ESET MAIL SECURITY

POUR MICROSOFT EXCHANGE SERVER

Manuel d'installation et guide de l'utilisateur

Microsoft® Windows® Server 2000 / 2003 / 2008 / 2008 R2 / 2012 / 2012 R2

Cliquez ici pour télécharger la dernière version de ce document.

ESET **MAIL SECURITY**

Service client : www.eset.com/support

RÉV. 5/2/2014

Table des

1. Introduction

ESET Mail Security 4 pour Microsoft Exchange Server est une solution intégrée qui protège les boîtes aux lettres de différents types de contenu malveillant, y compris les pièces jointes infectées par des vers ou des chevaux de Troie, les documents contenant des scripts malveillants, le hameçonnage et le courrier indésirable. ESET Mail Security fournit trois types de protection : antivirus, antispam et application de règles définies par l'utilisateur. ESET Mail Security filtre le contenu malveillant au niveau du serveur de messagerie, avant qu'il arrive dans la boîte de réception du destinataire, sur le client.

ESET Mail Security prend en charge Microsoft Exchange Server versions 2000 et ultérieures, ainsi que Microsoft Exchange Server dans un environnement en cluster. Dans les versions récentes (Microsoft Exchange Server 2007 et versions ultérieures), les rôles spécifiques (mailbox, hub, edge) sont également pris en charge. Vous pouvez gérer ESET Mail Security à distance dans des réseaux de grande taille grâce à ESET Remote Administrator.

ESET Mail Security fournit non seulement la protection de Microsoft Exchange Server, mais également tous les outils nécessaires à la protection du serveur proprement dit (protection résidente, protection de l'accès à Internet, protection du client de messagerie et protection antispam).

1.1 Nouveautés de la version 4,5

Par rapport à ESET Mail Security version 4,3, les nouveautés et améliorations suivantes ont été ajoutées à la version 4,5 :

- Paramètres antispam : facilement accessibles depuis l'interface graphique utilisateur afin de simplifier les modifications effectuées par les administrateurs
- Prise en charge de Microsoft Exchange Server 2013
- Prise en charge de Microsoft Windows Server 2012 / 2012 R2

1.2 Configuration système

Systèmes d'exploitation pris en charge :

- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003 (x86 et x64)
- Microsoft Windows Server 2008 (x86 et x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

Versions de Microsoft Exchange Server 2003 prises en charge :

- Microsoft Exchange Server 2000 SP1, SP2, SP3
- Microsoft Exchange Server 2003 SP1, SP2
- Microsoft Exchange Server 2007 SP1, SP2, SP3
- Microsoft Exchange Server 2010 SP1, SP2, SP3
- Microsoft Exchange Server 2013

La configuration matérielle dépend de la version du système d'exploitation et de celle de Microsoft Exchange Server. Il est recommandé de prendre connaissance de la documentation Microsoft Exchange Server pour plus d'informations sur la configuration matérielle.

1.3 Méthodes utilisées

Deux méthodes indépendantes sont utilisées pour analyser les messages :

Analyse de boîtes aux lettres via VSAPI 6
Filtrage de messages au niveau du serveur SMTP 6

1.3.1 Analyse de boîtes aux lettres via VSAPI

L'analyse de boîtes aux lettres est déclenchée et contrôlée par le serveur Microsoft Exchange. Les messages stockés dans la base de données du serveur Microsoft Exchange Server sont analysés en continu. En fonction de la version de Microsoft Exchange Server, de la version de l'interface VSAPI et des paramètres définis par l'utilisateur, l'analyse peut être déclenchée dans l'un des cas suivants :

- lorsque l'utilisateur accède à sa messagerie, dans un client de messagerie par exemple (les messages sont toujours analysés avec la dernière base des signatures de virus) ;
- en arrière-plan, lorsque l'utilisation du serveur Microsoft Exchange Server est faible ;
- de manière proactive (en fonction de l'algorithme interne de Microsoft Exchange Server).

L'interface VSAPI est utilisée pour l'analyse antivirus et la protection basée sur les règles.

1.3.2 Filtrage de messages au niveau du serveur SMTP

Le filtrage de messages au niveau du serveur SMTP est assuré par un plugin spécialisé. Dans Microsoft Exchange Server 2000 et 2003, ce plugin (*récepteur d'événements*) est enregistré sur le serveur SMTP dans le cadre des services IIS (Internet Information Services). Dans Microsoft Exchange Server 2007/2010, le plugin est enregistré en tant qu'agent de transport dans les rôles *Edge* ou *Hub* du serveur Microsoft Exchange.

Le filtrage au niveau du serveur SMTP effectué par un agent de transport offre une protection sous la forme de règles antivirus, antispam et définies par l'utilisateur. Contrairement au filtrage VSAPI, le filtrage au niveau du serveur SMTP est effectué avant l'arrivée des messages analysés dans la boîte aux lettres Microsoft Exchange Server.

1.4 Types de protection

Il existe trois types de protection :

1.4.1 Protection antivirus

La protection antivirus est l'une des fonctions de base d'ESET Mail Security. La protection antivirus vous prémunit des attaques contre le système en contrôlant les échanges de fichiers et de courrier, ainsi que les communications Internet. Si une menace comportant un code malveillant est détectée, le module Antivirus peut l'éliminer en la bloquant dans un premier temps, puis en nettoyant, en supprimant ou en mettant en quarantaine 95 l'objet infecté.

1.4.2 Protection antispam

La protection antispam intègre différentes technologies (RBL, DNSBL, empreintes digitales, vérification de la réputation, analyse de contenu, filtre bayésien, règles, création manuelle de liste blanche/noire, etc.) afin d'optimiser la détection des menaces par courrier électronique. Les résultats du moteur d'analyse antispam correspondent à la probabilité, exprimée sous forme de pourcentage (0 à 100) selon laquelle un message donné peut être un courrier indésirable.

Un autre composant du module de protection antispam est la technique d'inscription à la liste grise (par défaut, cette option est désactivée). La technique se fonde sur la spécification RFC 821 : le protocole SMTP étant considéré comme étant non fiable, chaque agent de transfert de message doit réessayer plusieurs fois de livrer un message électronique en cas de défaillance temporaire de livraison. Une partie importante de courrier indésirable est livrée une seule fois (à l'aide d'outils spécialisés) à une liste importante d'adresses électroniques générée automatiquement. Un serveur qui utilise la liste grise calcule une valeur de contrôle (hachage) pour l'adresse de l'expéditeur, l'adresse du destinataire et l'adresse IP de l'agent de transfert de message chargé de l'envoi. Si le serveur ne parvient pas à détecter la valeur de contrôle du triplet dans sa base de données, il refuse le message et

renvoie un code de défaillance temporaire (par exemple 451). Un serveur légitime essaie de renvoyer le message après une période définie qui peut être variable. La valeur de contrôle triplet est stockée dans la base de données des connexions vérifiées lors de la deuxième tentative, ce qui permet ensuite de transférer correctement tout autre message ayant les mêmes caractéristiques.

1.4.3 Application des règles définies par l'utilisateur

La protection basée sur les règles définies par l'utilisateur permet d'effectuer des analyses à l'aide de VSAPI et de l'agent de transport. L'interface utilisateur ESET Mail Security permet de créer différentes règles qui peuvent être combinées. Si une règle utilise plusieurs conditions, ces dernières sont liées à l'aide de l'opérateur logique AND. Par conséquent, la règle n'est exécutée que si toutes ses conditions sont remplies. Si plusieurs règles sont créées, l'opérateur logique OR est appliqué, ce qui signifie que le programme exécute la première règle dont les conditions sont remplies.

Dans la séquence d'analyse, la première technique utilisée est la mise en liste grise, si elle est activée. Les procédures suivantes utilisent toujours les techniques suivantes : protection basée sur des règles définies par l'utilisateur, suivie d'une analyse antivirus et enfin d'une analyse antispam.

1.5 Interface utilisateur

ESET Mail Security dispose d'une interface utilisateur graphique très intuitive. Elle permet d'accéder très facilement aux principales fonctions du programme.

Outre l'interface utilisateur principale, une **arborescence de configuration avancée** est accessible depuis tous les emplacements du programme par l'intermédiaire de la touche F5.

Lorsque vous appuyez sur la touche F5, la fenêtre de l'arborescence de configuration avancée apparaît et affiche la liste des fonctions du programme qui peuvent être configurées. Depuis cette fenêtre, vous pouvez configurer les paramètres et les options en fonction de vos besoins. L'arborescence est divisée en deux sections : **Protection du serveur** et **Protection de l'ordinateur**. La partie **Protection du serveur** contient des éléments relatifs aux paramètres ESET Mail Security et qui sont propres à la protection des serveurs Microsoft Exchange. La partie **Protection de l'ordinateur** contient les éléments configurables de la protection du serveur proprement dit.

2. Installation

Après l'achat d'ESET Mail Security, le programme d'installation peut être téléchargé à partir du site web d'ESET (www.eset.com) sous forme de package .msi.

Veuillez noter que vous devez exécuter le programme d'installation avec le compte **Administrateur intégré**. Aucun autre utilisateur, même membre du groupe Administrateurs, ne disposera de droits d'accès suffisants. Vous devez donc utiliser un compte Administrateur intégré dans la mesure où vous ne parviendrez à effectuer l'installation avec aucun autre compte que **Administrateur**.

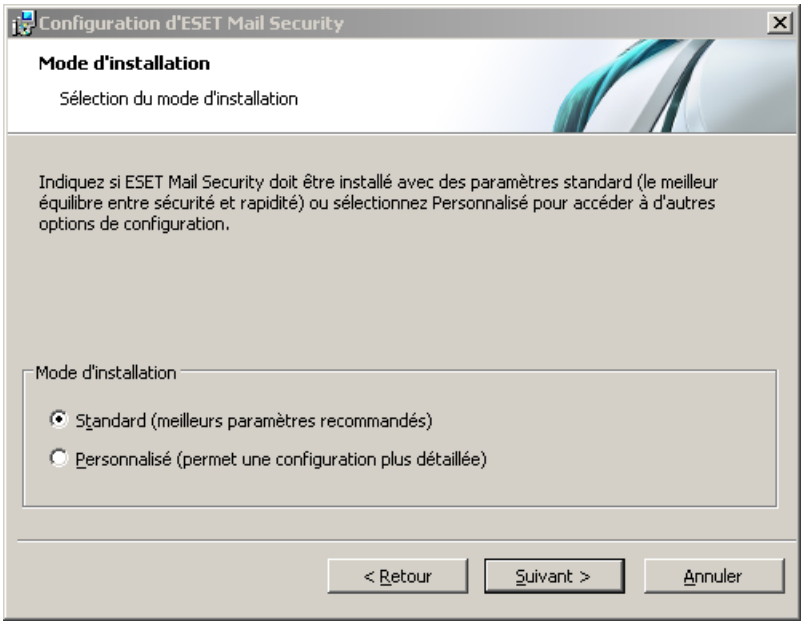
Il est possible d'exécuter le programme d'installation de deux façons :

- Vous pouvez vous connecter localement à l'aide des informations d'identification du compte Administrateur et simplement exécuter le programme d'installation
- Vous pouvez être connecté avec un autre compte d'utilisateur, mais vous devez ouvrir l'invite de commande avec **Exécuter en tant que...** et taper les informations d'identification du compte Administrateur pour que cmd s'exécute en tant qu'Administrateur, puis taper la command pour exécuter le programme d'installation (ex. `msiexec /i emsx_nt64_ENU.msi` mais vous devez remplacer `emsx_nt64_ENU.msi` par le nom de fichier précis du programme d'installation msi que vous avez téléchargé)

Lancez le programme d'installation ; l'assistant d'installation vous guide dans les opérations de configuration de base. Deux types d'installation sont disponibles, avec différents niveaux de détails de configuration :

1. **Installation standard**

2. **Installation personnalisée**



REMARQUE : Il est fortement recommandé, dans la mesure du possible, d'installer ESET Mail Security sur un système d'exploitation récemment installé et configuré. Toutefois, si vous n'avez pas besoin de l'installer sur un système existant, la meilleure solution consiste à désinstaller la version antérieure de ESET Mail Security, de redémarrer le serveur et d'installer ensuite la nouvelle version de ESET Mail Security.

2.1 Installation standard

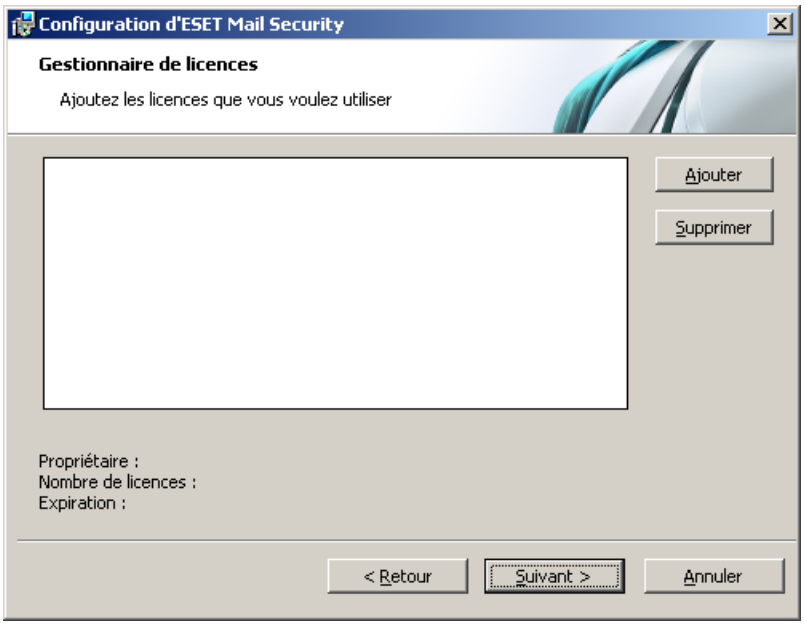
Le mode d'installation standard installe rapidement ESET Mail Security avec la configuration minimale pendant l'installation. L'installation standard est le mode d'installation par défaut ; elle est recommandée si vous n'avez pas encore d'exigence particulière pour certains paramètres. Après l'installation d'ESET Mail Security sur le système, vous pouvez modifier les options et les paramètres de configuration à tout moment. Ce guide de l'utilisateur décrit les paramètres et les fonctionnalités en détail. Le mode d'installation standard offre un excellent système de sécurité très facile à utiliser et des performances système très élevées.

Après avoir sélectionné le mode d'installation et cliqué sur Suivant, vous êtes invité à entrer votre nom d'utilisateur et votre mot de passe. Ces informations jouent un rôle très important dans la protection permanente de votre système, car le nom d'utilisateur et le mot de passe permettent les mises à jour 83 automatiques de la base des

signatures de virus.

Saisissez dans les champs correspondants le nom d'utilisateur et le mot de passe que vous avez reçus après l'achat ou l'enregistrement de votre produit. Si votre nom d'utilisateur et votre mot de passe ne sont pas disponibles, vous pouvez les indiquer ultérieurement directement dans le programme.

Dans la prochaine étape, **Gestionnaire de licences**, ajoutez le fichier de licence fourni par courrier électronique après l'achat de votre produit.



La dernière étape consiste à configurer le système d'alerte anticipé ThreatSense.Net. Le système d'avertissement anticipé ThreatSense.Net contribue à garantir qu'ESET est immédiatement et continuellement informé des nouvelles infiltrations dans le but de protéger ses clients. Le système permet de soumettre les nouvelles menaces au laboratoire de recherche sur les menaces d'ESET, où elles sont analysées, traitées puis ajoutées à la base des signatures de virus. Par défaut, l'option **Activer le système d'alerte anticipé ThreatSense.Net** est sélectionnée. Cliquez sur **Configuration avancée...** pour modifier les paramètres détaillés de soumission de fichiers suspects.

L'étape suivante de l'installation consiste à configurer la **Détection des applications potentiellement indésirables** . Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Reportez-vous au chapitre Applications potentiellement indésirables 139 pour plus d'informations.

Ces applications sont souvent associées à d'autres programmes et peuvent être difficiles à remarquer lors de l'installation. Ces applications affichent habituellement une notification pendant l'installation, mais elles peuvent facilement s'installer sans votre consentement.

Sélectionnez l'optio **Activer la détection des applications potentiellement indésirables** pour autoriser ESET Mail Security à détecter ce type d'applications. Si vous ne souhaitez pas utiliser cette fonctionnalité, sélectionnez l'option **Désaciver la détection des applications potentiellement indésirables.**

La dernière étape de l'installation standard consiste à confirmer l'installation en cliquant sur le bouton **Installer**.

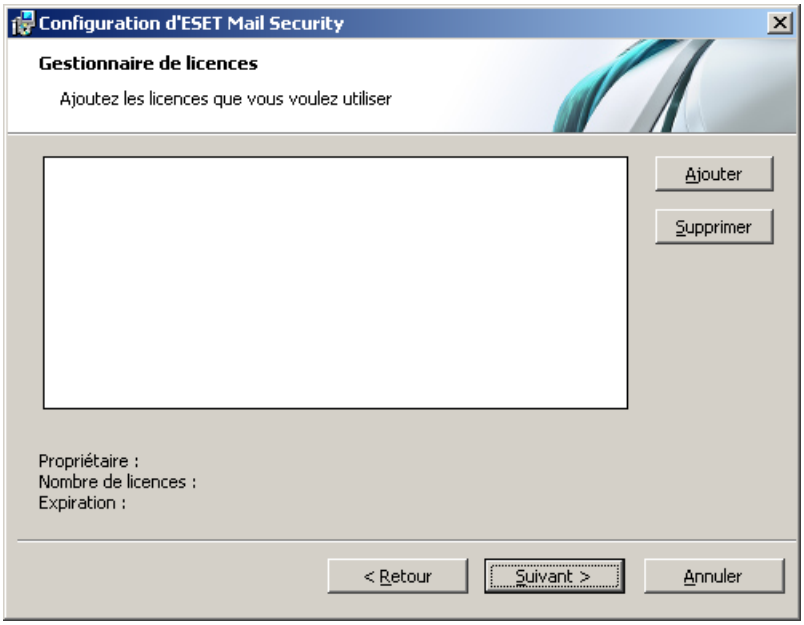
2.2 Installation personnalisée

L'installation personnalisée est destinée aux utilisateurs qui souhaitent configurer ESET Mail Security pendant l'installation.

Après avoir sélectionné le mode d'installation et cliqué sur **Suivant**, vous êtes invité à sélectionner un emplacement de destination pour l'installation. Par défaut, le programme s'installe dans le dossier *C:\Program Files\ESET\ESET Mail Security*. Cliquez sur **Parcourir...** pour changer d'emplacement (non recommandé).

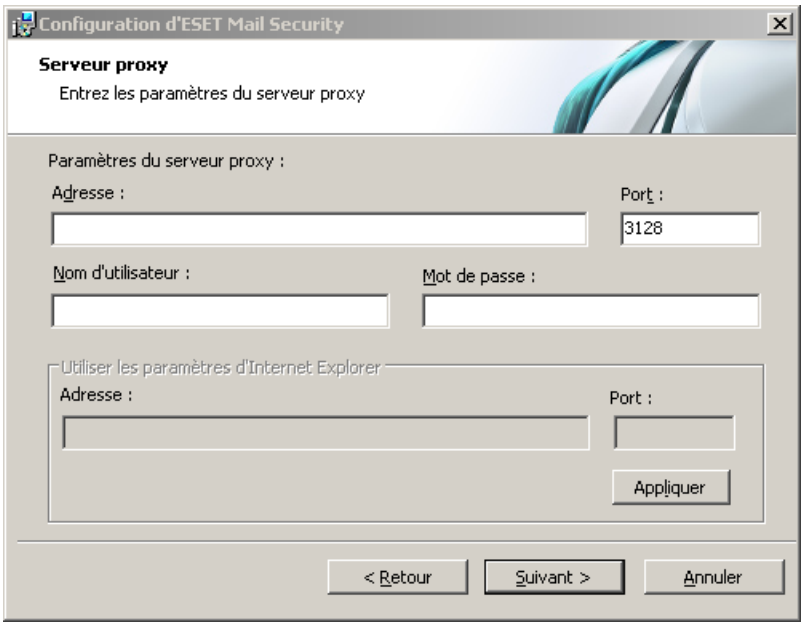
Entrez ensuite votre **nom d'utilisateur** et votre **mot de passe**. Cette étape est la même que dans l'installation standard (reportez-vous à Installation standard 8).

Dans la prochaine étape **Gestionnaire de licences**, ajoutez le fichier de licence fourni par courrier électronique après l'achat de votre produit.



Après avoir entré le nom d'utilisateur et le mot de passe, cliquez sur **Suivant** pour passer à l'étape **Configurez votre connexion Internet**.

Si vous utilisez un serveur proxy, ce dernier doit être configuré correctement pour que les mises à jour des signatures de virus fonctionnement correctement. Si vous souhaitez utiliser un serveur proxy configuré automatiquement, sélectionnez le paramètre par défaut **Je ne sais pas si ma connexion Internet utilise un serveur proxy. Utiliser les mêmes paramètres qu'Internet Explorer (Recommandé)** et cliquez sur **Suivant**. Si vous n'utilisez pas de serveur proxy, sélectionnez l'option **Je n'utilisse pas de serveur proxy**.

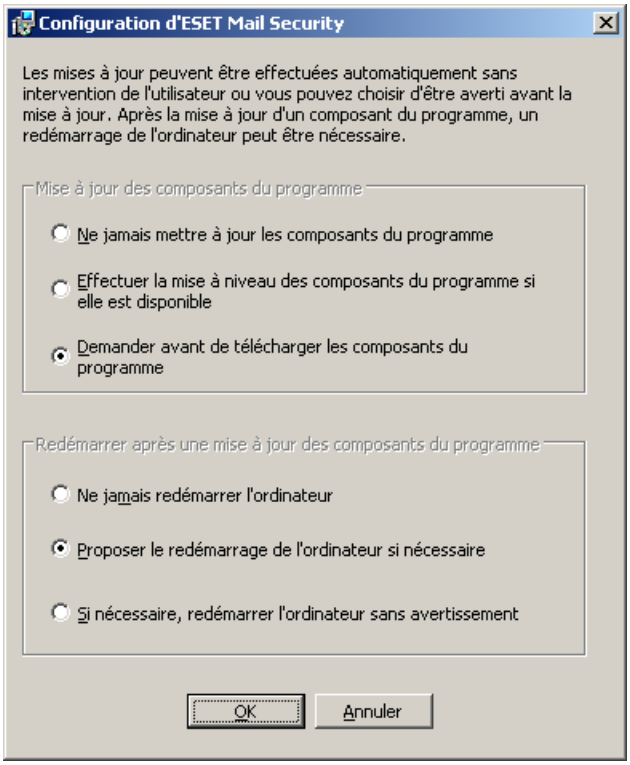


Si vous préférez indiquer les informations détaillées du serveur proxy par vous-même, vous pouvez configurer les paramètres du serveur proxy manuellement. Pour configurer les paramètres du serveur proxy, sélectionnez l'option **J'utilise un serveur proxy** et cliquez sur **Suivant**. Entrez l'adresse IP ou l'adresse URL de votre serveur proxy dans le champ **Adresse**. Dans le champ **Port**, spécifiez le port sur lequel le serveur proxy accepte les connexions (3128 par défaut). Si le serveur proxy exige une authentification, saisissez un **nom d'utilisateur** et un **mot de passe** pour accorder l'accès au serveur proxy. Les paramètres du serveur proxy peuvent être copiés depuis Internet Explorer. Une fois les détails du serveur proxy entrés, cliquez sur **Appliquer** et confirmez la sélection.

Cliquez sur **Suivant** pour passer à l'étape **Configurez les paramètres de mise à jour automatique**. Cette étape permet d'indiquer la façon dont les mises à jour des composants programme sont gérées sur le système. Cliquez sur **Changer...** pour accéder aux paramètres avancés.

Si vous ne voulez pas que les composants du programme soient mis à jour, sélectionnez l'option **Ne jamais mettre à jour les composants du programme**. L'option **Demander avant de télécharger les composants du programme** affiche une fenêtre de confirmation avant le téléchargement des composants du programme. Pour

télécharger les mises à niveau des composants du programme, sélectionnez l'option **Toujours mettre à jour les composants du programme**.



REMARQUE : le redémarrage du système est généralement nécessaire après la mise à jour des composants du programme. Il est recommandé de sélectionner l'option **Ne jamais redémarrer**. Les dernières mises à jour des composants entrent en vigueur au redémarrage suivant du serveur (qu'il soit planifié 93, manuel ou autre). Vous pouvez sélectionner l'option **Proposer de redémarrer si nécessaire** si vous souhaitez que le système vous rappelle de redémarrer le serveur après la mise à jour des composants. Avec ce paramètre, vous pouvez redémarrer le serveur immédiatement ou ultérieurement.

La fenêtre suivante de l'installation permet d'indiquer un mot de passe afin de protéger les paramètres du programme. Sélectionnez l'option **Protéger les paramètres de configuration par mot de passe** et choisissez un mot de passe à indiquer dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**.

Les deux étapes d'installation suivantes, **Activer le système d'alerte anticipé ThreatSense.Net et Détection des applications potentiellement indésirables** sont identiques aux étapes de l'installation standard (reportez-vous à « Installation standard » 8).

Cliquez sur **Installer** dans la fenêtre **Prêt à installer** pour terminer l'installation.

2.3 Terminal Server

Si vous avez installé ESET Mail Security sur un serveur Windows agissant comme Terminal Server, vous souhaiterez peut-être désactiver l'interface utilisateur graphique ESET Mail Security afin d'empêcher son démarrage à chaque connexion de l'utilisateur. Reportez-vous au chapitre Désactivation de l'interface utilisateur graphique sur Terminal Server 123 pour accéder aux étapes de désactivation.

2.4 Mise à niveau vers une version plus récente

Les nouvelles versions d'ESET Mail Security offrent des améliorations ou apportent des solutions aux problèmes que les mises à jour automatiques des modules ne pouvaient pas résoudre. Vous pouvez effectuer une mise à niveau vers la dernière version d'ESET Mail Security à l'aide des méthodes suivantes :

1. Mise à niveau automatique par l'intermédiaire d'une mise à jour des composants du programme
   Dans la mesure où les mises à jour des composants du programme sont distribuées à tous les utilisateurs et peuvent avoir un impact sur certaines configurations système, elles sont mises à disposition après de longues périodes de test afin que la mise à niveau s'effectue sans difficulté sur toutes les configurations système.
2. La mise à jour peut s'effectuer manuellement, par exemple si vous devez effectuer une mise à niveau vers une nouvelle version immédiatement après sa mise à disposition, ou vers la nouvelle génération d'ESET Mail Security (par exemple de la version 4.2 ou 4.3 à la version 4.5).

Vous pouvez effectuer une mise à niveau manuelle vers une nouvelle version de deux manières : par écrasement (la version la plus récente est installée sur la version existante) ou au moyen d'une installation propre (la version antérieure est d'abord désinstallée, puis la version la plus récente est installée).

Pour effectuer une mise à niveau manuelle :

1. Mise à niveau par écrasement : Installez la version la plus récente par-dessus la version existante d'ESET Mail Security, en suivant les étapes mentionnées à la section Installation 8. Tous les paramètres existants (y compris les paramètres de protection antispam) seront automatiquement importés dans la nouvelle version au cours de l'installation.

2. Installation propre :

   a) Exportez les paramètres/la configuration dans un fichier xml à l'aide de la fonction Importer et exporter les paramètres 130.

   b) Ouvrez ce fichier xml dans un éditeur xml dédié ou dans un éditeur de texte prenant en charge le format xml (par ex. : WordPad, Nodepad++, etc.), puis modifiez la valeur de la troisième ligne SECTION ID en « 1000404 » afin que cette ligne apparaisse ainsi :

   ```
   <SECTION ID="1000404">
   ```

   c) Téléchargez l'outil EMSX AntispamSettingsExport depuis cet article de la base de connaissances. Enregistrez `EMSX_AntispamSettingsExport.exe` sur le serveur Exchange que vous mettez à niveau vers la dernière version d'ESET Mail Security.

   d) Exécutez l'outil `EMSX_AntispamSettingsExport.exe` . Cet outil créera un fichier `cfg.xml` contenant les paramètres de protection antispam provenant de votre installation actuelle d'ESET Mail Security.

   e) Téléchargez le programme d'installation msi correspondant à la dernière version d'ESET Mail Security.

   f) Copiez le fichier `cfg.xml` créé par l'outil EMSX AntispamSettingsExport à l'emplacement où vous avez enregistré le programme d'installation msi d'ESET Mail Security (par ex. : `emsx_nt64_ENU.msi`).

   g) Désinstallez votre version actuelle d'ESET Mail Security.

   h) Exécutez le programme d'installation msi correspondant à ESET Mail Security 4.5. Les paramètres de protection antispam exportés vers `cfg.xml` seront automatiquement importés vers la nouvelle version.

   i) Une fois l'installation terminée, importez la configuration/les paramètres depuis le fichier xml que vous avez enregistré et modifié au cours des étapes a) et b) à l'aide de la fonction Paramètres d'importation et d'exportation 130 et d'un éditeur xml, afin de pouvoir utiliser les paramètres de votre configuration précédente dans la nouvelle version d'ESET Mail Security.

Une fois les opérations précédentes effectuées, la nouvelle version d'ESET Mail Security est installée sur votre système avec votre configuration personnalisée antérieure.

Pour plus de détails concernant le processus de mise à niveau, consultez cet article de la base de connaissances.

REMARQUE : Les deux processus de mise à niveau manuelle (par écrasement et installation propre) s'appliquent uniquement à la mise à niveau d'ESET Mail Security version 4.2 ou 4.3 vers ESET Mail Security version 4.5.

2.5 Rôles Exchange Server - Comparaison entre Edge et Hub

Par défaut, les fonctionnalités antispam sont activées sur les serveurs de transport Edge et désactivées sur les serveurs de transport Hub. Dans une organisation Exchange avec serveur de transport Edge, cette configuration est à privilégier. Il est recommandé que le serveur de transport Edge exécute le filtrage antispam ESET Mail Security sur les messages avant leur transmission dans l'organisation Exchange.

Le rôle Edge reste toutefois l'emplacement privilégié de l'analyse antispam, car il permet à ESET Mail Security de rejeter les courriers indésirables dans les premières phases du processus sans charger inutilement les couches réseau. Dans cette configuration, les messages entrants sont filtrés par ESET Mail Security sur le serveur de transport Edge, afin qu'ils puissent être envoyés en toute sécurité au serveur de transport Hub sans nécessiter de filtrage supplémentaire.

Si votre organisation n'utilise pas de serveur de transport Edge et ne dispose que d'un serveur de transport Hub, il est recommandé d'activer les fonctionnalités antispam de ce dernier qui reçoit via SMTP les messages entrants provenant d'Internet.

2.6 Rôles Exchange Server 2013

L'architecture d'Exchange Server 2013 est différente de celle des versions précédentes de Microsoft Exchange. Exchange 2013 ne propose que deux rôles de serveur : serveur d'accès client et serveur de messagerie. Si vous comptez protéger Microsoft Exchange 2013 avec ESET Mail Security, veillez à installer ESET Mail Security sur un système exécutant Microsoft Exchange 2013 avec le rôle de serveur de messagerie. Le rôle de serveur d'accès client n'est pas pris en charge par ESET Mail Security.

Il y a une exception si vous envisagez d'installer ESET Mail Security sur Windows SBS (Small Business Server). Sous Windows SBS, tous les rôles Exchange s'exécutent sur le même serveur ; par conséquent, ESET Mail Security s'exécute correctement et fournit tous les types de protection, y compris ceux du serveur de messagerie.

Toutefois, si vous installez ESET Mail Security sur un système exploité dans un rôle de serveur d'accès client uniquement (serveur CAS dédié), les fonctionnalités les plus importantes de ESET Mail Security ne sont pas opérationnelles, en particulier celles du serveur de messagerie. Dans ce cas, la protection du système de fichiers en temps réel et certains composants appartenant à la protection de l'ordinateur 61 sont les seuls composants à fonctionner, si bien qu'il n'y a aucune protection du serveur de messagerie. C'est la raison pour laquelle il n'est pas recommandé d'installer ESET Mail Security sur un serveur avec rôle de serveur d'accès client. Comme indiqué ci-dessus, cela ne s'applique pas à Windows SBS (Small Business Server).

REMARQUE: En raison de certaines restrictions techniques de Microsoft Exchange 2013, ESET Mail Security ne prend pas en charge le rôle de serveur d'accès client (CAS).

2.7 Installation dans un environnement à cluster

Un cluster est un groupe de serveurs (un serveur connecté à un cluster s'appelle « nœud ») qui fonctionnent ensemble comme s'il s'agissait d'un seul serveur. Ce type d'environnement rend les services disponibles extrêmement accessibles et fiables. Si l'un des nœuds du cluster est défaillant ou inaccessible, sa fonction est automatiquement prise en charge par un autre nœud du cluster. ESET Mail Security prend entièrement en charge les serveurs Microsoft Exchange Server connectés en cluster. Pour que ESET Mail Security fonctionne correctement, il est important que chaque nœud d'un cluster contienne la même configuration. Il suffit pour ce faire d'appliquer une stratégie à l'aide d'ESET Remote Administrator (ERA). Dans les chapitres suivants, nous allons indiquer comment installer et configurer ESET Mail Security sur les serveurs d'un environnement à cluster à l'aide d'ESET Remote Administrator.

Installation

Ce chapitre présente la méthode d'installation poussée. Toutefois, l'installation d'un produit sur l'ordinateur cible peut être effectuée à l'aide d'autres méthodes. Pour obtenir des informations sur les autres méthodes d'installation, reportez-vous au Guide d'utilisation d'ESET Remote Administrator.

1) Téléchargez le package d'installation ESET Mail Security *msi* depuis le site Internet d'ESET sur l'ordinateur où est installé ESET Remote Administrator Server. Dans ESET Remote Administrator Server, dans l'onglet **Installation à distance**, sélectionnez **Ordinateurs**, cliquez avec le bouton droit sur un ordinateur de la liste et choisissez **Gérer les**

packages dans le menu contextuel. Dans le menu déroulant **Type**, sélectionnez **Package Produits de sécurité ESET** et cliquez sur **Ajouter...** Dans la zone **Source**, localisez le package d'installation ESET Mail Security et cliquez sur **Créer**.

2) Dans **Modifier/Sélectionner la configuration associée à ce package**, cliquez sur **Modifier** et configurez les paramètres **ESET Mail Security** en fonction de vos besoins. Les paramètres ESET Mail Security se trouvent dans les branches suivantes : **ESET Smart Security, ESET NOD32 Antivirus > Protection du serveur de messagerie** et **Protection du serveur de messagerie pour Microsoft Exchange Server**. Vous pouvez également définir les paramètres d'autres modules inclus dans ESET Mail Security (module de mise à jour, analyse d'ordinateur, etc.). Il est recommandé d'exporter les paramètres configurés dans un fichier xml que vous pouvez utiliser ultérieurement, lors de la création d'un package d'installation, de l'application d'une tâche de configuration ou d'une stratégie.

3) Cliquez sur **Fermer**. Dans la boîte de dialogue suivante (**Voulez-vous enregistrer les packages sur le serveur ?**), sélectionnez **Oui** et saisissez le nom du package d'installation. Le package d'installation terminé (y compris le nom et la configuration) est enregistré sur le serveur. Généralement, ce package est utilisé pour une installation poussée, mais vous pouvez également l'enregistrer en tant que package d'installation *msi* standard et l'utiliser pour effectuer une installation directe sur le serveur (dans **Éditeur de packages d'installation** > **Enregistrer sous...**).

4) Maintenant que le package d'installation est prêt, vous pouvez démarrer l'installation à distance sur les nœuds d'un cluster. Dans ESET Remote Administrator Server, dans l'onglet **Installation à distance** > **Ordinateurs**, sélectionnez les nœuds sur lesquels vous souhaitez installer ESET Mail Security (Ctrl + clic gauche ou Maj + clic gauche). Cliquez avec le bouton droit sur l'un des ordinateurs sélectionnés et sélectionnez **Installation poussée** dans le menu contextuel. À l'aide des boutons **Définir**/**Définir tout**, définissez le **nom d'utilisateur** et le **mot de passe** d'un utilisateur de l'ordinateur cible (il doit s'agir d'un utilisateur avec des droits d'administrateur). Cliquez sur **Suivant** pour sélectionner le package d'installation et démarrez l'installation à distance en cliquant sur **Terminer**. Le package d'installation contenant ESET Mail Security et les paramètres de configuration personnalisés sont installés sur les ordinateurs/nœuds cibles sélectionnés. Après un bref instant, les clients disposant de ESET Mail Security apparaissent dans ESET Remote Administrator Server, dans l'onglet **Clients**. Vous pouvez maintenant gérer les clients à distance.

REMARQUE : pour que l'installation à distance s'effectue correctement, les ordinateurs cibles et le serveur ESET Remote Administrator Server doivent remplir certaines conditions. Pour plus de détails, reportez-vous au Guide d'utilisation d'ESET Remote Administrator.

Configuration

Pour que ESET Mail Security fonctionne correctement sur les nœuds d'un cluster, les nœuds doivent en permanence avoir la même configuration. Cette condition est remplie si vous avez suivi la méthode d'installation poussée ci-dessus. Il est néanmoins possible que la configuration soit modifiée par erreur, ce qui provoquerait des incohérences entre les produits ESET Mail Security d'un cluster. Vous pouvez éviter ce risque en utilisant une stratégie dans ESET Remote Administrator Server. Une stratégie est très semblable à une tâche de configuration standard : elle envoie aux clients la configuration définie dans l'éditeur de configuration. Elle diffère de la tâche de configuration, car elle est appliquée aux clients en permanence. Elle peut donc se définir comme une configuration appliquée régulièrement à un client ou à un groupe de clients.

Dans ESET Remote Administrator Server > **Outils** > **Gestionnaire de stratégies...**, un certain nombre d'options permettent d'utiliser une stratégie. Le plus simple consiste à utiliser l'option **Stratégie parent par défaut** ; elle sert également de **stratégie par défaut pour les clients principaux**. Ce type de stratégie est appliquée automatiquement à tous les clients connectés (dans ce cas, à tous les produits ESET Mail Security d'un cluster). Vous pouvez configurer la stratégie en cliquant sur **Modifier...** ou utiliser la configuration existante enregistrée dans le fichier *xml*, si vous en avez déjà créé un.

La deuxième possibilité consiste à créer une stratégie (**Ajouter une nouvelle stratégie enfant**) et à utiliser l'option **Ajouter des clients...** pour attribuer tous les produits ESET Mail Security à cette stratégie.

Cette configuration garantit qu'une même stratégie avec les mêmes paramètres est appliquée à tous les clients. Si vous souhaitez modifier les paramètres existants d'un serveur ESET Mail Security de cluster, il suffit de modifier la stratégie actuelle. Les modifications sont appliquées à tous les clients attribués à cette stratégie.

REMARQUE : reportez-vous au Guide d'utilisation d'ESET Remote Administrator pour plus d'informations sur les stratégies.

