indiquez dans le champ **Délai d'attente de la réponse du serveur en secondes** la durée maximale d'attente de la réponse du serveur LDAP en secondes.

Valeur par défaut : 20 s.

e. Cliquez sur le bouton **Appliquer**.

La fenêtre **Connexion au serveur LDAP** se ferme.

3. Dans l'espace de travail, cliquez sur le bouton **Ajouter**.

La fenêtre **Assistant de connexion au serveur LDAP** s'ouvre.

4. Sous l'onglet **Paramètres de connexion**, accédez au groupe de paramètres **Paramètres du serveur LDAP**, puis sélectionnez un des services d'annuaire externe suivants dans la liste **Serveur LDAP** :

- **LDAP générique** pour ajouter une connexion à un serveur de service d'annuaire compatible LDAP (par exemple, Red Hat Directory Server).
- **Active Directory** pour ajouter une connexion à un serveur Microsoft Active Directory.

5. Dans le groupe de paramètres **Paramètres du serveur LDAP**, saisissez dans le champ **Adresse du serveur** l'adresse IP du serveur LDAP auquel vous souhaitez vous connecter au format IPv4 ou FQDN.

6. Dans le groupe de paramètres **Paramètres du serveur LDAP**, indiquez dans la liste **Port de connexion** le port de connexion au serveur LDAP.

> En général, un serveur LDAP accepte les connexions entrantes sur le port 389, via les protocoles TCP ou UDP. La connexion au serveur LDAP via le protocole SSL s'opère souvent sur le port 636.

7. Dans le groupe de paramètres **Paramètres du serveur LDAP**, sélectionnez dans la liste **Type de connexion** une des options de chiffrement des données lors de la connexion au serveur LDAP :

   - **SSL** pour utiliser SSL.
   - **TLS** pour utiliser TLS.
   - **Sans chiffrement** pour ne pas utiliser de technologie de cryptage des données lors de la connexion au serveur LDAP.

8. Dans le groupe de paramètres **Paramètres d'authentification**, saisissez dans le champ **Nom d'utilisateur du serveur LDAP** le nom d'un utilisateur du serveur LDAP autorisé à lire les enregistrements de l'annuaire (BindDN). Saisissez le nom d'utilisateur dans un des formats suivants :

   - `cn=<nom d'utilisateur>, ou=<nom de la division>` (s'il y a lieu), `dc=<nom de domaine>, dc=<nom du domaine parent>`, si vous souhaitez ajouter une connexion à un serveur de service d'annuaires compatible avec LDAP (par exemple, Red Hat Directory Server).

     Par exemple, vous pouvez saisir `cn=LdapServerUser, dc=example, dc=com`, où `LdapServerUser` est le nom de l'utilisateur du serveur LDAP, `example`, le nom de domaine de l'annuaire auquel est rattaché le compte de l'utilisateur et `com` le nom du domaine parent sur lequel se trouve l'annuaire ;

   - `cn=<nom d'utilisateur>, ou=<nom du service>` (le cas échéant), `dc=<nom de domaine>, dc=<nom du domaine parent>` ou `<nom d'utilisateur>@<nom de domaine>.<nom du domaine parent>`, si vous souhaitez ajouter une connexion au serveur Microsoft Active Directory.

     Par exemple, vous pouvez saisir le nom d'utilisateur `LdapServerUser@example.com`, où `LdapServerUser` est le nom de l'utilisateur du serveur LDAP et `example.com` le nom de domaine de l'annuaire auquel est rattaché le compte de l'utilisateur.

9. Dans le groupe de paramètres **Paramètres d'authentification**, saisissez dans le champ **Mot de passe de l'utilisateur du serveur LDAP** le mot de passe permettant d'accéder au

serveur LDAP correspondant à l'utilisateur indiqué dans le champ **Nom d'utilisateur du serveur LDAP** .

10. Dans le groupe **Paramètres de recherche**, saisissez dans le champ **Base de recherche** le *DN* (*Distinguished Name* – nom unique) de l'objet d'annuaire à partir duquel Kaspersky Secure Mail Gateway effectue sa recherche dans les enregistrements.

    Saisissez la base de recherche sous la forme `ou=<nom de la division>` (s'il y a lieu), `dc=<nom de domaine>`, `dc=<nom de domaine parent>`.

    Par exemple, vous pouvez saisir la base de recherche `ou=people, dc=example, dc=com`, où `people` désigne le niveau dans la structure de répertoire à partir duquel Kaspersky Secure Mail Gateway recherche les enregistrements (La recherche inclut les niveaux `people` et inférieurs. Les objets supérieurs à ce niveau sont exclus de la recherche), `example` désigne le nom de domaine du répertoire dans lequel Kaspersky Secure Mail Gateway réalise la recherche d'enregistrements, `com` représente le nom du domaine parent dans lequel le répertoire se trouve.

11. Cliquez sur le bouton **Tester**.

    Kaspersky Secure Mail Gateway vérifie la connexion au serveur LDAP à partir des valeurs que vous avez saisies pour les paramètres de connexion et d'authentification.

12. Cliquez sur le bouton **Suivant**.

    L'onglet **Filtres** s'ouvre.

13. Dans le groupe de paramètres **Configurez les filtres LDAP**, indiquez dans le champ **Authentification de l'utilisateur** un filtre d'autorisation de l'utilisateur (par exemple, pour que l'utilisateur puisse accéder à ses messages dans la Sauvegarde).

14. Si vous souhaitez définir des valeurs par défaut pour le filtre d'autorisation de l'utilisateur, cliquez sur le lien **Etablir les valeurs par défaut** sous le champ **Authentification de l'utilisateur**.

15. Dans le groupe de paramètres **Configurez les filtres LDAP**, définissez dans le champ **Recherche d'un utilisateur ou d'un groupe** le filtre de recherche d'utilisateurs ou de groupes d'utilisateurs.

16. Si vous souhaitez définir des valeurs par défaut pour le filtre de recherche dans les utilisateurs ou les groupes d'utilisateurs, cliquez sur le lien **Etablir les valeurs par défaut** sous le champ **Recherche d'un utilisateur ou d'un groupe**.

17. Dans le groupe de paramètres **Configurez les filtres LDAP**, définissez dans le champ **Recherche dans les DN d'utilisateurs et de groupes selon l'adresse email** le filtre de la recherche de DN des utilisateurs et des groupes auxquels ils appartiennent sur la base de l'adresse email.

18. Si vous souhaitez définir des valeurs par défaut pour le filtre de recherche dans les DN des utilisateurs et des groupes auxquels ils appartiennent en fonction de leur adresse électronique, cliquez sur le lien **Etablir les valeurs par défaut** sous le champ **Recherche dans les DN d'utilisateurs et de groupes selon l'adresse email**.

19. Dans le champ **Recherche dans les groupes selon le DN des utilisateurs** du groupe de paramètres **Configurez les filtres LDAP**, définissez le filtre de recherche de groupes auquel appartient l'utilisateur, sur la base du DN de l'utilisateur. Ce filtre est utilisé quand il est impossible de déterminer le groupe d'utilisateurs à l'aide du filtre défini dans le champ **Recherche dans les DN d'utilisateurs et de groupes selon l'adresse email**.

20. Si vous souhaitez utiliser des valeurs par défaut pour le filtre de recherche des groupes auxquels appartient l'utilisateur en fonction de son DN, cliquez sur le lien **Etablir les valeurs par défaut** sous le champ **Recherche dans les groupes selon le DN des utilisateurs**.

21. Cochez la case **Utiliser la recherche récursive** pour activer la recherche des enregistrements LDAP dans les sous-groupes.

22. Cliquez sur le bouton **Terminer**.

    La fenêtre **Assistant de connexion au serveur LDAP** se ferme.

La connexion que vous avez ajoutée au service d'annuaire externe apparaît dans l'espace de travail de la section **LDAP** dans la fenêtre principale de l'interface Web.

Suppression de la connexion au serveur LDAP

Vous pouvez supprimer la connexion à un ou plusieurs serveurs LDAP.

► *Pour supprimer la connexion à un serveur LDAP, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **LDAP** dans l'arborescence de la console de gestion.

2. Dans la partie inférieure de l'espace de travail, cochez la case en regard de l'adresse du Serveur LDAP que vous souhaitez supprimer.

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

   La fenêtre de confirmation de l'opération **Suppression** s'ouvre.

4. Cliquez sur le bouton **Oui**.

   La fenêtre **Suppression** se ferme.

La connexion au serveur LDAP sera supprimée.

Activation et désactivation de la connexion au serveur LDAP

Vous pouvez activer ou désactiver la connexion à un ou plusieurs serveurs LDAP.

► *Pour activer ou désactiver l'utilisation de la connexion à un serveur LDAP, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **LDAP** dans l'arborescence de la console de gestion.

2. Dans la partie inférieure de l'espace de travail, exécutez l'une des opérations suivantes :

   - Activez le commutateur en regard de l'adresse du serveur LDAP dont vous souhaitez activer la connexion.

- Désactivez le commutateur en regard de l'adresse du serveur LDAP dont vous souhaitez désactiver la connexion.

Configuration des paramètres de connexion au serveur LDAP

► *Pour configurer les paramètres de connexion au serveur LDAP, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **LDAP** dans l'arborescence de la console de gestion.

2. Dans la partie inférieure de l'espace de travail, sélectionnez le serveur LDAP dont vous souhaitez configurer les paramètres de connexion.