2.8 Licence

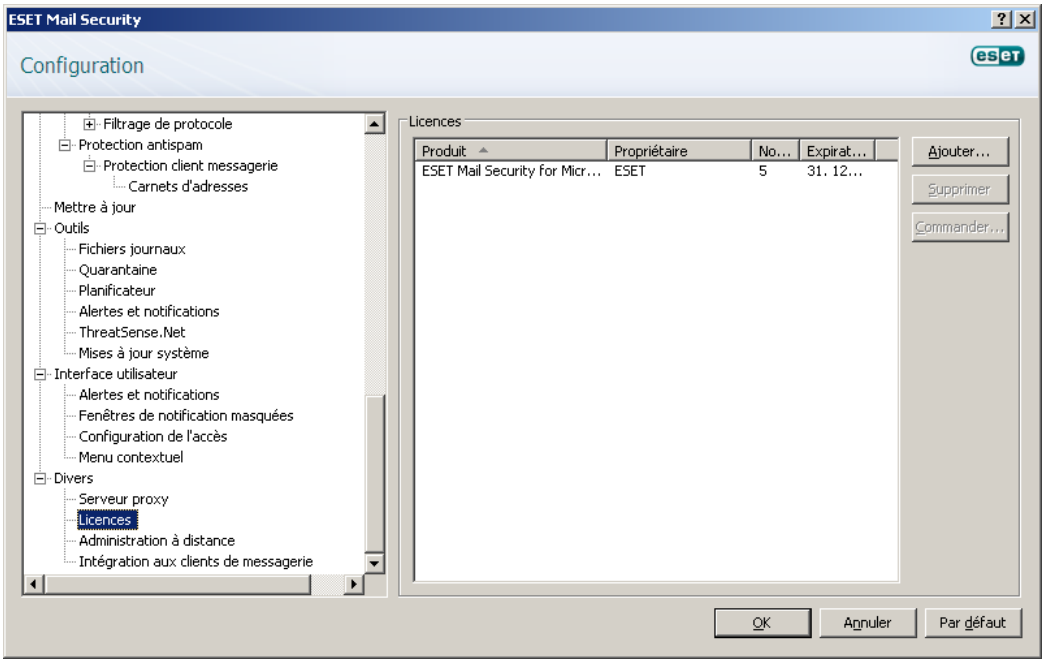
L'utilisateur du fichier de licence ESET Mail Security pour Microsoft Exchange Server est une étape très importante. Sans ce fichier de licence, la protection de la messagerie sur Microsoft Exchange Server ne fonctionne pas correctement. Si vous n'ajoutez pas le fichier de licence pendant l'installation, vous pouvez le faire ultérieurement dans les paramètres avancés, dans **Divers > Licences**.

ESET Mail Security vous permet d'utiliser plusieurs licences simultanément en les fusionnant comme l'indique la section ci-dessous.

1) Plusieurs licences d'un client (les licences attribuées au même nom de client) sont fusionnées et le nombre de boîtes aux lettres analysées augmente en conséquence. Le gestionnaire de licences continue à afficher les différentes licences.

2) Plusieurs licences de différents clients sont fusionnées. La fusion s'effectue de la même manière que dans le premier scénario (point 1 ci-dessus), à la différence près qu'une des licences en question au moins doit avoir un attribut particulier. Cet attribut est nécessaire à la fusion des licences de différents clients. Si cette licence vous intéresse, adressez-vous à votre distributeur local pour qu'il génère une licence de ce type.

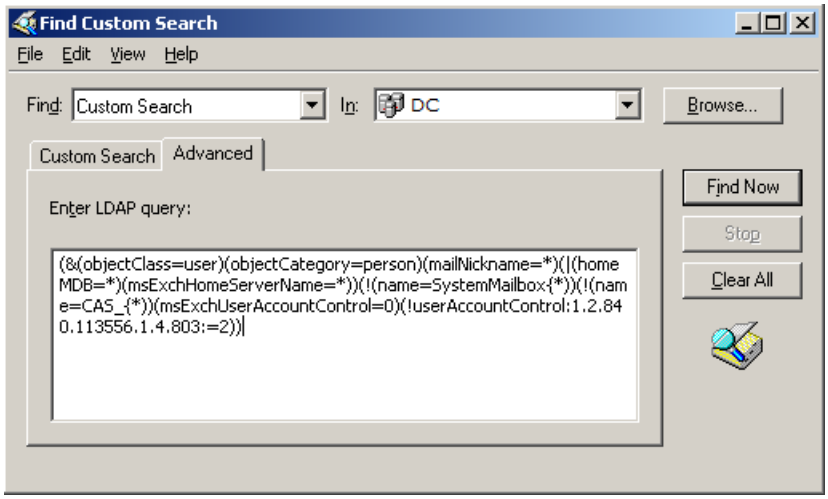
REMARQUE : la période de validité de la nouvelle licence créée est déterminée par la date d'expiration la plus proche de l'un de ses constituants.



ESET Mail Security pour Microsoft Exchange Server (EMSX) compare le nombre de boîtes aux lettres du répertoire actif à votre compte de licence. Chaque répertoire actif du serveur Exchange est vérifié afin de déterminer le nombre total de boîtes aux lettres. Les boîtes aux lettres système et désactivées, ainsi que les alias de messagerie ne sont pas comptabilisées dans le nombre de boîtes aux lettres. Dans un environnement à cluster, les nœuds avec rôle de boîte aux lettres de cluster ne sont pas comptabilisés dans le nombre de boîtes aux lettres.

Pour déterminer le nombre de boîtes aux lettres Exchange que vous avez, ouvrez **Utilisateurs et ordinateurs Active Directory** sur le serveur. Cliquez avec le bouton droit sur le domaine et cliquez sur **Rechercher...** Dans le menu déroulant **Rechercher**, sélectionnez **Recherche personnalisée** et cliquez sur l'onglet **Avancé**. Collez la requête LDAP (Lightweight Directory Access Protocol) suivante et cliquez sur **Rechercher** :

- `(&(objectClass=user)(objectCategory=person)(mailNickname=*)(|(homeMDB=*)(msExchHomeServerName=*))(!(name=SystemMailbox{*))(!(name=CAS_{*))(msExchUserAccountControl=0)(!userAccountControl:1.2.840.113556.1.4.803:=2))`



Si le nombre de boîtes aux lettres de votre répertoire actif est supérieur à votre nombre de licences, le message suivant est entré dans le journal du serveur Microsoft Exchange Server : Protection status changed due to exceeded number of mailboxes (count) covered by your license (count) (État de la protection modifié en raison du nombre de boîtes aux lettres (nombre) supérieur au nombre pris en charge par votre licence (nombre)). ESET Mail Security vous informe également en définissant l'**état de la protection** sur orange et en affichant un message vous informant qu'il vous reste 42 jours avant la désactivation de votre protection. Si vous recevez cette notification, contactez votre représentant pour faire l'acquisition de licences supplémentaires.

Si la période de 42 jours est échue et que vous n'avez pas ajouté les licences nécessaires à la prise en charge des boîtes aux lettres supplémentaires, l'**étant de la protection** devient rouge. Le message vous informe que votre protection a été désactivée. Si vous recevez cette notification, contactez immédiatement votre représentant pour faire l'acquisition de licences supplémentaires.

2.9 Configuration après l'installation

Plusieurs options doivent être configurées après l'installation du produit.

Configuration de la protection antispam

Cette section décrit les paramètres, méthodes et techniques que vous pouvez utiliser pour protéger votre réseau du courrier indésirable. Il est recommandé de lire les instructions suivantes avec soin avant de sélectionner la combinaison de paramètres la plus adéquate pour votre réseau.

Gestion du courrier indésirable

Afin de garantir une protection antispam de grande précision, vous devez définir les actions à effectuer sur les messages qui sont déjà marqués comme courrier indésirable.

Trois options sont disponibles :

1. **Suppression du courrier indésirable**
   Les critères ESET Mail Security qui définissent le marquage des messages comme courrier indésirable sont relativement élevés, ce qui réduit le risque de supprimer des messages légitimes. Plus les paramètres antispam sont spécifiques, moins les messages légitimes sont susceptibles d'être supprimés. Cette méthode présente l'avantage de consommer très peu de ressources système et nécessite moins d'opérations de gestion. En revanche, elle ne permet pas de restaurer localement les messages légitimes qui sont supprimés.

2. **Quarantaine**
   Cette option exclut tout risque de suppression des messages légitimes. Les messages peuvent être restaurés et renvoyés aux destinataires d'origine immédiatement. Toutefois, cette méthode consomme de grandes quantités de ressources système et la maintenance de la quarantaine de messages prend du temps. Vous avez à disposition deux méthodes pour mettre les messages en quarantaine :

   A. Quarantaine Exchange Server interne (s'applique uniquement à Microsoft Exchange Server 2007/2010) :
   - Si vous souhaitez utiliser la quarantaine interne du serveur, vérifiez que le champ **Quarantaine commune des messages** dans le volet de droite du menu des paramètres avancés (dans **Protection du serveur** > **Mise en quarantaine des messages**) est vide. Vérifiez également que l'option **Mettre le message dans la quarantaine du système de serveur de messagerie** est sélectionnée dans le menu déroulant situé au bas de la fenêtre. Cette méthode ne fonctionne qu'en présence d'une quarantaine interne Exchange. Par défaut, cette quarantaine interne n'est pas activée dans Exchange. Si vous souhaitez l'activer, vous devez ouvrir l'environnement de ligne de commande Exchange Management Shell et entrer la commande suivante :

   Set-ContentFilterConfig -QuarantineMailbox nom@domaine.com

   (remplacez nom@domaine.com par le nom de la boîte aux lettres que Microsoft Exchange doit utiliser comme boîte aux lettres de quarantaine interne, par exemple quarantaineexchange@entreprise.com)

   B. Boîte aux lettres de quarantaine personnalisée :
   - Si vous avez saisi la boîte aux lettres souhaitée dans le champ **Quarantaine commune des messages** , ESET Mail Security déplace tous les nouveaux messages de courrier indésirable dans votre boîte aux lettres personnalisée.

   Pour plus de détails sur la quarantaine et les différentes méthodes, reportez-vous au chapitre Mise en quarantaine des messages 25.

3. **Transfert de courrier indésirable**

   Le courrier indésirable est transmis à son destinataire. Toutefois, ESET Mail Security complète l'en-tête MIME pertinent de chaque message avec la valeur SCL. En fonction de la valeur SCL, l'action appropriée est exécutée par le système de filtrage de messages intelligent (IMF) du serveur Exchange.

Filtrage du courrier indésirable

Mise en liste grise

La mise en liste grise est une méthode qui protège les utilisateurs du courrier indésirable à l'aide de la technique suivante : L'agent de transport envoie une valeur de retour SMTP indiquant un rejet temporaire (*temporarily reject*) (la valeur par défaut est 451/4.7.1) pour tout message provenant d'un expéditeur inconnu. Un serveur légitime essaie de remettre de nouveau le message. Les expéditeurs de courrier indésirable n'essaient généralement pas de remettre le message une nouvelle fois, car ils envoient des messages à des milliers d'adresses électroniques et ne perdent pas de temps à relancer des expéditions.

Lors de l'évaluation de la source du message, la méthode prend en compte les configurations des listes d'**adresses IP approuvées**, **ignorées**, **autorisées** et d'**expéditeurs sûrs** sur le serveur Exchange et les paramètres AntispamBypass de la boîte aux lettres du destinataire. La mise en liste grise doit être configurée intégralement ; dans le cas contraire, des dysfonctionnements (délais de remise des messages légitimes, etc.) risquent de se produire. Ces effets négatifs diminuent progressivement, car cette méthode ajoute les connexions fiables à la liste blanche interne. Si vous ne connaissez pas cette méthode ou considérez que ses conséquences négatives sont inacceptables, il est recommandé de désactiver la méthode dans le menu des paramètres avancés dans **Protection antispam** > **Microsoft Exchange Server** > **Agent de transport** > **Activer la mise en liste grise**.

Il est recommandé de désactiver la mise en liste grise si vous envisagez de tester les fonctionnalités de base du produit et ne souhaitez pas configurer les fonctionnalités avancées du programme.

REMARQUE : la mise en liste grise est une couche supplémentaire de protection antispam et n'a aucun effet sur les fonctionnalités d'évaluation du module de blocage de courrier indésirable.

Configuration de la protection antivirus

Quarantaine

Selon le mode de nettoyage utilisé, il est recommandé de configurer une action à réaliser sur les messages infectés (non nettoyés). Cette option peut être définie dans la fenêtre des paramètres avancés : **Protection du serveur** > **Antivirus et antispyware** > **Microsoft Exchange Server** > **Agent de transport**.

Si l'option de déplacement des messages dans la quarantaine des messages est activée, vous devez configurer la quarantaine dans **Protection du serveur** > **Mise en quarantaine des messages** dans la fenêtre des paramètres avancés.

Performances

Si vous n'avez pas d'autres restrictions, il est recommandé d'augmenter le nombre de moteurs d'analyse ThreatSense dans la fenêtre des paramètres avancés (F5), dans **Protection de l'ordinateur** > **Antivirus et antispyware** > **Performances**, en fonction de la formule suivante : *nombre de moteurs d'analyse ThreatSense = (nombre d'unités centrales physiques x 2) + 1*. Le *nombre de threads d'analyse* doit également être égal au *nombre des moteurs d'analyse ThreatSense*. Vous pouvez configurer le nombre de threads d'analyse dans **Protection du serveur** > **Antivirus et antispyware** > **Microsoft Exchange Server** > **VSAPI** > **Performances**. Voici un exemple :

Imaginons que votre serveur comporte 4 unités centrales physiques. D'après la formule ci-dessus, vous devriez avoir, pour optimiser les performances 9 threads d'analyse et 9 moteurs d'analyse.

REMARQUE : La valeur acceptable est comprise entre 1 et 20 ; en d'autres termes, le nombre maximum de moteurs d'analyse ThreatSense que vous pouvez utiliser est de 20. La modification n'est appliquée qu'après le redémarrage.

REMARQUE : il est recommandé de définir le même nombre de threads d'analyse et de moteurs d'analyse ThreatSense. Le fait d'utiliser un nombre de threads d'analyse plus élevé que celui des moteurs d'analyse n'a aucune incidence sur les performances.

REMARQUE : Si vous utilisez ESET Mail Security sur un serveur Windows agissant comme Terminal Server et que vous ne souhaitez pas que l'interface utilisateur graphique ESET Mail Security démarre à chaque connexion de l'utilisateur, reportez-vous au chapitre Désactivation de l'interface utilisateur graphique sur Terminal Server 123 pour accéder à la procédure de désactivation.

3. ESET Mail Security : protection du serveur Microsoft Exchange Server

ESET Mail Security offre à votre serveur Microsoft Exchange Server une excellente protection. Il existe trois types essentiels de protection : antivirus, antispam et application de règles définies par l'utilisateur. ESET Mail Security vous protège de différents types de contenu malveillant, y compris les pièces jointes infectées par des vers ou des chevaux de Troie, les documents contenant des scripts malveillants, le hameçonnage et le courrier indésirable. ESET Mail Security exclut le contenu malveillant au niveau du serveur de messagerie, avant qu'il arrive dans la boîte de réception du destinataire, sur le client. Les chapitres suivants décrivent tous les paramètres et options que vous avez à disposition pour ajuster la protection Microsoft Exchange Server.

3.1 Paramètres généraux

Cette section décrit la gestion des règles, des fichiers journaux, de la quarantaine des messages et des paramètres de performances.

3.1.1 Serveur Microsoft Exchange Server

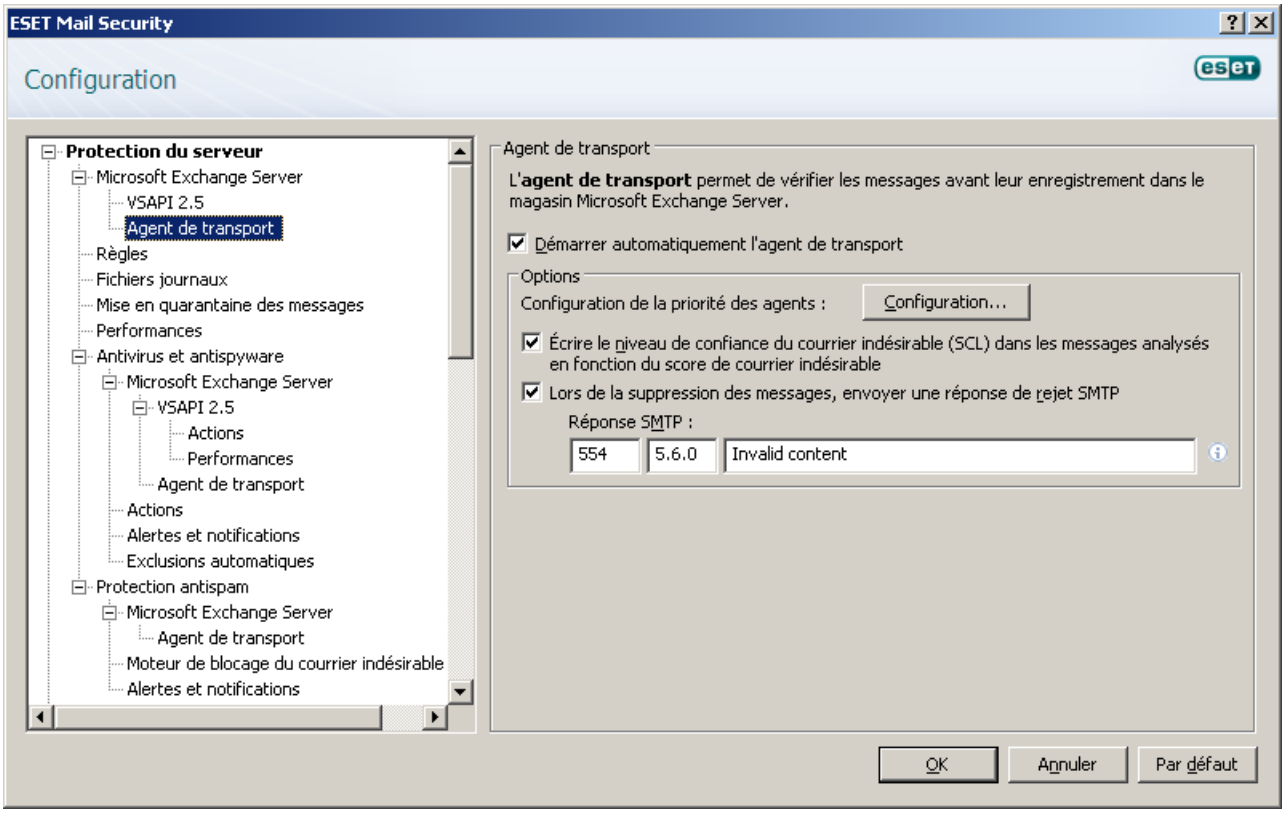
3.1.1.1 VSAPI (Virus-Scanning Application Programming Interface)

Microsoft Exchange Server offre un mécanisme qui garantit que chaque composant de message est analysé sur la base de la base des signatures de virus actuelle. Si un composant de message n'a pas été analysé, il est soumis à l'analyseur avant que le message soit envoyé au client. Chaque version prise en charge de Microsoft Exchange Server (2000/2003/2007/2010) propose une version différente de VSAPI.

Utilisez la case à cocher pour activer/désactiver le démarrage automatique de la version VSAPI utilisée par votre serveur Exchange.

3.1.1.2 Agent de transport

Dans cette section, vous pouvez configurer l'agent de transport pour qu'il démarre automatiquement et définir sa priorité de chargement. Sur Microsoft Exchange Server 2007 et les versions ultérieures, l'installation d'un agent de transport n'est possible que si le serveur a l'un des deux rôles suivants : *Transport Edge* ou *Transport Hub*.



REMARQUE : l'agent de transport n'est pas disponible dans Microsoft Exchange Server 5.5 (VSAPI 1.0).

Dans le menu **Configuration de la priorité des agents**, vous pouvez définir la priorité des agents ESET Mail Security. La plage des numéros de priorité des agents dépend de la version de Microsoft Exchange Server (plus le numéro est petit, plus la priorité est élevée).

Écrire le niveau de confiance du courrier indésirable (SCL) dans l'en-tête des messages analysés en fonction du score de courrier indésirable : la valeur normalisée SCL qui est attribuée à un message indique la vraisemblance selon laquelle le message est un courrier indésirable (en fonction des caractéristiques de l'en-tête du message, de son objet, de son contenu, etc.). La valeur 0 indique que le message n'est très probablement pas un courrier indésirable, tandis que la valeur 9 indique au contraire qu'il est très probablement un courrier indésirable. Les valeurs SCL peuvent être traitées plus précisément par le filtre de messages intelligent de Microsoft Exchange Server (ou par l'agent de filtrage de contenu). Pour plus d'informations, reportez-vous à la documentation Microsoft Exchange Server.

Option **Lors de la suppression des messages, envoyer une réponse de rejet SMTP** :

- Si cette option n'est pas cochée, le serveur envoie une réponse SMTP favorable à l'agent de transfert de message (MTA) de l'expéditeur au format '250 2.5.0 : Requested mail action okay, completed' ('250 2.5.0 : action demandée sur courrier OK, terminée'), puis effectue une suppression automatique.
- Si l'option est cochée, une réponse de rejet SMTP est renvoyée à l'agent de transfert de message (MTA) de l'expéditeur. Vous pouvez saisir un message de réponse au format suivant :

Code principal de réponse	Code d'état complémentaire	Description
250	2.5.0	Requested mail action okay, completed (Action demandée sur courrier OK, terminée)
451	4.5.1	Requested action aborted: local error in processing (Action demandée interrompue : erreur locale en cours de traitement)
550	5.5.0	Requested action not taken: mailbox unavailable (Action demandée non effectuée : boîte aux lettres non disponible)

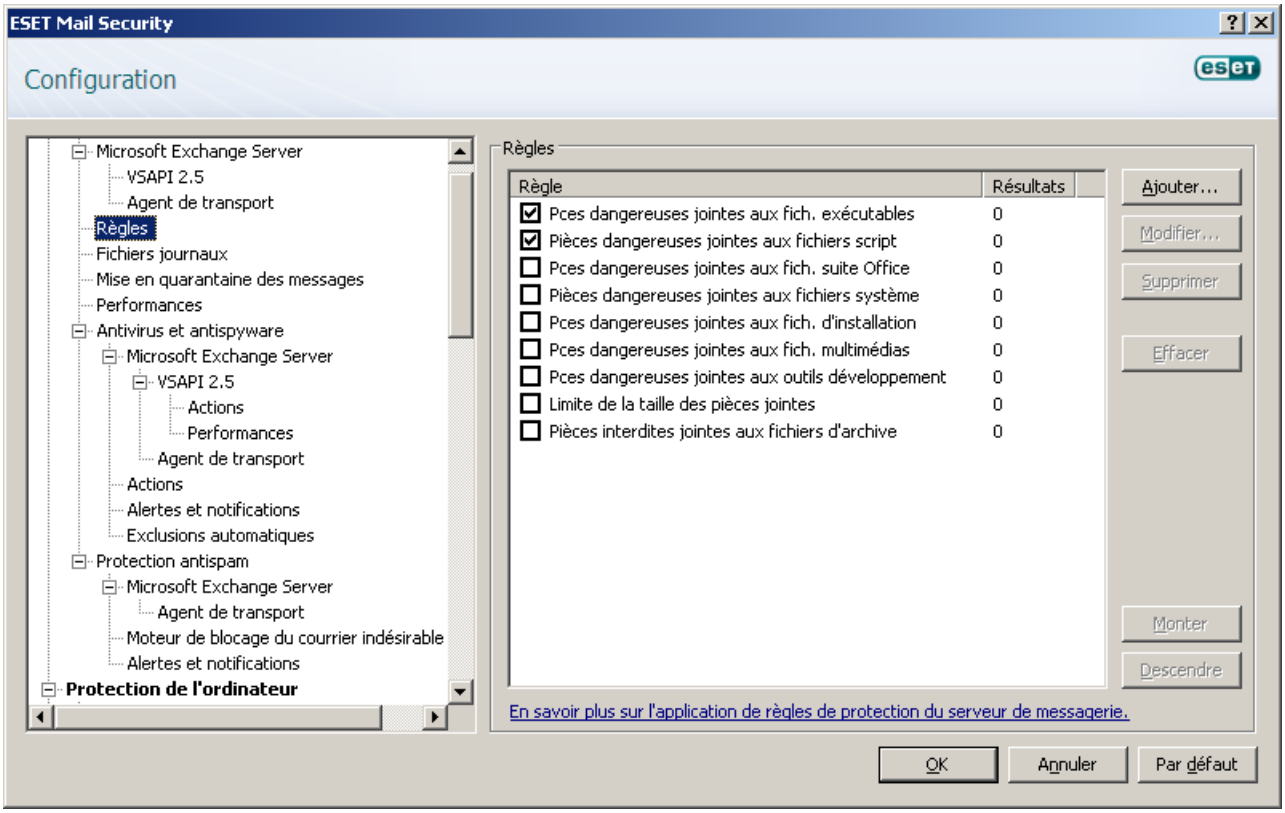
Avertissement : une syntaxe incorrecte des codes de réponses SMTP peut provoquer des dysfonctionnements des composants de programme et réduire l'efficacité.

REMARQUE : vous pouvez également utiliser des variables système pour configurer des réponses de rejet SMTP.

3.1.2 Règles

L'option de menu **Règles** permet aux administrateurs de définir manuellement les conditions de filtrage des emails et les actions à exécuter sur les emails filtrés. Les règles sont appliquées en fonction d'un ensemble de conditions combinées. Plusieurs conditions sont associées à l'aide de l'opérateur logique AND, ce qui permet d'appliquer la règle uniquement lorsque toutes les conditions sont remplies. La colonne **Numéro** (à côté du nom de chaque règle) affiche le nombre d'applications de la règle.

Les règles permettent de vérifier un message lorsque celui est traité par l'agent de transport ou VSAPI. Si les deux méthodes, agent de transport et VSAPI, sont activées et que le message correspond aux conditions de la règle, le nombre de règles peut augmenter de 2 ou plus. Le système VSAPI accède en effet à chacune des parties du message (corps et pièce jointe), ce qui signifie que les règles sont appliquées à chacune de ces parties. Les règles sont également appliquées lors des analyses en arrière-plan (par exemple lors de l'analyse répétée du stockage de la boîte aux lettres après la mise à jour des bases des signatures de virus), ce qui peut augmenter le nombre de règles.



- **Ajouter...** : ajoute une nouvelle règle
- **Modifier...** : modifie une règle existante
- **Supprimer** : supprime une règle sélectionnée
- **Effacer** : efface le compteur de règles (colonne Correspondances)
- **Monter** : déplace la règle sélectionnée vers le haut de la liste.
- **Descendre** : déplace la règle sélectionnée vers le bas de la liste.

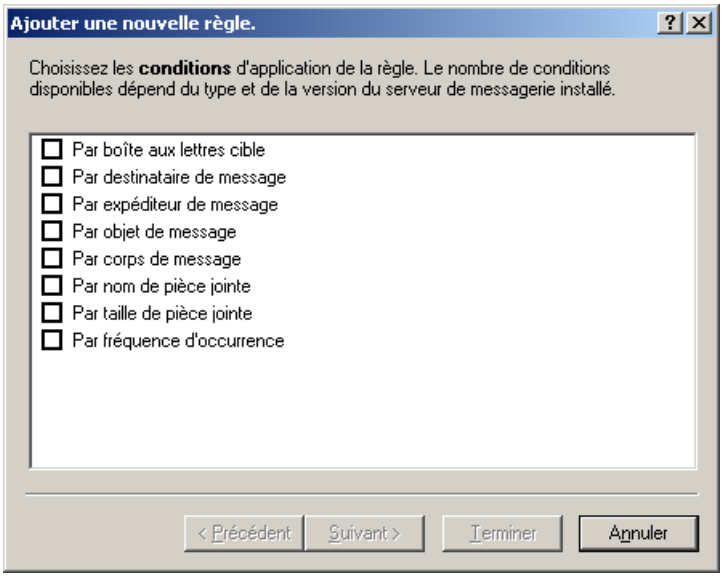
Décochez la case (à gauche du nom de chaque règle) pour désactiver la règle. La règle peut ainsi être réactivée si nécessaire.

REMARQUE : vous pouvez également utiliser des variables système (par exemple, *%PATHEXT%*) lors de la configuration des règles.

REMARQUE : si une nouvelle règle est ajoutée ou une règle existante est modifiée, une nouvelle analyse des messages démarre automatiquement à l'aide des règles créées/modifiées.

3.1.2.1 Ajout de nouvelles règles

Cet assistant vous guide dans l'ajout de règles spécifiées par l'utilisateur avec des conditions combinées.



REMARQUE : les conditions ne sont pas toutes applicables lorsque le message est analysé par l'agent de transport.

- **Par boîte aux lettres cible**s'applique au nom d'une boîte aux lettres (VSAPI)
- **Par destinataire de message** s'applique à un message envoyé à un destinataire spécifique (VSAPI + agent de transport).
- **Par expéditeur de message** s'applique à un message envoyé par un expéditeur spécifique (VSAPI + agent de transport).
- **Par objet de message** s'applique à un message avec une ligne d'objet spécifique (VSAPI + agent de transport).
- **Par corps de message** s'applique à un message avec un texte spécifique dans le corps du message (VSAPI).
- **Par nom de pièce jointe** s'applique à un message comportant une pièce jointe portant un nom spécifique (VSAPI dans Exchange 2000 et 2003, VSAPI + agent de transport dans Exchange 2007 et 2010)
- **Par taille de pièce jointe** s'applique à un message comportant une pièce jointe dont la taille dépasse une limite définie (VSAPI dans Exchange 2000 et 2003, VSAPI + agent de transport dans Exchange 2007 et 2010)
- **Par fréquence d'occurrence** s'applique aux objets (corps du message ou pièce jointe) dont le nombre d'occurrences dans l'intervalle défini est supérieur au nombre indiqué (VSAPI). Cette condition est particulièrement utile si vous recevez en permanence des courriers indésirables dont le corps du message ou la pièce jointe sont identiques.
- **Par type de pièce jointe** s'applique à un message dont le type de pièce jointe est spécifique (le type de fichier est détecté en fonction de son contenu, pas de l'extension du fichier) (VSAPI).

Lorsque vous indiquez les conditions ci-dessus (à l'exception de la condition **Par taille de pièce jointe**), il suffit d'indiquer une partie d'expression et de ne pas sélectionner l'option **Mot entier**. Les valeurs ne font pas la différence entre les majuscules et les minuscules, sauf si l'option **Respecter la casse** est sélectionnée. Si vous utilisez des caractères non alphanumériques, utilisez des parenthèses et des guillemets. Vous pouvez également créer des conditions à l'aide des opérateurs logiques AND, OR et NO.

REMARQUE : la liste des règles disponibles dépend des versions installées de Microsoft Exchange Server.

REMARQUE : Microsoft Exchange Server 2000 (VSAPI 2.0) n'évalue que le nom de l'expéditeur/du destinataire affiché, mais pas l'adresse électronique. Les adresses électroniques sont évaluées dans Microsoft Exchange Server 2003 (VSAPI 2.5) et les versions supérieures.

Exemples de saisie de conditions :

Par boîte aux lettres cible :martin

Par expéditeur de message :	martin@courrier.com
Par destinataire du message :	"J.Martin" ou "martin@courrier.com"

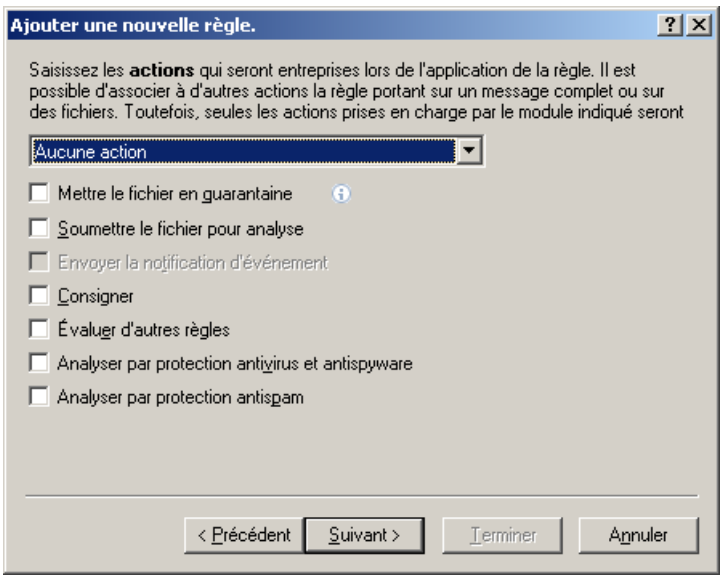
Par objet du message : " "

Par nom de pièce jointe : ".com" OR ".exe"

Par corps de message : ("gratuit" OR "loterie") AND ("gagner" OR "acheter")

3.1.2.2 Actions exécutées lors de l'application des règles

Cette section permet de sélectionner les actions à entreprendre sur les messages et/ou les pièces jointes qui correspondent aux conditions définies dans les règles. Vous pouvez choisir de n'entreprendre aucune action, de marquer le message comme s'il contenait une menace/un courrier indésirable ou de supprimer l'intégralité du message. Lorsqu'un message ou sa pièce jointe correspond aux conditions de la règle, il n'est pas analysé par les modules antivirus ou antispam par défaut, sauf si l'analyse est explicitement activée par la sélection des cases à cocher correspondantes situées dans la partie inférieure (l'action entreprise dépend alors des paramètres antivirus/ antispam).



- **Aucune action** : aucune action n'est entreprise sur le message
- **Entreprendre une action pour la menace non nettoyée** : le message est marqué comme s'il contenait une menace non nettoyée (qu'il contienne une menace ou non).
- **Entreprendre une action pour le message non sollicité** : le message est marqué comme s'il s'agissait d'un courrier indésirable (qu'il s'agisse ou non d'un courrier indésirable). Cette option ne fonctionne que si la protection antispam 37 est activée et que l'action est exécutée sur l'agent de transport. Dans le cas contraire, cette action n'est pas effectuée
- **Supprimer le message** : supprime l'intégralité du message dont le contenu répond aux conditions. Cette action ne fonctionne toutefois qu'avec VSAPI 2.5 et versions ultérieures (VSAPI 2.O et versions antérieures ne peut exécuter cette action)

- **Mettre le fichier en quarantaine** : met en quarantaine les pièces jointes, le ou les fichiers qui répondent aux critères de la règle seront placés dans la quarantaine de fichiers de ESET Mail Security, à ne pas confondre avec la quarantaine d'e-mails (pour plus d'informations sur la quarantaine d'e-mails, reportez-vous au chapitre Quarantaine de messages 25)
- **Soumettre le fichier pour analyse** : envoie les pièces jointes suspectes au laboratoire ESET pour analyse.
- **Envoyer la notification d'événement** : envoie une notification à l'administrateur (en fonction des paramètres définis dans **Outils** > **Alertes et notifications**)
- **Consigner** : écrit des informations sur la règle appliquée au journal de l'application.
- **Évaluer d'autres règles** : permet l'évaluation d'autres règles afin que l'utilisateur puisse définir plusieurs ensembles de conditions et d'actions à entreprendre en fonction de ces conditions.
- **Analyser par protection antivirus et antispyware** : analyse le message et ses pièces jointes afin d'y détecter les menaces.
- **Analyser par protection antispam** : analyse le message afin d'évaluer s'il s'agit de courrier indésirable.

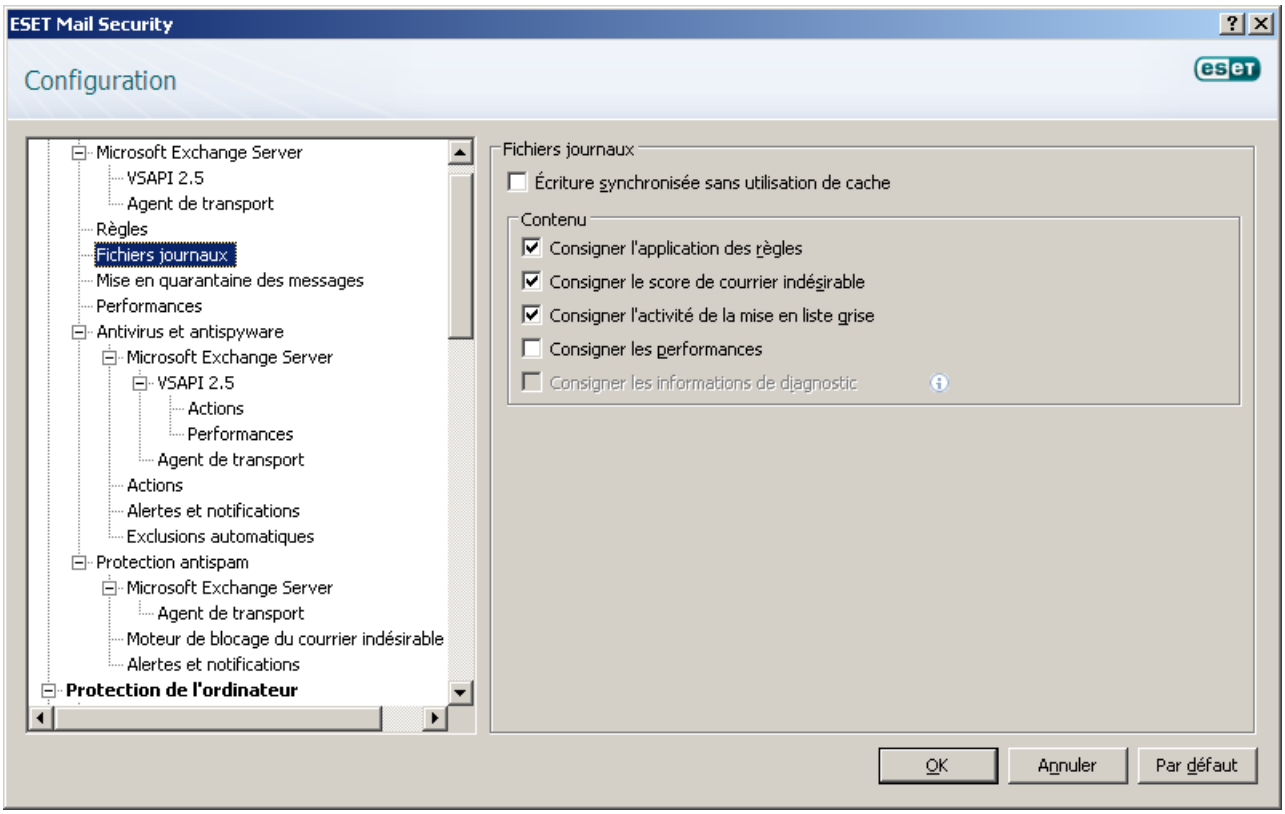
REMARQUE : cette option n'est disponible que dans Microsoft Exchange Server 2OOO et les versions ultérieures et uniquement si l'agent de transport est activé.

La dernière étape de l'assistant de création de règle consiste à nommer chaque règle créée. Vous pouvez également

ajouter un **commentaire sur la règle**. Ces informations sont stockées dans le journal Microsoft Exchange Server.

3.1.3 Fichiers journaux

Les paramètres des fichiers journaux vous permettent de sélectionner le mode d'assemblage du fichier journal. Les protocoles plus détaillés peuvent contenir des informations supplémentaires, mais risquent de ralentir les performances du serveur.



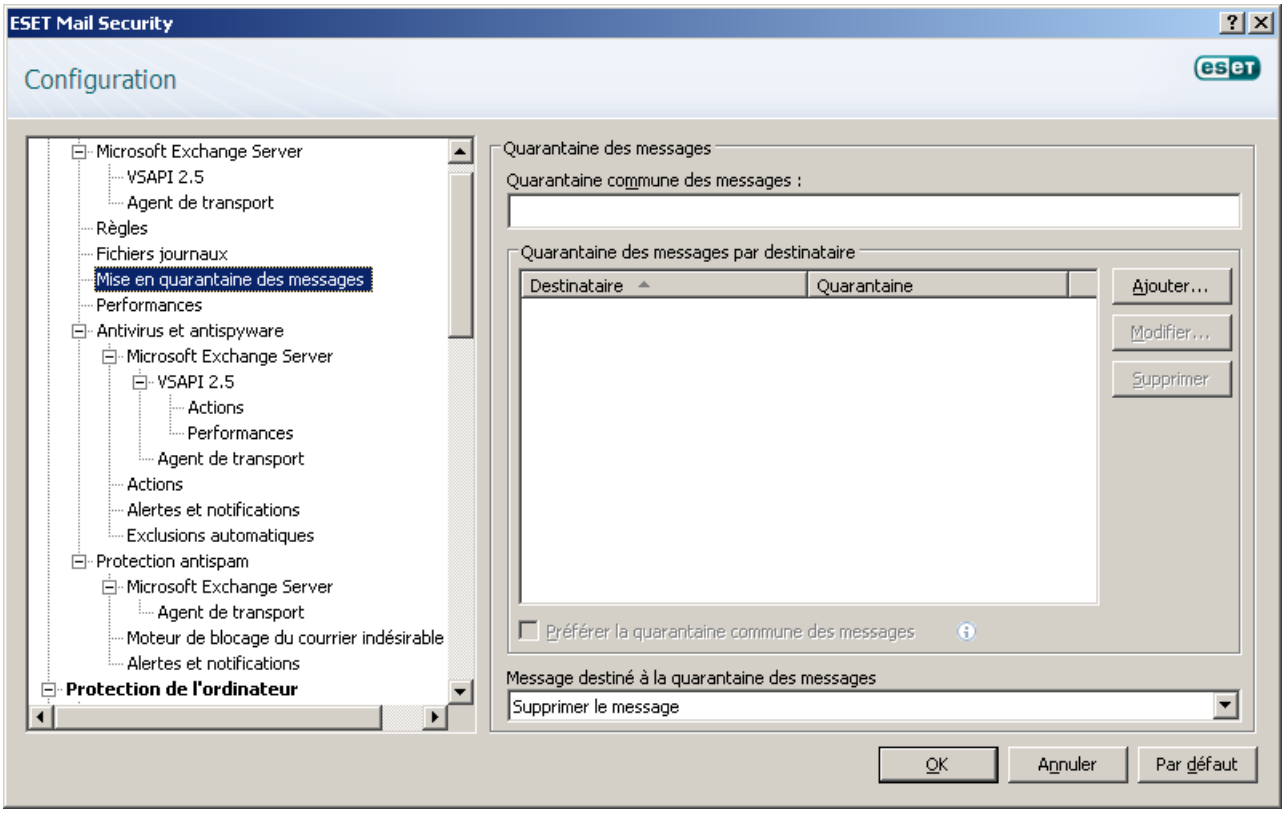
Si l'option **Écriture synchronisée sans utilisation de cache** est activée, toutes les entrées de journal sont immédiatement écrites dans le fichier journal sans stockage dans le cache du journal. Par défaut, les composants ESET Mail Security qui s'exécutent sur Microsoft Exchange Server stockent les messages du journal dans leur cache interne et les envoient au journal de l'application à des intervalles réguliers afin de préserver les performances. Dans ce cas toutefois, les entrées de diagnostic dans le journal risquent de ne pas être classées dans l'ordre correct. Il est recommandé de désactiver ce paramètre, sauf s'il est nécessaire aux opérations de diagnostic. Vous pouvez indiquer le type des informations stockées dans les fichiers journaux dans le menu **Contenu**.

- **Consigner l'application des règles** : lorsque cette option est activée, ESET Mail Security écrit dans le fichier journal le nom de toutes les règles activées.
- **Consigner le score de courrier indésirable** : utilisez cette option pour que l'activité relative au courrier indésirable soit écrite dans le journal du courrier indésirable 97. Lorsque le serveur de messagerie reçoit un message de courrier indésirable, les informations concernant la date et l'heure, l'expéditeur, le destinataire, l'objet, le score de courrier indésirable, le motif et l'action sont écrites dans le journal. Ces informations sont particulièrement utiles lorsque vous devez effectuer le suivi des messages de courrier indésirable afin de déterminer le moment de leur occurrence et l'action qui a été entreprise.
- **Consigner l'activité de la mise en liste grise** : active cette option si vous souhaitez que l'activité relative à la liste grise soit écrite dans le journal du courrier indésirable 97. Les informations concernent la date et l'heure, le domaine HELO, l'adresse IP, l'expéditeur, le destinataire, l'action, etc.
  REMARQUE : cette option n'est disponible que lorsque la liste grise est activée dans les options de l'agent de transport 38, dans **Protection du serveur** > **Protection antispam** > **Microsoft Exchange Server** > **Agent de transport** dans l'arborescence de configuration avancée (F5).
- **Consigner les performances** : consigne les informations sur l'intervalle d'une tâche, la taille de l'objet analysé, la vitesse de transfert (Ko/s) et le niveau des performances.
- **Consigner les informations de diagnostic** : consigne les informations de diagnostic nécessaires à l'ajustement du programme au protocole ; cette option est particulièrement adaptée au débogage et à l'identification des problèmes. Il n'est pas recommandé d'activer cette option. Pour afficher les informations de diagnostic fournies

par cette fonction, vous devez définir l'option Verbosité minimale des journaux sur **Entrées de diagnostic** dans le paramètre **Outils** > **Fichiers journaux** > **Verbosité minimale des journaux**.

3.1.4 Quarantaine des messages

La boîte aux lettres **Quarantaine des messages** est une boîte aux lettres spéciale définie par l'administrateur système pour stocker les messages potentiellement infectés et le courrier indésirable. Les messages en quarantaine peuvent être analysés ou nettoyés plus tard à l'aide d'une base des signatures de virus plus récente.



Il existe deux types de systèmes de quarantaine des messages.

L'un consiste à utiliser le système de quarantaine Microsoft Exchange (cela s'applique à Microsoft Exchange Server 2007/2010). Dans ce cas, le mécanisme interne Exchange stocke les messages potentiellement infectés et le courrier potentiellement indésirable. Par ailleurs, vous pouvez ajouter une ou plusieurs autres boîtes aux lettres de quarantaine pour certains destinataires si nécessaire. Cela signifie que les messages potentiellement infectés, qui étaient envoyés à l'origine à un destinataire défini, sont remis à une boîte aux lettres de quarantaine distincte au lieu d'aboutir dans la boîte aux lettres de quarantaine interne Exchange. Ce procédé peut être utile dans certains cas pour que les messages potentiellement infectés et le courrier indésirable restent organisés.

L'autre possibilité consiste à utiliser l'option **Quarantaine commune des messages**. Si vous utilisez une version antérieure de Microsoft Exchange Server (5.5, 2000 ou 2003), indiquez simplement **Quarantaine commune des messages** : cette boîte aux lettres permet de stocker les messages potentiellement infectés. Dans ce cas, le système de quarantaine interne à Exchange n'est pas utilisé. La boîte aux lettres spécifiée par l'administrateur système est utilisée à cette fin. Comme pour la première option, vous pouvez ajouter une ou plusieurs autres boîtes aux lettres de quarantaine pour certains destinataires. Par conséquent, les messages potentiellement infectés sont remis à une boîte aux lettres standard au lieu de la quarantaine commune des messages.

- **Quarantaine commune des messages** : vous pouvez indiquer l'adresse de la quarantaine commune des messages (par exemple quarantaine_principale@entreprise.com) ou utiliser le système de quarantaine interne de Microsoft Exchange Server 2007/2010 en ne complétant pas ce champ et en choisissant **Mettre le message dans la quarantaine du système de serveur de messagerie** dans le menu déroulant situé dans la partie inférieure (à condition que la quarantaine Exchange existe dans votre environnement). Les courriers sont ensuite remis à la quarantaine par le mécanisme interne Exchange avec ses propres paramètres.
  REMARQUE : par défaut, cette quarantaine interne n'est pas activée dans Exchange. Si vous souhaitez l'activer, vous devez ouvrir l'environnement de ligne de commande Exchange Management Shell et entrer la commande suivante :

  Set-ContentFilterConfig -QuarantineMailbox nom@domaine.com

  (remplacez nom@domaine.com par le nom de la boîte aux lettres que Microsoft Exchange doit utiliser comme boîte aux lettres de quarantaine interne, par exemple quarantaineexchange@entreprise.com)

- **Quarantaine des messages par destinataire** : cette option permet de définir les boîtes aux lettres de quarantaine de messages pour plusieurs destinataires. Chaque règle de quarantaine peut être activée ou désactivée en cochant ou décochant la case appropriée.

  Ajouter... : vous pouvez ajouter une nouvelle règle de quarantaine en saisissant l'adresse électronique du destinataire souhaité et l'adresse de la quarantaine des messages à laquelle le message sera transmis.

  Modifier... : modifie la règle de quarantaine sélectionné.

  Supprimer : supprime une règle de quarantaine sélectionnée

  Quarantaine des messages commune préférée : si cette option est activée, un message est remis à la quarantaine des messages commune indiquée si plusieurs règles de quarantaine sont satisfaites (par exemple, un message a plusieurs destinataires et certains d'entre eux sont définis dans plusieurs règles de quarantaine).

- **Message destiné à la quarantaine des messages non existants** (si vous n'avez pas indiqué de quarantaine commune des messages, les options suivantes permettent d'entreprendre des actions sur les messages potentiellement infectés et le courrier indésirable).

  Aucune action : le message est traité normalement, c'est-à-dire qu'il est remis au destinataire (non recommandé).
  Supprimer le message : le message est supprimé s'il est envoyé à un destinataire sans aucune règle de quarantaine et si aucune quarantaine des messages commune n'est définie. Dans ce cas, tous les messages potentiellement infectés et le courrier indésirable sont supprimés automatiquement sans être stockés.
  Mettre le message en quarantaine dans la quarantaine système du serveur de messagerie : un message est remis à la quarantaine interne Exchange où il est stocké (non disponible dans Microsoft Exchange Server 2003 et les versions antérieures).

REMARQUE : vous pouvez également utiliser des variables système (par exemple, *%USERNAME%*) lors de la configuration des paramètres de la quarantaine des messages.

3.1.4.1 Ajout d'une nouvelle règle de quarantaine

Entrez les adresses électroniques du destinataire et de la quarantaine dans les champs appropriés.

Si vous souhaitez supprimer un message adressé à un destinataire qui n'a pas de règle de quarantaine, vous pouvez sélectionner **Supprimer le message** dans le menu déroulant **Message destiné à la quarantaine des messages non existants**.

3.1.5 Performances

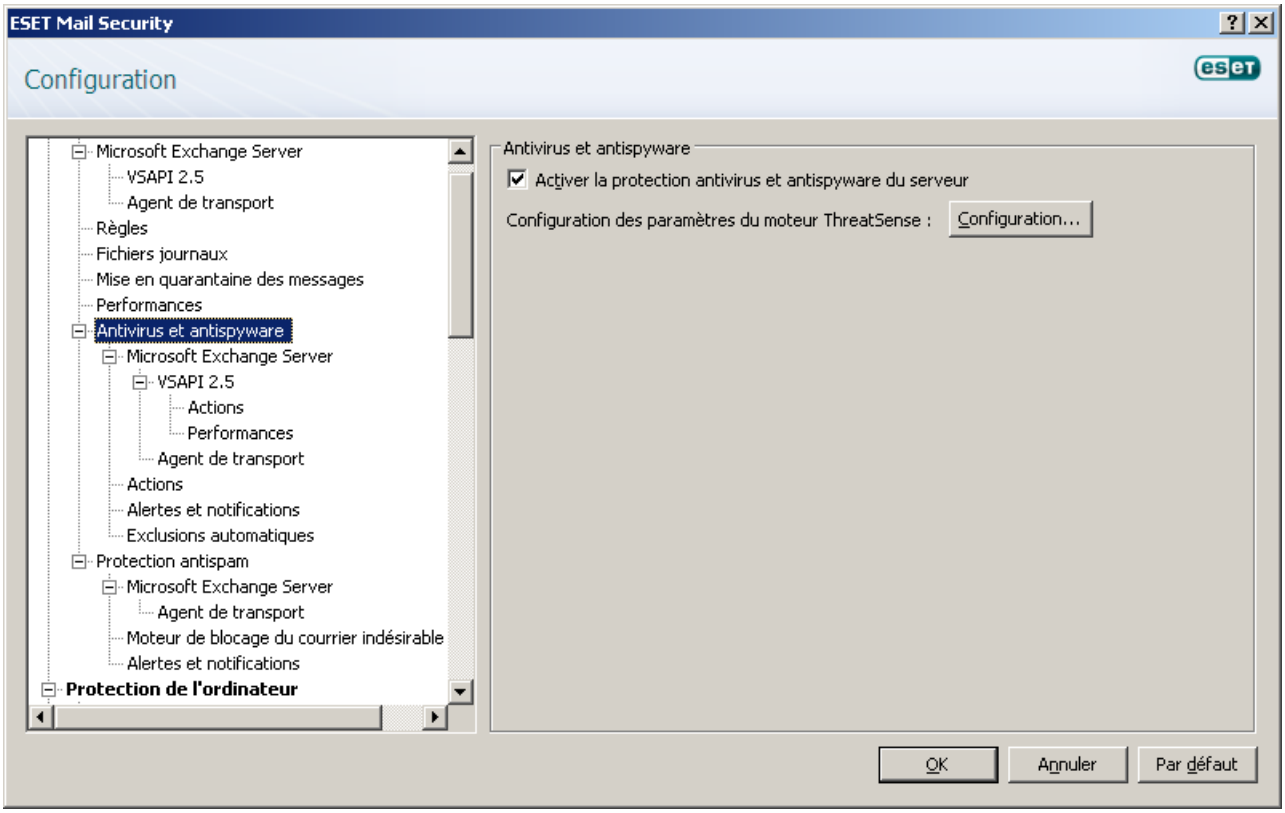
Dans cette section, vous pouvez définir un dossier dans lequel seront stockés les fichiers temporaires afin d'améliorer les performances du programme. Si vous n'indiquez aucun dossier, ESET Mail Security crée des fichiers temporaires dans le dossier temporaire du système.

REMARQUE : afin de réduire l'impact potentiel sur les entrées/sorties et la fragmentation, il est recommandé de placer le dossier temporaire dans un disque dur différent de celui sur lequel Microsoft Exchange Server est installé. Il est vivement recommandé de ne pas créer le dossier temporaire sur un support amovible de type disquette, clé USB, DVD, etc.

REMARQUE : vous pouvez utiliser les variables système (par exemple *%SystemRoot%\TEMP*) lors de la configuration des paramètres de performances.

3.2 Paramètres antivirus et antispyware

Vous pouvez activer la protection antivirus et antispyware du serveur de messagerie en sélectionnant l'option **Activer la protection antivirus et antispyware du serveur**. Notez que la protection antivirus et antispyware est activée automatiquement à chaque redémarrage du service/de l'ordinateur. La configuration des paramètres du moteur ThreatSense est accessible par le bouton **Configuration...**



3.2.1 Serveur Microsoft Exchange Server

En ce qui concerne la protection antivirus et antispyware, ESET Mail Security pour Microsoft Exchange Server utilise deux types d'analyse. L'un analyse les messages par l'intermédiaire de VSAPI et l'autre utilise l'agent de transport.

- La protection par VSAPI 28 analyse les messages directement dans la zone de stockage du serveur Exchange.
- La protection par l'agent de transport 34 analyse le trafic SMTP au lieu de la zone de stockage du serveur Exchange proprement dite. Si ce type de protection est activé, cela signifie que tous les messages et leurs composants sont analysés pendant le transport, avant même qu'ils atteignent la zone de stockage du serveur ou qu'ils soient envoyés par SMTP. Le filtrage de messages au niveau du serveur SMTP est assuré par un plugin spécialisé. Dans Microsoft Exchange Server 2000 et 2003, ce plugin (récepteur d'événements) est enregistré sur le serveur SMTP dans le cadre des services IIS (Internet Information Services). Dans Microsoft Exchange Server 2007/2010, le plugin est enregistré en tant qu'agent de transport dans les rôles Edge ou Hub du serveur Microsoft Exchange.

REMARQUE : l'agent de transport n'est pas disponible dans Microsoft Exchange Server 5.5 ; il l'est en revanche dans toutes les versions Microsoft Exchange Server plus récentes (à partir de la version 2000).

Les protections antivirus et antispyware par VSAPI et agent de transport peuvent fonctionner de pair (c'est la valeur par défaut et la configuration recommandée). Vous pouvez également choisir d'utiliser un seul type de protection (VSAPI ou agent de transport). Ces deux types peuvent être activés ou désactivés indépendamment l'un de l'autre. Nous recommandons d'utiliser les deux types afin de garantir une protection antivirus et antispyware maximum. Nous déconseillons en revanche de les désactiver tous les deux.

3.2.1.1 Interface VSAPI (Virus-Scanning Application Programming Interface)

Microsoft Exchange Server offre un mécanisme qui garantit que chaque composant de message est analysé sur la base de la base des signatures de virus actuelle. Si un message n'a pas été analysé, ses composants sont soumis à l'analyseur avant qu'il soit envoyé au client. Chaque version prise en charge de Microsoft Exchange Server (5.5/2000/2003/2007/2010) propose une version différente de VSAPI.

3.2.1.1.1 Microsoft Exchange Server 5.5 (VSAPI 1.0)

Cette version de Microsoft Exchange Server comprend VSAPI version 1.0.

Si l'option **Analyse en arrière-plan** est activée, il est possible d'analyser tous les messages en arrière-plan. En fonction de différents facteurs tels que la charge actuelle du système, le nombre d'utilisateurs actifs, etc., Microsoft Exchange Server décide si une analyse en arrière-plan doit s'exécuter, et conserve la liste des messages analysés et de la version de la base des signatures de virus utilisée. Si vous ouvrez un message qui n'a pas été analysé par la base des signatures de virus la plus à jour, Microsoft Exchange Server envoie le message à ESET Mail Security pour qu'il soit analysé avant d'être ouvert dans le client de messagerie.

L'analyse en arrière-plan pouvant avoir un impact sur la charge du système (elle est effectuée après chaque mise à jour de la base des signatures des virus), il est recommandé de planifier cette analyse en dehors des heures de travail. L'analyse en arrière-plan planifiée peut être configurée par l'intermédiaire d'une tâche spécifique dans le Planificateur. Lorsque vous planifiez une analyse en arrière-plan, vous pouvez définir l'heure de son lancement, le nombre de répétitions et d'autres paramètres disponibles dans le Planificateur. Une fois planifiée, la tâche apparaît dans la liste des tâches planifiées ; comme pour les autres tâches, vous pouvez modifier ses paramètres, la supprimer ou la désactiver temporairement.

3.2.1.1.1.1 Actions

Dans cette section, vous pouvez indiquer les actions à effectuer lorsqu'un message et/ou une pièce jointe est évalué comme étant infecté.

Le champ **Action à entreprendre si le nettoyage n'est pas possible** permet de **bloquer** le contenu infecté, **supprimer** le message ou n'entreprendre **aucune action** sur le contenu infecté du message. Cette action n'est entreprise que si le nettoyage automatique (défini dans **Configuration des paramètres du moteurThreatSense** > Nettoyage 80) n'a pas nettoyé le message.

Le champ **Suppression** vous permet de définir la **méthode de suppression des pièces jointes** à l'aide des options suivantes :

- **Tronquer le fichier à la longueur zéro** : ESET Mail Security tronque la pièce jointe à la longueur zéro et permet au destinataire de voir le nom et le type du fichier en pièce jointe.
- **Remplacer la pièce jointe par des informations sur l'action** : ESET Mail Security remplace le fichier infecté par un protocole de virus ou une description de règle.

Si vous cliquez sur le bouton **Analyser à nouveau**, vous lancez une nouvelle analyse sur des messages et des fichiers qui ont déjà été analysés.

3.2.1.1.1.2 Performances

Pendant une analyse, Microsoft Exchange Server vous permet de limiter la durée permettant d'ouvrir les pièces jointes de messages. Cette durée est définie dans le champ **Limite du temps de réponse (ms)** et représente la période après laquelle le client essaie de nouveau d'accéder au fichier qui était précédemment inaccessible en raison de l'analyse.

3.2.1.1.2 Microsoft Exchange Server 2000 (VSAPI 2.0)

Cette version de Microsoft Exchange Server comprend VSAPI version 2.0.

Si vous désélectionnez l'option **Activer la protection antivirus et antispyware VSAPI 2.0**, le plugin ESET Mail Security du serveur Exchange n'est pas déchargé depuis le processus du serveur Microsoft Exchange. Il passe uniquement en revue les messages sans rechercher les virus. En revanche, les messages font l'objet d'une recherche de courrier indésirable 38 et les règles 21 sont appliquées.

Si l'option **Analyse proactive** est activée, les nouveaux messages entrants sont analysés dans l'ordre dans lequel ils ont été reçus. Si cette option est activée et qu'un utilisateur ouvre un message qui n'a pas encore été analysé, ce message est analysé avant les autres messages dans la file d'attente.

L'option **Analyse en arrière-plan** permet d'analyser tous les messages en arrière-plan. En fonction de différents facteurs tels que la charge actuelle du système, le nombre d'utilisateurs actifs, etc., Microsoft Exchange Server décide si une analyse en arrière-plan doit s'exécuter, et conserve la liste des messages analysés et de la version de la base des signatures de virus utilisée. Si vous ouvrez un message qui n'a pas été analysé par la base des signatures de virus la plus à jour, Microsoft Exchange Server envoie le message à ESET Mail Security pour qu'il soit analysé avant d'être ouvert dans le client de messagerie.

L'analyse en arrière-plan pouvant avoir un impact sur la charge du système (elle est effectuée après chaque mise à jour de la base des signatures des virus), il est recommandé de planifier cette analyse en dehors des heures de travail. L'analyse en arrière-plan planifiée peut être configurée par l'intermédiaire d'une tâche spécifique dans le Planificateur. Lorsque vous planifiez une analyse en arrière-plan, vous pouvez définir l'heure de son lancement, le nombre de répétitions et d'autres paramètres disponibles dans le Planificateur. Une fois planifiée, la tâche apparaît dans la liste des tâches planifiées ; comme pour les autres tâches, vous pouvez modifier ses paramètres, la supprimer ou la désactiver temporairement.

Si vous souhaitez analyser les messages en texte brut, sélectionnez l'option **Analyser le corps des messages en texte brut**.

L'activation de l'option **Analyser le corps des messages RTF** active l'analyse des corps de messages RTF. Les corps de ces messages RTF peuvent contenir des macrovirus.

3.2.1.1.2.1 Actions

Dans cette section, vous pouvez indiquer les actions à effectuer lorsqu'un message et/ou une pièce jointe est évalué comme étant infecté.

Le champ **Action à entreprendre si le nettoyage n'est pas possible** permet de **bloquer** le contenu infecté, **supprimer** le message ou n'entreprendre **aucune action** sur le contenu infecté du message. Cette action n'est entreprise que si le nettoyage automatique (défini dans **Configuration des paramètres du moteur ThreatSense >** Nettoyage 80) n'a pas nettoyé le message.

L'option **Suppression** vous permet de définir la **méthode de suppression des messages** et la **méthode de suppression des pièces jointes**.

Vous pouvez définir la **méthode de suppression des messages** sur :

- **Supprimer le corps du message** : supprime le corps du message infecté ; le destinataire reçoit un message vide et les pièces jointes non infectées.
- **Réécrire le corps du message avec les informations sur l'action** : réécrit le corps du message infecté à l'aide des informations concernant les actions réalisées.

Vous pouvez définir la **méthode de suppression des pièces jointes** sur :

- **Tronquer le fichier à la longueur zéro** : ESET Mail Security tronque la pièce jointe à la longueur zéro et permet au destinataire de voir le nom et le type du fichier en pièce jointe.
- **Remplacer la pièce jointe par des informations sur l'action** : ESET Mail Security remplace le fichier infecté par un protocole de virus ou une description de règle.

Si vous cliquez sur le bouton **Analyser à nouveau**, vous lancez une nouvelle analyse sur des messages et des fichiers qui ont déjà été analysés.

3.2.1.1.2.2 Performances

Dans cette section, vous pouvez définir le nombre de threads d'analyse indépendantes utilisées à un moment donné. Un nombre supérieur de threads sur des ordinateurs multiprocesseurs peut augmenter la vitesse de l'analyse. Pour optimiser les performances des programmes, il est recommandé d'utiliser autant de moteurs d'analyse ThreatSense que de threads d'analyse.

L'option **Limite du temps de réponse (s)** permet de définir la durée maximum pendant laquelle une thread attend l'analyse d'un message. Si l'analyse n'est pas terminée à l'issue de cette période, Microsoft Exchange Server refuse l'accès du client à la messagerie. L'analyse n'est pas interrompue et, à son issue, toute autre tentative d'accès au fichier aboutit.

CONSEIL : pour vous aider à déterminer le **nombre de threads d'analyse**, le fournisseur de Microsoft Exchange Server recommande d'utiliser la formule suivante : [nombre de processeurs physiques] x 2 + 1.

REMARQUE : l'amélioration des performances n'est pas significative si les moteurs d'analyse ThreatSense sont plus nombreux que les threads d'analyse.

3.2.1.1.3 Microsoft Exchange Server 2003 (VSAPI 2.5)

Cette version de Microsoft Exchange Server comprend VSAPI version 2.5.

Si vous désélectionnez l'option **Activer la protection antivirus et antispyware VSAPI 2.5**, le plugin ESET Mail Security du serveur Exchange n'est pas déchargé depuis le processus du serveur Microsoft Exchange. Il passe uniquement en revue les messages sans rechercher les virus. En revanche, les messages font l'objet d'une recherche de courrier indésirable 38 et les règles 21 sont appliquées.

Si l'option **Analyse proactive** est activée, les nouveaux messages entrants sont analysés dans l'ordre dans lequel ils ont été reçus. Si cette option est activée et qu'un utilisateur ouvre un message qui n'a pas encore été analysé, ce message est analysé avant les autres messages dans la file d'attente.

L'option **Analyse en arrière-plan** permet d'analyser tous les messages en arrière-plan. En fonction de différents facteurs tels que la charge actuelle du système, le nombre d'utilisateurs actifs, etc., Microsoft Exchange Server décide si une analyse en arrière-plan doit s'exécuter, et conserve la liste des messages analysés et de la version de la base des signatures de virus utilisée. Si vous ouvrez un message qui n'a pas été analysé par la base des signatures de virus la plus à jour, Microsoft Exchange Server envoie le message à ESET Mail Security pour qu'il soit analysé avant d'être ouvert dans le client de messagerie.

L'analyse en arrière-plan pouvant avoir un impact sur la charge du système (elle est effectuée après chaque mise à jour de la base des signatures des virus), il est recommandé de planifier cette analyse en dehors des heures de travail. L'analyse en arrière-plan planifiée peut être configurée par l'intermédiaire d'une tâche spécifique dans le Planificateur. Lorsque vous planifiez une analyse en arrière-plan, vous pouvez définir l'heure de son lancement, le nombre de répétitions et d'autres paramètres disponibles dans le Planificateur. Une fois planifiée, la tâche apparaît dans la liste des tâches planifiées ; comme pour les autres tâches, vous pouvez modifier ses paramètres, la supprimer ou la désactiver temporairement.

L'activation de l'option **Analyser le corps des messages RTF** active l'analyse des corps de messages RTF. Les corps de ces messages RTF peuvent contenir des macrovirus.

L'option **Analyser les messages transportés** permet d'analyser les messages qui ne sont pas stockés sur le serveur Microsoft Exchange Server local et qui sont remis à d'autres serveurs de messagerie par l'intermédiaire du serveur Microsoft Exchange Server local. Le serveur Microsoft Exchange Server peut être configuré en tant que passerelle qui transmet les messages à d'autres serveurs de messagerie. Si l'analyse des messages transportés est activée, ESET Mail Security analyse également ces messages. Cette option est uniquement disponible lorsque l'agent de transport est désactivé.

REMARQUE : les corps des messages en texte brut ne sont pas analysés par VSAPI.

3.2.1.1.3.1 Actions

Dans cette section, vous pouvez indiquer les actions à effectuer lorsqu'un message et/ou une pièce jointe est évalué comme étant infecté.

Le champ **Action à entreprendre si le nettoyage n'est pas possible** permet de **bloquer** le contenu infecté, de **supprimer** le contenu infecté du message, de **supprimer l'intégralité du message**, y compris le contenu infecté, ou de n'entreprendre **aucune action**. Cette action n'est entreprise que si le nettoyage automatique (défini dans **Configuration des paramètres du moteur ThreatSense >** Nettoyage 80) n'a pas nettoyé le message.

L'option **Suppression** vous permet de définir la **méthode de suppression des messages** et la **méthode de suppression des pièces jointes**.

Vous pouvez définir la **méthode de suppression des messages** sur :

- **Supprimer le corps du message** : supprime le corps du message infecté ; le destinataire reçoit un message vide et les pièces jointes non infectées.
- **Réécrire le corps du message avec les informations sur l'action** : réécrit le corps du message infecté à l'aide des informations concernant les actions réalisées.
- **Supprimer l'intégralité du message** : supprime l'intégralité du message, y compris les pièces jointes ; vous pouvez définir l'action à entreprendre lors de la suppression des pièces jointes.

Vous pouvez définir la **méthode de suppression des pièces jointes** sur :

- **Tronquer le fichier à la longueur zéro** : ESET Mail Security tronque la pièce jointe à la longueur zéro et permet au destinataire de voir le nom et le type du fichier en pièce jointe.
- **Remplacer la pièce jointe par des informations sur l'action** : ESET Mail Security remplace le fichier infecté par un protocole de virus ou une description de règle.
- **Supprimer l'intégralité du message** : supprime l'intégralité du message, y compris les pièces jointes ; vous pouvez définir l'action à entreprendre lors de la suppression des pièces jointes.

Si vous cliquez sur le bouton **Analyser à nouveau**, vous lancez une nouvelle analyse sur des messages et des fichiers qui ont déjà été analysés.

3.2.1.1.3.2 Performances

Dans cette section, vous pouvez définir le nombre de threads d'analyse indépendantes utilisées à un moment donné. Un nombre supérieur de threads sur des ordinateurs multiprocesseurs peut augmenter la vitesse de l'analyse. Pour optimiser les performances des programmes, il est recommandé d'utiliser autant de moteurs d'analyse ThreatSense que de threads d'analyse.

L'option **Limite du temps de réponse (s)** permet de définir la durée maximum pendant laquelle une thread attend l'analyse d'un message. Si l'analyse n'est pas terminée à l'issue de cette période, Microsoft Exchange Server refuse l'accès du client à la messagerie. L'analyse n'est pas interrompue et, à son issue, toute autre tentative d'accès au fichier aboutit.

CONSEIL : pour vous aider à déterminer le **nombre de threads d'analyse**, le fournisseur de Microsoft Exchange Server recommande d'utiliser la formule suivante : [nombre de processeurs physiques] x 2 + 1.

REMARQUE : l'amélioration des performances n'est pas significative si les moteurs d'analyse ThreatSense sont plus nombreux que les threads d'analyse.

3.2.1.1.4 Microsoft Exchange Server 2007/2010 (VSAPI 2.6)

Cette version de Microsoft Exchange Server comprend VSAPI version 2.6.

Si vous désélectionnez l'option **Activer la protection antivirus et antispyware VSAPI 2.6**, le plugin ESET Mail Security du serveur Exchange n'est pas déchargé depuis le processus du serveur Microsoft Exchange. Il passe uniquement en revue les messages sans rechercher les virus. En revanche, les messages font l'objet d'une recherche de courrier indésirable 38 et les règles 21 sont appliquées.

Si l'option **Analyse proactive** est activée, les nouveaux messages entrants sont analysés dans l'ordre dans lequel ils ont été reçus. Si cette option est activée et qu'un utilisateur ouvre un message qui n'a pas encore été analysé, ce message est analysé avant les autres messages dans la file d'attente.

L'option **Analyse en arrière-plan** permet d'analyser tous les messages en arrière-plan. En fonction de différents facteurs tels que la charge actuelle du système, le nombre d'utilisateurs actifs, etc., Microsoft Exchange Server décide si une analyse en arrière-plan doit s'exécuter, et conserve la liste des messages analysés et de la version de la base des signatures de virus utilisée. Si vous ouvrez un message qui n'a pas été analysé par la base des signatures de virus la plus à jour, Microsoft Exchange Server envoie le message à ESET Mail Security pour qu'il soit analysé avant d'être ouvert dans le client de messagerie. Vous pouvez choisir d'**analyser uniquement les messages avec pièce jointe** et de les filtrer en fonction de leur heure de réception à l'aide des options **Niveau d'analyse** suivantes :

- **Tous les messages**
- **Messages reçus au cours de l'année dernière**
- **Messages reçus au cours des 6 derniers mois**
- **Messages reçus au cours des 3 derniers mois**
- **Messages reçus au cours du dernier mois**
- **Messages reçus au cours de la semaine dernière**

L'analyse en arrière-plan pouvant avoir un impact sur la charge du système (elle est effectuée après chaque mise à jour de la base des signatures des virus), il est recommandé de planifier cette analyse en dehors des heures de travail. L'analyse en arrière-plan planifiée peut être configurée par l'intermédiaire d'une tâche spécifique dans le Planificateur. Lorsque vous planifiez une analyse en arrière-plan, vous pouvez définir l'heure de son lancement, le nombre de répétitions et d'autres paramètres disponibles dans le Planificateur. Une fois planifiée, la tâche apparaît dans la liste des tâches planifiées ; comme pour les autres tâches, vous pouvez modifier ses paramètres, la supprimer ou la désactiver temporairement.

L'activation de l'option **Analyser le corps des messages RTF** active l'analyse des corps de messages RTF. Les corps de ces messages RTF peuvent contenir des macrovirus.

REMARQUE : les corps des messages en texte brut ne sont pas analysés par VSAPI.

3.2.1.1.4.1 Actions

Dans cette section, vous pouvez indiquer les actions à effectuer lorsqu'un message et/ou une pièce jointe est évalué comme étant infecté.

Le champ **Action à entreprendre si le nettoyage n'est pas possible** permet de **bloquer** le contenu infecté, de **supprimer** le contenu infecté du message, de **supprimer l'intégralité du message**, y compris le contenu infecté, ou de n'entreprendre **aucune action**. Cette action n'est entreprise que si le nettoyage automatique (défini dans Configuration des paramètres du moteur **ThreatSense** > Nettoyage 80) n'a pas nettoyé le message.

Comme nous l'avons indiqué précédemment, vous pouvez définir l'option **Action à entreprendre si le nettoyage n'est pas possible** sur :

- **Aucune action** : aucune action à entreprendre sur le contenu infecté du message.
- **Bloquer** : bloque le message avant sa réception dans la zone de stockage de Microsoft Exchange Server.
- **Supprimer l'objet** : supprime le contenu infecté du message.
- **Supprimer l'intégralité du message** : supprime l'intégralité du message, y compris son contenu infecté.

L'option **Suppression** vous permet de définir la **méthode de suppression des messages** et la **méthode de suppression des pièces jointes**.

Vous pouvez définir la **méthode de suppression des messages** sur :

- **Supprimer le corps du message** : supprime le corps du message infecté ; le destinataire reçoit un message vide et les pièces jointes non infectées.
- **Réécrire le corps du message avec les informations sur l'action** : réécrit le corps du message infecté à l'aide des informations concernant les actions réalisées.
- **Supprimer l'intégralité du message** : supprime l'intégralité du message, y compris les pièces jointes ; vous pouvez définir l'action à entreprendre lors de la suppression des pièces jointes.

Vous pouvez définir la **méthode de suppression des pièces jointes** sur :

- **Tronquer le fichier à la longueur zéro** : ESET Mail Security tronque la pièce jointe à la longueur zéro et permet au destinataire de voir le nom et le type du fichier en pièce jointe.
- **Remplacer la pièce jointe par des informations sur l'action** : ESET Mail Security remplace le fichier infecté par un protocole de virus ou une description de règle.
- **Supprimer l'intégralité du message** : supprime la pièce jointe.

Si l'option **Utiliser la quarantaine VSAPI** est activée, les messages infectés sont stockés dans la quarantaine du serveur de messagerie. Veuillez noter qu'il s'agit de la quarantaine VSAPI gérée sur le serveur (pas la quarantaine du serveur ni la boîte aux lettres de quarantaine). Les messages infectés et stockés dans la quarantaine du serveur de messagerie sont inaccessibles jusqu'à ce qu'ils soient nettoyés par la dernière version de la base des signatures de virus.

Si vous cliquez sur le bouton **Analyser à nouveau**, vous lancez une nouvelle analyse sur des messages et des fichiers qui ont déjà été analysés.

3.2.1.1.4.2 Performances

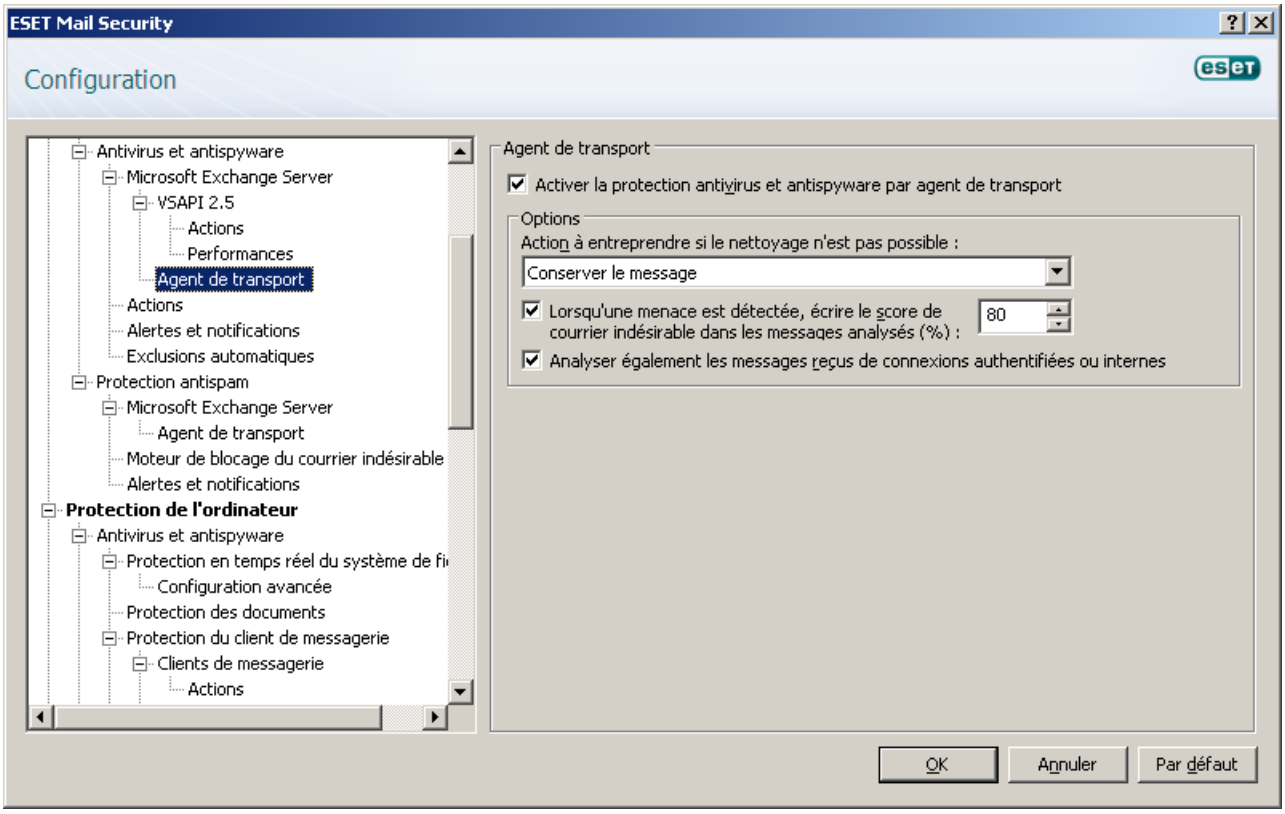
Dans cette section, vous pouvez définir le nombre de threads d'analyse indépendantes utilisées à un moment donné. Un nombre supérieur de threads sur des ordinateurs multiprocesseurs peut augmenter la vitesse de l'analyse. Pour optimiser les performances des programmes, il est recommandé d'utiliser autant de moteurs d'analyse ThreatSense que de threads d'analyse.