3. Dans le groupe de paramètres **Paramètres de connexion au serveur LDAP** du serveur sélectionné, cliquez sur n'importe quel lien pour ouvrir la fenêtre **Paramètres de connexion au serveur LDAP**.

4. Dans le groupe de paramètres **Paramètres du serveur LDAP**, sélectionnez dans la liste **Serveur LDAP** l'un des services d'annuaire externes :

   - **LDAP générique** pour ajouter une connexion à un serveur de service d'annuaire compatible LDAP (par exemple, Red Hat Directory Server).

   - **Active Directory** pour ajouter une connexion à un serveur Microsoft Active Directory.

5. Dans le groupe de paramètres **Paramètres du serveur LDAP**, saisissez dans le champ **Adresse du serveur** l'adresse IP du serveur LDAP auquel vous souhaitez vous connecter au format IPv4 ou FQDN.

6. Dans le groupe de paramètres **Paramètres du serveur LDAP**, indiquez dans la liste **Port de connexion** le port de connexion au serveur LDAP.

   En général, un serveur LDAP accepte les connexions entrantes sur le port 389, via les protocoles TCP ou UDP. La connexion au serveur LDAP via le protocole SSL s'opère souvent sur le port 636.

7. Dans le groupe de paramètres **Paramètres du serveur LDAP**, sélectionnez dans la liste **Type de connexion** une des options de chiffrement des données lors de la connexion au serveur LDAP :

   - **SSL** pour utiliser SSL.
   - **TLS** pour utiliser TLS.
   - **Sans chiffrement** pour ne pas utiliser de technologie de cryptage des données lors de la connexion au serveur LDAP.

8. Dans le groupe de paramètres **Paramètres d'authentification**, saisissez dans le champ **Nom d'utilisateur du serveur LDAP** le nom d'un utilisateur du serveur LDAP autorisé à lire les enregistrements de l'annuaire (BindDN). Saisissez le nom d'utilisateur dans un des formats suivants :

   - `cn=<nom d'utilisateur>, ou=<nom de la division>` (s'il y a lieu), `dc=<nom de domaine>, dc=<nom du domaine parent>`, si vous souhaitez ajouter une connexion à un serveur de service d'annuaires compatible avec LDAP (par exemple, Red Hat Directory Server).

     Par exemple, vous pouvez saisir `cn=LdapServerUser, dc=example, dc=com`, où `LdapServerUser` est le nom de l'utilisateur du serveur LDAP, `example`, le nom de domaine de l'annuaire auquel est rattaché le compte de l'utilisateur et `com` le nom du domaine parent sur lequel se trouve l'annuaire ;

   - `cn=<nom d'utilisateur>, ou=<nom du service>` (le cas échéant), `dc=<nom de domaine>, dc=<nom du domaine parent>` ou `<nom d'utilisateur>@<nom de domaine>.<nom du domaine parent>`, si vous souhaitez ajouter une connexion au serveur Microsoft Active Directory.

     Par exemple, vous pouvez saisir le nom d'utilisateur `LdapServerUser@example.com`, où `LdapServerUser` est le nom de l'utilisateur du serveur LDAP et `example.com` le nom de domaine de l'annuaire auquel est rattaché le compte de l'utilisateur.

9. Dans le groupe de paramètres **Paramètres d'authentification**, saisissez dans le champ **Mot de passe de l'utilisateur du serveur LDAP** le mot de passe permettant d'accéder au

serveur LDAP correspondant à l'utilisateur indiqué dans le champ **Nom d'utilisateur du serveur LDAP** .

10. Dans le groupe **Paramètres de recherche**, saisissez dans le champ **Base de recherche** le *DN* (*Distinguished Name* – nom unique) de l'objet d'annuaire à partir duquel Kaspersky Secure Mail Gateway effectue sa recherche dans les enregistrements.

    Saisissez la base de recherche sous la forme `ou=<nom de la division>` (s'il y a lieu), `dc=<nom de domaine>, dc=<nom de domaine parent>`.

    Par exemple, vous pouvez saisir la base de recherche `ou=people, dc=example, dc=com`, où `people` désigne le niveau dans la structure de répertoire à partir duquel Kaspersky Secure Mail Gateway recherche les enregistrements (La recherche inclut les niveaux `people` et inférieurs. Les objets supérieurs à ce niveau sont exclus de la recherche), `example` désigne le nom de domaine du répertoire dans lequel Kaspersky Secure Mail Gateway réalise la recherche d'enregistrements, `com` représente le nom du domaine parent dans lequel le répertoire se trouve.

11. Cliquez sur le bouton **Tester**.

    Kaspersky Secure Mail Gateway vérifie la connexion au serveur LDAP à partir des valeurs que vous avez saisies pour les paramètres de connexion et d'authentification.

12. Cliquez sur le bouton **Appliquer**.

    La fenêtre **Paramètres de connexion au serveur LDAP** se ferme.

Configuration des filtres de connexion au serveur LDAP

► *Pour configurer les filtres de connexion aux serveurs LDAP, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **LDAP** dans l'arborescence de la console de gestion.

2. Dans la partie inférieure de l'espace de travail, sélectionnez le serveur LDAP dont vous souhaitez configurer les filtres de connexion.

3. Dans le groupe de paramètres **Paramètres des filtres LDAP** du serveur sélectionné, cliquez sur n'importe quel lien pour ouvrir la fenêtre **Paramètres des filtres LDAP**.

4. Dans le groupe de paramètres **Configurez les filtres LDAP**, indiquez dans le champ **Authentification de l'utilisateur** un filtre d'autorisation de l'utilisateur (par exemple, pour que l'utilisateur puisse accéder à ses messages dans la Sauvegarde).

5. Si vous souhaitez définir des valeurs par défaut pour le filtre d'autorisation de l'utilisateur, cliquez sur le lien **Etablir les valeurs par défaut** sous le champ **Authentification de l'utilisateur** .

6. Dans le groupe de paramètres **Configurez les filtres LDAP**, définissez dans le champ **Recherche d'un utilisateur ou d'un groupe** le filtre de recherche d'utilisateurs ou de groupes d'utilisateurs.

7. Si vous souhaitez définir des valeurs par défaut pour le filtre de recherche dans les utilisateurs ou les groupes d'utilisateurs, cliquez sur le lien **Etablir les valeurs par défaut** sous le champ **Recherche d'un utilisateur ou d'un groupe** .

8. Dans le groupe de paramètres **Configurez les filtres LDAP**, définissez dans le champ **Recherche dans les DN d'utilisateurs et de groupes selon l'adresse email** le filtre de la recherche de DN des utilisateurs et des groupes auxquels ils appartiennent sur la base de l'adresse email.

9. Si vous souhaitez définir des valeurs par défaut pour le filtre de recherche dans les DN des utilisateurs et des groupes auxquels ils appartiennent en fonction de leur adresse électronique, cliquez sur le lien **Etablir les valeurs par défaut** sous le champ **Recherche dans les DN d'utilisateurs et de groupes selon l'adresse email**.

10. Dans le champ **Recherche dans les groupes selon le DN des utilisateurs** du groupe de paramètres **Configurez les filtres LDAP**, définissez le filtre de recherche de groupes auquel appartient l'utilisateur, sur la base du DN de l'utilisateur. Ce filtre est utilisé quand il est impossible de déterminer le groupe d'utilisateurs à l'aide du filtre défini dans le champ **Recherche dans les DN d'utilisateurs et de groupes selon l'adresse email**.

11. Si vous souhaitez utiliser des valeurs par défaut pour le filtre de recherche des groupes auxquels appartient l'utilisateur en fonction de son DN, cliquez sur le lien **Etablir les valeurs par défaut** sous le champ **Recherche dans les groupes selon le DN des utilisateurs**.

12. Cochez la case **Utiliser la recherche récursive** pour activer la recherche des enregistrements LDAP dans les sous-groupes.

13. Cliquez sur le bouton **OK**.

    La fenêtre **Paramètres des filtres LDAP** se ferme.

Utilisation de l'application via le protocole SNMP

Cette section contient des informations sur l'utilisation de l'application via le protocole SNMP ainsi que sur la configuration des interruptions pour les événements survenus pendant l'utilisation de Kaspersky Secure Mail Gateway.

Dans cette section

Présentation des informations sur le fonctionnement de l'application via le protocole SNMP

SNMP (Simple Network Management Protocol ou protocole simple de gestion de réseau) est un protocole de gestion des périphériques réseau.

Kaspersky Secure Mail Gateway utilise le protocole SNMP de la manière suivante :

1. L'*agent SNMP* est un module logiciel d'administration réseau de Kaspersky Secure Mail Gateway qui suit les informations relatives au fonctionnement de Kaspersky Secure Mail Gateway.

2. Kaspersky Secure Mail Gateway peut envoyer ces informations sous la forme d'*interruptions SNMP* qui sont des notifications sur les événements du fonctionnement de l'application.

Le protocole SNMP permet d'accéder aux informations suivantes de Kaspersky Secure Mail Gateway :

- Informations générales.
- Statistiques de fonctionnement de Kaspersky Secure Mail Gateway depuis l'installation de l'application.
- Données relatives aux événements survenus pendant le fonctionnement de Kaspersky Secure Mail Gateway.

Par exemple, Kaspersky Secure Mail Gateway envoie une interruption SNMP dans les cas suivants :

- La licence a été renouvelée.

  L'interruption SNMP contient le numéro de la licence, le type de licence, les fonctionnalités disponibles et la date de fin de validité de la licence.