CONSEIL : pour vous aider à déterminer le **nombre de threads d'analyse**, le fournisseur de Microsoft Exchange Server recommande d'utiliser la formule suivante : [nombre de processeurs physiques] x 2 + 1.

REMARQUE : l'amélioration des performances n'est pas significative si les moteurs d'analyse ThreatSense sont plus nombreux que les threads d'analyse.

3.2.1.1.5 Agent de transport

Dans cette section, vous pouvez activer ou désactiver la protection antivirus et antispyware par l'agent de transport. Sur Microsoft Exchange Server 2007 et les versions ultérieures, l'installation d'un agent de transport n'est possible que si le serveur a l'un des deux rôles suivants : *Transport Edge* ou *Transport Hub*.



Si un message ne peut pas être nettoyé, il est traité conformément aux paramètres définis dans la section de l'agent de transport. Le message peut être supprimé, envoyé à la boîte aux lettres de quarantaine ou conservé.

Si vous désélectionnez l'option **Activer la protection antivirus et antispyware par agent de transport**, le plugin ESET Mail Security du serveur Exchange n'est pas déchargé depuis le processus du serveur Microsoft Exchange. Il passe uniquement en revue les messages sans rechercher les virus. En revanche, les messages font l'objet d'une recherche de courrier indésirable 38 et les règles 21 sont appliquées.

Lorsque vous sélectionnez l'option **Activer la protection antivirus et antispyware par agent de transport**, vous pouvez définir l'option **Action à entreprendre si le nettoyage n'est pas possible** :

- **Conserver le message** : conserve un message infecté qui n'a pas pu être nettoyé.
- **Mettre le message en quarantaine** : envoie un message infecté à la boîte aux lettres de quarantaine.
- **Supprimer le message** : supprime un message infecté

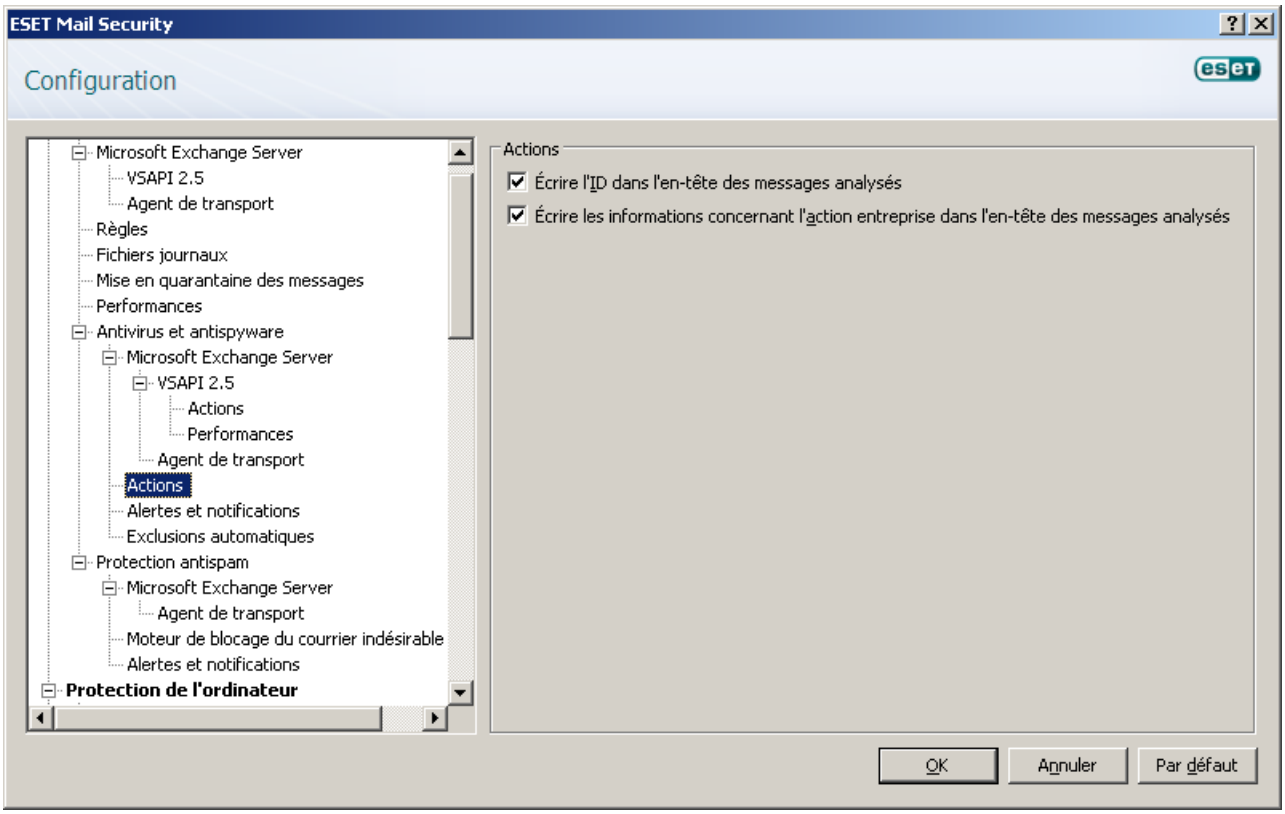
Lorsqu'une menace est détectée, écrire le score de courrier indésirable dans l'en-tête des messages analysés (%) : définit le score de courrier indésirable (la probabilité selon laquelle le message est un courrier indésirable) sur une valeur définie exprimée en pourcentage

Si une menace est détectée, un score de courrier indésirable (valeur spécifiée en %) est écrit dans le message analysé. Les botnets étant responsables de l'envoi de la majorité des messages infectés, les messages distribués de cette manière doivent être classés dans la catégorie du courrier indésirable. Pour que ce système fonctionne de manière efficace, l'option **Écrire le niveau de confiance du courrier indésirable (SCL) dans les messages analysés en fonction du score de courrier indésirable**, accessible dans **Protection du serveur** > **Microsoft Exchange Server** > Agent de transport 19 doit être activée.

Si l'option **Analyser également les messages reçus de connexions authentifiées ou internes** est activée, ESET Mail Security analyse également les messages reçus de sources authentifiées ou de serveurs locaux. Il est recommandé d'analyser ces messages afin d'améliorer la protection, mais cette opération est facultative.

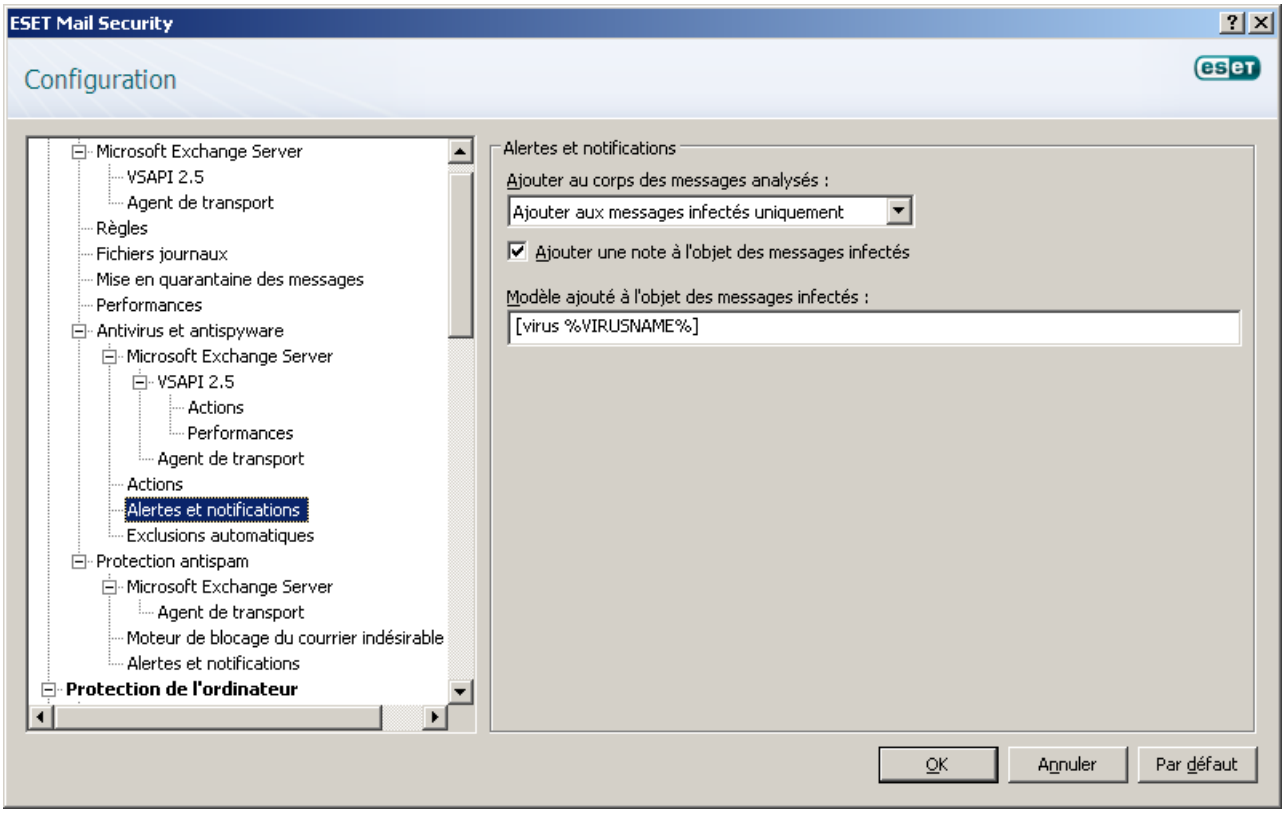
3.2.2 Actions

Dans cette section, vous pouvez choisir d'ajouter un ID de tâche d'analyse et/ou des informations sur les résultats d'analyse à l'en-tête des messages analysés.



3.2.3 Alertes et notifications

ESET Mail Security vous permet d'ajouter du texte à l'objet ou au corps d'origine des messages infectés.



Ajouter au corps des messages analysés : propose trois options :

- **Ne pas ajouter aux messages**
- **Ajouter aux messages infectés uniquement**
- **Ajouter à tous les messages analysés** (ne s'applique pas aux messages internes)

Si vous activez l'option **Ajouter une note à l'objet des messages infectés**, ESET Mail Security ajoute une notification à l'objet du message dont la valeur est définie dans le champ de texte **Modèle ajouté à l'objet des messages infectés** (par défaut [*virus %VIRUSNAME%*]). Les modifications mentionnées précédemment permettent d'automatiser le filtrage des messages infectés en fonction d'un objet défini (si votre client de messagerie prend en charge cette fonctionnalité) et de les placer dans un dossier distinct.

REMARQUE : vous pouvez également utiliser des variables système lors de l'ajout d'un modèle à l'objet du message.

3.2.4 Exclusions automatiques

Les développeurs d'applications et de systèmes d'exploitation serveur recommandent d'exclure des analyses antivirus les ensembles de dossiers et fichiers de travail critiques pour la plupart de leurs produits. Les analyses antivirus peuvent avoir une influence négative sur les performances d'un serveur, ce qui peut provoquer des conflits et même empêcher l'exécution de certaines applications sur le serveur. Les exclusions permettent de réduire le risque de conflits potentiels et d'augmenter les performances globales du serveur lors de l'exécution du logiciel antivirus.

ESET Mail Security identifie les applications serveur et les fichiers du système d'exploitation serveur critiques, puis les ajoute automatiquement à la liste des exclusions. Une fois ajouté à la liste, le processus/l'application serveur peut être activé (option par défaut) ou désactivé en sélectionnant/désélectionnant la case appropriée, ce qui donne le résultat suivant :

1) Si l'exclusion d'une application/d'un système d'exploitation reste activée, les fichiers et dossiers critiques correspondants sont ajoutés à la liste des fichiers exclus de l'analyse (**Configuration avancée** > **Protection de l'ordinateur** > **Antivirus et antispyware** > **Exclusions**). À chaque redémarrage du serveur, le système vérifie automatiquement les exclusions et restaure celles qui auraient pu être supprimées de la liste. Ce paramètre est recommandé si vous souhaitez vous assurer que les exclusions automatiques conseillées sont toujours appliquées.

2) Si l'exclusion d'une application/d'un système d'exploitation est désactivée, les fichiers et dossiers critiques correspondants restent dans la liste des fichiers exclus de l'analyse (**Configuration avancée** > **Protection de l'ordinateur** > **Antivirus et antispyware** > **Exclusions**). Toutefois, ils ne sont pas vérifiés et renouvelés automatiquement dans la liste **Exclusions** à chaque redémarrage du serveur (reportez-vous au point 1 ci-dessus). Ce paramètre est recommandé pour les utilisateurs avancés qui souhaitent supprimer ou modifier certaines des exclusions standard. Si vous souhaitez supprimer les exclusions de la liste sans redémarrer le serveur, vous devez les supprimer de la liste manuellement (**Configuration avancée** > **Protection de l'ordinateur** > **Antivirus et antispyware** > **Exclusions)**.

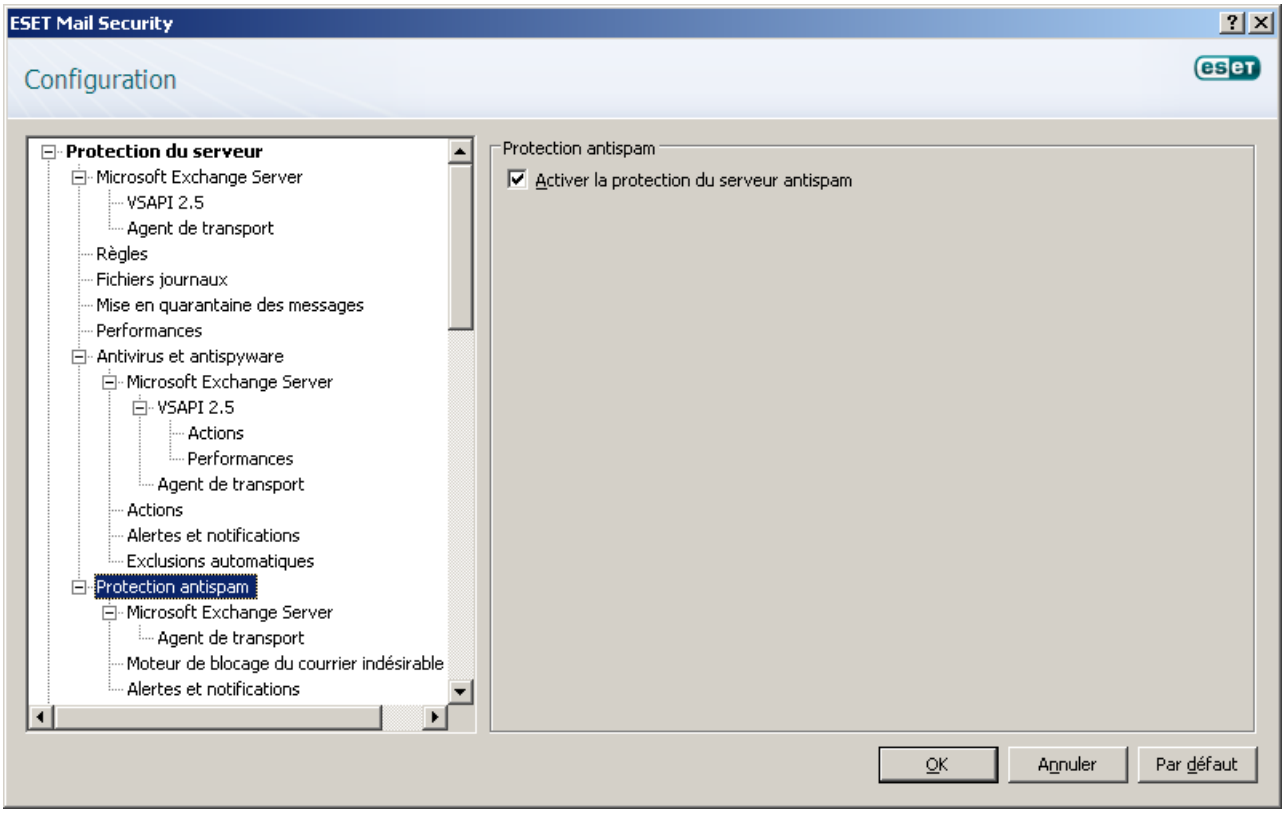
Toutes les exclusions définies par l'utilisateur et saisies manuellement dans **Configuration avancée** > **Protection de l'ordinateur** > **Antivirus et antispyware** > **Exclusions** ne sont pas concernées par les paramètres décrits ci-dessus.

Les exclusions automatiques des applications/systèmes d'exploitation serveur sont sélectionnées en fonction des recommandations de Microsoft. Pour plus d'informations, utilisez les liens suivants :

http://support.microsoft.com/kb/822158
http://support.microsoft.com/kb/245822
http://support.microsoft.com/kb/823166
http://technet.microsoft.com/fr-fr/library/bb332342(EXCHG.80).aspx
http://technet.microsoft.com/fr-fr/library/bb332342.aspx

3.3 Protection antispam

Dans la section **Protection antispam**, vous pouvez activer ou désactiver la protection antispam du serveur de messagerie installé, configurer les paramètres du moteur du blocage de courrier indésirable et définir d'autres niveaux de protection.



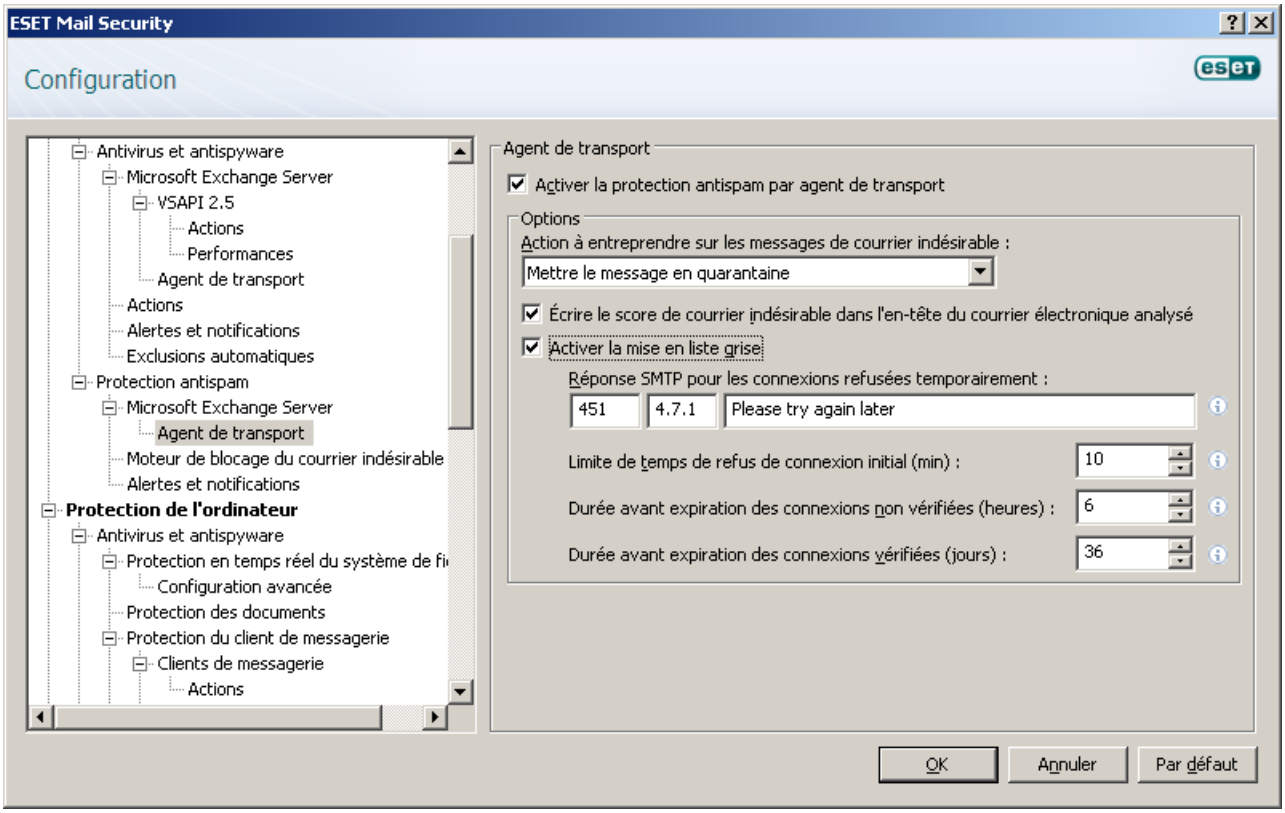
REMARQUE : la base de données antispam doit être mise à jour régulièrement pour que le module de blocage de courrier indésirable offre la meilleure protection. Pour que la base de données antispam soit mise à jour correctement, assurez-vous que ESET Mail Security a accès à des adresses IP particulières sur certains ports. Pour plus d'informations sur les adresses IP et les ports à activer sur le pare-feu tiers, reportez-vous à cet article de base de connaissances.

REMARQUE : les miroirs 90 ne peuvent pas être utilisés pour les mises à jour de base de données antispam. Pour que la base de données antispam soit mise à jour correctement, ESET Mail Security doit avoir accès aux adresses IP répertoriées dans l'article de base de connaissances mentionné ci-dessus. S'il n'a pas accès à ces adresses IP, le module de blocage de courrier indésirable ne sera pas en mesure de fournir les résultats les plus précis ni la meilleure des protections.

3.3.1 Serveur Microsoft Exchange Server

3.3.1.1 Agent de transport

Dans cette section, vous pouvez configurer les options de protection antispam à l'aide de l'agent de transport.



REMARQUE : l'agent de transport n'est pas disponible dans Microsoft Exchange Server 5.5.

Lorsque vous sélectionnez l'option **Activer la protection antispam par agent de transport**, vous pouvez choisir l'une des options **Action à entreprendre sur les messages de courrier indésirable** suivantes :

- **Conserver le message** : conserve le message même s'il est marqué comme étant courrier indésirable
- **Mettre le message en quarantaine** : envoie un message marqué comme courrier indésirable à la boîte aux lettres de quarantaine
- **Supprimer le message** : supprime un message marqué comme courrier indésirable

Si vous souhaitez inclure des informations concernant le score de courrier indésirable du message dans son en-tête, activez l'option **Écrire le score de courrier indésirable dans l'en-tête des messages analysés**.

Grâce à la fonction **Utiliser les listes blanches Exchange Server pour ignorer automatiquement la protection antispam**, ESET Mail Security peut utiliser les listes blanches spécifiques d'Exchange. Lorsqu'elle est activée, les éléments suivants sont à prendre en compte :

- L'adresse IP du serveur d'envoi figure dans la liste des adresses IP autorisées du serveur Exchange.
- La boîte aux lettres du destinataire du message comporte un indicateur de non-prise en charge de la protection antispam.
- Le destinataire du message dispose de l'adresse de l'expéditeur dans la liste Expéditeurs sûrs (vérifiez que vous avez configuré la synchronisation de la liste Expéditeurs sûrs dans l'environnement de serveur Exchange, y compris Association de listes sûres).

Si l'un des cas ci-dessus s'applique à un message entrant, la vérification antispam est ignorée pour ce message. Par conséquent, l'éventuelle nature INDÉSIRABLE de ce message n'est pas évaluée et il est remis à la boîte aux lettres du destinataire.

L'option **Accepter l'indicateur de non-prise en charge de la protection antispam défini sur la session SMTP** est utile si vous avez authentifié les sessions SMTP entre les serveurs Exchange avec le paramètre de contournement antispam. Par exemple, si vous avez un serveur Edge et un serveur Hub, il n'est pas nécessaire d'exécuter l'analyse antispam sur le trafic entre ces deux serveurs. L'option **Accepter l'indicateur de non-prise en charge de la protection antispam défini sur la session SMTP** est activée par défaut et est appliquée si un indicateur de

contournement antispam est configuré pour la session SMTP sur le serveur Exchange. Si vous désactivez l'option **Accepter l'indicateur de non-prise en charge de la protection antispam défini sur la session SMTP** en décochant la case, ESET Mail Security analyse la session SMTP et y recherche le courrier indésirable, quel que soit le paramétrage de contournement antispam du serveur Exchange.

La fonction **Activer la mise en liste grise** active une fonctionnalité qui protège les utilisateurs du courrier indésirable à l'aide de la technique suivante : L'agent de transport envoie une valeur de retour SMTP indiquant un rejet temporaire (temporarily reject) (la valeur par défaut est 451/4.7.1) pour tout message qui ne provient pas d'un expéditeur reconnu. Un serveur légitime essaie de renvoyer le message après un délai. Les serveurs de courrier indésirable n'essaient généralement pas de renvoyer le message, car ils envoient des messages à des milliers d'adresses électroniques et ne perdent pas de temps à relancer des expéditions. La mise en liste grise est une couche supplémentaire de protection antispam et n'a aucun effet sur les fonctionnalités d'évaluation du module de blocage de courrier indésirable.

Lors de l'évaluation de la source du message, la méthode prend en compte les configurations des listes d'**adresses IP approuvées**, **ignorées**, **autorisées** et **d'expéditeurs sûrs** et sur le serveur Exchange et les paramètres AntispamBypass de la boîte aux lettres du destinataire. Les messages de ces listes d'adresses IP/d'expéditeurs ou ceux remis à une boîte aux lettres dont l'option AntispamBypass est activée sont ignorés par la méthode de détection de mise en liste grise.

Le champ **Réponse SMTP pour les connexions refusées temporairement** définit la réponse SMTP de refus temporaire envoyée au serveur SMTP si un message est refusé.

Exemple de message de réponse SMTP :

Code principal de réponse	Code d'état complémentaire	Description
451	4.7.1	Requested action aborted: local error in processing (Action demandée interrompue : erreur locale en cours de traitement)

Avertissement : une syntaxe incorrecte des codes de réponses SMTP peut provoquer un dysfonctionnement de la protection par mise en liste grise. En conséquence, les messages de courrier indésirable peuvent être remis à des clients ou des messages ne peuvent pas être délivrés du tout.

Durée limite du refus de connexion initial (min) : lorsqu'un message est remis pour la première fois et qu'il est refusé temporairement, ce paramètre définit la période pendant laquelle le message est toujours refusé (mesuré depuis le premier refus). Une fois la période écoulée, le message est reçu correctement. La valeur minimum que vous entrez est de 1 minute.

Durée avant expiration des connexions non vérifiées (heures) : ce paramètre définit l'intervalle minimum pendant lequel les données de triplet sont stockées. Un serveur valide doit renvoyer un message souhaité avant l'expiration de cette période. Cette valeur doit être supérieure à la valeur **Durée limite du refus de connexion initial**.

Durée avant expiration des connexions vérifiées (jours) : nombre minimum de jours pendant lesquels les informations de triplet doivent être stockées et pendant lesquels les messages d'un expéditeur défini sont reçus sans délai. Cette valeur doit être supérieure à la valeur **Durée avant expiration des connexions non vérifiées**.

REMARQUE : vous pouvez également utiliser des variables système lors de la définition de la réponse SMTP de rejet.

3.3.1.2 Connecteur POP3 et protection antispam

Les versions Microsoft Windows Small Business Server (SBS) comprennent un connecteur POP3 qui permet au serveur de récupérer des e-mails depuis des serveurs POP3 externes. L'implémentation de ce connecteur POP3 « standard » diffère d'une version SBS à l'autre.

ESET Mail Security ne prend pas en charge le connecteur POP3 SBS de Microsoft sur SBS 2008. Les messages téléchargés via ce connecteur POP3 sont analysés afin de détecter d'éventuels messages indésirables. Ce mécanisme est basé sur le transport des messages dans Microsoft Exchange via SMTP. Cependant, le connecteur POP3 SBS de Microsoft sur SBS 2003 n'est pas pris en charge par ESET Mail Security. Les messages ne sont donc pas analysés à la recherche de courrier indésirable. Cela est dû au fait que les messages contourne en réalité la file d'attente SMTP.

Il existe également plusieurs connecteurs POP3 de fournisseurs tiers. Le fait que les messages récupérés via un

certain connecteur POP3 soient analysés à la recherche de courrier indésirable dépend de la méthode qu'utilise réellement ce connecteur POP3 pour récupérer les messages. Par exemple, GFI POP2Exchange transporte les messages via Pickup Directory. Ces messages ne sont donc pas analysés dans ce cadre. Des problèmes similaires peuvent survenir avec les produits qui transportent les messages via une session authentifiée (telle que IGetMail). alternativement quand Microsoft Exchange les marques comme messages internes pour lesquels la protection antispam est contournée par défaut. Ce paramètre peut être modifié dans le fichier de configuration. Exportez la configuration au format xml, modifiez la valeur du paramètre `AgentASScanSecureZone` en `"1"` et réimportez la configuration (pour plus de détails sur la procédure d'importation et d'exportation du fichier de configuration, consultez la section Importation et exportation des paramètres 130). Vous pouvez également essayer de désactiver **Accepter l'activation de l'indicateur de contournement d'antispam dans une session SMTP** dans l'arborescence complète (F5), sous **Protection du serveur** > **Protection antispam** > **Serveur Microsoft Exchange** > **Agent de transport**. Après ce paramétrage, ESET Mail Security analysera la session SMTP à la recherche de courrier indésirable, sans tenir compte du paramètre de contournement d'antispam du serveur Exchange.

3.3.2 Moteur de blocage du courrier indésirable

Vous pouvez configurer les paramètres du **moteur de blocage du courrier indésirable**. Pour ce faire, cliquez sur le bouton **Configurer...** La fenêtre qui apparaît permet de configurer ces paramètres du moteur de blocage du courrier indésirable.

Classification des messages

Le moteur du blocage de courrier indésirable ESET Mail Security attribue à chaque message analysé un score de courrier indésirable de 0 à 100. Si vous modifiez les limites des scores de courrier indésirable dans cette section, vous modifiez les éléments suivants :

1) si un message est classé comme courrier indésirable ou non. Tous les messages dont le score de courrier indésirable est supérieur ou égal à la valeur **Score définissant un message comme étant du courrier indésirable** sont considérés comme du courrier indésirable. Par conséquent, les actions définies dans l'agent de transport 38 sont appliquées à ces messages.

2) Si un message est enregistré dans le journal du courrier indésirable 97 (**Outils** > **Fichiers journaux** > **Antispam**). Tous les messages dont le score de courrier indésirable est supérieur ou égal à la valeur **Seuil de score définissant la probabilité qu'un message soit du courrier indésirable ou du courrier souhaité** sont enregistrés par le journal.

3) dans quelle section des statistiques de courrier indésirable le message en question est compté (**État de la protection > Statistiques > Protection antispam du serveur de messagerie**)

Messages évalués comme étant du COURRIER INDÉSIRABLE : le score de courrier indésirable du message est supérieur ou égal à la valeur définie pour **Score définissant un message comme étant du courrier indésirable**

Messages évalués comme étant probablement du COURRIER INDÉSIRABLE : : le score de courrier indésirable du message est supérieur ou égal à la valeur définie pour **Seuil de score définissant la probabilité qu'un message soit du courrier indésirable ou du courrier souhaité**

Messages évalués comme n'étant probablement PAS du COURRIER INDÉSIRABLE : le score de courrier indésirable du message est inférieur à la valeur définie pour **Seuil de score définissant la probabilité qu'un message soit du courrier indésirable ou du courrier souhaité**

Messages évalués comme n'étant PAS du COURRIER INDÉSIRABLE : le score de courrier indésirable du message est inférieur ou égal à la valeur définie pour **Score définissant un message comme n'étant pas du courrier indésirable**

3.3.2.1 Configuration du moteur de blocage du courrier indésirable

3.3.2.1.1 Analyse

Vous pouvez, dans cette section, configurer le mode d'analyse des messages pour la recherche de courrier indésirable, ainsi que leur traitement ultérieur.

Analyser les pièces jointes des messages : cette option permet de choisir si le moteur de blocage du courrier indésirable analyse les pièces jointes et les prend en compte lors du calcul du score de courrier indésirable.

Utiliser les deux sections MIME : le moteur de blocage du courrier indésirable analyse les sections MIME en texte brut et au format HTML d'un message. S'il est nécessaire d'améliorer les performances, il est possible de n'analyser qu'une section. Si cette option est désactivée (coche retirée), une seule section est analysée.

Taille de mémoire pour le calcul de score (octets) : cette option indique au moteur de blocage du courrier indésirable de ne pas lire, dans le tampon de message, plus d'octets que le nombre configurable lors du traitement des règles.

Taille de mémoire pour le calcul d'échantillon (octets) : cette option indique au moteur de blocage du courrier indésirable de ne pas lire plus d'octets que le nombre défini lors du calcul de l'empreinte de message. Cette option est utile pour obtenir des empreintes cohérentes.

Utiliser la mémoire cache LegitRepute : permet d'utiliser un cache LegitRepute pour réduire les faux positifs, en particulier pour les bulletins d'informations.

Convertir en UNICODE : améliore la précision et le résultat des corps de message au format Unicode, notamment dans les langues à double octet, en convertissant les messages en octets simples.

Utiliser la mémoire cache de domaine : permet d'utiliser un cache de réputation de domaine. Si cette option est activée, les domaines sont extraits des messages et comparés au cache de réputation de domaine.

3.3.2.1.1.1 Exemples

Utiliser la mémoire cache : permet d'utiliser un cache d'empreinte (option activée par défaut).

Activer MSF : permet d'utiliser un autre algorithme d'empreinte appelé MSF. Lorsque cette option est activée, vous pouvez définir les limites et les seuils suivants :

- **Nombre de messages correspondant à un message volumineux** : cette option indique le nombre de messages semblables minimum pour que ces messages soient considérés comme un message volumineux.
- **Fréquence de nettoyage de la mémoire cache** : cette option indique une variable interne qui détermine la fréquence de nettoyage du cache MSF en mémoire.
- **Deux exemples correspondant à la sensibilité** : cette option indique le seuil de correspondance (en pourcentage) de deux empreintes. Si le pourcentage de correspondance est supérieur à ce seuil, les messages sont considérés comme étant identiques.
- **Nombre d'exemples stockés en mémoire** : cette option indique le nombre d'empreintes MSF à conserver en mémoire. Plus le nombre est élevé, plus la mémoire est utilisée et plus la précision est fine.

3.3.2.1.1.2 SpamCompiler

Activer SpamCompiler : accélère le traitement des règles, mais nécessite un peu plus de mémoire.

Version préférée : indique la version de SpamCompiler à utiliser. Lorsque cette option est définie sur **Automatique** , le moteur de blocage du courrier indésirable choisit le meilleur moteur à utiliser.

Utiliser la mémoire cache : si cette option est activée, SpamCompiler stocke les données compilée sur le disque au lieu de la mémoire afin de réduire l'utilisation de la mémoire.

Liste des fichiers de mémoire cache : cette option indique quels sont les fichiers de règles compilés sur le disque au lieu de la mémoire.

Définissez les index de fichiers de règles qui seront stockés dans la mémoire cache du disque. Pour gérer les index de fichiers de règles, vous pouvez :

- **Ajouter...**
- **Modifier...**
- **Supprimer**

REMARQUE : les chiffres sont les seules valeurs acceptables.

3.3.2.1.2 Formation

Utiliser la formation pour le score d'empreinte du message : permet d'activer la formation concernant le décalage du score d'empreinte.

Utiliser les mots de formation : cette option indique si l'analyse bayésienne des jetons de mots est utilisée. La précision peut être largement améliorée, mais dans ce cas, la mémoire utilisée est plus importante et les performances sont légèrement plus lentes.

- **Nombre de mots en mémoire cache** : cette option indique le nombre de jetons de mots en cache à tout moment. Plus le nombre est élevé, plus la mémoire est utilisée et plus la précision est fine. Pour saisir le numéro, activez d'abord l'option **Utiliser les mots de formation**.

Utiliser la base de données de formation uniquement pour la lecture : cette option indique si le mot, les règles et les bases de données de formation des empreintes peuvent être modifiés ou s'ils sont en lecture seule après le premier chargement. Une base de données de formation en lecture seule est plus rapide.

- **Sensibilité de formation automatique** : définit un seuil pour l'auto-formation. Si un message obtient un score supérieur ou égal au seuil supérieur, ce message est considéré comme étant un courrier indésirable défini. Il est alors utilisé pour former tous les modules bayésiens activés (règles et/ou mot), mais pas l'expéditeur ou l'empreinte. Si un message obtient un score inférieur ou égal au seuil inférieur, ce message est considéré comme étant un courrier souhaité défini. Il est alors utilisé pour former tous les modules bayésiens activés (règles et/ou mot), mais pas l'expéditeur ou l'empreinte. Pour saisir la valeur des seuils inférieur et supérieur, activez d'abord l'option **Utiliser la base de données de formation uniquement pour la lecture** .

Montant minimum de données de formation : à l'origine, seules les pondérations de règle sont utilisées pour calculer le score de courrier indésirable. Lorsqu'un ensemble minimum de données de formation est obtenu, les données de formation de règle/mot remplacent les pondérations de règles. La valeur minimale par défaut est de 100, ce qui signifie qu'elle doit être formée sur une base équivalant au moins à 100 messages connus comme étant souhaités et à 100 messages de courrier indésirable, pour un total de 200 messages, avant que les données de formation remplacent les pondérations de règles. Si le nombre est trop faible, le résultat risque d'être imprécis, car les données sont insuffisantes. Si le nombre est trop élevé, les données de formation ne sont pas totalement exploitées. Si la valeur est égale à 0, les pondérations de règles sont toujours ignorées.

Utiliser uniquement les données de formation : indique si les données de formation doivent avoir une pondération complète. Si cette option est activée, le calcul de score est uniquement basé sur les données de formation. Si cette option est désactivée (coche retirée), les règles et les données de formation sont utilisées.

Nombre de messages analysés avant leur écriture sur le disque : lors de la formation, le moteur de blocage du courrier indésirable traite une quantité configurable de messages avant l'écriture de la base de données de formation sur le disque. Cette option détermine le nombre de messages à traiter avant l'écriture sur le disque. Pour des performances optimales, ce nombre doit être aussi élevé que possible. Dans le cas improbable où un programme se termine inopinément avant l'écriture du tampon sur le disque, la formation effectuée depuis la dernière écriture sur le disque est perdue. Le tampon est écrit sur le disque lorsque le programme se termine normalement.

Utiliser les données de pays pour la formation : indique si les informations de routage du pays doivent être prises en compte lors de la formation et du calcul de score des messages.

3.3.2.1.3 Règles

Utiliser des règles : cette option indique si les règles heuristiques lentes sont utilisées. La précision peut être largement améliorée, mais la mémoire utilisée devient plus importante et les performances sont beaucoup plus lentes.

- **Utiliser l'extension de l'ensemble de règles** : active l'ensemble de règles étendu.
- **Utiliser l'extension du second ensemble de règles** : active le second ensemble de règles étendu.

Pondération des règles : cette option permet d'ignorer les pondérations associées aux différentes règles.

Liste des fichiers de règles téléchargés : cette option indique quels sont les fichiers de règles téléchargés.

Pondération de catégorie permet à l'utilisateur de régler les pondérations des catégories utilisées dans sc18 et dans les fichiers utilisés dans la liste de règles personnalisées. Catégorie : nom de catégorie, généralement limité à SPAM, PHISH, BOUNCE, ADULT, FRAUD, BLANK, FORWARD et REPLY. Ce champ ne fait pas de distinction entre les majuscules et les minuscules. Score : tout nombre entier ou BLOCK ou APPROVE. La pondération des règles qui correspondent à la catégorie adéquate est multipliée par le facteur de mise à l'échelle pour produire une autre pondération efficace.

Liste des règles personnalisées permet aux utilisateurs d'indiquer une liste de règles personnalisées (courrier indésirable, courrier souhaité ou mots/expressions d'hameçonnage). Les fichiers de règles personnalisées contiennent des expressions au format suivant sur plusieurs lignes : expression, type, probabilité, expression caseSensitivity. Il peut s'agir de n'importe quel texte, à l'exception des virgules. Toutes les virgules dans l'expression doivent être supprimées. Le type peut être SPAM, PHISH, BOUNCE, ADULT ou FRAUD. Si les éléments spécifiés sont différents, la valeur TYPE est automatiquement considérée comme SPAM. La probabilité peut être comprise entre 1 et 100. Si le type est SPAM, la valeur 100 indique une forte probabilité de message indésirable. Si le type est PHISH, la valeur 100 indique une forte probabilité de hameçonnage. Si le type est BOUNCE, la valeur 100 indique une forte probabilité d'expression liée à des réponses automatiques. Plus la probabilité est élevée, plus l'impact sur le score final est important. La valeur de 100 est un cas spécial. Si le type est SPAM, la valeur 100 attribue au message le score de 100. Si le type est PHISH, la valeur 100 attribue au message le score de 100. Si le type est BOUNCE, la valeur 100 attribue au message le score de 100. Comme toujours, toute liste blanche est prioritaire par rapport à toute liste noire. La valeur caseSensitivity de 1 indique que l'expression fait la différence entre les majuscules et les minuscules ; la valeur de 0 indique qu'aucune différence n'est faite entre les majuscules et les minuscules. Exemples :

spamming is fun, SPAM, 100,0
phishing is Phun, PHISH, 90,1
return to sender, BOUNCE, 80,0

La première ligne indique que toutes les variations de « spamming is fun » sont considérées comme courrier indésirable avec une probabilité de 100. L'expression ne fait pas la différence entre les majuscules et les minuscules. La deuxième ligne indique que toutes les variations de « phishing is phun » sont considérées comme un hameçonnage avec une probabilité de 90. L'expression fait la différence entre les majuscules et les minuscules. La troisième ligne indique que toutes les variations de « return to sender » sont considérées comme une réponse automatique avec une probabilité de 80. L'expression ne fait pas la différence entre les majuscules et les minuscules.

Supprimer les anciennes règles après leur mise à jour : le moteur antispam, par défaut, supprime les anciens fichiers de règles du répertoire de configuration lorsqu'un nouveau fichier est récupéré du réseau SpamCatcher. Toutefois, certains utilisateurs du moteur antispam souhaitent archiver les anciens fichiers de règles. Il suffit pour ce faire de désactiver cette fonctionnalité de nettoyage.

Afficher une notification après la mise à jour des règles :

3.3.2.1.3.1 Pondération des règles

Définissez les index de fichiers de règles et leur pondération. Pour ajouter une pondération de règle, cliquez sur **Ajouter**. Pour modifier une pondération existante, cliquez sur **Modifier**. Pour supprimer une adresse, cliquez sur **Supprimer**.

Indiquez les valeurs **Index** et **Pondération** .

3.3.2.1.3.2 Liste des fichiers de règles téléchargés

Définissez les index de fichiers de règles qui doivent être téléchargés sur le disque. Utilisez les boutons **Ajouter**, **Modifier** et **Supprimer** pour gérer les index de fichiers de règles.

3.3.2.1.3.3 Pondération de catégorie

Définissez les catégories de règles et leur pondération. Utilisez les boutons **Ajouter**, **Modifier** et **Supprimer** pour gérer les catégories et leur pondération.

Pour ajouter une pondération de catégorie, cliquez sur **Catégorie** dans la liste. Les options disponibles sont les suivantes :

- **Courrier indésirable**
- **Hameçonnage**
- **Rapport de non-livraison**
- **Messages de contenu ancien**
- **Messages frauduleux**
- **Messages vides**
- **Transfert de messages**
- **Réponse aux messages**

Sélectionnez ensuite une action :

- **Autoriser**
- **Bloquer**
- **Pondération :**

3.3.2.1.3.4 Liste des règles personnalisées

Vous pouvez utiliser des fichiers de règles personnalisées contenant des phrases. D'une manière générale, ce sont des fichiers .txt. Pour connaître leurs caractéristiques et le format des phrases, veuillez consulter le sujet Règles 43 (section **Liste de règles personnalisées**).

Pour utiliser des fichiers contenant les règles personnalisées qui seront utilisées pour l'analyse des messages, ces fichiers doivent se trouver à l'emplacement suivant :

si vous exécutez Windows Server 2008 et versions ultérieures, le chemin d'accès est :
C:\ProgramData\ESET\ESET Mail Security\ServerAntispam

si vous utilisez Windows Server 2003 et versions ultérieures, le chemin d'accès est :
C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\ServerAntispam

Pour charger les fichiers, cliquez sur le bouton **...** (parcourir), accédez à l'emplacement mentionné ci-dessus et sélectionnez un fichier texte (*.txt). Utilisez les boutons **Ajouter**, **Modifier** et **Supprimer** pour gérer la liste des règles personnalisées.

REMARQUE : Le fichier .txt contenant les règles personnalisées doit être placé dans le dossier *ServerAntispam*, sans quoi ce fichier ne sera pas chargé.

3.3.2.1.4 Filtrage

Dans cette section, vous pouvez configurer les listes autorisées, bloquées et ignorées en indiquant des critères tels que l'adresse IP ou la plage d'adresses IP, le nom du domaine, l'adresse électronique, etc. Pour ajouter, modifier ou supprimer des critères, il vous suffit d'accéder à la liste que vous souhaitez gérer en cliquant sur le bouton approprié.

3.3.2.1.4.1 Expéditeurs autorisés

Les expéditeurs et les domaines figurant sur une liste blanche peuvent contenir une adresse électronique ou un domaine. Les adresses sont saisies au format « boîte aux lettres@domaine » et les domaines au format « domaine ».

REMARQUE : Les espaces à gauche et à droite sont ignorés ; les expressions régulières ne sont pas prises en charge et l'astérisque (*) est également ignoré.

3.3.2.1.4.2 Expéditeurs bloqués

Les expéditeurs et les domaines figurant sur une liste noire peuvent contenir une adresse électronique ou un domaine. Les adresses sont saisies au format « boîte aux lettres@domaine » et les domaines au format « domaine ».

REMARQUE : Les espaces à gauche et à droite sont ignorés ; les expressions régulières ne sont pas prises en charge et l'astérisque (*) est également ignoré.

3.3.2.1.4.3 Adresses IP autorisées

Cette option permet d'indiquer les adresses IP qui doivent être approuvées. Les plages peuvent être indiquées de trois manières :

a) adresse IP de début - adresse IP de fin
b) Adresse IP et masque réseau
c) Adresse IP

Si les premières adresses IP non ignorées figurant dans l'en-tête Reçu : correspondent à celles figurant dans la liste, le message a le score de 0 et aucune autre vérification n'est effectuée.

3.3.2.1.4.4 Adresses IP ignorées

Cette option permet d'indiquer les adresses IP qui doivent être ignorées lors des vérifications RBL. Les options suivantes sont toujours ignorées implicitement :

10.0.0.0/8, 127.0.0.0/8, 192.168.0.0/16, 172.16.0.0

Les plages peuvent être indiquées de trois manières :

a) Adresse IP de début - adresse IP de fin
b) Adresse IP et masque réseau
c) Adresse IP

3.3.2.1.4.5 Adresses IP bloquées

Cette option permet d'indiquer les adresses IP qui doivent être bloquées. Les plages peuvent être indiquées de trois manières :

a) adresse IP de début - adresse IP de fin
b) Adresse IP et masque réseau
c) Adresse IP

Si des adresses IP figurant dans l'en-tête Reçu : correspondent à celles figurant dans la liste, le message a le score de 100 et aucune autre vérification n'est effectuée.

3.3.2.1.4.6 Domaines autorisés

Cette option permet d'indiquer les adresses IP et les domaines, dans le corps des messages, qui doivent toujours être approuvés.

3.3.2.1.4.7 Domaines ignorés

Cette option permet d'indiquer les domaines, dans le corps des messages, qui doivent toujours être exclus des vérifications DNSBL et ignorés.

3.3.2.1.4.8 Domaines bloqués

Cette option permet d'indiquer les adresses IP et les domaines, dans le corps des messages, qui doivent toujours être bloqués.

3.3.2.1.4.9 Expéditeurs usurpés

Permet de bloquer les spammeurs qui usurpent le nom de votre domaine et d'autres noms de domaine. Par exemple, les spammeurs utilisent souvent le nom de domaine du destinataire tel qu'il est indiqué dans le nom de domaine De . Cette liste permet d'indiquer les serveurs de messagerie autorisés à utiliser les noms de domaine de l'adresse De .

3.3.2.1.5 Vérification

La vérification est une fonction supplémentaire de la protection antispam. Elle permet de vérifier les messages par l'intermédiaire de serveurs externes en fonction des critères définis. Choisissez une liste de l'arborescence pour configurer ses critères. Les listes sont les suivantes :

- **RBL** (Realtime Blackhole List)
- **LBL** (Last Blackhole List)
- **DNSBL** (DNS Blocklist)

3.3.2.1.5.1 RBL (Realtime Blackhole List)

Serveurs RBL : indique la liste des serveurs RBL (Realtime Blackhole List) à interroger lors de l'analyse des messages. Reportez-vous à la section RBL de ce document pour plus d'informations.

Sensibilité de vérification RBL : les vérifications RBL pouvant réduire et ralentir les performances, cette option permet de vérifier les RBL de manière conditionnelle, en fonction du score établi avant ces vérifications RBL. si le score est supérieur à la valeur « élevée », seuls les serveurs RBL pouvant indiquer un score inférieur à cette valeur sont interrogés. Si le score est inférieur à la valeur « faible », seuls les serveurs RBL pouvant indiquer un score supérieur à cette valeur sont interrogés. Si le score est compris entre les valeurs « faible » et « élevée », tous les serveurs RBL sont interrogés.

Limite d'exécution de requête RBL (en secondes) : cette option permet de définir un délai maximum pour la finalisation de toutes les interrogations RBL. Les réponses RBL utilisées sont celles qui proviennent exclusivement des serveurs RBL qui ont répondu dans les temps. Si la valeur est 0, aucun délai n'est imposé.

Nombre maximum de domaines vérifiés par rapport à RBL : cette option permet de limiter le nombre d'adresses IP qui sont interrogées sur le serveur RBL. Notez que le nombre total d'interrogations RBL correspond au nombre d'adresses IP figurant dans les en-têtes Reçu (jusqu'à un maximum d'adresses IP maxcheck RBL) multiplié par le nombre de serveurs RBL indiqués dans la liste RBL. Si la valeur est 0, un nombre illimité d'en-têtes reçus est vérifié. Notez que les adresses IP figurant dans la liste des adresses IP ignorées ne sont pas prises en compte dans la limite des adresses IP RBL.

Pour gérer la liste, utilisez les boutons **Ajouter**, **Modifier** ou **Supprimer**.

La liste se compose de trois colonnes :

Adresse
Réponse
Score

3.3.2.1.5.2 LBL (Last Blackhole List)

Serveurs LBL : la dernière adresse IP de connexion est interrogée sur le serveur LBL. Vous pouvez indiquer une autre recherche DNS pour la dernière adresse IP entrante de connexion. Pour la dernière adresse IP entrante de connexion, la liste interrogée est la liste LBL au lieu de la liste RBL. Dans le cas contraire, les options de la liste RBL, telles que le seuil RBL, sont également appliquées à la liste LBL.

Adresses IP non vérifiées par rapport à la liste LBL : si la dernière adresse IP de connexion correspond à une adresse IP de la liste, elle est interrogée sur le ou les serveurs RBL et non sur le ou les serveurs LBL.

Pour gérer la liste, utilisez les boutons **Ajouter**, **Modifier** ou **Supprimer**.

La liste se compose de trois colonnes :

Adresse
Réponse
Score

Vous pouvez indiquer les adresses IP qui ne seront pas vérifiées par rapport à la liste LBL. Pour gérer la liste, utilisez les boutons **Ajouter**, **Modifier** ou **Supprimer**.

3.3.2.1.5.3 DNSBL (DNS Block List)

Serveurs DNSBL : : indique la liste des serveurs DNSBL (DNS Blocklist) à interroger, avec les domaines et les adresses IP extraits du corps du message.

Sensibilité de vérification DNSBL : si le score est supérieur à la valeur « élevée », seuls les serveurs DNSBL pouvant abaisser le score en dessous de cette valeur sont interrogés. Si le score est inférieur à la valeur « faible », seuls les serveurs DNSBL pouvant remonter le score au-dessus de cette valeur sont interrogés. Si le score est compris entre les valeurs « faible » et « élevée », tous les serveurs DNSBL sont interrogés.

Limite d'exécution de requête DNSBL (en secondes) : permet de définir un délai maximum pour la finalisation de toutes les interrogations DNSBL.

Nombre maximum de domaines vérifiés par rapport à DNSBL : permet de limiter le nombre de domaines et d'adresses IP qui sont interrogés sur le serveur DNSBL.

Pour gérer la liste, utilisez les boutons **Ajouter**, **Modifier** ou **Supprimer**.

La liste se compose de trois colonnes :

Adresse
Réponse
Score

3.3.2.1.6 DNS

Utiliser la mémoire cache : permet la mise en cache interne des requêtes DNS.

Nombre de requêtes DNS stockées en mémoire : limite le nombre d'entrées dans le cache DNS interne.

Enregistrer la mémoire cache sur le disque : si cette option est activée, le cache DNS stocke les entrées sur le disque lors de l'arrêt et lit les informations sur le disque à l'initialisation.

Adresse du serveur DNS : les serveurs DNS peuvent désormais être indiqués spécifiquement pour ignorer la valeur par défaut.

Accès DNS direct : lorsque cette option est activée et qu'aucun serveur DNS n'est indiqué, le moteur de blocage du courrier indésirable envoie des requêtes LiveFeed directement aux serveurs LiveFeed. Cette option est ignorée si le serveur DNS est indiqué, car il est prioritaire. Cette option doit être définie sur **Oui** lorsque les interrogations

directes sont plus efficaces que les serveurs DNS par défaut.

Durée de vie de la requête DNS (en secondes) : cette option permet de paramétrer une valeur TTL minimale pour les entrées du cache DNS interne du moteur de blocage du courrier indésirable. Cette option est indiquée en secondes. Pour les réponses DNS dont la valeur TTL est inférieure à la valeur TTL minimale indiquée, le cache interne du moteur de blocage du courrier indésirable utilise la valeur TTL indiquée au lieu de celle de la réponse DNS.

3.3.2.1.7 Score

Activer l'historique du score : active le suivi des scores historiques pour les expéditeurs récurrents.

Arrêter l'analyse lorsque le seuil de score de courrier indésirable est atteint : cette option permet d'indiquer au moteur de blocage du courrier indésirable d'arrêter l'analyse du message lorsque ce score a été atteint Ce procédé peut réduire le nombre de règles et d'autres vérifications et, par conséquent, améliore le résultat.

Utiliser l'analyse accélérée avant que le score de seuil de message souhaité soit atteint : cette option permet d'indiquer au moteur de blocage du courrier indésirable d'ignorer les lentes vérifications de règles si le message est probablement souhaité.

Classification des messages

- **Valeur de score à partir de laquelle un message est considéré comme courrier indésirable** : le moteur de blocage du courrier indésirable attribue à un message analysé un score compris entre 0 et 100. La définition des valeurs limites de score a une incidence sur les messages qui sont considérés comme courrier indésirable et sur ceux évalués comme messages souhaités. Si ces valeurs ne sont pas définies correctement, les résultats de la détection du moteur antispam risquent de perdre en qualité.
- **Valeur de score qui définit la limite entre un message considéré comme courrier probablement indésirable ou probablement souhaité** : le moteur de blocage du courrier indésirable attribue à un message analysé un score compris entre 0 et 100. La définition des valeurs limites de score a une incidence sur les messages qui sont considérés comme courrier indésirable et sur ceux évalués comme messages souhaités. Si ces valeurs ne sont pas définies correctement, les résultats de la détection du moteur antispam risquent de perdre en qualité.
- **Valeur de score jusqu'à laquelle un message est considéré comme certainement souhaité** : le moteur de blocage du courrier indésirable attribue à un message analysé un score compris entre 0 et 100. La définition des valeurs limites de score a une incidence sur les messages qui sont considérés comme courrier indésirable et sur ceux évalués comme messages souhaités. Si ces valeurs ne sont pas définies correctement, les résultats de la détection du moteur antispam risquent de perdre en qualité.

3.3.2.1.8 Spambait

Adresse de courrier indésirable : si l'adresse du destinataire figurant sur l'enveloppe SMTP correspond à une adresse électronique de cette liste, le fichier de statistiques enregistre les jetons dans le message envoyé à une adresse Spambait. Les adresses doivent correspondre exactement, mais l'utilisation des majuscules et des minuscules n'a pas d'importance. Par ailleurs, les caractères génériques ne sont pas pris en charge.

Adresses considérées comme inexistantes : si l'adresse du destinataire figurant sur l'enveloppe SMTP correspond à une adresse électronique de cette liste, le fichier de statistiques enregistre les jetons dans le message envoyé à une adresse inexistante. Les adresses doivent correspondre exactement, mais l'utilisation des majuscules et des minuscules n'a pas d'importance. Par ailleurs, les caractères génériques ne sont pas pris en charge.

3.3.2.1.8.1 Adresses Spambait

Vous pouvez définir des adresses électroniques qui ne reçoivent que du courrier indésirable. Pour ajouter une adresse électronique, saisissez-la au format standard et cliquez sur le bouton **Ajouter**. Pour modifier une adresse existante, utilisez le bouton **Modifier**. Pour supprimer une adresse, cliquez sur **Supprimer**.

3.3.2.1.8.2 Adresses considérées comme inexistantes

Vous pouvez définir des adresses électroniques qui apparaissent comme étant inexistantes à l'extérieur. Pour ajouter une adresse électronique, saisissez-la au format standard et cliquez sur le bouton **Ajouter**. Pour modifier une adresse existante, utilisez le bouton **Modifier**. Pour supprimer une adresse, cliquez sur **Supprimer**.

3.3.2.1.9 Communication

Durée d'une seule requête SpamLabs (en secondes) : limite la durée d'une requête vers la protection antispam SpamLabs. La valeur est indiquée en unités de secondes complètes. La valeur 0 désactive cette fonctionnalité et aucune limite n'est définie.

Utiliser le protocole v.4x : communique avec la protection antispam SpamLabs pour déterminer le score par l'intermédiaire de l'ancien protocole v4.x, plus lent. Lorsque vous définissez cette option sur **Automatiquement**, le moteur de blocage du courrier indésirable utilise automatiquement la fonction netcheck comme solution de secours pour les interrogations LiveFeed.

- **Plage d'utilisation du protocole v4.x** : les réseaux pouvant réduire et ralentir les performances, cette option permet de vérifier le réseau de manière conditionnelle, en fonction du score. Le réseau n'est interrogé que si le score est compris entre les valeurs « faible » et « élevée » spécifiées dans cette option.

Adresse de serveur LiveFeed : indique le serveur à interroger pour les requêtes LiveFeed.

Durée de vie de requête LiveFeed (en secondes) : cette option permet de paramétrer une valeur TTL minimale pour les entrées du cache LiveFeed interne du moteur de blocage du courrier indésirable. Cette option est indiquée en secondes. Pour les réponses LiveFeed dont la valeur TTL est inférieure à la valeur TTL minimale indiquée, le cache interne du moteur de blocage du courrier indésirable utilise la valeur TTL indiquée au lieu de celle de la réponse LiveFeed.

Type d'authentification du serveur proxy : indique le type d'authentification de proxy HTTP à utiliser.

3.3.2.1.10 Performances

Taille maximale de la pile de threads utilisée : définit la taille maximale de la pile de threads. Si la taille de pile de threads est définie sur 64 Ko, cette variable doit être définie sur 100 ou sur une valeur inférieure. Si la taille de pile de threads est définie sur une valeur supérieure à 1 Mo, cette variable doit être définie sur 10 000 ou sur une valeur inférieure. Si cette variable est définie sur une valeur inférieure à 200, la précision peut être réduire de quelques pourcentages.

Résultats souhaités (en messages par seconde) : cette option permet d'indiquer les résultats souhaités en messages par seconde. Le moteur antispam essaie d'atteindre ce niveau en optimisant les règles exécutées. Il est possible que la précision soit réduite. La valeur 0 désactive l'option.

Joindre les fichiers incrémentiels en un seul fichier : le moteur antispam, par défaut, fusionne plusieurs fichiers incrémentiels dans un seul fichier complet et mis à jour. Cela permet de réduire les encombrements de fichiers dans le répertoire de configuration.

Télécharger uniquement les fichiers incrémentiels : le moteur antispam, par défaut, essaie de télécharger la combinaison fichier complet/fichier incrémentiel la plus pertinente en fonction du volume. Le moteur antispam peut être forcé de ne télécharger que le fichier incrémentiel si cette option est définie sur Oui.

Taille maximale des fichiers incrémentiels : afin de réduire l'utilisation du processeur lors de la mise à jour des fichiers de règles, les fichiers de mise en cache sur disque (sc*.tmp) ne sont plus régénérés à chaque mise) jour de règle. Ils sont en fait régénérés si un fichier sc*.bin.full plus récent est détecté ou si le total cumulé du fichier sc*.bin. incr est supérieur au nombre d'octets indiqués pour la taille maximale des fichiers incrémentiels.

Emplacement des fichiers temporaires : ce paramètre contrôle l'emplacement de création des fichiers temporaires par le moteur antispam.

3.3.2.1.11 Paramètres régionaux

Liste des langues privilégiées : cette option vous permet de définir les langues privilégiées dans vos e-mails. Les codes de pays sont des codes de langue ISO-639 sur deux caractères.

Liste des pays privilégiés : cette option permet d'indiquer la liste des pays considérés comme pays « privilégiés ». Les messages acheminés par l'intermédiaire d'un pays qui ne figure pas dans cette liste sont évalués de manière plus sévère. Si cette option est vide, aucune pénalité n'est affectée.

Liste des pays bloqués : permet le blocage par pays. Si une adresse IP figurant dans un en-tête reçu correspond à un pays figurant dans la liste, l'e-mail est considéré comme courrier indésirable. Les codes de pays ne sont pas appliqué aux adresses des expéditeurs. Notez qu'il est possible qu'un message passe par plusieurs pays avant d'atteindre sa destination finale. Cette option n'est pertinente qu'à 98 %. Le blocage des pays peuvent donc générer des faux positifs.

Liste des jeux de caractères bloqués : permet le blocage par jeu de caractères. La valeur de score de courrier indésirable par défaut est de 100, mais vous pouvez la régler séparément pour chaque jeu de caractères bloqué. L'association langue-jeu de caractères n'est pas pertinente à 100 %. Le blocage des jeux de caractères peut donc générer des faux positifs.

3.3.2.1.11.1 Liste des langues privilégiées

Définissez les langues que vous considérez comme des langues privilégiées et dans lesquelles vous préférez recevoir des messages. Pour ajouter une langue privilégiée, sélectionnez-la dans la colonne **Codes de langue** et cliquez sur le bouton **Ajouter**. La langue est placée dans la colonne des **langues privilégiées**. Pour supprimer la langue de la colonne des **langues privilégiées**, sélectionnez son code et cliquez sur le bouton **Supprimer**.

Bloquer les langues non privilégiées : cette option indique si les langues, qui ne sont pas répertoriées dans la colonne des langues privilégiées, seront bloquées. Trois options sont possibles :

- **Oui**
- **Non**
- **Automatiquement**

Liste des codes de langue (en fonction de la norme ISO 639) :

Afrikaans	af
Amharique	am
Arabe	ar
Biélorusse	be
Bulgare	bg
Catalan	ca
Tchèque	cs
Gallois	cy
Danois	da
Allemand	de
Grec	el
Anglais	en
Espéranto	eo
Espagnol	es
Estonien	et
Basque	eu
Perse	fa
Finnois	fi
Français	fr
Frison	fy
Irlandais	ga
Gaélique	gd
Hébreu	he
Hindi	hi
Croate	hr
Hongrois	hu
Arménien	hy
Indonésien	id

Islandais	est
Italien	it
Japonais	ja
Géorgien	ka
Coréen	ko
Latin	la
Lituanien	lt
Letton	lv
Marathi	mr
Malais	ms
Népali	ne
Néerlandais	nl
Norvégien	non
Polonais	pl
Portugais	pt
Quéchua	qu
Rhéto-roman	rm
Roumain	ro
Russe	ru
Sanskrit	sa
Écossais	sco
Slovaque	sk
Slovène	sl
Albanais	sq
Serbe	sr
Suédois	sv
Swahili	sw
Tamoul	ta
Thaï	th
Tagalog	tl
Turc	tr
Ukrainien	uk
Vietnamien	vi
Yiddish	yi
Chinois	zh

3.3.2.1.11.2 Liste des pays privilégiés

Définissez les pays que vous considérez comme des pays privilégiés et desquels vous préférez recevoir des messages. Pour ajouter un pays privilégié, sélectionnez-le dans la colonne **Codes de pays** et cliquez sur le bouton **Ajouter**. Le pays est placé dans la colonne des **pays privilégiés**. Pour supprimer le pays de la colonne des **pays privilégiés**, sélectionnez son code et cliquez sur le bouton **Supprimer**.

Liste des codes de pays (en fonction de la norme ISO 3166) :

AFGHANISTAN	AF
ÎLES D'ÅLAND	AX
ALBANIE	AL
ALGÉRIE	DZ
SAMOA AMÉRICAINES	AS
ANDORRE	AD
ANGOLA	AO
ANGUILLA	AI
ANTARCTIQUE	AQ
ANTIGUA ET BARBUDA	AG
ARGENTINE	AR
ARMÉNIE	AM
ARUBA	AW
AUSTRALIE	AU
AUTRICHE	AT
AZERBAÏDJAN	AZ
BAHAMAS	BS
BAHREÏN	BH
BANGLADESH	BD

BARBADE	BB
BÉLARUS	BY
BELGIQUE	BE
BELIZE	BZ
BÉNIN	BJ
BERMUDES	BM
BHOUTAN	BT
BOLIVIE	BO
BOSNIE-HERZÉGOVINE	BA
BOTSWANA	BW
ÎLE BOUVET	BV
BRÉSIL	BR
TERRITOIRE BRITANNIQUE DE L'OCÉAN INDIEN	IO
BRUNEI DARUSSALAM	BN
BULGARIE	BG
BURKINA FASO	BF
BURUNDI	BI
CAMBODGE	KH
CAMEROUN	CM
CANADA	CA
CAP-VERT	CV
ÎLES CAÏMANS	KY
RÉPUBLIQUE CENTRAFRICAINE	CF
TCHAD	TD
CHILI	CL
CHINE	CN
ÎLE CHRISTMAS	CX
ÎLES COCOS	CC
COLOMBIE	CO
ÎLES COMORES	KM
CONGO	CG
CONGO, RÉPUBLIQUE DÉMOCRATIQUE	CD
ÎLES COOK	CK
COSTA RICA	CR
CÔTE D'IVOIRE	CI
CROATIE	HR
CUBA	CU
CHYPRE	CY
RÉPUBLIQUE TCHÈQUE	CZ
DANEMARK	DK
DJIBOUTI	DJ
DOMINIQUE	DM
RÉPUBLIQUE DOMINICAINE	DO
ÉQUATEUR	EC
ÉGYPTE	EG
EL SALVADOR	SV
GUINÉE ÉQUATORIALE	GQ
ÉRYTHRÉE	ER
ESTONIE	EE
ÉTHIOPIE	ET
ÎLES MALOUINES	FK
ÎLES FÉROÉ	FO
FIDJI	FJ
FINLANDE	FI
FRANCE	FR
GUYANE FRANÇAISE	GF
POLYNÉSIE FRANÇAISE	PF
TERRES AUSTRALES FRANÇAISES	TF
GABON	GA
GAMBIE	GM
GÉORGIE	GE

ALLEMAGNE	DE
GHANA	GH
GIBRALTAR	GI
GRÈCE	GR
GROENLAND	GL
GRENADE	GD
GUADELOUPE	GP
GUAM	GU
GUATEMALA	GT
GUINÉE	GN
GUINÉE-BISSAU	GW
GUYANA	GY
HAÏTI	HT
ÎLES HEARD ET MCDONALD	HM
SAINT-SIÈGE (CITÉ DU VATICAN)	VA
HONDURAS	HN
HONG KONG	HK
HONGRIE	HU
ISLANDE	IS
INDE	IN
INDONÉSIE	Identificateur (ID)
IRAN, RÉPUBLIQUE ISLAMIQUE	IR
IRAQ	IQ
IRLANDE	IE
ISRAËL	IL
ITALIE	IT
JAMAÏQUE	JM
JAPON	JP
JORDANIE	JO
KAZAKHSTAN	KZ
KENYA	KE
KIRIBATI	KI
CORÉE, RÉPUBLIQUE POPULAIRE DÉMOCRATIQUE	KP
CORÉE, RÉPUBLIQUE	KR
KOWEÏT	KW
KIRGHIZISTAN	KG
LAOS, RÉPUBLIQUE POPULAIRE DÉMOCRATIQUE	LA
LETTONIE	LV
LIBAN	LB
LESOTHO	LS
LIBÉRIA	LR
LIBYE	LY
LIECHTENSTEIN	LI
LITUANIE	LT
LUXEMBOURG	LU
MACAO	MO
MACÉDOINE, ANCIENNE RÉPUBLIQUE DE YOUGOSLAVIE	MK
MADAGASCAR	MG
MALAWI	MW
MALAISIE	MY
MALDIVES	MV
MALI	ML
MALTE	MT
ÎLES MARSHALL	MH
MARTINIQUE	MQ
MAURITANIE	MR
MAURICE	MU
MAYOTTE	YT
MEXIQUE	MX

MICRONÉSIE, ÉTATS FÉDÉRÉS	FM
MOLDAVIE, RÉPUBLIQUE	MD
MONACO	MC
MONGOLIE	MN
MONTSERRAT	MS
MAROC	MA
MOZAMBIQUE	MZ
MYANMAR	MM
NAMIBIE	NA
NAURU	NR
NÉPAL	NP
PAYS-BAS	NL
ANTILLES NÉERLANDAISES	AN
NOUVELLE-CALÉDONIE	NC
NOUVELLE-ZÉLANDE	NZ
NICARAGUA	NI
NIGER	NE
NIGERIA	NG
NIOUÉ	NU
ÎLE NORFOLK	NF
ÎLES MARIANNES DU NORD	MP
NORVÈGE	NO
OMAN	OM
PAKISTAN	PK
PALAOS	PW
TERRITOIRES PALESTINIENS OCCUPÉS	PS
PANAMA	PA
PAPOUASIE-NOUVELLE-GUINÉE	PG
PARAGUAY	PY
PÉROU	PE
PHILIPPINES	PH
PITCAIRN	PN
POLOGNE	PL
PORTUGAL	PT
PUERTO RICO	PR
QATAR	QA
RÉUNION	RE
ROUMANIE	RO
FÉDÉRATION DE RUSSIE	RU
RWANDA	RW
SAINTE-HÉLÈNE	SH
SAINT-KITTS-ET-NEVIS	KN
SAINTE-LUCIE	LC
SAINT-PIERRE ET MIQUELON	PM
SAINT-VINCENT-ET-LES GRENADINES	VC
SAMOA	WS
SAINT-MARIN	SM
SAO TOMÉ-ET-PRINCIPE	ST
ARABIE SAOUDITE	SA
SÉNÉGAL	SN
SERBIE-MONTÉNÉGRO	CS
SEYCHELLES	SC
SIERRA LEONE	SL
SINGAPOUR	SG
SLOVAQUIE	SK
SLOVÉNIE	SI
ÎLES SALOMON	SB
SOMALIE	SO
AFRIQUE DU SUD	ZA
GÉORGIE DU SUD ET ÎLES SANDWICH DU SUD	GS
ESPAGNE	ES

SRI LANKA	LK
SOUDAN	SD
SURINAME	SR
SVALBARD ET ÎLE DE JAN MAYEN	SJ
SWAZILAND	SZ
SUÈDE	SE
SUISSE	CH
RÉPUBLIQUE ARABE SYRIENNE	SY
TAÏWAN, PROVINCE DE CHINE	TW
TADJIKISTAN	TJ
TANZANIE, RÉPUBLIQUE UNIE	TZ
THAÏLANDE	TH
TIMOR-ORIENTAL	TL
TOGO	TG
TOKELAU	TK
TONGA	TO
TRINITÉ-ET-TOBAGO	TT
TUNISIE	TN
TURQUIE	TR
TURKMÉNISTAN	TM
ÎLES TURKS ET CAICOS	TC
TUVALU	TV
OUGANDA	UG
UKRAINE	UA
ÉMIRATS ARABES UNIS	AE
ROYAUME-UNI	Go
ÉTATS-UNIS	US
ÎLES MINEURES ÉLOIGNÉES DES ÉTATS-UNIS	UM
URUGUAY	UY
OUZBÉKISTAN	UZ
VANUATU	VU
CITÉ DU VATICAN (SAINT-SIÈGE)	VA
VENEZUELA	VE
VIETNAM	VN
ÎLES VIERGES BRITANNIQUES	VG
ÎLES VIERGES AMÉRICAINES	VI
WALLIS-ET-FUTUNA	WF
RÉPUBLIQUE ARABE SAHRAOUIE DÉMOCRATIQUE	EH
YÉMEN	YE
ZAÏRE (RÉPUBLIQUE DÉMOCRATIQUE DU CONGO)	CD
ZAMBIE	ZM
ZIMBABWE	ZW

3.3.2.1.11.3 Liste des pays bloqués

Définissez les pays que vous souhaitez bloquer et desquels vous ne souhaitez pas recevoir de messages. Pour ajouter un pays à la liste **Pays bloqués**, sélectionnez-le dans la colonne **Codes de pays** et cliquez sur le bouton **Ajouter**. Pour supprimer un pays de la liste **Pays bloqués**, sélectionnez le code du pays et cliquez sur le bouton **Supprimer**.

Pour obtenir la liste des codes de pays, consultez la rubrique Liste des pays privilégiés 51.

3.3.2.1.11.4 Liste des jeux de caractères bloqués

Définissez les jeux de caractères que vous souhaitez bloquer. Les messages rédigés dans ces jeux de caractères ne seront pas reçus. Pour ajouter un jeu de caractères, sélectionnez-le dans la colonne **Jeux de caractères** et cliquez sur le bouton **Ajouter**. Le jeu de caractères est placé dans la colonne **Jeux de caractères bloqués** . Pour supprimer le jeu de caractères de la colonne **Jeux de caractères bloqués**, sélectionnez le code du jeu de caractères et cliquez sur le bouton **Supprimer**.

Lorsque vous ajoutez un jeu de caractères à des jeux de caractères bloqués, vous pouvez indiquer votre propre valeur de score de courrier indésirable pour ce jeu de caractères particulier. La valeur par défaut est de 100. Vous pouvez définir le score de chaque jeu de caractères séparément.

3.3.2.1.12 Fichiers journaux

Activer la journalisation détaillée : active la journalisation détaillée.

Nouveau routage des fichiers de résultats : redirige le fichier de résultats vers le répertoire indiqué dans ce champ. Cliquez sur le bouton **...** pour parcourir les répertoires au lieu de saisir le chemin manuellement.

3.3.2.1.13 Statistiques

Activer la journalisation des données statistiques : journalise les adresses IP, les domaines, les adresses URL, les mots suspects, etc. dans le système de fichiers configurés. Les journaux peuvent être téléchargés automatiquement sur les serveurs d'analyse du moteur de blocage du courrier indésirable. Les journaux peuvent être convertis en texte brut pour l'affichage.

- **Envoyer des données statistiques pour l'analyse** : lance une thread pour télécharger automatiquement les fichiers statistiques sur les serveurs d'analyse du moteur de blocage du courrier indésirable.
- **Adresse de serveur d'analyse** : adresse URL vers laquelle les fichiers statistiques sont téléchargés.

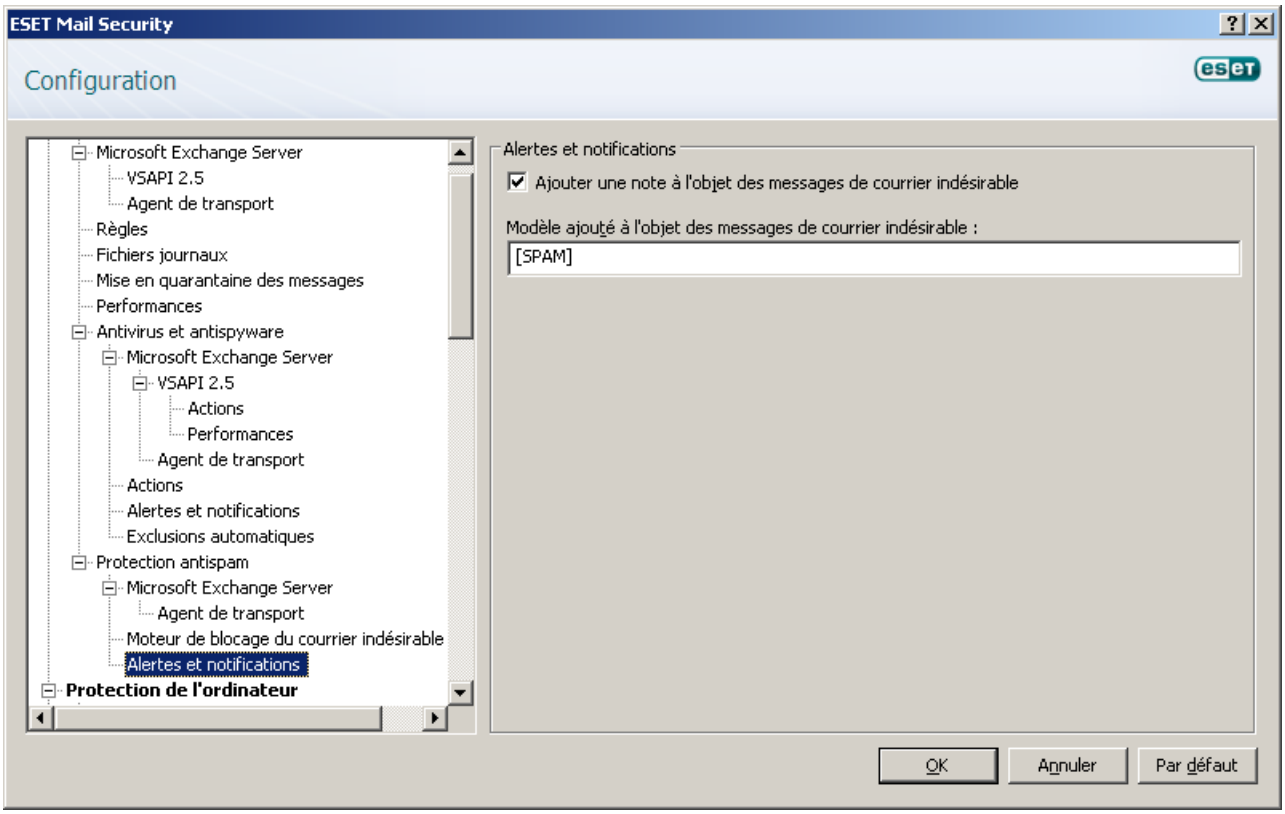
3.3.2.1.14 Options

Configuration automatique : définit les options sur la base des exigences indiquées par l'utilisateur en matière de performances, de ressources et de système.

Créer un fichier de configuration : crée le fichier *antispam.cfg* qui contient la configuration du moteur antispam. Il est stocké dans *C:\ProgramData\ESET\ESET Mail Security\ServerAntispam* (Windows Server 2008) ou *C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\ServerAntispam* (Windows Server 2000 et 2003).