- Période de grâce pour la validité de la licence.

  L'interruption SNMP contient le numéro de la licence et le nombre de jours restant avant l'expiration de la période de grâce.

  L'interruption SNMP démarre au début de la période de grâce, puis une fois par jour et lors du redémarrage de Kaspersky Secure Mail Gateway.

L'accès est uniquement octroyé en lecture.

Activation et désactivation de l'utilisation de SNMP dans Kaspersky Secure Mail Gateway

► *Pour activer ou désactiver l'utilisation de SNMP dans le fonctionnement de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **SNMP** dans l'arborescence de la console de gestion.

2. Exécutez une des actions suivantes :

   - Activez le commutateur en regard du nom du groupe de paramètres **Utiliser SNMP** pour activer l'utilisation de SNMP.

   - Désactivez le commutateur en regard du nom du groupe de paramètres **Utiliser SNMP** pour désactiver l'utilisation de SNMP.

Configuration des paramètres de connexion au serveur SNMP

► *Pour configurer les paramètres de connexion au serveur SNMP, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **SNMP** dans l'arborescence de la console de gestion.

2. Cliquez sur le lien **Adresse et port de connexion au serveur SNMP** ou **Attendre la réponse du serveur SNMP** pour ouvrir la fenêtre **Paramètres de connexion au serveur SNMP**.

3. Saisissez dans le champ **Adresse et port de connexion au serveur SNMP** l'adresse et le port de la connexion au serveur SNMP.

   Par exemple, vous pouvez saisir tcp:localhost:705.

4. Indiquez dans le champ **Attendre la réponse du serveur SNMP** la durée maximale d'attente de la réponse du serveur SNMP en secondes. Cette valeur peut être comprise entre 1 et 255 secondes.

   Valeur par défaut : 15 s.

5. Cliquez sur le bouton **OK**.

Activation et désactivation de l'envoi d'interruptions SNMP

► *Pour activer ou désactiver l'envoie d'interruptions SNMP pour les événements survenus pendant le fonctionnement de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **SNMP** dans l'arborescence de la console de gestion.

2. Activez le commutateur en regard du groupe de paramètres **Utiliser SNMP** s'il est désactivé.

3. Dans le groupe **Utiliser SNMP**, exécutez l'une des actions suivantes :

   - Activez le commutateur en regard du nom du groupe de paramètres **Envoyer une interruption SNMP** pour activer l'envoi d'interruptions SNMP.

   - Désactivez le commutateur en regard du nom du groupe de paramètres **Envoyer une interruption SNMP** pour désactiver l'envoi d'interruptions SNMP.

Messages de notification de Kaspersky Secure Mail Gateway

Cette section contient des informations sur les messages de notification de Kaspersky Secure Mail Gateway et sur la configuration de leurs paramètres.

Dans cette section

A propos des messages de notification

Un *message de notification* (ou "notification") est un message électronique décrivant les événements de l'application ou les événements de l'analyse des messages que Kaspersky Secure Mail Gateway envoie aux adresses email indiquées.

Vous pouvez configurer l'envoi de notifications aux adresses électroniques suivantes :

- Administrateur du serveur de messagerie ;
- Expéditeur des messages ;
- Destinataire des messages ;
- Adresses électroniques complémentaires.

Les *notifications relatives aux événements de Kaspersky Secure Mail Gateway* contiennent des informations sur les paramètres de l'application, sur ses erreurs de fonctionnement et sur les messages expédiés qui n'ont pas été livrés à leur destinataire en cas de problème de livraison.

Vous pouvez configurer l'envoi d'une notification **Message non parvenu** aux expéditeurs des messages qui n'ont pas été livrés.

Vous pouvez configurer l'envoi de notifications à l'administrateur du serveur de messagerie concernant les événements suivants de Kaspersky Secure Mail Gateway :

- **Les bases du module Anti-spam sont obsolètes**.
- **Les bases antivirus sont obsolètes**.
- **Les bases du module Anti-phishing sont obsolètes**.
- **Erreur lors du placement des messages dans la Sauvegarde**.
- **Erreur lors du nettoyage de la Sauvegarde**.
- **La Sauvegarde est presque pleine**.
- **Envoi du résumé sur la Sauvegarde personnelle**.
- **La licence arrive bientôt à échéance**.
- **La durée de validité de la licence est écoulée**.
- **Clé bloquée**.
- **Période de grâce**.
- **Licence mise à jour**.
- **Erreur lors de la connexion au serveur LDAP**.

Les notifications sur les événements d'analyse des messages contiennent des informations sur le message traité et les objets supprimés au sein de ce-dernier. Les notifications pour l'utilisateur de l'application contiennent également le texte du message électronique d'origine.

Vous pouvez configurer l'envoi des notifications de messagerie (cf. section "Configuration des notifications sur les événements d'analyse des messages pour une règle" à la page 367) à

l'administrateur, à l'expéditeur, au destinataire des messages ou à d'autres destinataires pour les événements suivants survenus pendant l'analyse des messages :

- **Des objets malveillants ont été détectés**.
- **Des objets chiffrés ont été découverts**.
- **Des erreurs d'analyse ont été découvertes**.
- **Le filtrage du contenu a fonctionné**.
- **Messages de phishing détectés**.
- **Des macros ont été découvertes dans la pièce jointe**.

Modification des modèles de notification

► *Pour modifier un modèle de notification, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Notifications** dans l'arborescence de la console de gestion.
2. Sélectionnez le groupe correspondant au type de notification dont vous souhaitez modifier le modèle.

   Par exemple, vous pouvez choisir le groupe **Les bases du module Anti-spam sont obsolètes**.
3. Dans le groupe sélectionné, cliquez sur le lien **Objet du message** ou **Texte du message** pour ouvrir la fenêtre **Paramètres de notification**.

   Par exemple, pour modifier le modèle de notification concernant les bases obsolètes du module Anti-Spam, cliquez sur les liens **Objet du message sur les bases obsolètes** ou **Message sur les bases obsolètes**.

   La fenêtre **Paramètres de notification** s'ouvre.
4. Dans le champ **Objet**, indiquez l'objet de la notification dont vous modifiez le modèle.

5. Dans le champ **Texte du message**, indiquez le texte de la notification dont vous souhaitez modifier le modèle.

6. Cliquez sur le bouton **Enregistrer**.

   La fenêtre **Paramètres de notification** se ferme.

Configuration de l'envoi de notifications sur la Sauvegarde personnelle

► *Pour configurer l'envoi de notifications sur la Sauvegarde personnelle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Notifications** dans l'arborescence de la console de gestion.

2. Sélectionnez le groupe **Envoi du résumé sur la Sauvegarde personnelle**.

3. Cliquez sur le lien **Objet du message**, **Texte du message**, **Planification** ou **Ne pas envoyer aux adresses** pour ouvrir la fenêtre **Paramètres de notification**.

4. Saisissez dans le champ **Objet** l'objet de la notification sur la Sauvegarde personnelle. Par exemple, vous pouvez saisir l'objet "Weekly Backup".

5. Saisissez dans le champ **Texte du message** le texte de la notification sur la Sauvegarde personnelle. Par exemple, vous pouvez utiliser le texte par défaut de la notification sur la Sauvegarde personnelle.

6. Indiquez dans les champs **Envoyer les notifications à** le jour de la semaine et l'heure de l'envoi des notifications sur la Sauvegarde personnelle.

7. Si vous voulez exclure des adresses quelconques de la diffusion des notifications sur la Sauvegarde personnelle, exécutez les actions suivantes pour chaque adresse que vous souhaitez exclure :

   a. Saisissez l'adresse email dans le champ **Ne pas envoyer aux adresses.**

Les adresses électroniques sont saisies une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses électroniques.

Vous pouvez utiliser les caractères "*" et "?" pour créer des masques d'adresses ainsi que des expressions régulières en utilisant le préfixe "re:".

Les expressions régulières ne respectent pas la casse.

b. Cliquez sur le bouton **Ajouter** situé à droite du champ.

8. Cliquez sur le bouton **Enregistrer**.

Configuration des notifications sur les événements d'analyse des messages pour une règle

Vous pouvez configurer l'envoi de messages de notification concernant les événements survenus lors de l'analyse des messages pour une ou plusieurs règles.

Vous pouvez configurer l'envoi des notifications de messagerie (cf. section "Configuration des notifications sur les événements d'analyse des messages pour une règle" à la page 367) à l'administrateur, à l'expéditeur, au destinataire des messages ou à d'autres destinataires pour les événements suivants survenus pendant l'analyse des messages :

- **Des objets malveillants ont été détectés**.
- **Des objets chiffrés ont été découverts**.
- **Des erreurs d'analyse ont été découvertes**.
- **Le filtrage du contenu a fonctionné**.
- **Messages de phishing détectés**.
- **Des macros ont été découvertes dans la pièce jointe**.

► Pour configurer l'envoi de notifications sur les événements d'analyse des messages, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez configurer l'envoi de notifications.

3. Sélectionnez le groupe **Notifications**.

4. Sélectionnez l'événement d'analyse des messages pour lequel vous souhaitez configurer l'envoi de notifications.

   Par exemple, vous pouvez sélectionner l'événement **Des objets malveillants ont été détectés**.

5. Dans le groupe de paramètres portant le nom de l'événement sélectionné (par exemple, **Des objets malveillants ont été détectés**), cochez les cases en regard des paramètres :

   - **Prévenir l'administrateur** si vous voulez activer l'envoi de notifications sur l'événement choisi à l'adresse de l'administrateur (cf. section "la Configuration des adresses email de l'administrateur" à la page 212) de Kaspersky Secure Mail Gateway.