3.3.3 Alertes et notifications

Chaque courrier analysé par ESET Mail Security et marqué comme courrier indésirable peut être marqué par l'ajout d'une notification à l'objet du message. Par défaut, la notification est [*SPAM*], mais il peut également s'agir d'une chaîne définie par l'utilisateur.



REMARQUE : vous pouvez également utiliser des variables système lors de l'ajout d'un modèle à l'objet du message.

3.4 FAQ

Q : après l'installation d'EMSX avec protection antispam, les messages ne sont plus remis dans les boîtes aux lettres.

R : si l'option de mise en liste grise est activée, ce comportement est normal. Dans les premières heures de fonctionnement, les messages peuvent arriver avec plusieurs heures de retard. Si le problème persiste, il est recommandé de désactiver (ou de reconfigurer) la liste grise.

Q : lorsque VSAPI analyse les pièces jointes, analyse-t-il également le corps des messages ?

R : dans Microsoft Exchange Server 2000 SP2 et les versions ultérieures, VSAPI analyse également les corps des messages.

Q : pourquoi l'analyse des messages continue-t-elle lorsque l'option VSAPI est désactivée ?

R : les modifications apportées aux paramètres VSAPI s'effectuent de manière asynchrone, ce qui signifie que les paramètres VSAPI modifiés doivent être appelés par le serveur Microsoft Exchange Server pour entrer en vigueur. Ce cycle s'exécute à des intervalles d'environ une minute. C'est le cas également de tous les autres paramètres VSAPI.

Q : l'interface VSAPI peut-elle supprimer un message complet contenant une pièce jointe infectée ?

R : oui, VSAPI peut supprimer l'intégralité du message. Il est néanmoins nécessaire de sélectionner d'abord l'option **Supprimer l'intégralité du message** dans la section **Actions** section des paramètres VSAPI. cette option est disponible dans Microsoft Exchange Server 2003 et les versions ultérieures. Les anciennes versions de Microsoft

Exchange Server ne prennent pas en charge la suppression des messages dans leur intégralité.

Q : les messages sortants font-ils également l'objet d'une analyse antivirus par VSAPI ?

R : oui, VSAPI analyse les messages sortants, à moins que vous n'ayez configuré dans votre client de messagerie un serveur SMTP différent du serveur Microsoft Exchange Server. Cette fonctionnalité s'applique dans Microsoft Exchange Server 2000 Service Pack 3 et les versions ultérieures.

Q : est-il possible d'ajouter un texte de notification par VSAPI à chaque message analysé, de la même manière qu'avec l'agent de transport ?

R : l'ajout de texte à des messages analysés par VSAPI n'est pas pris en charge dans Microsoft Exchange Server.

Q : il m'arrive parfois de ne pas pouvoir ouvrir un message dans Microsoft Outlook. Pourquoi ?

R : L'option Action à entreprendre si le nettoyage n'est pas possible dans les paramètres VSAPI de la section **Actions** est définie vraisemblablement sur **Bloquer** ou vous avez créé une règle qui comprend l'action **Bloquer**. L'un de ces paramètres marque et bloque les messages infectés et/ou les messages correspondant à la règle mentionnée ci-dessus.

Q : à quoi sert l'option **Limite du temps de réponse** de la section **Performances** ?

R : si vous utilisez Microsoft Exchange Server 2000 SP2 ou une version ultérieure, la valeur **Limite du temps de réponse** représente la durée maximum en secondes nécessaire à l'analyse par VSAPI d'une thread. Si l'analyse n'est pas terminée à l'issue de cette période, Microsoft Exchange Server refuse l'accès du client à la messagerie. L'analyse n'est pas interrompue et, à son issue, toute autre tentative d'accès au fichier aboutit. Si vous utilisez Microsoft Exchange Server 5.5 SP3 ou SP4, la valeur est exprimée en millisecondes et représente la période après laquelle le client essaie de nouveau d'accéder au fichier qui était précédemment inaccessible en raison de l'analyse.

Q : quelle peut être la longueur de la liste des types de fichiers dans une règle ?

R : la liste des extensions de fichier peut contenir un maximum de 255 caractères dans une règle.

Q : j'ai activé l'option **Analyse en arrière-plan** dans VSAPI. Jusqu'à présent, les messages sur Microsoft Exchange Server étaient toujours analysés après chaque mise à jour de la base des signatures des virus. Depuis la dernière mise à jour, ce n'est plus le cas. Quel est le problème ?

R : le fait d'analyser tous les messages immédiatement ou lorsque l'utilisateur essaie d'accéder à un message dépend de plusieurs facteurs, notamment de la charge du serveur, du temps processeur nécessaire à l'analyse de tous les messages et du nombre total de messages. Le serveur Microsoft Exchange Server analyse chaque message avant qu'il accède à la boîte de réception du client.

Q : pourquoi le nombre de règles augmente-t-il de plus d'une unité après la réception d'un seul message ?

R : Les règles permettent de vérifier un message lorsque celui est traité par l'agent de transport ou VSAPI. Si les deux méthodes, agent de transport et VSAPI, sont activées et que le message correspond aux conditions de la règle, le nombre de règles peut augmenter de 2 ou plus. Le système VSAPI accède en effet à chacune des parties du message (corps et pièce jointe), ce qui signifie que les règles sont appliquées à chacune de ces parties. Par ailleurs, les règles sont également appliquées lors des analyses en arrière-plan (par exemple lors de l'analyse répétée du stockage de la boîte aux lettres après la mise à jour des bases des signatures de virus), ce qui peut augmenter le nombre de règles.

Q : Le programme ESET Mail Security 4 pour Microsoft Exchange Server est-il compatible avec le filtre de messages intelligent ?

R : Oui, le programme ESET Mail Security 4 pour Microsoft Exchange Server est-il compatible avec le filtre de messages intelligent. Un message évalué comme courrier indésirable est traité comme suit :

- Si l'option **Supprimer le message** (ou **Mettre le message en quarantaine**) du module antispam ESET Mail Security est activée, elle est exécutée, quelle que soit l'action définie dans le filtre de messagerie instantanée Microsoft Exchange.

- Si l'action **Aucune action** du module antispam ESET Mail Security est définie, les paramètres du filtre de messagerie instantanée Microsoft Exchange sont utilisés et l'action pertinente exécutée (suppression, rejet, archivage par exemple). L'option **Écrire le niveau de confiance du courrier indésirable (SCL) dans les messages analysés en fonction du score de courrier indésirable** (dans **Protection du serveur > Microsoft Exchange Server > Agent de transport**) doit être activée pour que ce système fonctionne correctement.

Q : comment configurer ESET Mail Security pour que les messages non sollicités soient déplacés dans le dossier de courrier indésirable Microsoft Outlook défini par l'utilisateur ?

R : avec les paramètres ESET Mail Security par défaut, Microsoft Outlook stocke les messages non sollicités dans le dossier **Courriers indésirables**. Pour que cela fonctionne, désélectionnez l'option **Écrire le score de courrier indésirable dans l'en-tête du courrier électronique analysé** (dans **F5 > Protection du serveur > Protection antispam > Microsoft Exchange Server > Agent de transport**). Si vous souhaitez que les messages non sollicités soient stockés dans un autre dossier, veuillez prendre connaissance des instructions suivantes :

1) Dans ESET Mail Security :

- accédez à l'arborescence complète avec **F5**,

- accédez à **Protection du serveur** > **Protection antispam** > **Serveur Microsoft Exchange** > **Agent de transport**

- sélectionnez **Conserver les messages** dans le menu déroulant **Action à entreprendre sur les messages de courrier indésirable**

- décochez la case **Écrire le score de courrier indésirable dans l'en-tête des messages analysés**

- accédez à **Alertes et notifications** sous **Protection antispam**

- définissez une balise texte qui sera ajoutée au champ objet des messages indésirables, par ex. : « [SPAM] », dans le champ **Modèle ajouté à l'objet des messages indésirables**

2) Dans Microsoft Outlook :

- configurez une règle afin de garantir que les messages contenant un texte spécifique (« [SPAM] ») dans l'objet soient déplacés vers le dossier souhaité.

Pour consulter des instructions plus détaillées, consultez cet article de la base de connaissances.

Q : dans les statistiques de la protection antispam, de nombreux messages sont classés dans la catégorie **Non analysé**. Quel message n'est pas analysé par la protection antispam ?

R : La catégorie **Non analysé** se compose des éléments suivants :

Général :

- Tous les messages analysés alors que la protection antispam est désactivée sur toutes les couches (serveur de messagerie, agent de transport)

Microsoft Exchange Server 2003 :

- Tous les messages entrants depuis une **adresse IP**, c'est-à-dire dans le filtrage IMF de la **liste d'acceptation globale**.
- Messages d'expéditeurs authentifiés

Microsoft Exchange Server 2007 :

- Tous les messages envoyés dans l'organisation (tous sont analysés par une protection antivirus)
- Messages d'expéditeurs authentifiés
- Messages d'utilisateurs configurés pour contourner la protection antispam
- Tous les messages envoyés dans la boîte de messagerie dont l'option de **contournement de la protection antispam** est activée.
- Tous les messages d'expéditeurs de la liste des **expéditeurs sécurisés**

REMARQUE : Adresses définies dans les paramètres de liste blanche et de moteur de blocage du courrier indésirable qui n'entrent pas dans la catégorie **Non analysé**,, car ce groupe est composé uniquement des messages traités par la protection antispam.

Q : les utilisateurs téléchargent des messages sur leur client de messagerie via POP3 (en ignorant le serveur Microsoft Exchange), mais les boîtes aux lettres sont stockées sur le serveur Microsoft Exchange Server. Ces messages font-ils l'objet d'une analyse antivirus et antispam ESET Mail Security ?

R : dans ce type de configuration, ESET Mail Security analyse les messages stockés sur le serveur Microsoft Exchange Server uniquement pour la présence de virus (via VSAPI). L'analyse antispam n'est pas effectuée, car elle nécessite un serveur SMTP.

Q : puis-je définir le niveau de score de courrier indésirable que le message doit atteindre pour être classé comme courrier indésirable ?

R : oui, vous pouvez définir cette limite dans ESET Mail Security version 4.3 et les versions ultérieures (reportez-vous au chapitre Moteur de blocage du courrier indésirable 40).

Q : le module de protection antispam ESET Mail Security analyse-t-il également les messages qui sont téléchargés par l'intermédiaire du connecteur POP3 ?

R :ESET Mail Security ne prend pas en charge le connecteur POP3 SBS standard de Microsoft sur SBS 2008. Par conséquent, les messages téléchargés via ce connecteur POP3 sont analysés afin de détecter d'éventuels messages indésirables. Cependant, le connecteur POP3 SBS standard de Microsoft sur SBS 2003 n'est pas pris en charge. Des connecteurs POP3 de fournisseurs tiers sont également disponibles. L'analyse des messages récupérés via ces connecteurs POP3 de fournisseurs tiers soient analysés à la recherche de courrier indésirable dépend de la conception particulière de ce connecteur POP3 et de la manière dont il récupère les messages. Pour plus d'informations, consultez le sujet Connecteur POP3 et protection antispam 39.

4. ESET Mail Security : protection du serveur

ESET Mail Security fournit non seulement la protection de Microsoft Exchange Server, mais également tous les outils nécessaires à la protection du serveur proprement dit (protection résidente, protection de l'accès à Internet, protection du client de messagerie et protection antispam).

4.1 Protection antivirus et antispyware

La protection antivirus vous prémunit des attaques contre le système en contrôlant les échanges de fichiers et de courrier, ainsi que les communications Internet. Si une menace comportant du code malveillant est détectée, le module antivirus peut l'éliminer en la bloquant dans un premier temps, puis en nettoyant, en supprimant ou en mettant en quarantaine l'objet infecté.

4.1.1 Protection en temps réel du système de fichiers

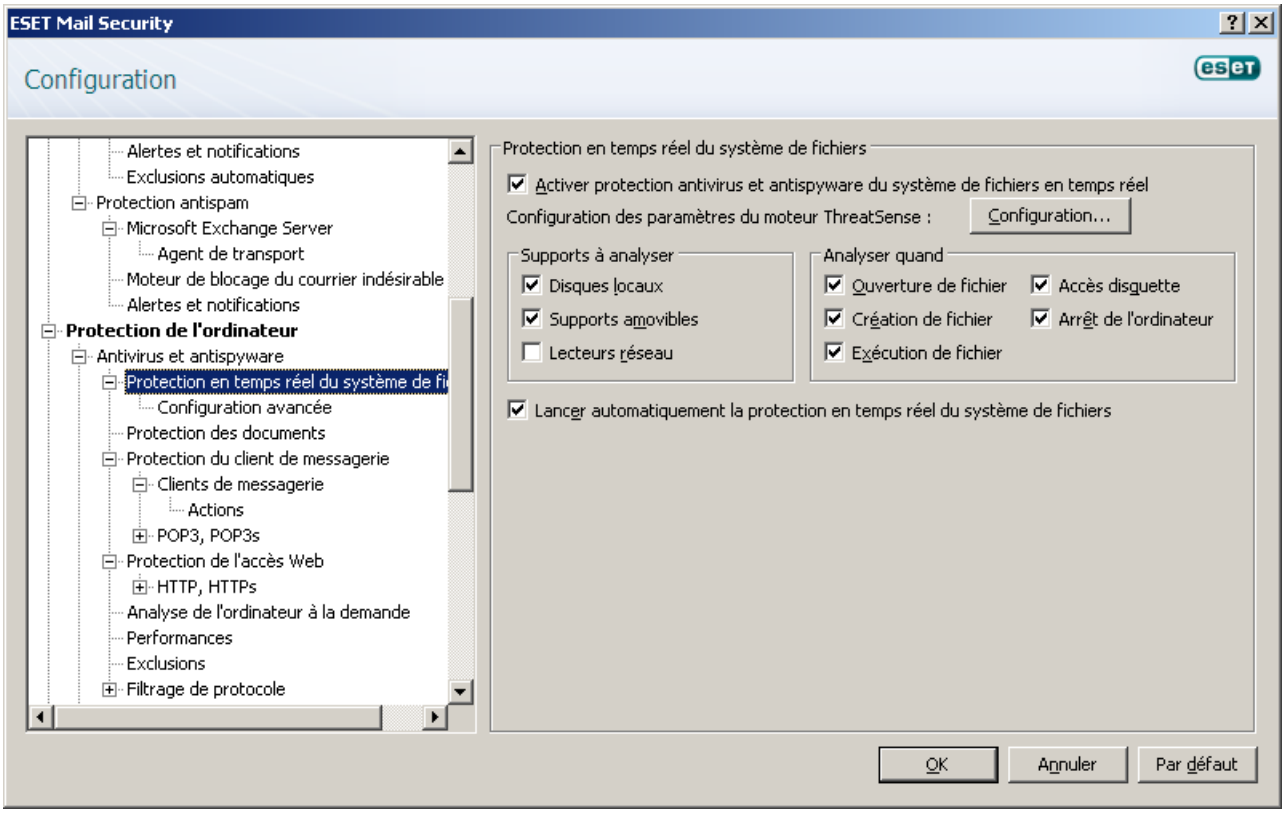
La protection en temps réel du système de fichiers contrôle tous les événements liés à l'antivirus dans le système. Elle analyse tous les fichiers à la recherche de code malveillant lors de l'ouverture, de la création ou de l'exécution de ces fichiers sur l'ordinateur. La protection en temps réel du système de fichiers est lancée au démarrage du système.

4.1.1.1 Configuration du contrôle

La protection en temps réel du système de fichiers vérifie tous les types de supports et le contrôle est déclenché par différents événements. Lors de l'utilisation des méthodes de détection de la technologie ThreatSense (décrites dans la section Configuration des paramètres du moteur ThreatSense 77), la protection du système de fichiers en temps réel est différente pour les nouveaux fichiers et pour les fichiers existants. Pour les nouveaux fichiers, il est possible d'appliquer un niveau de contrôle plus approfondi.

Pour réduire l'impact de la protection en temps réel sur le système, les fichiers déjà analysés ne sont pas analysés plusieurs fois (sauf s'ils ont été modifiés). Les fichiers sont immédiatement réanalysés après chaque mise à jour de la base des signatures de virus. Ce comportement est configuré à l'aide de l'optimisation intelligente. Si cette fonction est désactivée, tous les fichiers sont analysés à chaque accès. Pour modifier cette option, ouvrez la fenêtre Configuration avancée et cliquez sur **Antivirus et antispyware** > **Protection en temps réel du système de fichiers** dans l'arborescence de configuration avancée. Cliquez ensuite sur le bouton **Configuration...** à côté de l'option **Configuration des paramètres du moteur ThreatSense**, cliquez sur **Autre** et sélectionnez ou désélectionnez l'option **Activer l'optimisation intelligente**.

Par défaut, la protection en temps réel est lancée au démarrage du système d'exploitation, assurant ainsi une analyse ininterrompue. Dans certains cas (par exemple en cas de conflit avec un autre analyseur en temps réel), il est possible de mettre fin à la protection en temps réel en désactivant l'option **Lancer automatiquement la protection en temps réel du système de fichiers**.



4.1.1.1.1 Supports à analyser

Par défaut, tous les types de supports font l'objet de recherches de menaces potentielles.

Disques locaux : contrôle tous les disques durs système.

Supports amovibles : disquettes, périphériques USB, etc.

Disques réseau : analyse tous les lecteurs mappés.

Nous recommandons de conserver les paramètres par défaut et de ne les modifier que dans des cas spécifiques, par exemple lorsque l'analyse de certains supports ralentit de manière significative les transferts de données.

4.1.1.1.2 Analyser quand (analyse déclenchée par un événement)

Par défaut, tous les fichiers sont analysés lors de leur ouverture, création ou exécution. Il est recommandé de conserver les paramètres par défaut, car ils offrent le niveau maximal de protection en temps réel pour votre ordinateur.

L'option **Accès disquette** contrôle le secteur d'amorçage des disquettes lors de l'accès au lecteur. L'option **Arrêt de l'ordinateur** contrôle les secteurs d'amorçage du disque dur lors de l'arrêt de l'ordinateur. Bien que les virus d'amorçage soient rares de nos jours, il est recommandé de laisser ces options activées, car le risque existe toujours d'une infection par un virus d'amorçage provenant d'autres sources.

4.1.1.1.3 Options d'analyse avancées

Vous trouverez des options de configuration détaillées dans **Protection de l'ordinateur** > **Antivirus et antispyware** > **Protection en temps réel du système de fichiers** > **Configuration avancée**.

Autres paramètres ThreatSense pour les fichiers nouveaux et modifiés - La probabilité d'infection dans les nouveaux fichiers ou les fichiers modifiés est comparativement supérieure à celle des fichiers existants.. C'est la raison pour laquelle le programme vérifie ces fichiers avec des paramètres d'analyse supplémentaires. Outre les méthodes d'analyse basées sur les signatures, l'heuristique avancée est utilisée, ce qui améliore sensiblement les taux de détection. Outre les nouveaux fichiers, l'analyse porte également sur les fichiers auto-extractibles (.sfx) et les fichiers exécutables compressés (en interne). Par défaut, les archives sont analysées jusqu'au dixième niveau d'imbrication et sont contrôlées indépendamment de leur taille réelle. Désactivez l'option Paramètres d'analyse d'archive par défaut pour modifier les paramètres d'analyse d'archive.

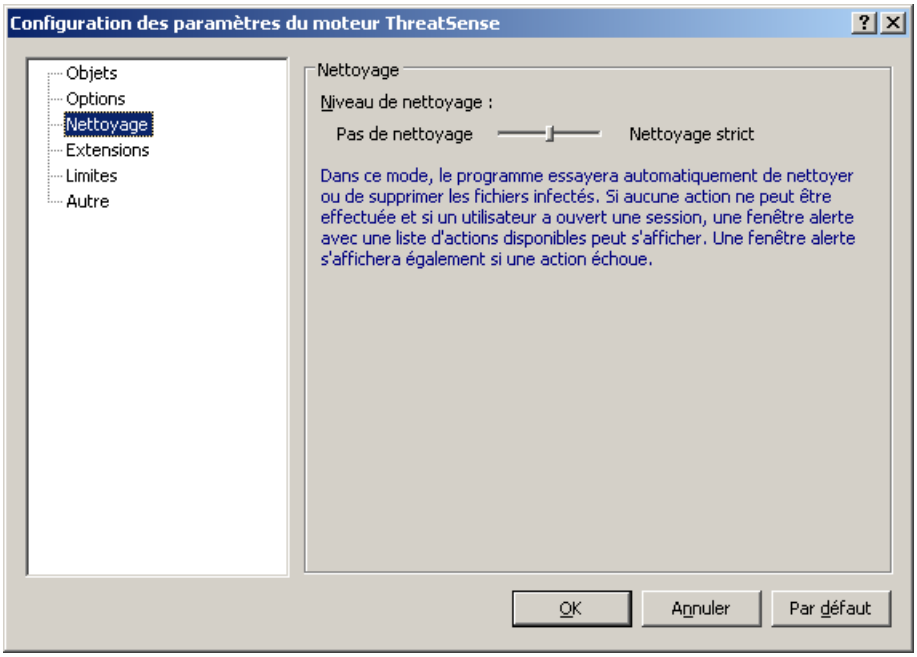
Autres paramètres ThreatSense.Net pour les fichiers exécutés : par défaut, l'heuristique avancée n'est pas

utilisée lors de l'exécution des fichiers.. Toutefois, vous souhaiterez dans certains cas activer cette option (en cochant l'option **Heuristique avancée à l'exécution du fichier**). Notez que l'heuristique avancée peut ralentir l'exécution de certains programmes en raison de la charge système accrue.

4.1.1.2 Niveaux de nettoyage

La protection en temps réel offre trois niveaux de nettoyage. Pour sélectionner un niveau de nettoyage, cliquez sur le bouton **Configuration...** dans la section **Protection en temps réel du système de fichiers**, puis cliquez sur la branche **Nettoyage**.

- Le premier niveau, **Pas de nettoyage**, affiche une fenêtre d'avertissement qui propose des options pour chaque infiltration détectée. L'utilisateur doit choisir une action pour chaque infiltration. Ce niveau est conçu pour les utilisateurs expérimentés qui connaissent les actions à entreprendre en cas d'infiltration.
- Le niveau par défaut choisit et exécute automatiquement une action prédéfinie (selon le type d'infiltration). La détection et la suppression d'un fichier infecté sont signalées par un message affiché dans l'angle inférieur droit de l'écran. Les actions automatiques ne sont pas réalisées si l'infiltration se trouve dans une archive (qui contient également des fichiers intacts) ou si les objets infectés n'ont pas d'action prédéfinie.
- Le troisième niveau, **Nettoyage strict**, est le plus « agressif » : tous les fichiers infectés sont nettoyés. Ce niveau pouvant éventuellement entraîner la perte de fichiers valides, il n'est recommandé que dans des situations spécifiques.



4.1.1.3 Quand faut-il modifier la configuration de la protection en temps réel

La protection en temps réel est le composant essentiel de la sécurisation du système. Il faut donc procéder avec prudence lors de la modification des paramètres de ce module. Il est recommandé de ne modifier les paramètres que dans des cas très précis. Ce peut être le cas notamment lorsqu'il y a conflit avec une autre application ou avec l'analyseur en temps réel d'un autre logiciel antivirus.

Après l'installation d'ESET Mail Security, tous les paramètres sont optimisés pour garantir aux utilisateurs le niveau maximum de sécurité du système. Pour rétablir les paramètres par défaut, cliquez sur le bouton **Par défaut** situé dans la partie inférieure droite de la fenêtre **Protection en temps réel du système de fichiers** (**Configuration avancée** > **Antivirus et antispyware** > **Protection en temps réel du système de fichiers**).

4.1.1.4 Vérification de la protection en temps réel

Pour vérifier que la protection en temps réel fonctionne et détecte les virus, utilisez un fichier de test d'eicar.com. Ce fichier de test est un fichier spécial inoffensif, détectable par tous les programmes antivirus. Le fichier a été créé par la société EICAR (European Institute for Computer Antivirus Research) et permet de tester la fonctionnalité des programmes antivirus. Le fichier eicar.com est téléchargeable depuis http://www.eicar.org/download/eicar.com

REMARQUE : avant d'effectuer une vérification de la protection en temps réel, vous devez désactiver le pare-feu. S'il est activé, il détecte le fichier et empêche le téléchargement des fichiers de test.

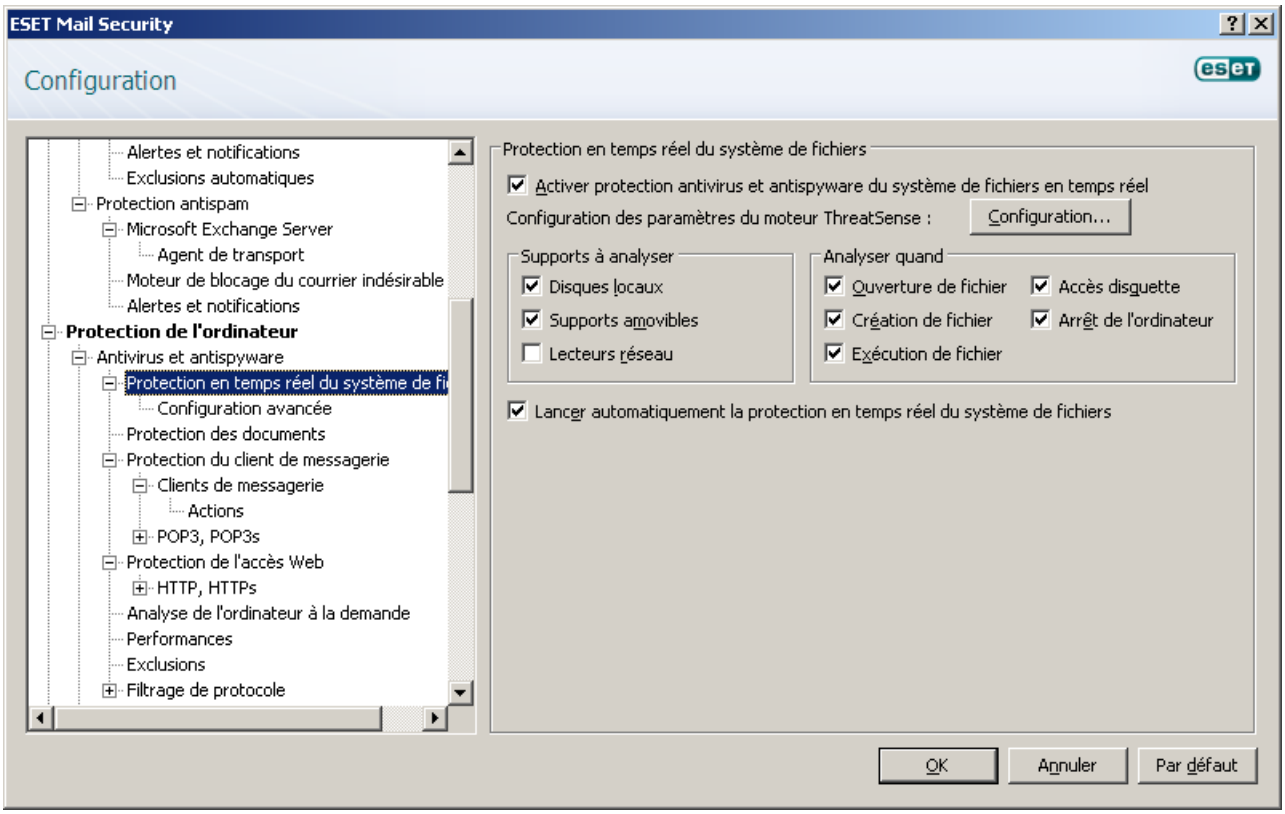
4.1.1.5 Que faire si la protection en temps réel ne fonctionne pas ?

Dans le chapitre suivant, nous décrivons des problèmes qui peuvent survenir lors de l'utilisation de la protection en temps réel, ainsi que la façon de les résoudre.

La protection en temps réel est désactivée

Si la protection en temps réel a été désactivée par mégarde par un utilisateur, elle doit être réactivée. Pour réactiver la protection en temps réel, sélectionnez **Configuration** > **Antivirus et antispyware** et cliquez sur **Activer dans la** section **Protection en temps réel du système de fichiers** dans la fenêtre principale du programme.

Si la protection en temps réel ne se lance pas au démarrage du système, c'est probablement dû au fait que l'option **Lancement automatique de la protection en temps réel du système de fichiers est désactivée**. Pour activer cette option, sélectionnez Configuration avancée (F5) et cliquez sur **Protection en temps réel du système de fichiers** dans l'arborescence de configuration avancée. Dans la section **Configuration avancée** dans la partie inférieure de la fenêtre, vérifiez que la case **Lancer automatiquement la protection en temps réel du système de fichiers** est cochée.



Si la protection en temps réel ne détecte et ne nettoie pas les infiltrations

Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes de protection en temps réel sont activés en même temps, il peut y avoir un conflit entre les deux. Nous recommandons de désinstaller tout autre antivirus de votre système.

La protection en temps réel ne démarre pas

Si la protection en temps réel n'est pas lancée au démarrage du système (et si l'option **Lancer automatiquement la protection en temps réel du système de fichiers** est activée), le problème peut provenir de conflits avec d'autres programmes. Dans ce cas, consultez les spécialistes du service client ESET.

4.1.2 Protection du client de messagerie

La protection du courrier permet de contrôler la communication par courrier électronique effectuée via le protocole POP3. ESET Mail Security utilise le plugin pour Microsoft Outlook pour contrôler toutes les communications impliquant le client de messagerie (POP3, MAPI, IMAP, HTTP).

Lorsqu'il examine les messages entrants, le programme utilise toutes les méthodes d'analyse avancées offertes par le moteur d'analyse ThreatSense. Autrement dit, la détection des programmes malveillants s'effectue avant la comparaison avec la base des signatures de virus. L'analyse des communications via le protocole POP3 est indépendante du client de messagerie utilisé.

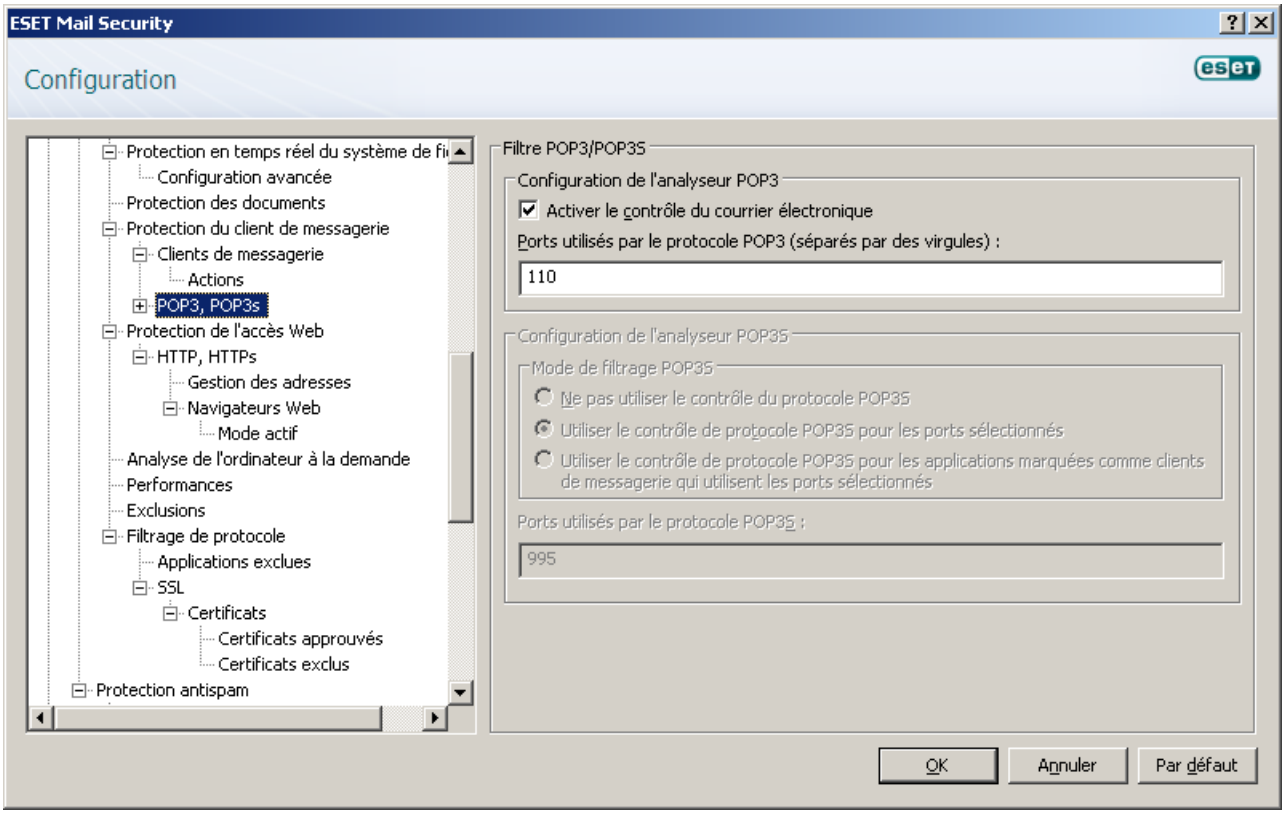
4.1.2.1 Contrôle POP3

Le protocole POP3 est le protocole le plus répandu pour la réception de messages dans un client de messagerie. ESET Mail Security protège ce protocole, quel que soit le client de messagerie utilisé.

Le module de protection qui assure ce contrôle est automatiquement lancé au démarrage du système d'exploitation et reste ensuite actif en mémoire. Pour que le module fonctionne correctement, assurez-vous qu'il est activé. Le contrôle POP3 s'effectue automatiquement sans qu'il faille reconfigurer le client de messagerie. Par défaut, toute communication sur le port 110 est soumise à une analyse, mais d'autres ports de communication peuvent être ajoutés au besoin. Les numéros de ports doivent être séparés par des virgules.

Les communications chiffrées ne sont pas contrôlées.

Pour utiliser le filtrage POP3/POP3S, vous devez activer d'abord le filtrage de protocole. Si les options POP3/POP3S sont grisées, sélectionnez **Protection de l'ordinateur** > **Antivirus et antispyware** > **Filtrage de protocole** depuis l'arborescence de configuration avancée et cochez l'option **Activer le filtrage du contenu des protocoles d'application**. Reportez-vous à la section Filtrage de protocole pour plus d'informations sur le filtrage et la configuration.



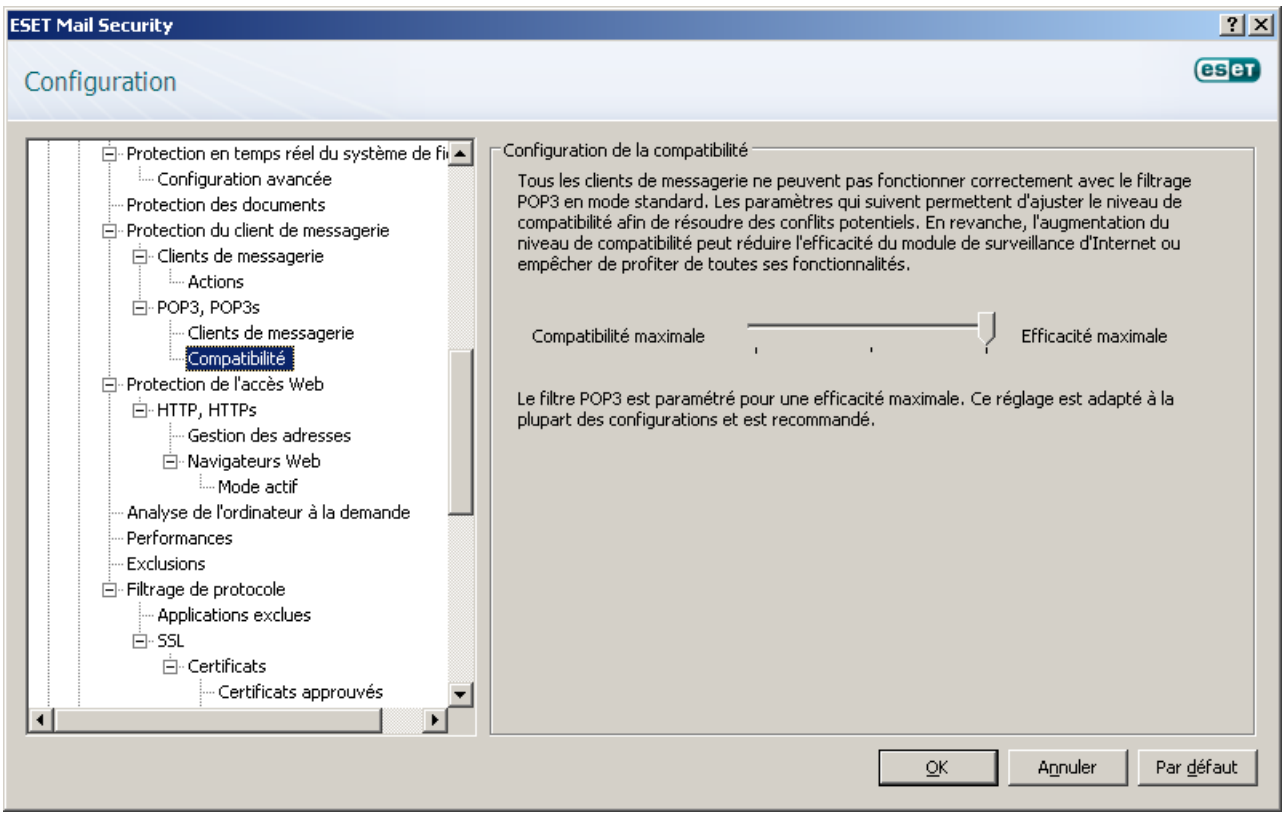
4.1.2.1.1 Compatibilité

Certains programmes de messagerie peuvent rencontrer des problèmes liés au filtrage POP3 (par exemple si vous recevez des messages sur une connexion Internet lente, la vérification peut entraîner des dépassements de délai). Dans ce cas, essayez de modifier la façon dont le contrôle est effectué. Une diminution du niveau de contrôle peut accélérer le processus de nettoyage. Pour ajuster le niveau de contrôle du filtrage POP3, sélectionnez, dans l'arborescence de configuration avancée, **Antivirus et antispyware** > **Protectiono du client de messagerie** > **POP3, POP3s** > **Compatibilité**.

Si l'option **Efficacité maximale** est activée, les infiltrations sont supprimées des messages infectés et les informations concernant l'infiltration sont insérées avant l'objet d'origine du message (les options **Supprimer** ou **Nettoyer** ou le niveau de nettoyage **Strict** ou **Par défaut** doivent être activés).

Une compatibilité moyenne modifie la façon dont les messages sont reçus. Les messages sont envoyés progressivement au client de messagerie. Une fois transféré, le message est analysé et les infiltrations sont recherchées. Avec ce niveau de contrôle, le risque d'infection est accru. Le niveau de nettoyage et la gestion des notifications (notes d'alerte ajoutées à l'objet et au corps des messages) sont identiques à ceux utilisés avec le paramètre d'efficacité maximale.

Avec le niveau de **compatibilité maximum**, vous êtes averti par l'affichage d'une fenêtre qui signale la réception d'un message infecté. Aucune information concernant les fichiers infectés n'est ajoutée à l'objet ni au corps des messages et les infiltrations ne sont pas supprimées automatiquement. Vous devez supprimer les infiltrations du client de messagerie.