   - **Prévenir l'expéditeur** si vous voulez activer l'envoi des notifications sur l'événement sélectionné aux adresses des expéditeurs des messages.

   - **Prévenir le destinataire** si vous voulez activer l'envoi des notifications sur l'événement sélectionné aux adresses des destinataires des messages.

   - **Adresses complémentaires** si vous voulez activer l'envoi des notifications sur l'événement sélectionné à des adresses email additionnelles.

6. Si vous avez activé l'envoi de notifications à l'adresse des destinataires des messages, vous devez configurer les paramètres d'envoi de ces notifications. Pour ce faire, procédez comme suit :

   a. Cliquez sur le lien à droite du paramètre **Prévenir le destinataire** pour ouvrir la fenêtre **Paramètres d'envoi des notifications au destinataire**.

   b. Sélectionnez l'une des options suivantes :

- **Notification seule** si vous voulez configurer l'envoi de la notification aux destinataires sans le message original.
- **Notification accompagnée du message original** si vous voulez configurer l'envoi de la notification aux destinataires avec le message original en pièce jointe.

c. Cliquez sur le bouton **OK**.

La fenêtre **Paramètres d'envoi des notifications au destinataire** se ferme.

7. Si vous avez activé l'envoi de notifications à d'autres adresses électroniques, vous devez indiquer les adresses des destinataires des notifications. Pour ce faire, procédez comme suit :

   a. Cliquez sur le lien à droite du paramètre **Adresses complémentaires** pour ouvrir la fenêtre **Adresses pour l'envoi des notifications**.

   b. Saisissez dans le champ **Adresses pour l'envoi des notifications** l'adresse email du destinataire des notifications.

   Les adresses électroniques sont saisies une à une. Répétez l'opération autant de fois que nécessaire pour ajouter d'autres adresses à la liste des adresses électroniques.

   Vous pouvez utiliser les caractères "*" et "?" pour créer des masques d'adresses ainsi que des expressions régulières en utilisant le préfixe "re:".

   Les expressions régulières ne respectent pas la casse.

   c. Cliquez sur le bouton d'ajout d'enregistrements situé à droite du champ de saisie.

   Dans le champ situé en dessous du bouton d'ajout apparaît la liste des adresses électroniques des autres destinataires des notifications.

   d. Cliquez sur le bouton **OK**.

   La fenêtre **Adresses pour l'envoi des notifications** se ferme.

8. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Activation et désactivation de l'envoi de notifications sur les événements de l'application

► *Pour activer ou désactiver l'envoi de notifications concernant les événements de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Notifications** dans l'arborescence de la console de gestion.

2. Dans le groupe du type de notification dont vous souhaitez activer ou désactiver l'envoi, exécutez une des actions suivantes :

   - Activez le commutateur en regard du nom du groupe sélectionné (dans notre exemple, **Les bases du module Anti-spam sont obsolètes**) pour activer l'envoi de notification concernant cet événement.

   - Désactivez le commutateur en regard du nom du groupe sélectionné (dans notre exemple, **Les bases du module Anti-spam sont obsolètes**) pour désactiver l'envoi de notification concernant cet événement.

Remarques et avertissements de Kaspersky Secure Mail Gateway

Cette section contient des informations sur les remarques et avertissements de Kaspersky Secure Mail Gateway et sur la configuration de leurs paramètres.

Dans cette section

A propos des remarques sur les messages et des avertissements concernant un message dangereux

Une *remarque concernant le message* (ci-après "remarque") est un texte que Kaspersky Secure Mail Gateway peut ajouter au début ou à la fin d'un message électronique.

Vous pouvez configurer des modèles de remarque, définir le format d'affichage des remarques dans les messages et activer ou désactiver leur utilisation pour une ou plusieurs règles de traitement des messages.

Un *avertissement concernant un message dangereux* (ci-après "avertissement") est un texte que Kaspersky Secure Mail Gateway peut ajouter au début ou à la fin des messages électroniques présentant l'un des états suivants à la suite de l'analyse par les modules de l'application :

- *Encrypted (crypté)* ;
- *Phishing (tentative de phishing)* ;
- *Infected (infecté)* ;
- *Error (erreur d'analyse)*.

Vous pouvez configurer des modèles d'avertissement, définir le format d'affichage des avertissements dans les messages et activer ou désactiver leur utilisation pour une ou plusieurs règles de traitement des messages.

Création d'un modèle de remarque ou d'avertissement

► *Pour créer un modèle de remarque ou d'avertissement, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Avertissements** dans l'arborescence de la console de gestion.
2. Cliquez sur le bouton **Créer** situé dans la partie supérieure de l'espace de travail.

   Un nouveau modèle de remarque ou d'avertissement s'ouvre.
3. Dans le champ **Nom du modèle**, indiquez le nom du modèle.

   C'est ce nom qui vous permet de sélectionner le modèle à utiliser lors de la configuration des paramètres des règles de traitement des messages.
4. La liste déroulante **Position** permet de choisir l'emplacement des remarques ou des avertissements. Vous pouvez configurer l'affichage de la remarque ou d'un avertissement avant le message ou après celui-ci.
5. Au-dessus du champ **Texte du message**, sélectionnez l'un des onglets suivants :

- **Sans balises** pour que le message soit affiché au format texte.
- **HTML** pour que le message soit affiché au format HTML.

  Kaspersky Secure Mail Gateway choisit par défaut le format du texte en fonction du format du message électronique.

  Si le message électronique est au format **HTML**, Kaspersky Secure Mail Gateway ajoute la remarque ou l'avertissement au format **HTML**.

  Si le message électronique est au format **Sans balises**, Kaspersky Secure Mail Gateway ajoute la remarque ou l'avertissement au format **Sans balises**.

6. Dans le champ **Texte du message**, saisissez le texte de la remarque ou de l'avertissement.
7. S'il s'agit d'un texte au format HTML, cliquez sur le lien **Parcourir** sous le champ **Texte du message** pour voir à quoi ressemblera le message.
8. Cochez la case **Texte uniquement** si vous souhaitez que le message ne contienne que du texte.

   Lors de l'ajout d'une remarque ou d'un avertissement au format **Texte uniquement** dans un message électronique au format **HTML**, le format du message peut être perturbé.

9. Cliquez sur le bouton **Créer** situé dans la partie inférieure de l'espace de travail.

Le modèle de remarque ou d'avertissement que vous avez créé apparaît dans la liste des modèles de remarques et d'avertissements dans l'espace de travail de la fenêtre principale de l'interface Web.

Modification d'un modèle de remarque ou d'avertissement

► *Pour modifier un modèle de remarque ou d'avertissement, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Avertissements** dans l'arborescence de la console de gestion.

2. Dans l'espace de travail, sélectionnez dans la liste des modèles de remarque et d'avertissement le modèle à modifier.

3. Dans le champ **Nom du modèle**, vous pouvez modifier le nom du modèle.

   C'est ce nom qui vous permet de sélectionner le modèle à utiliser lors de la configuration des paramètres des règles de traitement des messages.

4. La liste déroulante **Position** permet de modifier l'emplacement des remarques ou des avertissements. Vous pouvez configurer l'affichage de la remarque ou d'un avertissement avant le message ou après celui-ci.

5. Au-dessus du champ **Texte du message**, sélectionnez l'un des onglets suivants :

   - **Sans balises** pour que le message soit affiché au format texte.

   - **HTML** pour que le message soit affiché au format HTML.

6. Dans le champ **Texte du message**, vous pouvez modifier le texte de la remarque ou de l'avertissement.

7. S'il s'agit d'un texte au format HTML, cliquez sur le lien **Parcourir** sous le champ **Texte du message** pour voir à quoi ressemblera le message.

8. Cochez la case **Texte uniquement** si vous souhaitez que le message ne contienne que du texte.

9. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Suppression d'un modèle de remarque ou d'avertissement

► *Pour supprimer un modèle de remarque ou d'avertissement, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Avertissements** dans l'arborescence de la console de gestion.

2. Cochez la case en regard du nom du ou des modèles de remarque ou d'avertissement à supprimer.

3. Cliquez sur le bouton **Supprimer** situé dans la partie supérieure de l'espace de travail.

Les modèles de remarque et d'avertissement que vous avez sélectionnés sont supprimés.

Activation et désactivation des remarques sur les messages pour une règle

Vous pouvez activer ou désactiver l'ajout de remarques aux messages pour une ou plusieurs règles. L'ajout de remarque aux messages est désactivé par défaut.

► *Pour activer ou désactiver l'ajout de remarques aux messages pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez activer ou désactiver l'ajout de remarques.

3. Choisissez le groupe **Avertissement concernant un message**.

4. Exécutez une des actions suivantes :

- Activez le commutateur en regard du nom du groupe de paramètres **Avertissement concernant un message** pour activer l'ajout de remarques aux messages pour cette règle.

- Désactivez le commutateur en regard du nom du groupe de paramètres **Avertissement concernant un message** pour désactiver l'ajout de remarques aux messages pour cette règle.

5. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Ajout d'une remarque aux événements d'analyse des messages pour une règle

► *Pour ajouter une remarque aux événements d'analyse des messages pour une règle, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez ajouter une remarque aux événements d'analyse des messages.