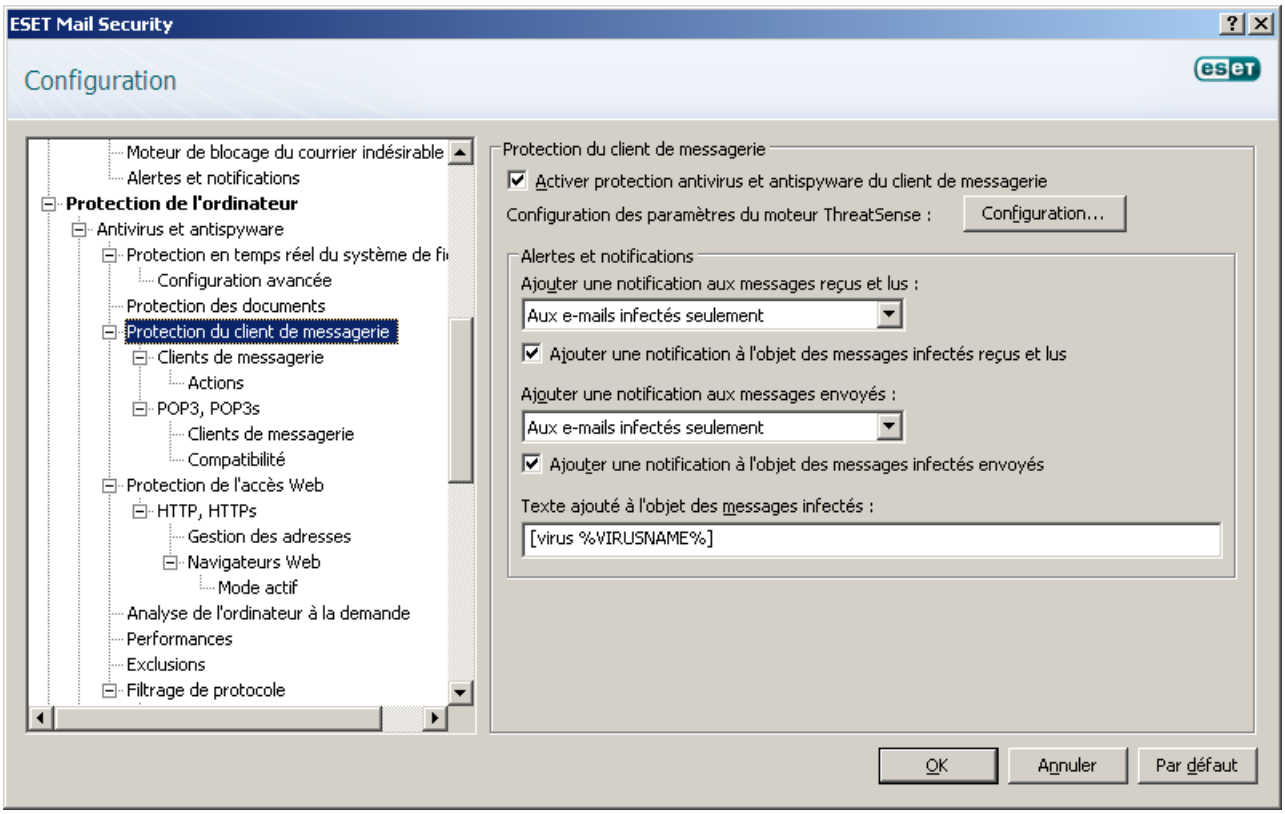
4.1.2.2 Intégration aux clients de messagerie

L'intégration d'ESET Mail Security aux clients de messagerie augmente le niveau de protection active contre les codes malveillants dans les messages électroniques. Si votre client de messagerie est pris en charge, cette intégration peut être activée dans ESET Mail Security. Si l'intégration est activée, la barre d'outils de protection antispam de ESET Mail Security est insérée directement dans le client de messagerie, ce qui permet de protéger les messages plus efficacement. Les paramètres d'intégration se trouvent dans la section **Configuration** > **Accéder à l'arborescence de la configuration avancée complète...** > **Divers** > **Intégration aux clients de messagerie**. L'intégration du client de messagerie permet d'activer l'intégration avec les clients de messagerie pris en charge. Les clients de messagerie pris en charge sont Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail et Mozilla Thunderbird.

Sélectionnez l'option **Désactiver la vérification au changement de contenu de la boîte aux lettres** si vous constatez un ralentissement du système lors de l'utilisation du client de messagerie. Une telle situation peut se

présenter lors du téléchargement de messages à partir du magasin Kerio Outlook Connector.

Pour activer la protection de messagerie, cliquez sur **Configuration** > **Accéder à l'arborescence de configuration avancée complète...** > **Antivirus et antispyware** > **Protection du client de messagerie** et sélectionnez l'option **Activer protection antivirus et antispyware du client de messagerie**.



4.1.2.2.1 Ajout d'une notification au corps d'un courrier

Chaque courrier analysé par ESET Mail Security peut être marqué par l'ajout d'une notification à l'objet ou au corps du message. Cette fonction augmente la crédibilité du destinataire et, en cas de détection d'une infiltration, fournit des informations précieuses sur le niveau de menace d'un message ou d'un expéditeur.

Les options de cette fonctionnalité sont disponibles dans **Configuration avancée** > **Antivirus et antispyware** > **Protection du client de messagerie**. Vous pouvez sélectionner les options **Ajouter une notification aux messages reçus et lus** et **Ajouter une notification aux messages envoyés**. Vous pouvez également décider d'ajouter les notifications à tous les messages analysés, aux messages infectés uniquement ou à aucun des messages.

ESET Mail Security vous permet également d'ajouter des messages à l'objet d'origine des messages infectés. Pour activer l'ajout à l'objet, sélectionnez les options **Ajouter une notification à l'objet des messages infectés reçus et lus** et **Ajouter une notification à l'objet des messages infectés envoyés**.

Vous pouvez modifier le contenu des notifications dans le champ **Texte ajouté à l'objet des messages infectés**. Les modifications mentionnées précédemment permettent d'automatiser le filtrage des messages infectés, car elles vous permettent de filtrer des messages en fonction de leur objet (si votre client de messagerie prend en charge cette fonctionnalité) et de les placer dans un dossier distinct.

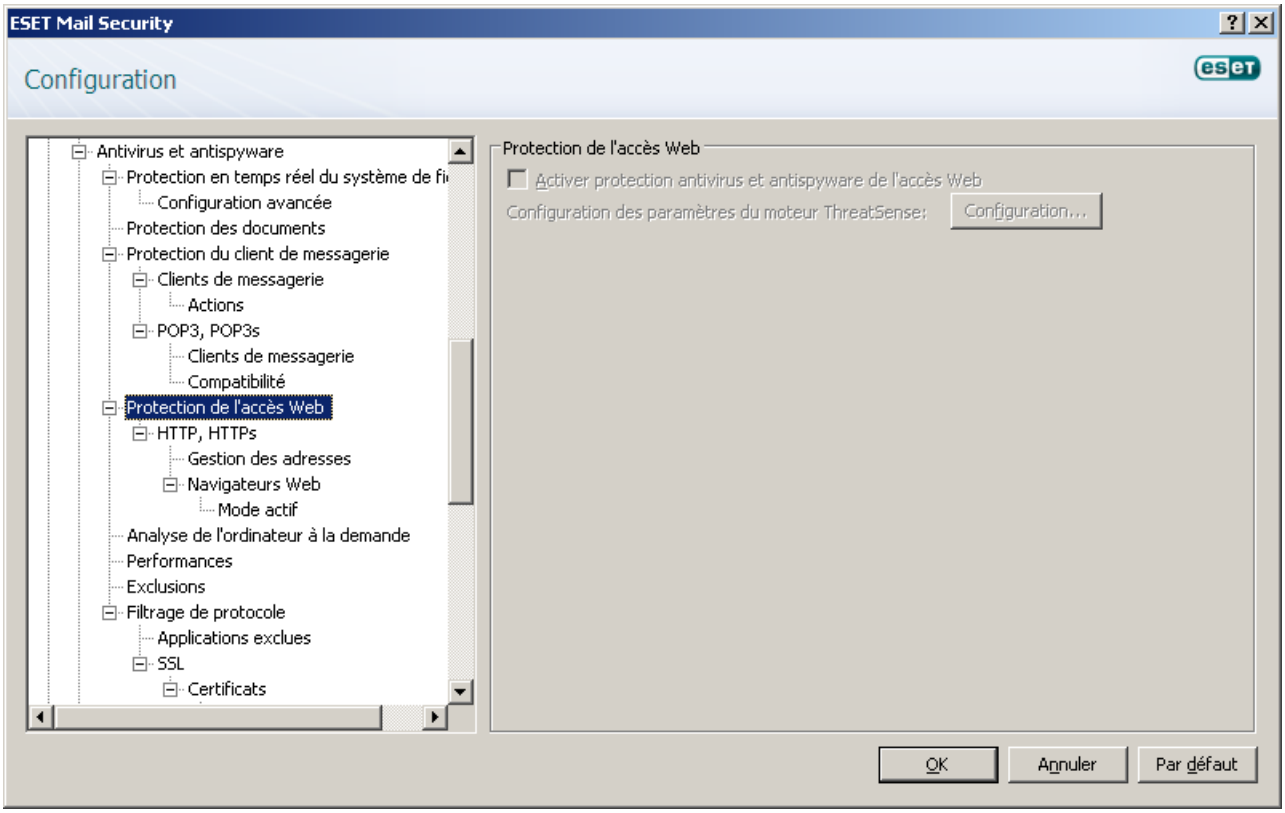
4.1.2.3 Suppression d'infiltrations

En cas de réception d'un message infecté, une fenêtre d'alerte s'affiche. Cette fenêtre indique le nom de l'expéditeur, son message et le nom de l'infiltration. La partie inférieure de la fenêtre présente les options disponibles concernant l'objet détecté : **Nettoyer**, **Supprimer** ou **Aucune action**. Dans la plupart des cas, nous recommandons de sélectionner **Nettoyer** ou **Supprimer**. Dans les situations particulières où vous souhaitez vraiment recevoir le fichier infecté, sélectionnez **Aucune action**.

Si le niveau **nettoyage strict** est activé, une fenêtre d'information sans options s'affiche.

4.1.3 Protection de l'accès Web

La connectivité Internet est une fonctionnalité standard des ordinateurs personnels. Elle est malheureusement devenue le principal mode de transfert des codes malveillants. Il est donc essentiel de surveiller de près la protection de l'accès à Internet. Il est vivement recommandé de sélectionner l'option **Afficher la notification de fin d'analyse dans une fenêtre séparée**. Cette option est disponible dans **Configuration avancée** (F5) > **Antivirus et antispyware** > **Protection de l'accès Web**.

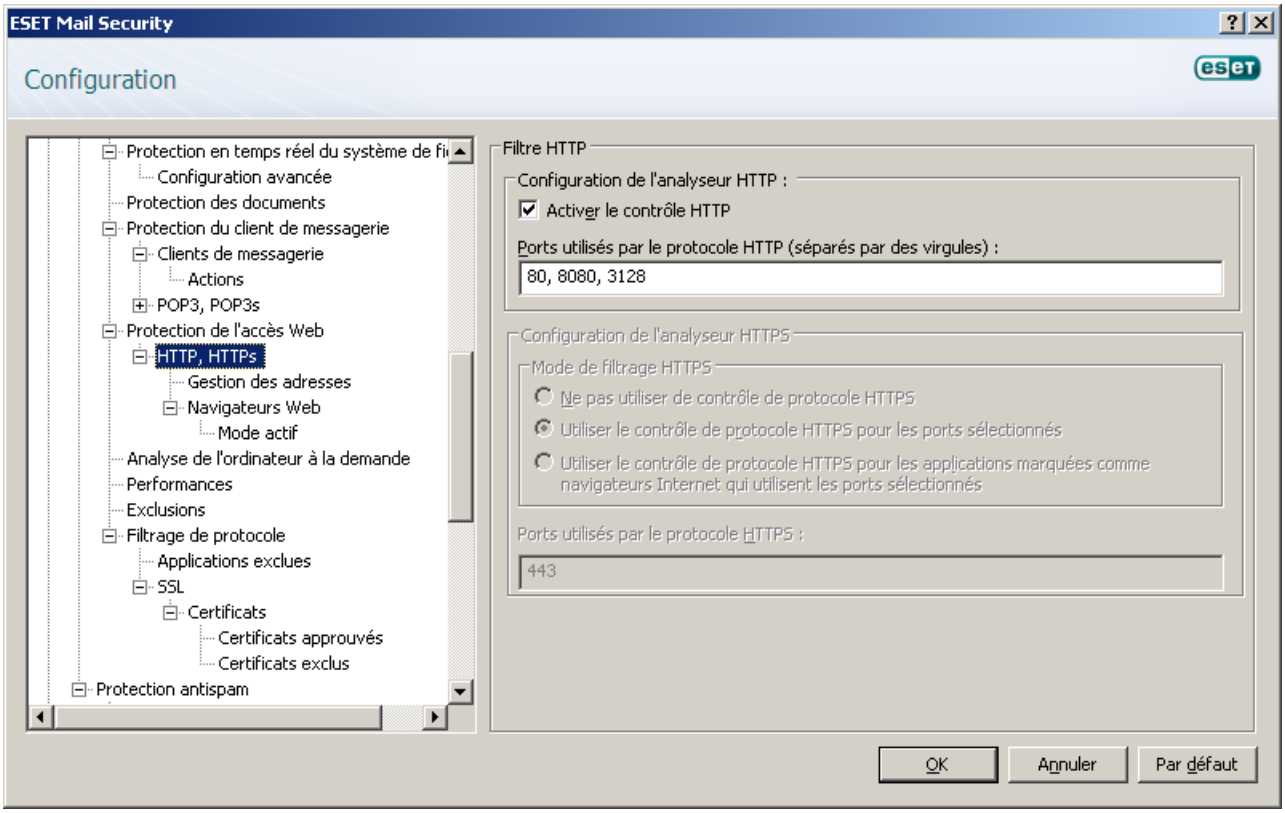


4.1.3.1 HTTP, HTTPs

La protection de l'accès Web opère par surveillance des communications entre les navigateurs Internet et les serveurs distants, conformément aux règles des protocoles HTTP et HTTPs (communications chiffrées). Par défaut, ESET Mail Security est configuré pour utiliser les normes de la plupart des navigateurs Internet. Toutefois, vous pouvez modifier les options de configuration de l'analyseur HTTP dans la section **Configuration avancée** (F5) > **Antivirus et antispyware** > **Protection de l'accès Web** > **HTTP, HTTPS**. Dans la fenêtre principale du filtre HTTP, vous pouvez activer ou désactiver l'option **Activer le contrôle HTTP**. Vous pouvez également définir les numéros de port utilisés pour la communication HTTP. Par défaut, les numéros de ports 80, 8080 et 3128 sont prédéfinis. Le contrôle HTTPs peut être effectué dans les modes suivants :

Ne pas utiliser de contrôle de protocole HTTPS : les communications chiffrées ne sont pas vérifiées.

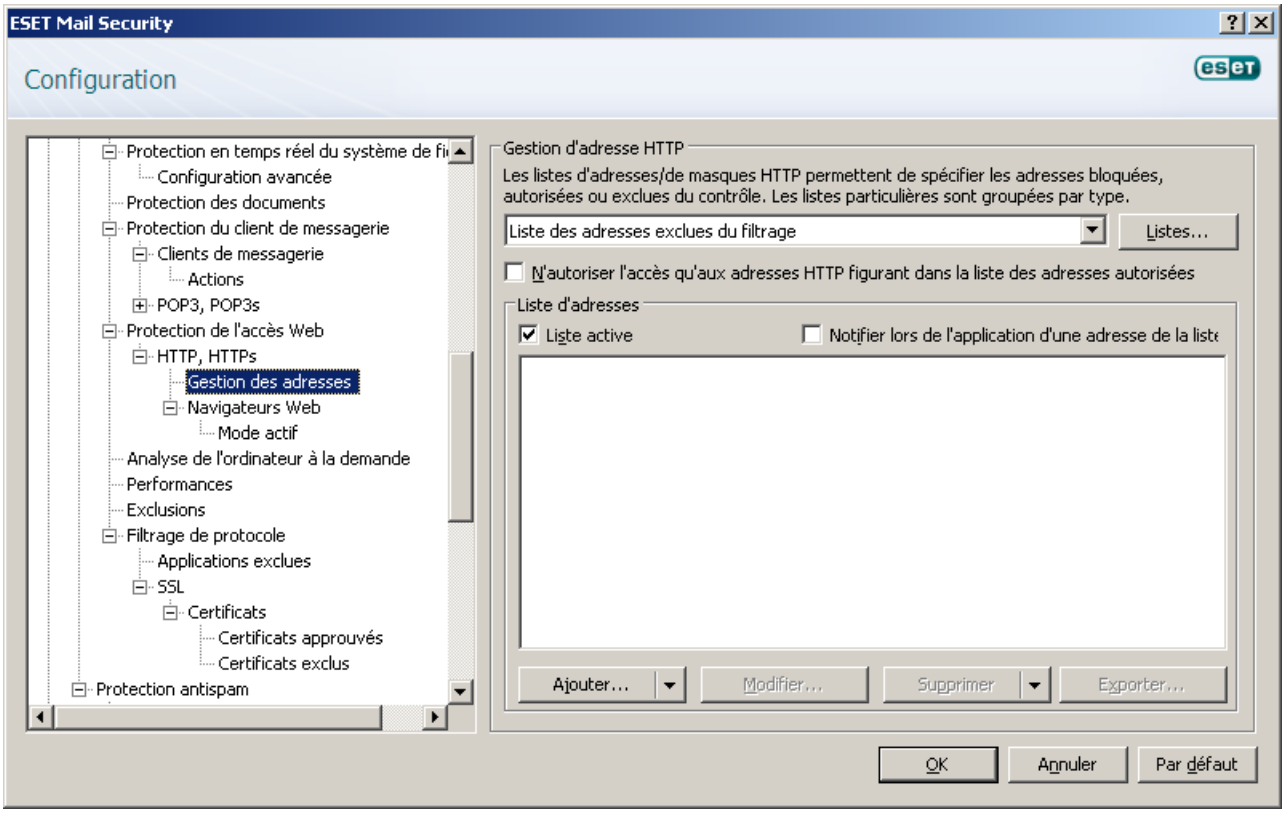
Utiliser le contrôle de protocole HTTPs pour les ports sélectionnés : le contrôle HTTPs n'a lieu que pour les ports définis dans **Ports utilisés par le protocole HTTPs**.



4.1.3.1.1 Gestion des adresses

Cette section permet de spécifier des listes d'adresses HTTP qui seront bloquées, autorisées ou exclues de la vérification. Les boutons **Ajouter...**, **Modifier...**, **Supprimer** et **Exporter...** permettent de gérer les listes d'adresses. Les sites Web figurant dans la liste des adresses bloquées ne seront pas accessibles. Les sites Web figurant dans la liste des adresses exclues sont accessibles sans aucune analyse de code malveillant. Si vous sélectionnez l'option **N'autoriser l'accès qu'aux adresses HTTP figurant dans la liste des adresses autorisées**, seules les adresses figurant dans la liste des adresses autorisées sont accessibles ; toutes les autres adresses HTTP sont bloquées.

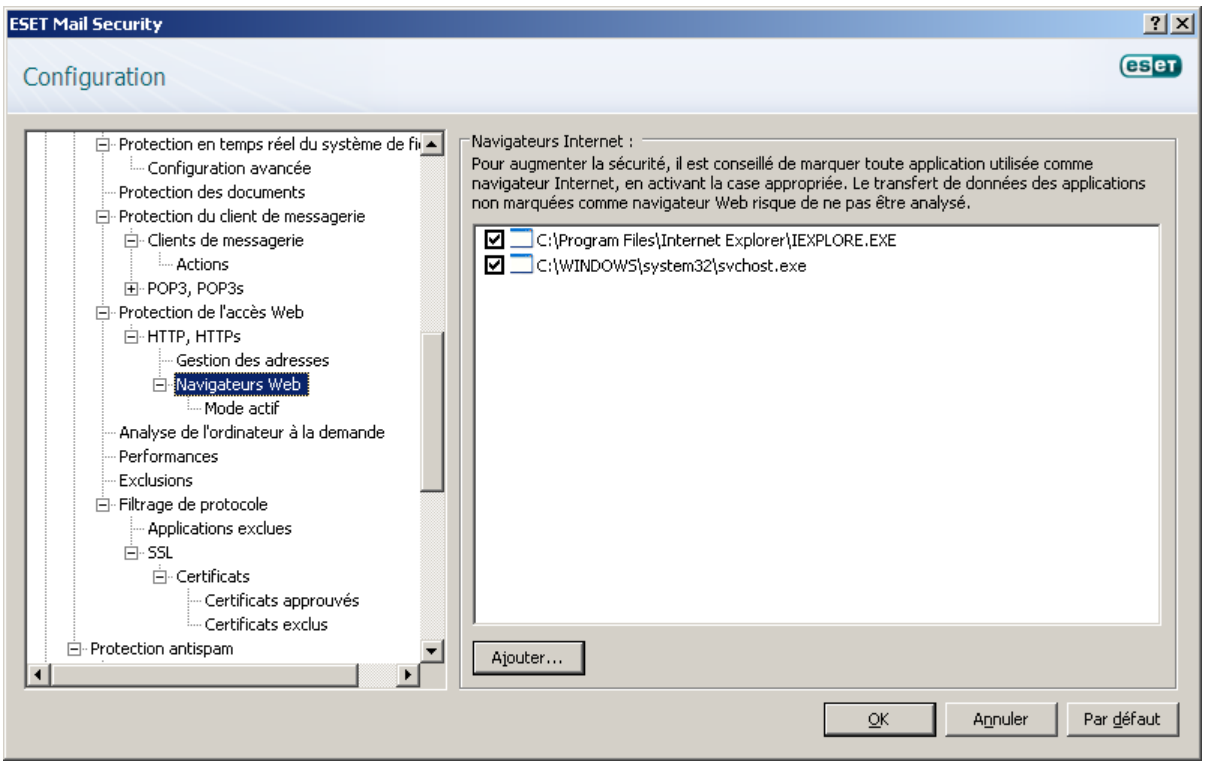
Dans toutes les listes, vous pouvez utiliser les symboles spéciaux « * » (astérisque) et « ? » (point d'interrogation). L'astérisque remplace n'importe quelle chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère. Un soin particulier doit être apporté à la spécification des adresses exclues, car la liste ne doit contenir que des adresses sûres et de confiance. De la même manière, veillez à employer correctement les symboles « * » et « ? » dans cette liste. Pour activer une liste, sélectionnez l'option **Liste active**. Pour être informé lors de l'entrée d'une adresse à partir de la liste actuelle, sélectionnez l'option **Notifier lors de l'application d'une adresse de la liste**.



4.1.3.1.2 Mode actif

ESET Mail Security contient une fonction Navigateurs Web qui permet de définir si une application donnée est un navigateur. Si une application est marquée par l'utilisateur comme étant un navigateur, toutes les communications provenant de cette application sont contrôlées, quels que soient les numéros de ports concernés.

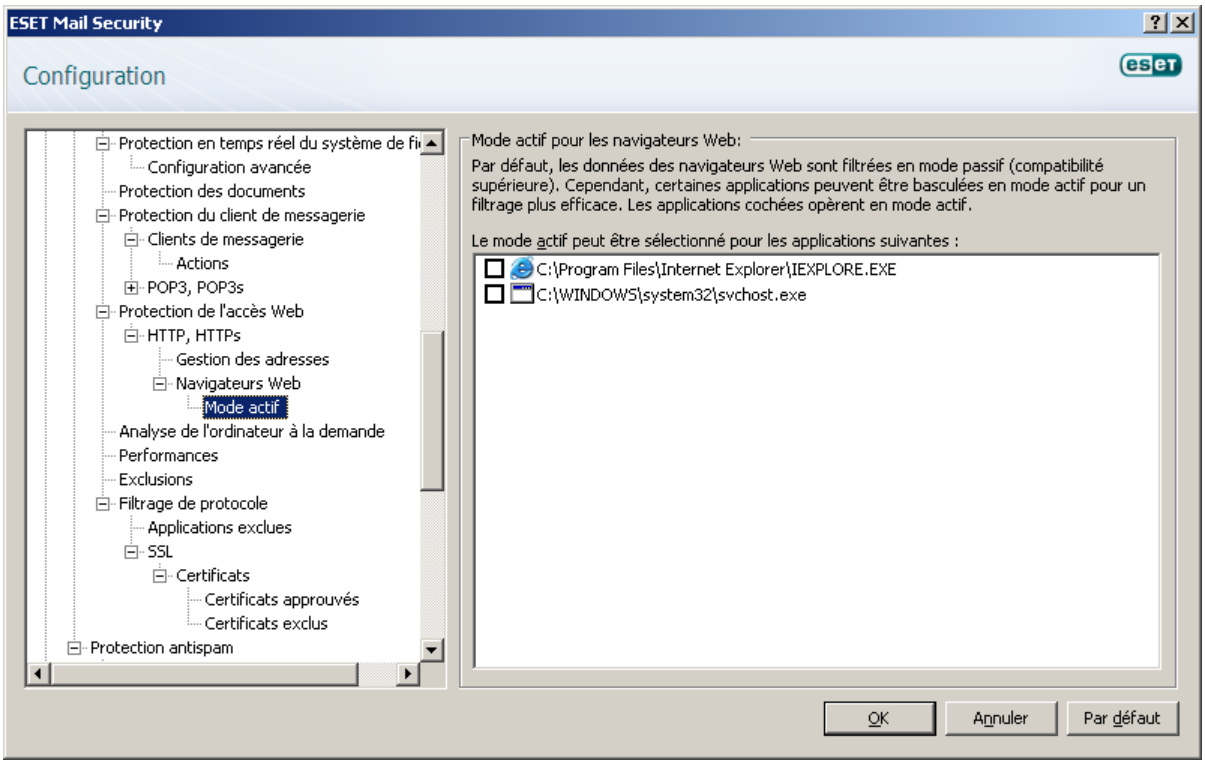
La fonction Navigateurs Web complète la fonction de contrôle HTTP, laquelle ne s'applique qu'à des ports prédéfinis. Or, de nombreux services Internet utilisent des numéros de ports qui changent ou qui sont inconnus. Pour prendre cela en compte, la fonction Navigateurs Web permet de contrôler les communications sur les ports, quels que soient les paramètres de connexion.



La liste des applications comme étant des navigateurs Web est accessible directement depuis le sous-menu **Navigateurs Web** de la branche **HTTP, HTTPs**. Cette section contient également le sous-menu **Mode actif** qui

définit le mode de contrôle des navigateurs Internet.

Avec le **Mode actif**, les données transférées sont examinées dans leur ensemble. Si l'option n'est pas activée, la communication des applications est contrôlée progressivement, par lots. La vérification des données est alors moins efficace, mais la compatibilité avec les applications répertoriées est meilleure. Si le Mode actif ne pose pas de problèmes, nous recommandons de l'activer en cochant la case située à côté de l'application souhaitée.



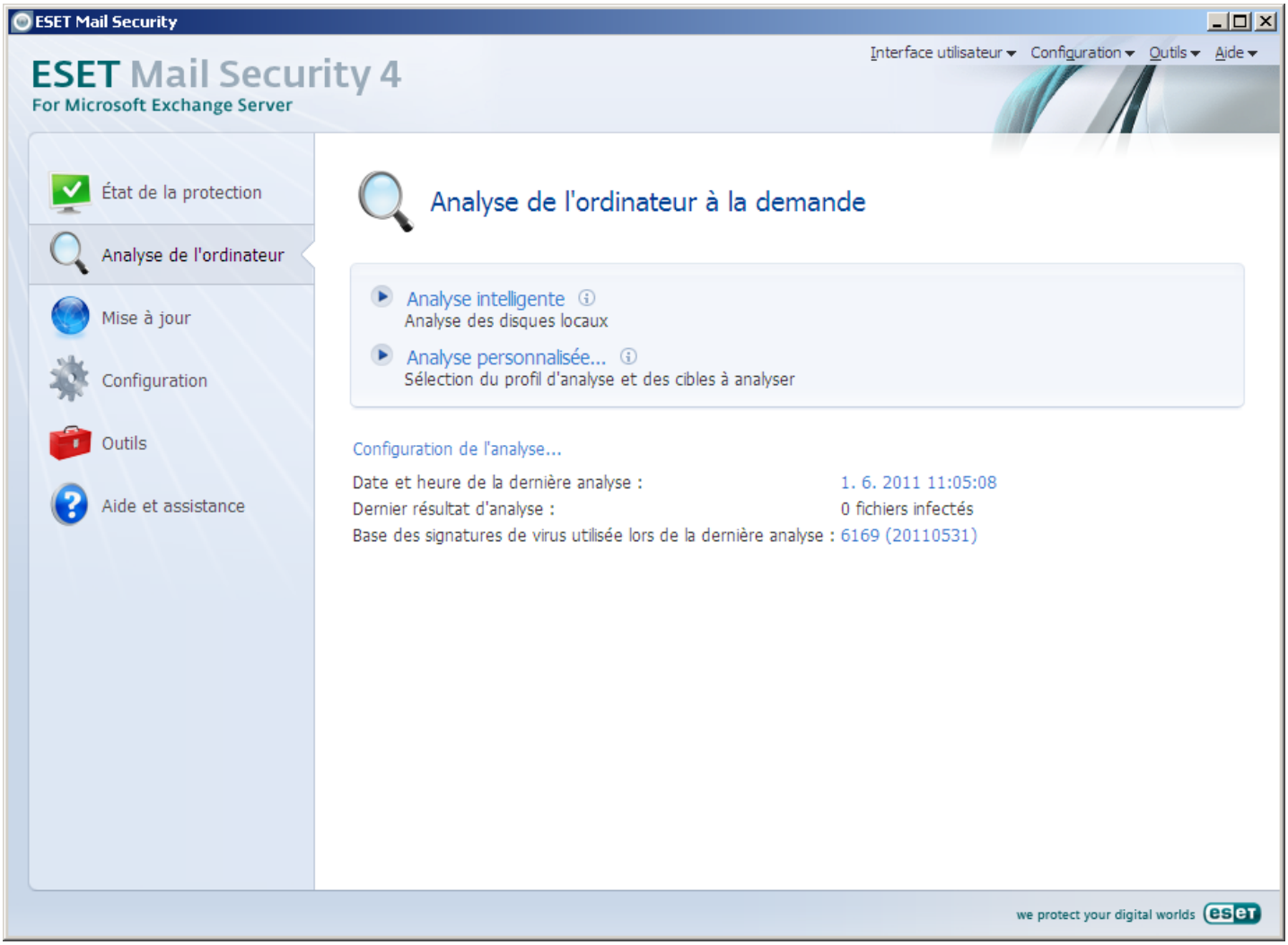
4.1.4 Analyse de l'ordinateur à la demande

Si vous pensez que votre ordinateur peut être infecté (en raison d'un comportement anormal), exécutez une analyse à la demande pour rechercher d'éventuelles infiltrations. Pour votre sécurité, il est essentiel que l'ordinateur soit analysé non seulement en cas de suspicion d'une infection, mais aussi régulièrement dans le cadre de mesures de sécurité routinières. Une analyse régulière peut détecter des infiltrations non détectées par l'analyseur en temps réel au moment de leur enregistrement sur le disque. Cela peut se produire si l'analyseur en temps réel est désactivé au moment de l'infection ou si la base des signatures de virus n'est plus à jour.

Nous recommandons d'exécuter une analyse d'ordinateur à la demande au moins une fois par mois. L'analyse peut être configurée comme tâche planifiée dans **Outils** > **Planificateur**.

4.1.4.1 Type d'analyse

Deux types d'analyses de l'ordinateur à la demande sont disponibles. L'**analyse intelligente** analyse le système sans exiger de reconfiguration des paramètres d'analyse. L'**analyse personnalisée** permet de sélectionner l'un des profils d'analyse prédéfinis, ainsi que de choisir des cibles spécifiques à analyser.



4.1.4.1.1 Analyse intelligente

L'analyse intelligente permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. Elle présente l'avantage d'être facile à utiliser, sans aucune configuration d'analyse détaillée. L'analyse intelligente vérifie tous les fichiers des disques locaux, et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé sur sa valeur par défaut. Pour plus d'informations sur les types de nettoyage, reportez-vous à la section Nettoyage 80.

4.1.4.1.2 Analyse personnalisée

L'analyse personnalisée est une solution optimale si vous souhaitez spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. L'analyse personnalisée a l'avantage de permettre la configuration précise des paramètres. Les configurations peuvent être enregistrées sous forme de profils d'analyse définis par l'utilisateur, utiles pour effectuer régulièrement une analyse avec les mêmes paramètres.

Pour sélectionner des cibles à analyser, sélectionnez **Analyse de l'ordinateur** > **Analyse personnalisée**, puis sélectionnez une option dans le menu déroulant **Cibles à analyser** ou sélectionnez des cibles spécifiques dans l'arborescence. Une cible d'analyse peut aussi être spécifiée plus précisément : vous devez indiquer le chemin d'accès au dossier ou aux fichiers à inclure. Si vous souhaitez uniquement effectuer une analyse du système sans ajouter d'actions de nettoyage supplémentaires, sélectionnez l'option **Analyse sans nettoyage**. Vous pouvez aussi choisir parmi trois niveaux de nettoyage en cliquant sur **Configuration...** > **Nettoyage**.

4.1.4.2 Cibles à analyser

Le menu déroulant des cibles à analyser permet de sélectionner les fichiers, dossiers et périphériques (disques) à soumettre à l'analyse antivirus.

Par paramètres de profil : permet de sélectionner les cibles indiquées dans le profil d'analyse sélectionné.

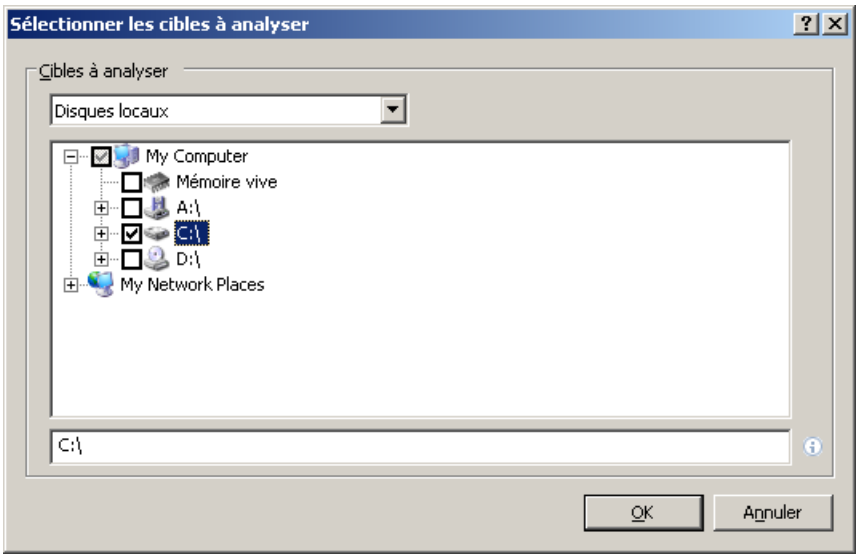
Supports amovibles : permet de sélectionner les disquettes, les périphériques USB, les CD/DVD, etc.

Disques locaux : permet de sélectionner tous les disques durs système.

Disques réseau : permet de sélectionner tous les lecteurs mappés.

Aucune sélection : annule toutes les sélections.

Vous pouvez également définir plus précisément une cible d'analyse en entrant le chemin du dossier ou des fichiers à inclure dans l'analyse. Sélectionnez les cibles dans l'arborescence des périphériques disponibles sur l'ordinateur.

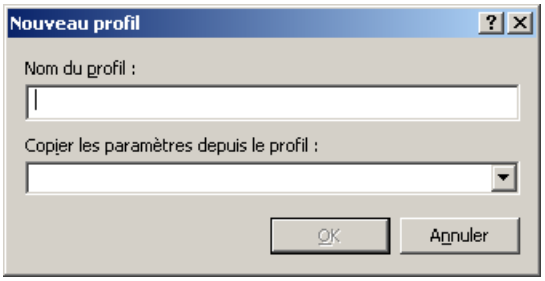


4.1.4.3 Profils d'analyse

Vos paramètres d'analyse préférés peuvent être enregistrés pour les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un nouveau profil, ouvrez la fenêtre Configuration avancée (F5) et cliquez sur **Analyse de l'ordinateur à la demande** > **Profils...** La fenêtre **Profils de configuration** dispose d'un menu déroulant répertoriant les profils d'analyse existants, ainsi qu'une option permettant de créer un profil. Pour plus d'informations sur la création d'un profil d'analyse, reportez-vous à la section Configuration du moteur ThreatSense 77; vous y trouverez la description de chaque paramètre de configuration de l'analyse.

EXEMPLE : Supposons la situation suivante : vous souhaitez créer votre propre profil d'analyse et la configuration d'analyse intelligente est partiellement adéquate. En revanche, vous ne souhaitez analyser ni les fichiers exécutables compressés par un compresseur d'exécutables, ni les applications potentiellement dangereuses. Vous souhaitez effectuer un **nettoyage strict**. Dans la fenêtre **Profils de configuration**, cliquez sur le bouton **Ajouter...** Saisissez le nom de votre nouveau profil dans le champ **Nom du profil** et sélectionnez **Analyse intelligente** dans le menu déroulant **Copier les paramètres depuis le profil** : . Adaptez ensuite les autres paramètres à vos besoins.



4.1.4.4 Ligne de commande

Le module antivirus d'ESET Mail Security peut être lancé depuis la ligne de commande, manuellement (avec la commande « ecls ») ou au moyen d'un fichier de traitement par lots (« bat »).

Les paramètres suivants peuvent être utilisés lors de l'exécution de l'analyseur à la demande à partir de la ligne de commande :

Options générales :

- help	afficher l'aide et quitter
- version	afficher les informations de version et quitter
- base-dir = FOLDER	charger les modules depuis le DOSSIER
- quar-dir = FOLDER	DOSSIER de quarantaine
- aind	afficher l'indicateur d'activité

Cibles :

- files	analyser les fichiers (valeur par défaut)
- no-files	ne pas analyser les fichiers
- boots	analyser les secteurs d'amorçage (valeur par défaut)
- no-boots	ne pas analyser les secteurs d'amorçage
- arch	analyser les archives (valeur par défaut)
- no-arch	ne pas analyser les archives
- max-archive-level = LEVEL	niveau (LEVEL) d'imbrication maximum d'archives
- scan-timeout = LIMIT	analyser les archives pendant un maximum de LIMIT (LIMITE) secondes. Si la durée d'analyse atteint cette limite, l'analyse de l'archive s'arrête et reprend au fichier suivant.
- max-arch-size=SIZE	analyser uniquement les SIZE (TAILLE) premiers octets des archives (valeur par défaut 0 = illimité)
- mail	analyser les fichiers de courriers électroniques
- no-mail	ne pas analyser les fichiers des courriers électroniques
- sfx	analyser les archives auto-extractibles
- no-sfx	ne pas analyser les archives auto-extractibles
- rtp	analyser les fichiers exécutables compressés
- no-rtp	ne pas analyser les fichiers exécutables compressés
- exclude = FOLDER	exclure de l'analyse le dossier FOLDER
- subdir	analyser les sous-dossiers (valeur par défaut)
- no-subdir	ne pas analyser les sous-dossiers
- max-subdir-level = LEVEL	Niveau (LEVEL) d'imbrication maximum de sous-dossiers (valeur par défaut 0 - illimité)
- symlink	suivre les liens symboliques (valeur par défaut)
- no-symlink	ignorer les liens symboliques
- ext-remove = EXTENSIONS	
- ext-exclude = EXTENSIONS	exclure de l'analyse les EXTENSIONS délimitées par deux-

	points

Méthodes :

- adware	rechercher les adware/spyware/riskware
- no-adware	ne pas rechercher les adware/spyware/riskware
- unsafe	rechercher les applications potentiellement dangereuses
- no-unsafe	ne pas rechercher les applications potentiellement dangereuses
- unwanted	rechercher les applications potentiellement indésirables
- no-unwanted	ne pas rechercher les applications potentiellement indésirables
- pattern	utiliser les signatures
- no-pattern	ne pas utiliser les signatures
- heur	activer l'heuristique
- no-heur	désactiver l'heuristique
- adv-heur	activer l'heuristique avancée
- no-adv-heur	désactiver l'heuristique avancée

Nettoyage :

- action = ACTION	appliquer l'ACTION aux objets infectés. Actions disponibles : none (aucune), clean (nettoyer), prompt (demander)
- quarantine	copier les fichiers infectés en quarantaine (complète ACTION)
- no-quarantine	ne pas copier les fichiers infectés vers Quarantaine

Journaux :

- log-file=FILE	journaliser les résultats dans un fichier (FICHIER)
- log-rewrite	écraser le fichier de résultats (valeur par défaut - ajouter)
- log-all	également journaliser les fichiers nettoyés
- no-log-all	ne pas journaliser les fichiers nettoyés (valeur par défaut)

Différents codes sortie d'analyse :

0	- aucune menace détectée
1	- menace détectée mais pas nettoyée
10	- certains fichiers infectés restants
101	- erreur d'archive
102	- erreur d'accès
103	- erreur interne

REMARQUE : un code sortie supérieur à 100 signale un fichier non analysé qui est potentiellement infecté.