3. Choisissez le groupe **Avertissement concernant un message**.

4. Activez le commutateur en regard du groupe de paramètres **Avertissement concernant un message** s'il est désactivé.

5. Cliquez sur le lien à droite du nom du paramètre **Nom du modèle d'avertissement** dans le groupe de paramètres **Ajouter l'avertissement suivant**.

6. La fenêtre **Modèle d'avertissement** s'ouvre.

7. Dans la liste **Modèle d'avertissement**, sélectionnez le modèle à ajouter aux événements d'analyse des messages pour cette règle.

8. Cliquez sur le bouton **OK**.

   La fenêtre **Modèle d'avertissement** se ferme.

La remarque que vous avez ajoutée apparaît dans le groupe **Avertissement concernant un message** de l'espace de travail dans la fenêtre principale de l'interface Web de l'application.

9. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que l'ajout de remarques aux messages pour la règle est activé (cf. section "Activation et désactivation des remarques sur les messages pour une règle" à la page 375), et que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Ajout d'un avertissement concernant un message dangereux pour une règle

► Pour ajouter un avertissement concernant un message dangereux pour une règle, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Règles** dans l'arborescence de la console de gestion.

2. Dans la liste des règles, cliquez sur le lien portant le nom de la règle pour laquelle vous souhaitez ajouter un avertissement concernant un message dangereux.

3. Choisissez le groupe **Avertissement concernant un message dangereux**.

4. Cochez les cases en regard du ou des types de messages auxquels vous souhaitez ajouter un avertissement :

   - **Ajouter aux messages chiffrés** pour ajouter un avertissement aux messages auxquels les modules de Kaspersky Secure Mail Gateway ont attribué l'état d'analyse *Encrypted (crypté)*.

   - **Ajouter aux messages de phishing** pour ajouter un avertissement aux messages auxquels les modules de Kaspersky Secure Mail Gateway ont attribué l'état d'analyse *Phishing (tentative de phishing)*.

- **Ajouter aux messages infectés** pour ajouter un avertissement aux messages auxquels les modules de Kaspersky Secure Mail Gateway ont attribué l'état d'analyse *Infected (infecté)*.

- **Ajouter aux messages avec erreurs d'analyse** pour ajouter un avertissement aux messages auxquels les modules de Kaspersky Secure Mail Gateway ont attribué l'état d'analyse *Error (erreur d'analyse)*.

5. Dans le groupe de paramètres **Ajouter l'avertissement suivant**, cliquez sur le lien situé à droite du nom du paramètre **Modèle d'avertissement.**

6. La fenêtre **Modèle d'avertissement** s'ouvre.

7. Dans la liste **Modèle d'avertissement**, sélectionnez le modèle d'avertissement concernant un message dangereux à ajouter à la règle.

8. Cliquez sur le bouton **OK**.

   La fenêtre **Modèle d'avertissement** se ferme.

   L'avertissement que vous avez ajout apparaît dans le groupe **Avertissement concernant un message dangereux** de l'espace de travail dans la fenêtre principale de l'interface Web de l'application.

9. Cliquez sur le bouton **Appliquer** situé dans la partie inférieure de l'espace de travail.

Pour que les paramètres que vous avez configurés soient utilisés dans Kaspersky Secure Mail Gateway, confirmez que la règle dont vous avez configuré les paramètres est activée (cf. section "Activation et désactivation d'une règle de traitement de messages" à la page 145).

Journal des événements de Kaspersky Secure Mail Gateway

Cette section contient des informations sur le journal des événements de Kaspersky Secure Mail Gateway.

Dans cette section

Présentation du journal des événements

Différents événements peuvent survenir pendant le fonctionnement de Kaspersky Secure Mail Gateway. Ils témoignent d'une modification de l'état de l'application. Pour que l'administrateur de l'application puisse analyser les erreurs commises lors de la configuration des paramètres de l'application et pour que les experts de Kaspersky Lab puissent offrir une assistance technique efficace, Kaspersky Secure Mail Gateway consigne les informations relatives à ces événements dans le *journal des événements*.

Ces journaux sont conservés pendant toute la durée d'utilisation de Kaspersky Secure Mail Gateway et sont supprimés de manière irréversible lors de la suppression de l'application. Un nouveau fichier de journal des événements est formé dès que le fichier actuel atteint la taille limite maximale.

Kaspersky Secure Mail Gateway tient le journal des événements dans le journal du système d'exploitation (syslog), catégorie Mail. Il est possible de modifier la catégorie du journal des événements.

Kaspersky Secure Mail Gateway répartit les événements selon les niveaux suivants :

- *Error* : événements relatifs aux erreurs de fonctionnement de l'application.
- *Info* : informations.

> Les événements du niveau *Info* peuvent contenir les adresses électroniques des expéditeurs et des destinataires des messages, les noms des pièces jointes, les adresses IP des ordinateurs d'origine des message ainsi que les résultats détaillés de l'analyse des messages.

Par défaut, Kaspersky Secure Mail Gateway consigne dans le journal des événements uniquement les événements avec le niveau d'importance *Info* (cf. tableau ci-après). Vous pouvez configurer la consignation dans le journal des événements de tous les événements qui se produisent durant le fonctionnement de l'application.

Tableau 2. Evénements dans le journal des événements

Evénement	Description	Niveau d'événement
RuleSettingsChangedEvent	Modification des paramètres de la règle de traitement des messages.	Info
TaskSettingsChangedEvent	Modification des paramètres d'une tâche.	Info
MessageProcessedEvent	Le message a été traité.	Info
MessageNotProcessedEvent	Le message n'a pas été traité.	Info
MessageQuarantinedEvent	Le message a été placé dans la Sauvegarde.	Info
ProductStartEvent	L'application a été lancée.	Info
ScheduledReportError	Une erreur lors de la création d'un rapport selon une planification est survenue.	Error
ScheduledReportGenerated	La création du rapport selon la planification a réussi.	Info
BackupLimitReachedEvent	La taille maximale de la Sauvegarde a été atteinte.	Info
BackupRestoreAvThreatEvent	Le message de la Sauvegarde a été enregistré dans un fichier ou envoyé aux destinataires.	Info
BackupAddErrorEvent	Une erreur s'est produite lors de l'ajout du message à la Sauvegarde.	Error
BackupRotateErrorEvent	Une erreur s'est produite lors de l'augmentation automatique de l'espace disque dans la Sauvegarde.	Error

Evénement	Description	Niveau d'événement
AvUpdateErrorEvent	Une erreur s'est produite lors de la mise à jour des bases antivirus.	Error
AvBasesLoadError	Une erreur s'est produite lors du téléchargement des bases anti-virus.	Error
AspUpdateErrorEvent	Erreur de mise à jour des bases Anti-Spam.	Error
AspBasesLoadError	Une erreur s'est produite lors du téléchargement des bases de l'Anti-Spam.	Error
ApUpdateErrorEvent	Une erreur s'est produite lors de la mise à jour des bases de l'Anti-Phishing.	Error
ApBasesLoadError	Une erreur s'est produite lors du téléchargement des bases de l'Anti-Phishing.	Error
AvBasesAttachedEvent	La mise à jour des bases anti-virus a réussi.	Info
ApBasesAttachedEvent	La mise à jour des bases de l'Anti-Phishing a réussi.	Info
AspBasesAttachedEvent	La mise à jour des bases de l'Anti-Spam a réussi.	Info
NothingToUpdateEvent	La mise à jour de la base de données n'est pas requise.	Info
AvBasesOutdatedEvent	Les bases antivirus sont obsolètes.	Info
AspBasesOutdatedEvent	Les bases Anti-Spam sont obsolètes.	Info

Evénement	Description	Niveau d'événement
ApBasesOutdatedEvent	Les bases Anti-Phishing sont obsolètes.	Info
AvBasesObsoleteEvent	Les bases antivirus sont fortement dépassées.	Info
AspBasesObsoleteEvent	Les bases Anti-Spam sont fortement dépassées.	Info
ApBasesObsoleteEvent	Les bases Anti-Phishing sont fortement dépassées.	Info
AvBasesAppliedEvent	Le chargement des bases anti-virus a réussi.	Info
AspBasesAppliedEvent	Le chargement des bases Anti-Spam a réussi.	Info
ApBasesAppliedEvent	Le chargement des bases Anti-Phishing a réussi.	Info
LicenseBlacklistedEvent	La clé est présente dans la liste noire.	Error
LicenseExpiredEvent	La licence a expiré.	Error
LicenseExpiresSoonEvent	La licence arrivera bientôt à échéance.	Info
LicenseErrorEvent	Erreur de clé.	Error
LicenseInstalledEvent	Clé ajoutée avec succès.	Info
LicenseRevokedEvent	Clé supprimée avec succès.	Info
TaskCrashEvent	Le fonctionnement du processus s'est soldé sur un échec.	Error

Evénement	Description	Niveau d'événement
TaskRestartEvent	Le processus a été restauré.	Info
QueueFlushMessageSuccessEvent	L'envoi forcé d'un message distinct de la file d'attente a réussi.	Info
QueueFlushMessageFailureEvent	Echec de l'envoi forcé d'un message distinct de la file d'attente.	Error
QueueFlushAllSuccessEvent	L'envoi forcé de tous les messages de la file d'attente a réussi.	Info
QueueFlushAllFailureEvent	Echec de l'envoi forcé de tous les messages de la file d'attente.	Error
QueueDeleteMessageSuccessEvent	La suppression d'un message distinct de la file d'attente a réussi.	Info
QueueDeleteMessageFailureEvent	Echec de la suppression d'un message distinct de la file d'attente.	Error
QueueDeleteAllSuccessEvent	La suppression de tous les messages de la file d'attente a réussi.	Info
QueueDeleteAllFailureEvent	Echec de la suppression de tous les messages de la file d'attente.	Error
MailProcessingChangeSuccessEvent	Modification de l'état de l'envoi ou de la réception des messages : a réussi.	Info
MailProcessingChangeFailureEvent	Modification de l'état de l'envoi ou de la réception des messages : erreur.	Error
TLSServerCertificateWasChanged	Modification du certificat TLS.	Info

Consultation du journal des événements

► *Pour consulter le journal des événements de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.

2. Sélectionnez la catégorie du journal des événements que vous souhaitez consulter dans la liste **Catégorie de journal**.

3. Sélectionnez le nombre d'enregistrements à consulter dans la liste **Derniers**.

4. Cliquez sur le bouton **Consulter**.

Chargement du journal des événements sur le disque dur

► *Pour charger le journal des événements de Kaspersky Secure Mail Gateway sur le disque dur, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.

2. Sélectionnez la catégorie du journal des événements que vous souhaitez charger dans la liste **Catégorie de journal**.

3. Cliquez sur le lien **Télécharger** à droite de la liste **Catégorie de journal** pour ouvrir la fenêtre de chargement du journal des événements.

Le journal des événements est enregistré sur le disque dur de l'ordinateur, dans le répertoire qui a été indiqué comme répertoire de téléchargement des fichiers Internet dans les paramètres du navigateur que vous utilisez avec Kaspersky Secure Mail Gateway.

Informations relatives au système pour le Support Technique

Vous pouvez créer une archive contenant les informations relatives au système (fonctionnement de Kaspersky Secure Mail Gateway) en vue de l'envoyer au Support technique de Kaspersky Lab. Il se peut que cette archive contienne des informations relatives à votre entreprises jugées confidentielles. L'administrateur de Kaspersky Secure Mail Gateway doit absolument déterminer le contenu de l'archive à envoyer en coopération avec le service de sécurité de votre entreprise.

Avant d'envoyer l'archive, supprimez toutes les données que vous jugez confidentielles contenues dans celle-ci.

Dans cette section

Création d'une archive reprenant les informations relatives au système

► *Pour créer une archive reprenant des informations relatives au système, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.

2. Dans le coin inférieur droit de la fenêtre, cliquez sur le lien **Informations sur le système**.

La fenêtre **Informations sur le système pour le Support Technique** s'ouvre.

3. Cliquez sur le bouton **Créer**.

   La fenêtre **Créer une archive reprenant les informations du système** s'ouvre.

Après quelques secondes, l'archive contenant les informations relatives au fonctionnement de Kaspersky Secure Mail Gateway apparaît dans la liste des archives dans la fenêtre **Informations sur le système pour le Support Technique**.

Chargement sur le disque dur de l'archive contenant des informations sur le système

► *Pour charger l'archive contenant les informations relatives au système sur le disque dur, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.

2. Dans le coin inférieur droit de la fenêtre, cliquez sur le lien **Informations sur le système**.

   La fenêtre **Informations sur le système pour le Support Technique** s'ouvre. La liste des archives contenant des informations relatives au système s'affiche. Si la liste ne contient pas d'archives avec des informations relatives au système, vous pouvez créer une archive (cf. section "Création d'une archive reprenant les informations relatives au système" à la page 386).

3. Cliquez sur le lien portant le nom de l'archive pour lancer le processus de chargement de l'archive sur le disque dur.

L'archive au format TGZ est chargée sur le disque dur de l'ordinateur, dans le répertoire qui a été indiqué comme répertoire de téléchargement des fichiers Internet dans les paramètres du navigateur que vous utilisez avec Kaspersky Secure Mail Gateway.

Suppression de l'archive contenant des informations sur le système

► *Pour supprimer une ou plusieurs archives contenant des informations relatives au système, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.

2. Dans le coin inférieur droit de la fenêtre, cliquez sur le lien **Informations sur le système**.

   La fenêtre **Informations sur le système pour le Support Technique** s'ouvre. La liste des archives contenant des informations relatives au système s'affiche.

3. Cochez les cases à gauche des noms des archives que vous souhaitez supprimer.

4. Cliquez sur le bouton **Supprimer**.

5. Si vous souhaitez purger toute la liste des archives contenant des informations sur le système, cliquez sur le bouton **Tout supprimer**.

Les archives contenant des informations sur le système sont supprimées.

Journal d'audit de Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway enregistre les événements liés à l'analyse des messages électroniques dans le journal d'audit.

Cette section fournit des informations sur l'utilisation du journal d'audit de Kaspersky Secure Mail Gateway et explique comment trier et filtrer les événements du journal d'audit ou lancer une recherche selon une des colonnes du tableau sur un critère que vous avez choisi.

Dans cette section

Consultation du journal d'audit et des événements dans le journal d'audit

► *Pour consulter le journal d'audit de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.

2. Dans le coin inférieur droit de la fenêtre, cliquez sur le lien **Journal d'audit**.

La fenêtre **Journal d'audit** qui reprend le tableau des événements dans le journal d'audit de Kaspersky Secure Mail Gateway s'ouvre.

Le tableau affiche les 500 premiers événements du journal d'audit. Pour afficher un plus grand nombre d'événements, utilisez le filtrage et la recherche d'événements dans le journal d'audit.

► *Pour consulter un événement dans le journal d'audit de Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.

2. Dans le coin inférieur droit de la fenêtre, cliquez sur le lien **Journal d'audit**.

   La fenêtre **Journal d'audit** qui reprend le tableau des événements dans le journal d'audit de Kaspersky Secure Mail Gateway s'ouvre.

3. Cliquez sur le lien des informations relatives à l'événement que vous souhaitez consulter pour ouvrir la fenêtre contenant ces informations.

4. Si vous voulez revenir au tableau des événements, cliquez sur le bouton **Dans le journal d'audit**.

Tri des événements dans le journal d'audit

► Pour trier *les événements dans le journal d'audit*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.

2. Dans le coin inférieur droit de la fenêtre, cliquez sur le lien **Journal d'audit**.

   La fenêtre **Journal d'audit** qui reprend le tableau des événements dans le journal d'audit de Kaspersky Secure Mail Gateway s'ouvre.

3. Cliquez sur le bouton à gauche du nom de la colonne du tableau selon laquelle vous souhaitez trier les événements. Vous pouvez trier les événements selon un des paramètres suivants :

   - **Heure de l'événement** : date et heure de l'événement.
   - **Type d'événement** : te type d'événement de Kaspersky Secure Mail Gateway. Par exemple, **Analyse des messages**.
   - **ID du sujet** : ID du sujet. Par exemple, le nom de domaine du serveur de Kaspersky Secure Mail Gateway.
   - **Résultat** : résultat de l'événement Kaspersky Secure Mail Gateway. Par exemple, **Terminé** ou **Erreur**.
   - **Description** : description de l'événement et son résultat. Par exemple, le résultat de l'analyse du message à l'aide des modules de l'application ou le message indiquant que la mise à jour des bases de l'application a échoué.

► *Pour modifier l'ordre du tri des messages dans la file d'attente,*

cliquez sur le bouton  ou  à gauche du nom de la colonne du tableau dont vous souhaitez changer l'ordre.

Filtrage et recherche des événements selon la date et l'heure

► Pour filtrer ou trouver des événements en fonction de la *date et de l'heure*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.

2. Dans le coin inférieur droit de la fenêtre, cliquez sur le lien **Journal d'audit**.

   La fenêtre **Journal d'audit** qui reprend le tableau des événements dans le journal d'audit de Kaspersky Secure Mail Gateway s'ouvre.

3. Cliquez sur le lien **Heure de l'événement** pour développer la liste des intervalles de recherche d'événements.

4. Sélectionnez un des intervalles suivants :

   - **Dernière heure**.
   - **Dernier jour**.
   - **Dernière semaine**.
   - **Personnalisé**.

5. Si vous avez choisi l'intervalle défini par l'utilisateur pour la recherche d'événements, procédez comme suit :

   a. Dans le calendrier qui s'ouvre, indiquez la date de début et la date de fin de la période d'affichage des messages dans le journal d'audit.

   b. Cliquez sur le bouton **Appliquer**.

   Le calendrier se referme.

L'espace de travail de la fenêtre **Journal d'audit** affiche le tableau des événements dans le journal d'audit obtenu selon les conditions du filtre.

Si le filtre de la recherche de messages n'est pas défini, le tableau affiche les 500 premiers événements du journal d'audit.

Filtrage et recherche des événements selon le type

► Pour filtrer ou trouver des événements en fonction du *type d'événement*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.
2. Dans le coin inférieur droit de la fenêtre, cliquez sur le lien **Journal d'audit**.

   La fenêtre **Journal d'audit** qui reprend le tableau des événements dans le journal d'audit de Kaspersky Secure Mail Gateway s'ouvre.
3. Cliquez sur le lien **Type d'événement** pour ouvrir la fenêtre de configuration du filtrage des événements.
4. Saisissez dans le champ **Type d'événement** quelques caractères ou tous les caractères du type d'événement. Par exemple, vous pouvez saisir **Analyse des messages**.
5. Cliquez sur le bouton **Appliquer**.

L'espace de travail de la fenêtre **Journal d'audit** affiche le tableau des événements du journal d'audit obtenu selon les conditions du filtre.

Si le filtre de la recherche de messages n'est pas défini, le tableau affiche les 500 premiers événements du journal d'audit.

Filtrage et recherche des événements selon l'identifiant du sujet

► Pour filtrer ou trouver des événements en fonction de *l'identifiant du sujet*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.

2. Dans le coin inférieur droit de la fenêtre, cliquez sur le lien **Journal d'audit**.

   La fenêtre **Journal d'audit** qui reprend le tableau des événements dans le journal d'audit de Kaspersky Secure Mail Gateway s'ouvre.

3. Cliquez sur le lien **ID du sujet** pour ouvrir la fenêtre de configuration du filtrage des événements.

4. Saisissez dans le champ **ID du sujet** quelques caractères ou tous les caractères de l'identifiant du sujet. Par exemple, vous pouvez saisir le nom de domaine du serveur Kaspersky Secure Mail Gateway.

5. Cliquez sur le bouton **Appliquer**.

L'espace de travail de la fenêtre **Journal d'audit** affiche le tableau des événements du journal d'audit obtenu selon les conditions du filtre.

Si le filtre de la recherche de messages n'est pas défini, le tableau affiche les 500 premiers événements du journal d'audit.

Filtrage et recherche des événements d'après le résultat de l'événement

► Pour filtrer ou trouver des événements en fonction du *résultat de l'événement*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.

2. Dans le coin inférieur droit de la fenêtre, cliquez sur le lien **Journal d'audit**.

   La fenêtre **Journal d'audit** qui reprend le tableau des événements dans le journal d'audit de Kaspersky Secure Mail Gateway s'ouvre.

3. Cliquez sur le lien **Résultat** pour développer la liste des résultats de l'événement.

4. Choisissez un des résultats suivants de l'événement :

   - **Terminé**.
   - **Erreur**.

5. Cliquez sur le bouton **Appliquer**.

L'espace de travail de la fenêtre **Journal d'audit** affiche le tableau des événements du journal d'audit obtenu selon les conditions du filtre.

Si le filtre de la recherche de messages n'est pas défini, le tableau affiche les 500 premiers événements du journal d'audit.

Filtrage et recherche des événements selon la description de l'événement

► Pour filtrer ou trouver des événements en fonction de la *description de l'événement*, procédez comme suit :

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Journal des événements** dans l'arborescence de la console de gestion.

2. Dans le coin inférieur droit de la fenêtre, cliquez sur le lien **Journal d'audit**.

   La fenêtre **Journal d'audit** qui reprend le tableau des événements dans le journal d'audit de Kaspersky Secure Mail Gateway s'ouvre.

3. Cliquez sur le lien **Description** pour ouvrir la fenêtre de configuration du filtrage des événements.

4. Saisissez dans le champ **Description** quelques caractères de la description de l'événement.

5. Cliquez sur le bouton **Appliquer**.

L'espace de travail de la fenêtre **Journal d'audit** affiche le tableau des événements du journal d'audit obtenu selon les conditions du filtre.

Si le filtre de la recherche de messages n'est pas défini, le tableau affiche les 500 premiers événements du journal d'audit.

Configuration de la date et de l'heure de Kaspersky Secure Mail Gateway

► *Pour régler la date et l'heure dans Kaspersky Secure Mail Gateway, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Date et heure** dans l'arborescence de la console de gestion.

2. Dans le groupe **Définition de la date et de l'heure**, cliquez sur l'icône d'édition.

3. Sélectionnez l'une des options suivantes :

   - Si vous voulez synchroniser l'heure de l'application avec celle de l'hôte, choisissez l'option **Synchroniser avec l'hôte VMWare™**.

   - Si vous voulez synchroniser l'heure avec le serveur NTP, sélectionnez l'option **Synchroniser avec le serveur NTP**, puis saisissez l'adresse du serveur NTP dans le champ **Adresse du serveur NTP**.

     Si vous choisissez cette option, il est conseillé de désactiver la synchronisation de l'heure (voir la section "Désactivation de la synchronisation de l'heure de la machine virtuelle et de l'hôte" à la page 103) de la machine virtuelle et de l'hôte à l'aide des outils de l'hyperviseur.

   - Si vous souhaitez régler la date et l'heure manuellement, sélectionnez l'option **Définir la date et l'heure manuellement** et dans les champs de saisie du bas, renseignez les valeurs souhaitées pour la date et l'heure.

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

► *Pour définir le fuseau horaire, procédez comme suit :*

1. Sur la fenêtre principale de l'interface Web de l'application, sélectionnez la section **Paramètres** puis la sous-section **Date et heure** dans l'arborescence de la console de gestion.
2. Dans le groupe **Définition du fuseau horaire**, cliquez sur l'icône d'édition.
3. Sélectionnez le pays requis dans la liste déroulante **Pays**.
4. Sélectionnez le fuseau horaire requis dans la liste déroulante **Fuseau horaire**.
5. Cliquez sur le bouton **OK**.

Enregistrement des données des utilisateurs

Il incombe à l'administrateur de Kaspersky Secure Mail Gateway de garantir lui-même la sécurité des données exploitées par l'application. L'administrateur de Kaspersky Secure Mail Gateway est responsable de l'accès à ces données.

Kaspersky Secure Mail Gateway utilise dans le cadre de son fonctionnement certaines données de l'utilisateur. Le tableau ci-dessous reprend les informations relatives aux données des utilisateurs, à leur exploitation par l'application et aux utilisateurs qui ont accès à ces données.

Tableau 3. Utilisation des données des utilisateurs

Données des utilisateurs	Emplacement de l'utilisation	Utilisateurs dotés d'un accès
Statistiques sur les messages électroniques : • Adresse de l'expéditeur et des destinataires. • Noms des pièces jointes infectées.	Rapports.	Utilisateur sous le compte utilisateur HelpDesk.
Informations des messages électroniques : • Adresse IP de l'expéditeur. • Adresse de l'expéditeur et des destinataires. • Objet du message. • Le corps du message. • En-tête de service du message. • Pièce jointe.	• Rapports. • Sauvegarde. • Journaux et fichiers de trace de l'application. • Kaspersky Anti Targeted Attack Platform (dans le cadre de l'intégration de KSMG à KATA). Les données sont transmises sous forme chiffrées. • File d'attente de messages MTA. • Quarantaine de l'Anti-spam. • Quarantaine KATA. • Fichiers dump. • Mémoire vive.	• Administrateur dans le cadre de l'utilisation de l'application dans la console et en mode Technical Support Mode. • Administrateur de l'interface Web de l'application. • Administrateur de l'application Kaspersky Anti Targeted Attack Platform.

Données des utilisateurs	Emplacement de l'utilisation	Utilisateurs dotés d'un accès
Nom d'utilisateur, mot de passe et adresse IP utilisés pour ouvrir une session dans l'interface Web de l'application.	• Journaux et fichiers de trace de l'application. • Fichiers dump. • Mémoire vive.	• Administrateur dans le cadre de l'utilisation de l'application dans la console et en mode Technical Support Mode. • Administrateur de l'interface Web de l'application.
Identifiants des utilisateurs LDAP ou Active Directory.	• Journaux et fichiers de trace de l'application. • Fichiers dump. • Cache LDAP. • Mémoire vive.	• Administrateur dans le cadre de l'utilisation de l'application dans la console et en mode Technical Support Mode. • Administrateur de l'interface Web de l'application.
Configuration de l'application : • Listes noires et blanches d'adresses. • Comptes utilisateur de l'administrateur de l'application et de l'utilisateur HelpDesk. • Comptes utilisateur pour la connexion au serveur LDAP et au serveur proxy.	• Fichiers de configuration de l'application. • Mémoire vive. • Fichiers dump.	• Administrateur dans le cadre de l'utilisation de l'application dans la console et en mode Technical Support Mode. • Administrateur de l'interface Web de l'application.

Données des utilisateurs	Emplacement de l'utilisation	Utilisateurs dotés d'un accès
Données relatives aux mises à jour : • Adresses IP utilisées par l'ordinateur lors de la connexion aux sources des mises à jour. • Adresses IP des sources des mises à jour. • Informations sur le fichier chargé et sur la vitesse du chargement.	Journaux et fichiers de trace de l'application.	• Administrateur dans le cadre de l'utilisation de l'application dans la console et en mode Technical Support Mode. • Administrateur de l'interface Web de l'application.

Contacter le Support technique

Cette section contient des informations sur les modes et les conditions d'obtention de l'assistance technique.

Dans cette section

Modes d'obtention du Support Technique

Si vous n'avez pas trouvé la solution à votre problème dans la documentation ou dans une des sources d'informations sur l'application (cf. section "Sources d'informations sur l'application" à la page 24), veuillez contacter le Support technique. Les experts du Support technique répondront à vos questions sur l'installation et l'utilisation de l'application.

Le support technique est fourni uniquement aux utilisateurs de l'application ayant acheté une licence commerciale. Les utilisateurs qui disposent d'une licence d'évaluation n'ont pas droit au support technique.

> Avant de contacter le Support technique, prenez connaissance des règles d'octroi de l'assistance technique (http://support.kaspersky.com/fr/support/rules).

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

- Téléphoner au Support technique (https://support.kaspersky.fr/b2c) ;

- envoyer une demande au Support Technique de Kaspersky Lab via le portail Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Support 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 du Support 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/fr/b2b).

Avant de contacter le Support technique, prenez connaissance des règles d'octroi de l'assistance technique (http://support.kaspersky.com/fr/support/rules).

Support technique via le Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) est un portail destiné aux organisations qui utilisent les applications de 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 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 sur 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 Kaspersky CompanyAccount, veuillez consulter le site Internet du Support technique (http://support.kaspersky.com/fr/faq/companyaccount_help).

Glossaire

A

Advanced persistent threat (APT)

Attaque ciblée complexe contre l'infrastructure informatique d'une organisation et qui implique l'utilisation simultanée de diverses méthodes de pénétration du réseau, de positionnement dans le réseau et d'obtention d'un accès régulier aux données confidentielles.

Agent SNMP

Module logiciel d'administration de réseau de Kaspersky Secure Mail Gateway. Il surveille les informations relatives au fonctionnement de Kaspersky Secure Mail Gateway.

Analyse heuristique

Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky Lab. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu.

Après avoir identifié le code malveillant, l'analyse heuristique attribue aux fichiers concernés l'état infecté.

Anti-phishing

Module de Kaspersky Secure Mail Gateway dont le rôle consiste à détecter les messages classés comme phishing.

Anti-spam

Module de Kaspersky Secure Mail Gateway dont le rôle consiste à détecter les messages classés comme spam.

Antivirus

Composant de Kaspersky Secure Mail Gateway destiné à la détection de virus dans les messages électroniques et les pièces jointes de ces messages.

Attaque ciblée

Attaque ciblée contre un individu ou une organisation en particulier. À la différence des attaques massives impliquant des virus informatiques qui cherchent à infecter un maximum d'ordinateurs, les attaques ciblées cherchent à infecter le réseau d'une organisation en particulier, voire un serveur défini au sein de l'infrastructure informatique. Un cheval de Troie spécial peut être programmé pour chaque attaque ciblée.

Attaque "0jour"

Attaque contre l'infrastructure informatique d'une organisation qui repose sur l'exploitation d'une vulnérabilité "0jour" dans une application. Cette vulnérabilité est connue des individus malintentionnés avant que l'éditeur de l'application n'a eu le temps de diffuser une mise à jour contenant un correctif.

Authentification DKIM des expéditeurs

Vérification de la signature numérique des messages.

Authentification DMARC des expéditeurs

Vérifie si le message a bel et bien été envoyé depuis le domaine indiqué.

Authentification SPF des expéditeurs

Comparaison des adresses IP des expéditeurs de message à la liste des sources de messages possibles composée par l'administrateur du serveur de messagerie.

C

Courrier indésirable

Envoi massif non autorisé de messages électroniques, le plus souvent à caractère publicitaire.

D

DNSBL

DNS blacklist et DNS blocklist. Liste de serveurs DNSBL établie par l'utilisateur et utilisée pour augmenter le niveau de détection du spam. Les listes des adresses IP contenant des adresses qui se sont illustrées par le passé dans la diffusion de courrier indésirable et auxquelles Anti-Spam attribue un coefficient et un des états d'analyse des messages sont stockées sur les serveurs DNSBL.

F

Fichier clé

Le fichier au format xxxxxxxx.key qui permet d'utiliser une application de Kaspersky Lab selon les termes d'une licence d'évaluation ou commerciale. Le fichier clé est généré par l'application sur la base du code d'activation. Vous ne pouvez pas utiliser l'application sans fichier clé.

Filtrage de contenu

Filtrage des messages électroniques selon la taille du message, des masques des noms de pièce jointe et des formats des fichiers joints. Les résultats du filtrage du contenu permettent de limiter le transfert des messages au serveur de messagerie.

Filtrage de la réputation

Service dans le nuage qui utilise la technologie de définition de la réputation des messages. Les informations relatives à l'apparition des nouveaux types de spam sont plus vite disponibles dans le nuage que dans les bases du module Anti-Spam, ce qui permet d'accélérer la détection des éléments de courrier indésirable dans les messages et d'améliorer la précision de cette détection.

I

Interruption SNMP

Notification relative aux événements survenus pendant le fonctionnement de l'application et envoyées par l'agent SNMP.

K

Kaspersky Anti Targeted Attack Platform

Solution destinée à la protection de l'infrastructure informatique d'une organisation et la détection opportune de menaces telles que *les attaques "0jour"*, *les attaques ciblées* et les attaques ciblées complexes *advanced persistent threats* (ci-après *"APT"*).

Kaspersky Private Security Network

Il s'agit d'une solution qui permet aux utilisateurs des logiciels antivirus de Kaspersky Lab d'accéder aux données de Kaspersky Security Network sans envoyer d'informations aux serveurs de Kaspersky Security Network de Kaspersky Lab.

Kaspersky Security Network (KSN)

Infrastructure de services dans le cloud qui donne accès à la base de données de Kaspersky Lab sur la réputation des fichiers, des ressources Internet et des applications. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky Lab face aux menaces, augmente l'efficacité de fonctionnement de certains modules de la protection et réduit la possibilité de faux positifs.

L

La Sauvegarde

Stockage spécial destiné à la conservation des copies de sauvegarde des objets. Les copies de sauvegarde sont créées avant la désinfection ou la suppression des objets infectés.

LDAP

Lightweight Directory Access Protocol est un protocole client-serveur léger permettant d'accéder à des services d'annuaire.

Liens malveillants

Adresses Internet qui mènent à des ressources malveillantes, à savoir des ressources utilisées pour propager des programmes malveillants.

M

Machine virtuelle

Système logiciel complètement isolé qui est capable d'imiter un système d'exploitation, une application ou un périphérique (par exemple, un ordinateur) via l'exécution d'un code indépendant de la machine ou d'un code machine du processeur.

N

Notification par courrier

Message électronique contenant une description d'un événement de l'application ou de l'analyse des messages et qui est envoyé par Kaspersky Secure Mail Gateway à des adresses électroniques définies.

P

Phishing

Type de fraude sur Internet dont le but est d'obtenir un accès non autorisé aux données confidentielles des utilisateurs.

S

Service d'annuaires

Suite logicielle qui rassemble au même endroit les informations sur les ressources réseau (les utilisateurs, par exemple), afin de centraliser leur gestion.

SURBL

Spam URI Realtime Blocklists. Liste de serveurs SURBL établie par l'utilisateur et utilisée pour augmenter le niveau de détection du spam. Les listes des adresses Internet contenant des adresses qui ont été repérées par le passé dans l'objet ou le corps de messages identifiés comme indésirables et auxquelles Anti-Spam attribue un coefficient et un des états d'analyse des messages sont stockées sur les serveurs SURBL.

V

Vulnérabilité "0jour"

Vulnérabilité au sein d'une application détectée par des individus malintentionnés avant la diffusion d'une mise à jour contenant le correctif adéquat.

AO Kaspersky Lab

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection informatique contre diverses menaces dont les virus et autres programmes malveillants, 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 de sécurité informatique pour les utilisateurs finaux (classement " IDC Worldwide Endpoint Security Revenue by Vendor "). D'après les données d'IDC, Kaspersky Lab est l'éditeur préféré de systèmes de protection informatique pour particuliers en Russie ("IDC Endpoint Tracker 2014").

Kaspersky Lab a vu le jour en Russie en 1997. Kaspersky Lab est devenu un groupe international qui compte 38 bureaux dans 33 pays. 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 comprend des applications qui assurent la protection de l'information sur les ordinateurs de bureau et les ordinateurs portables, ainsi que sur les tablettes, les smartphones et autres périphériques nomades.

La société offre des solutions et des technologies de protection et de contrôle des postes de travail, des périphériques mobiles, des machines virtuelles, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. Elle propose également des produits spécialisés dans la protection contre les attaques DDoS, la protection des équipements gérés par l'automatisation industrielle et la prévention des escroqueries financières. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace et automatisée de toute 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 24 h/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 les signatures de ces menaces 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 dès lors pas un hasard si le noyau logiciel de Kaspersky Anti-Virus a été adopté par de nombreux autres éditeurs de logiciels comme : Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, H3C, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu ou 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 remporté des centaines de récompenses. Ainsi, Kaspersky Lab est devenue en 2014 une des deux sociétés détenant le plus de certificats Advanced+ à l'issue de tests réalisés par le laboratoire antivirus autrichien AV-Comparatives. Ces performances ont valu le certificat Top Rated à Kaspersky Lab. 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 officiel de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie de virus :	https://securelist.fr/
Laboratoire d'étude des virus :	https://virusdesk.kaspersky.fr/ (pour l'analyse de fichiers et de sites Internet suspects)
Forum de Kaspersky Lab :	http://forum.kaspersky.fr

Information sur le code tiers

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

Avis de marque déposée

Les marques déposées et les marques de services appartiennent à leurs propriétaires respectifs.

Apache et le logo de la plume Apache sont des marques de commerce de Apache Software Foundation.

Google Chrome est une marque de Google, Inc.

Linux est une marque de Linus Torvalds déposée aux Etats-Unis et dans autres pays.

Active Directory, Hyper-V, Microsoft, Internet Explorer et Windows sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

Mozilla et Firefox sont des marques de Mozilla Foundation.

CentOS est une marque déposée de la compagnie Red Hat, Inc.

Red Hat est une marque de Red Hat Inc. déposée aux Etats-Unis et dans autres pays.

Debian est une marque déposée par Software in the Public Interest, Inc.

VMware, VMware ESXi et VMware vSphere sont des marques de VMware, Inc. qui peuvent être déposées aux Etats-Unis ou dans d'autres juridictions.

Index

A

C

D

F

I

J

K

L

M

N

P

R

S

T

V