4.1.5 Performances

Dans cette section, vous pouvez définir le nombre de moteurs d'analyse ThreatSense qui doivent être utilisés pour l'analyse de virus. Un nombre supérieur de moteurs d'analyse ThreatSense sur des ordinateurs multiprocesseurs peut augmenter la vitesse de l'analyse. Une valeur acceptable est comprise entre 1 et 20.

En l'absence d'autres restrictions, nous recommandons d'augmenter le nombre de moteurs d'analyse ThreatSense dans la fenêtre Paramères avancés (F5) sous **Protection de l'ordinateur** > **Antivirus et antispyware** > **Performances**, en respectant la formule suivante : *nombre de moteurs d'analyse ThreatSense = (nombre de processeurs physiques x 2) + 1*. Le *nombre de threads d'analyse* doit également être égal au *nombre des moteurs d'analyse ThreatSense*. Vous pouvez configurer le nombre de threads d'analyse dans **Protection du serveur** > **Antivirus et antispyware** > **Microsoft Exchange Server** > **VSAPI** > **Performances**. Voici un exemple :

Imaginons que votre serveur comporte 4 unités centrales physiques. Pour des performances optimales, conformément à la formule qui précède, vous devez avoir 9 threads d'analyse et 9 moteurs d'analyse.

REMARQUE : il est recommandé de définir le même nombre de threads d'analyse et de moteurs d'analyse ThreatSense. Le fait d'utiliser un nombre de threads d'analyse plus élevé que celui des moteurs d'analyse n'a aucune incidence sur les performances.

REMARQUE : les modifications apportées ici sont appliquées uniquement après le redémarrage.

4.1.6 Filtrage des protocoles

La protection antivirus des protocoles d'application POP3 et HTTP est fournie par le moteur d'analyse ThreatSense qui intègre en toute transparence toutes les techniques avancées d'analyse des logiciels malveillants. Le contrôle fonctionne automatiquement, indépendamment du navigateur Internet ou du client de messagerie utilisés. Les options suivantes sont disponibles pour le filtrage des protocoles (si l'option **Activer le filtrage du contenu des protocoles d'application** est sélectionnée) :

Ports HTTP et POP3 : limite l'analyse de la communication aux ports HTTP et POP3 connus.

Applications marquées comme navigateurs Internet et clients de messagerie : activez cette option pour ne filtrer la communication que des applications marquées comme navigateurs (**Protection de l'accès Web** > **HTTP, HTTPS** > **Navigateurs Web**) et clients de messagerie (**Protection du client de messagerie** > **POP3, POP3s** > **Clients de messagerie**).

Ports et applications marqués comme navigateurs Internet ou clients de messagerie : les ports et les navigateurs font l'objet de recherches de logiciels malveillants.

REMARQUE : à partir de Windows Vista Service Pack 1 et de Windows Server 2008, une nouvelle méthode de filtrage des communications est utilisée. Par conséquent, la section relative au filtrage des protocoles n'est plus disponible.

4.1.6.1 SSL

ESET Mail Security vous permet de vérifier les protocoles encapsulés dans le protocole SSL. Vous pouvez utiliser plusieurs modes d'analyse pour les communications SSL protégées à l'aide de certificats approuvés, de certificats inconnus ou de certificats exclus de la vérification des communications SSL protégées.

Toujours analyser le protocole SSL : sélectionnez cette option pour analyser toutes les communications SSL protégées, à l'exception des communications protégées par des certificats exclus de la vérification. Si une nouvelle communication utilisant un certificat signé inconnu est établie, vous n'êtes pas informé et la communication est automatiquement filtrée. Lorsque vous accéder à un serveur disposant d'un certificat non approuvé et que vous marquez comme approuvé (il est ajouté à la liste des certificats approuvés), la communication vers le serveur est autorisée et le contenu du canal de communication est filtré.

Demander pour les sites non visités (des exclusions peuvent être définies) : si vous accédez à un nouveau site protégé par SSL (dont le certificat est inconnu), vous êtes invité à confirmer que vous souhaitez le visiter avant d'être autorisé à le faire. Ce mode vous permet de créer la liste des certificats SSL qui seront exclus de l'analyse.

Ne pas analyser le protocole SSL : si cette option est activée, le programme n'analyse pas les communications SSL.

S'il est impossible de vérifier le certificat à l'aide du TRCA (**Filtrage des protocoles** > **SSL** > **Certificats**) :

Interroger sur la validité de la certification : invite l'utilisateur à choisir une action à exécuter.

Bloquer toute communication utilisant le certificat : met fin à la connexion au site utilisant le certificat.

Si le certificat est non valide ou endommagé (**Filtrage de protocole** > **SSL** > **Certificats**) :

Interroger sur la validité de la certification : invite l'utilisateur à choisir une action à exécuter.

Bloquer toute communication utilisant le certificat : met fin à la connexion au site utilisant le certificat.

4.1.6.1.1 Certificats approuvés

Outre le magasin TRCA intégré dans lequel ESET Mail Security stocke les certificats approuvés, vous pouvez créer une liste personnalisée de certificats approuvés qui est disponible dans **Configuration avancée** (F5) > **Filtrage des protocoles** > **SSL** > **Certificats** > **Certificats approuvés**.

4.1.6.1.2 Certificats exclus

La section Certificats exclus contient des certificats considérés comme étant sûrs. Le contenu des communications chiffrées qui utilisent les certificats répertoriés dans la liste des certificats exclus ne fait pas l'objet de recherche de menaces. Il est recommandé de n'exclure que les certificats Web qui sont garantis comme étant sécurisés et dont la communication utilisant les certificats n'a pas besoin d'être vérifiée.

4.1.7 Configuration des paramètres du moteur ThreatSense

ThreatSense est une technologie qui comprend des méthodes de détection de menaces complexes. C'est une technologie proactive : elle fournit une protection dès les premières heures de propagation d'une nouvelle menace. Elle utilise une combinaison de plusieurs méthodes (analyse de code, émulation de code, signatures génériques, signatures de virus) qui se conjuguent pour améliorer sensiblement la sécurité du système. Ce moteur d'analyse est capable de contrôler plusieurs flux de données simultanément, ce qui maximise l'efficacité et le taux de détection. La technologie ThreatSense élimine avec succès les rootkits.

Les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

- les types de fichiers et les extensions à analyser ;
- la combinaison de plusieurs méthodes de détection ;
- les niveaux de nettoyage, etc.

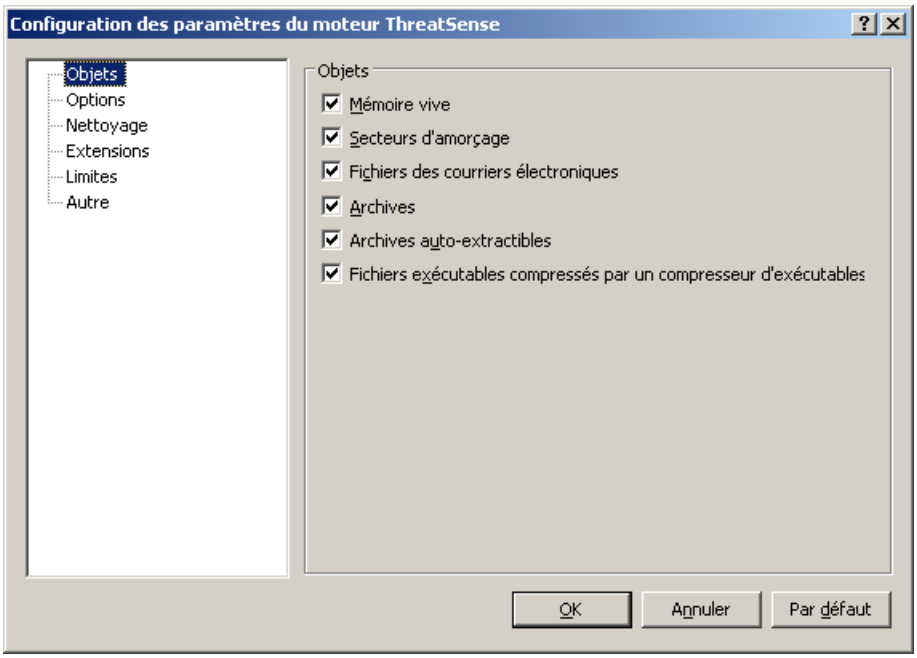
Pour ouvrir la fenêtre de configuration, cliquez sur le bouton **Configuration...** situé dans la fenêtre de configuration de tous les modules qui utilisent la technologie ThreatSense (reportez-vous aux informations ci-dessous). Chaque scénario de sécurité peut exiger une configuration différente. ThreatSense est configurable individuellement pour les modules de protection suivants :

- Protection en temps réel du système de fichiers 61
- Contrôle des fichiers de démarrage du système
- Protection de la messagerie 65
- Protection de l'accès Web 68
- Analyse de l'ordinateur à la demande 71

Les paramètres ThreatSense sont spécifiquement optimisés pour chaque module et leur modification peut avoir une incidence significative sur le fonctionnement du système. Par exemple, en modifiant les paramètres pour toujours analyser les fichiers exécutables compressés par un compresseur d'exécutables ou pour autoriser l'heuristique avancée dans le module de protection en temps réel du système de fichiers, vous pouvez dégrader les performances du système (normalement, seuls les nouveaux fichiers sont analysés par ces méthodes). Il est donc recommandé de ne pas modifier les paramètres par défaut de ThreatSense pour tous les modules, à l'exception du module d'analyse à la demande de l'ordinateur.

4.1.7.1 Configuration des objets

La section **Objets** permet de définir les fichiers et les composants de l'ordinateur qui vont faire l'objet d'une analyse visant à rechercher les éventuelles infiltrations.



Mémoire vive : lance une analyse visant à rechercher les menaces qui attaquent la mémoire vive du système.

Secteurs d'amorçage : analyse les secteurs d'amorçage afin de détection la présence éventuelle de virus dans l'enregistrement d'amorçage principal.

Fichiers : analyse tous les types de fichiers courants (programmes, images, musiques, vidéos, bases de données, etc.).

Fichiers des courriers électroniques : analyse les fichiers spéciaux contenant des messages électroniques.

Archives : analyse les fichiers compressés dans les archives (.rar, .zip, .arj, .tar, etc.).

Archives auto-extractibles : analyse les fichiers contenus dans les archives auto-extractibles et portant généralement l'extension .exe.

Fichiers exécutables compressés par un compresseur d'exécutables : contrairement aux types d'archives standard, les fichiers exécutables compressés par un compresseur d'exécutables sont décompressés en mémoire, en plus des fichiers exécutables compressés statiques standard (UPX, yoda, ASPack, FGS, etc.).

REMARQUE: Lorsqu'un point bleu s'affiche en regard d'un paramètre, cela indique que son réglage diffère de celui défini pour d'autres modules qui utilisent également ThreatSense. Étant donné que vous pouvez configurer le même paramètre différemment pour chaque module, ce point bleu n'est qu'un simple rappel que ce même paramètre est configuré différemment pour d'autres modules. L'absence de point bleu signifie que le paramètre de tous les modules est configuré de la même manière.

4.1.7.2 Options

Vous pouvez sélectionner dans la section **Options** les méthodes à utiliser lors de la recherche d'infiltrations dans le système. Les options disponibles sont les suivantes :

Heuristique : l'heuristique est un algorithme qui analyse l'activité (malveillante) des programmes. La détection heuristique présente l'avantage de détecter les nouveaux logiciels malveillants qui n'existaient pas auparavant ou qui ne figurent pas dans la liste des virus connus (base des signatures de virus).

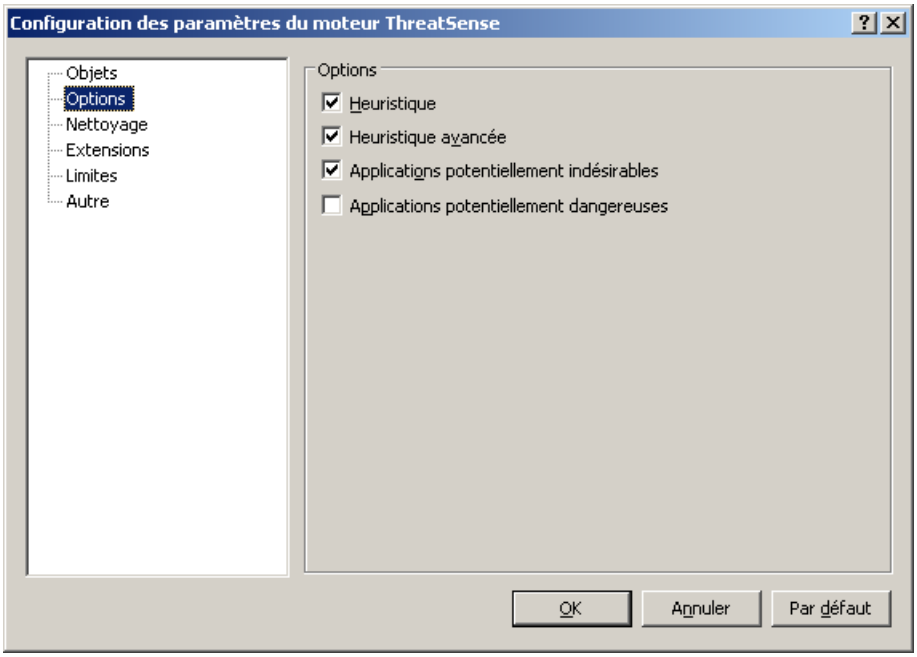
Heuristique avancée : cette option utilise un algorithme heuristique unique développé par ESET et optimisé pour la détection de vers informatiques et de chevaux de Troie écrits dans des langages de programmation de haut niveau. Grâce à l'heuristique avancée, les capacités de détection du programme sont très élevées.

Détection des applications potentiellement indésirables : les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur les performances de votre

ordinateur. Ces applications sont habituellement installées après consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Les changements les plus significatifs concernent l'affichage indésirable de fenêtres contextuelles, l'activation et l'exécution de processus cachés, l'augmentation de l'utilisation des ressources système, les changements dans les résultats de recherche et les applications communiquant avec des serveurs distants.

Applications potentiellement dangereuses : cette classification couvre les logiciels commerciaux légitimes. Elle inclut des programmes tels que des outils d'accès à distance. C'est pour cette raison que cette option est désactivée par défaut.

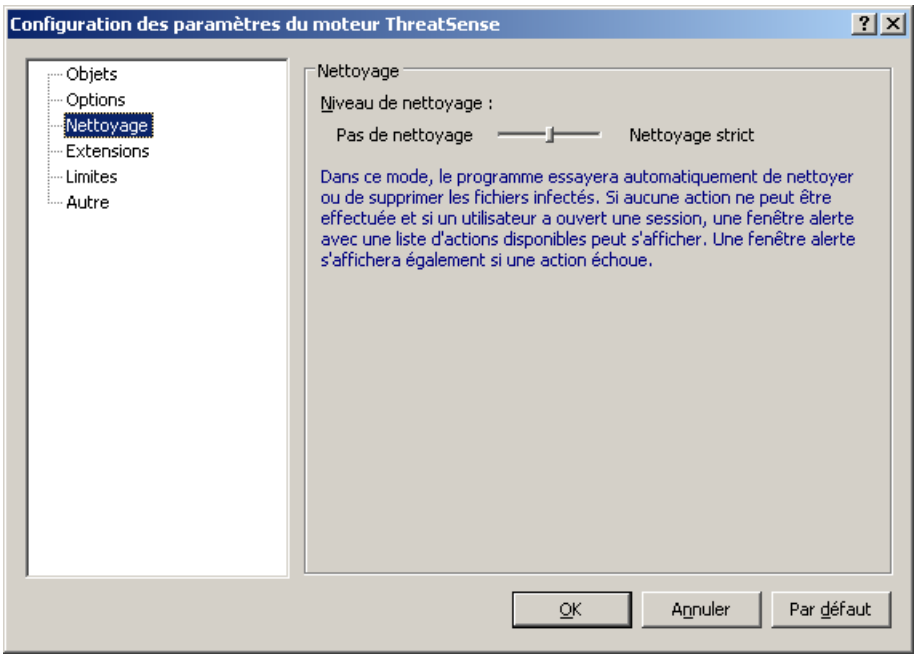
Pièces jointes potentiellement dangereuses
L'option Pièces jointes potentiellement dangereuses offre une protection contre les menaces malveillantes qui se propagent généralement sous forme de pièce jointe, telles que les chevaux de Troie « ransomware ». Ce type de menace peut correspondre à un fichier exécutable ressemblant à un fichier de document standard (PDF par exemple) lorsqu'il est ouvert par l'utilisateur, permettant ainsi à la menace de s'infiltrer dans le système. Cette menace essaie ensuite d'accomplir ses objectifs malveillants.



REMARQUE: Lorsqu'un point bleu s'affiche en regard d'un paramètre, cela indique que son réglage diffère de celui défini pour d'autres modules qui utilisent également ThreatSense. Étant donné que vous pouvez configurer le même paramètre différemment pour chaque module, ce point bleu n'est qu'un simple rappel que ce même paramètre est configuré différemment pour d'autres modules. L'absence de point bleu signifie que le paramètre de tous les modules est configuré de la même manière.

4.1.7.3 Nettoyage

Les paramètres de nettoyage déterminent le comportement de l'analyseur lors du nettoyage des fichiers infectés. Trois niveaux de nettoyage sont possibles :



Pas de nettoyage : les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche une fenêtre d'avertissement et permet à l'utilisateur de choisir une action.

Nettoyage standard : le programme essaie de nettoyer ou de supprimer automatiquement tout fichier infecté. S'il n'est pas possible de sélectionner automatiquement l'action correcte, le programme propose différentes actions de suivi. Cette sélection s'affiche également si une action prédéfinie ne peut pas être menée à bien.

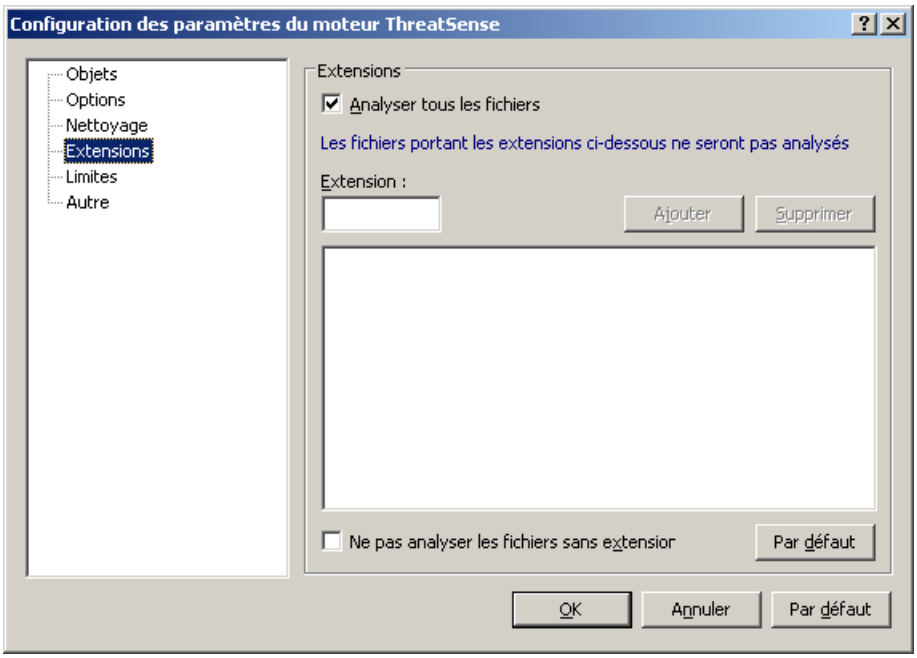
Nettoyage strict : le programme nettoie ou supprime tous les fichiers infectés (y compris les archives). Les seules exceptions sont les fichiers système. S'il n'est pas possible de les nettoyer, la fenêtre d'avertissement qui s'affiche propose différentes options.

Avertissement : Dans le mode par défaut, le fichier d'archive n'est entièrement supprimé que si tous les fichiers qu'il contient sont infectés. Si l'archive contient également des fichiers légitimes, elle n'est pas supprimée. Si un fichier d'archive infecté est détecté dans le mode Nettoyage strict, le fichier entier est supprimé, même s'il contient également des fichiers intacts.

REMARQUE: Lorsqu'un point bleu s'affiche en regard d'un paramètre, cela indique que son réglage diffère de celui défini pour d'autres modules qui utilisent également ThreatSense. Étant donné que vous pouvez configurer le même paramètre différemment pour chaque module, ce point bleu n'est qu'un simple rappel que ce même paramètre est configuré différemment pour d'autres modules. L'absence de point bleu signifie que le paramètre de tous les modules est configuré de la même manière.

4.1.7.4 Extensions

L'extension est la partie du nom de fichier située après le point. Elle définit le type et le contenu du fichier. Cette section de la configuration des paramètres ThreatSense vous permet de définir les types de fichiers à analyser.



Par défaut, tous les fichiers sont analysés, quelle que soit leur extension. Toutes les extensions peuvent être ajoutées à la liste des fichiers exclus de l'analyse. Si l'option **Analyser tous les fichiers** est désélectionnée, la liste change et affiche toutes les extensions des fichiers analysés. Les boutons **Ajouter** et **Supprimer** permettent d'activer ou d'empêcher l'analyse des extensions souhaitées.

Pour activer l'analyse de fichiers sans extension, sélectionnez l'option **Analyser les fichiers sans extension**.

L'exclusion de fichiers de l'analyse peut être utile si l'analyse de certains types de fichiers provoque un dysfonctionnement du programme utilisant ces extensions. Par exemple, il peut être judicieux d'exclure les extensions .edb, .eml et .tmp si vous utilisez le serveur Microsoft Exchange.

REMARQUE: Lorsqu'un point bleu s'affiche en regard d'un paramètre, cela indique que son réglage diffère de celui défini pour d'autres modules qui utilisent également ThreatSense. Étant donné que vous pouvez configurer le même paramètre différemment pour chaque module, ce point bleu n'est qu'un simple rappel que ce même paramètre est configuré différemment pour d'autres modules. L'absence de point bleu signifie que le paramètre de tous les modules est configuré de la même manière.

4.1.7.5 Limites

La section Limites permet de spécifier la taille maximale des objets et les niveaux d'imbrication des archives à analyser :

Taille d'objet maximale : définit la taille maximum des objets à analyser. Le module antivirus n'analyse alors que des objets d'une taille inférieure à celle spécifiée. Il n'est pas recommandé de modifier la valeur par défaut et il n'y a généralement aucune raison de le faire. Cette option ne doit être modifiée que par des utilisateurs chevronnés ayant des raisons très précises d'exclure de l'analyse les objets plus volumineux.

Durée d'analyse maximale pour l'objet (s) : définit la durée maximum attribuée à l'analyse d'un objet. Si la valeur de ce champ a été définie par l'utilisateur, le module antivirus cesse d'analyser un objet une fois ce temps écoulé, que l'analyse soit terminée ou non.

Niveau d'imbrication des archives : indique le nombre maximal de niveaux analysés dans les archives. Il n'est pas recommandé de modifier la valeur par défaut (10). Dans des circonstances normales, il n'y a aucune raison de le faire. Si l'analyse prend fin prématurément en raison du nombre d'archives imbriquées, l'archive reste non vérifiée.

Taille maximale de fichier dans l'archive : cette option permet de spécifier la taille maximale (après extraction) des fichiers à analyser qui sont contenus dans les archives. Si l'analyse d'une archive prend fin prématurément pour cette raison, l'archive reste non vérifiée.

REMARQUE: Lorsqu'un point bleu s'affiche en regard d'un paramètre, cela indique que son réglage diffère de celui défini pour d'autres modules qui utilisent également ThreatSense. Étant donné que vous pouvez configurer le même paramètre différemment pour chaque module, ce point bleu n'est qu'un simple rappel que ce même paramètre est configuré différemment pour d'autres modules. L'absence de point bleu signifie que le paramètre de tous les modules est configuré de la même manière.

4.1.7.6 Autre

Analyser les flux de données alternatifs (ADS) : les flux de données alternatifs (ADS) utilisés par le système de fichiers NTFS sont des associations de fichiers et de dossiers que les techniques d'analyse ordinaires ne permettent pas de détecter. De nombreuses infiltrations tentent d'éviter la détection en se faisant passer pour des flux de données alternatifs.

Exécuter les analyses en arrière-plan avec une priorité faible : toute séquence d'analyse consomme une certaine quantité de ressources système. Si vous utilisez des programmes qui exigent beaucoup de ressources système, vous pouvez activer l'analyse en arrière-plan à faible priorité de manière à réserver des ressources pour vos applications.

Journaliser tous les objets : si cette option est sélectionnée, le fichier journal affiche tous les fichiers analysés, même ceux qui ne sont pas infectés.

Activer l'optimalisation intelligente : sélectionnez cette option pour que les fichiers déjà analysés ne soient pas analysés plusieurs fois (sauf s'ils ont été modifiés). Les fichiers sont immédiatement réanalysés après chaque mise à jour de la base des signatures de virus.

Conserver la date et l'heure du dernier accès : sélectionnez cette option pour conserver l'heure d'accès d'origine des fichiers analysés au lieu de la mettre à jour (par exemple pour l'utiliser avec des systèmes de sauvegarde de données).

Dérouler journal : cette option permet d'autoriser/interdire le défilement du journal. Si cette option est sélectionnée, les informations défilent vers le haut dans la fenêtre d'affichage.

Afficher la notification de fin d'analyse dans une fenêtre séparée : ouvre une fenêtre indépendante contenant des informations sur les résultats d'analyse.

REMARQUE: Lorsqu'un point bleu s'affiche en regard d'un paramètre, cela indique que son réglage diffère de celui défini pour d'autres modules qui utilisent également ThreatSense. Étant donné que vous pouvez configurer le même paramètre différemment pour chaque module, ce point bleu n'est qu'un simple rappel que ce même paramètre est configuré différemment pour d'autres modules. L'absence de point bleu signifie que le paramètre de tous les modules est configuré de la même manière.

4.1.8 Une infiltration est détectée

Des infiltrations peuvent atteindre le système à partir de différents points d'entrée : pages Web, dossiers partagés, courrier électronique ou périphériques amovibles (USB, disques externes, CD, DVD, disquettes, etc.).

Si votre ordinateur montre des signes d'infection par un logiciel malveillant (ralentissement, blocages fréquents, etc.), nous recommandons d'effectuer les opérations suivantes :

- Ouvrez ESET Mail Security et cliquez sur Analyse de l'ordinateur.
- Cliquez sur **Analyse intelligente** (pour plus d'informations, reportez-vous à la section Analyse intelligente 72).
- Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.

Si vous ne souhaitez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez des cibles à analyser.

Pour donner un exemple général de la façon dont les infiltrations sont traitées dans ESET Mail Security, supposons qu'une infiltration soit détectée par la protection en temps réel du système de fichiers, qui utilise le niveau de nettoyage par défaut. Le programme tente de nettoyer ou de supprimer le fichier. Si aucune action n'est prédéfinie pour le module de protection en temps réel, vous êtes invité à sélectionner une option dans une fenêtre d'avertissement. Généralement, les options **Nettoyer**, **Supprimer** et **Aucune action** sont disponibles. Il n'est pas recommandé de sélectionner **Aucune action**, car les fichiers infectés sont conservés tels quels. La seule exception concerne les situations où vous êtes sûr que le fichier est inoffensif et qu'il a été détecté par erreur.

Nettoyage et suppression : utilisez le nettoyage si un fichier sain a été attaqué par un virus qui y a joint du code malveillant. Dans ce cas, essayez d'abord de nettoyer le fichier infecté pour le restaurer dans son état d'origine. Si le

fichier se compose uniquement de code malveillant, il est supprimé.

Si un fichier infecté est « verrouillé » ou utilisé par un processus système, il n'est généralement supprimé qu'après avoir été déverrouillé (normalement, après un redémarrage du système).

Suppression de fichiers dans des archives : en mode de nettoyage par défaut, l'archive complète n'est supprimée que si elle ne contient que des fichiers infectés et aucun fichier sain. Autrement dit, les archives ne sont pas supprimées si elles contiennent également des fichiers sains. Cependant, soyez prudent si vous choisissez un nettoyage strict : dans ce mode, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

4.2 Mise à jour du programme

La mise à jour régulière d'ESET Mail Security est la condition de base pour l'obtention du niveau maximum de sécurité. Le module de mise à jour veille à ce que le programme soit toujours à jour de deux façons : en mettant à jour la base des signatures de virus et en mettant à jour les composants système.

En cliquant sur **Mettre à jour** dans le menu principal, vous pouvez connaître l'état actuel de la mise à jour, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire. La fenêtre Mise à jour contient également la version de la base des signatures de virus. Cette indication numérique est un lien actif vers le site Web d'ESET, qui répertorie toutes les signatures ajoutées dans cette mise à jour.

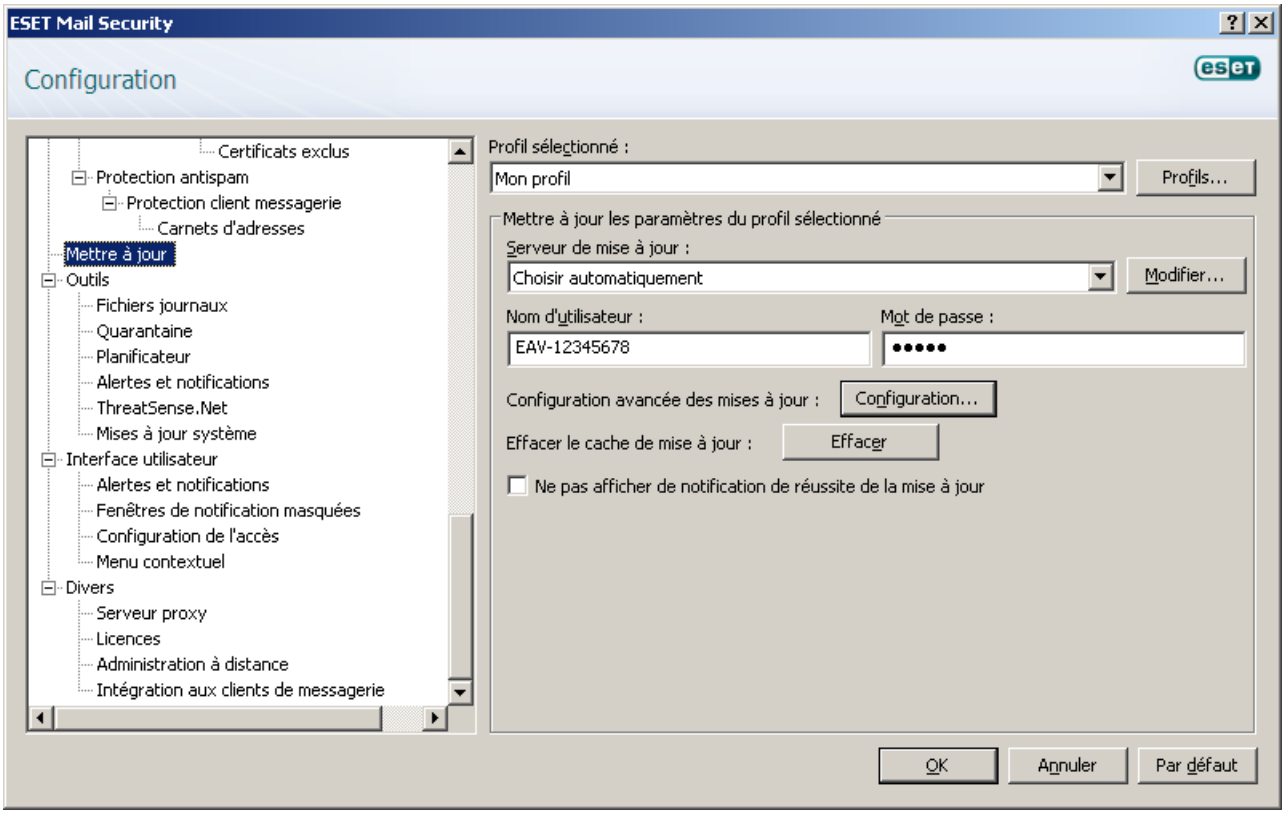
Par ailleurs, l'option permettant de commencer manuellement le processus de mise à jour, **Mettre à jour la base des signatures de virus**, est disponible, de même que les options de configuration de base de la mise à jour telles que le nom d'utilisateur et le mot de passe permettant d'accéder aux serveurs de mise à jour d'ESET.

Utilisez le lien **Activation de produit** pour ouvrir un formulaire d'enregistrement qui nous permet d'activer le produit de sécurité ESET et de vous envoyer un courrier électronique avec vos données d'authentification (nom d'utilisateur et mot de passe).

REMARQUE : le nom d'utilisateur et le mot de passe sont fournis par ESET après l'achat d'ESET Mail Security.

4.2.1 Configuration des mises à jour

La section de la configuration des mises à jour permet de spécifier les informations concernant les sources des mises à jour, telles que les serveurs de mise à jour et les données d'authentification donnant accès à ces serveurs. Par défaut, le menu déroulant **Serveur de mise à jour** est défini sur l'option **Choisir automatiquement**, ce qui garantit que les fichiers de mise à jour sont téléchargés automatiquement depuis le serveur ESET en utilisant le moins de ressources réseau possible. Les options de configuration des mises à jour sont disponibles dans l'arborescence de configuration avancée (touche F5), dans **Mettre à jour**.

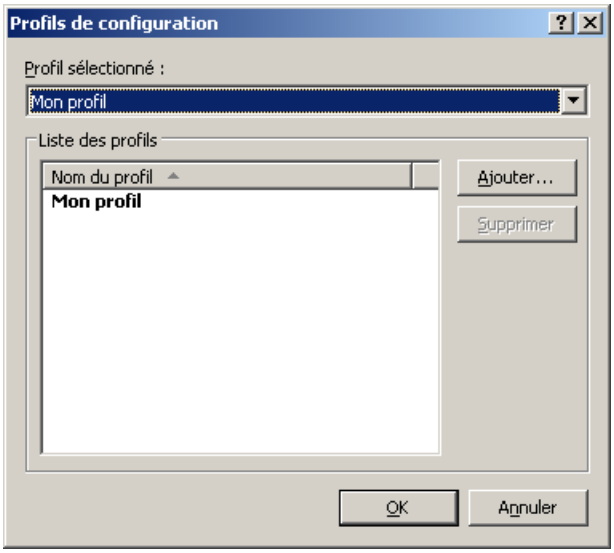


La liste des serveurs de mise à jour disponibles est accessible par l'intermédiaire du menu déroulant **Serveur de mise à jour**. Pour ajouter un nouveau serveur de mise à jour, cliquez sur **Modifier...** dans la section **Mettre à jour les paramètres du profil sélectionné**, puis cliquez sur le bouton **Ajouter**. L'authentification des serveurs de mise à jour est basée sur le **nom d'utilisateur** et le **mot de passe** générés et qui vous ont été envoyés après l'achat.

4.2.1.1 Profils de mise à jour

Les profils de mise à jour ne peuvent pas être créés pour différentes configurations et tâches de mise à jour. La création de profils de mise à jour est particulièrement utile pour les utilisateurs mobiles qui peuvent créer un autre profil correspondant aux propriétés de connexion Internet qui changent régulièrement.

Le menu déroulant **Profil sélectionné** affiche le profil sélectionné ; il est défini par défaut sur **Mon profil**. Pour créer un nouveau profil, cliquez sur les boutons **Profils...** et **Ajouter...**, puis indiquez votre propre **Nom du profil**. Lorsque de la création d'un nouveau profil, vous pouvez copier les paramètres d'un profil existant en le sélectionnant dans le menu déroulant **Copier les paramètres depuis le profil**.



Dans la fenêtre de configuration du profil, vous pouvez indiquer le serveur de mise à jour dans la liste des serveurs disponibles ou encore ajouter un nouveau serveur. La liste des serveurs de mise à jour existants est accessible par l'intermédiaire du menu déroulant **Serveur de mise à jour** : . Pour ajouter un nouveau serveur de mise à jour, cliquez sur **Modifier...** dans la section **Mettre à jour les paramètres du profil sélectionné**, puis cliquez sur le bouton **Ajouter**.

4.2.1.2 Configuration avancée des mises à jour

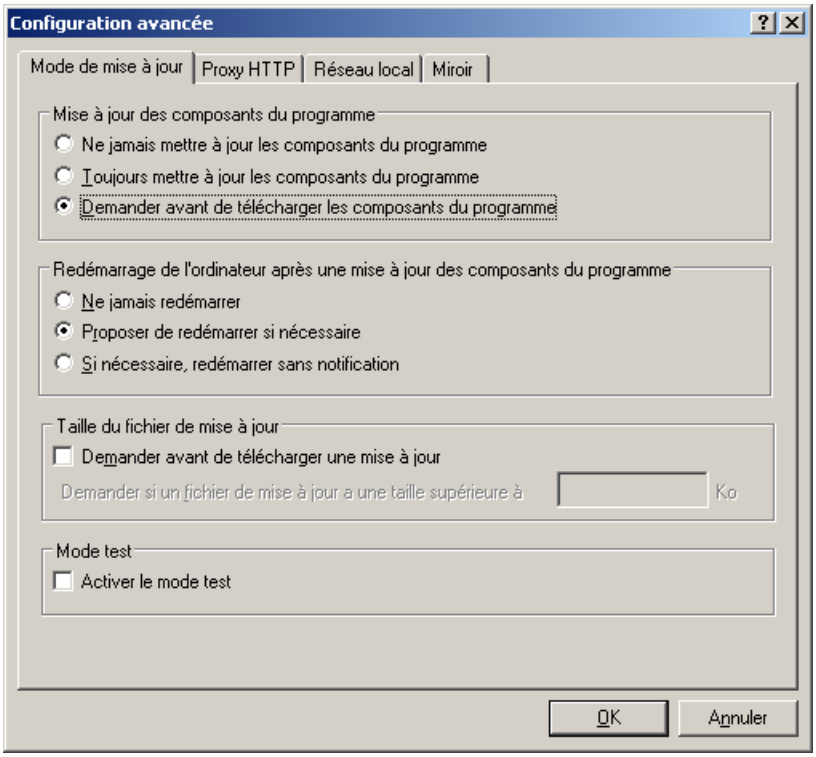
Pour afficher la configuration avancée des mises à jour, cliquez sur le bouton **Configuration...**. Les options de configuration avancée de mise à jour englobent les options **Mode de mise à jour**, **Proxy HTTP**, **Réseau local** et **Miroir**.

4.2.1.2.1 Mode de mise à jour

L'onglet **Mode de mise à jour** contient les options concernant la mise à jour des composants du programme.

Dans la section **Mise à jour des composants du programme**, trois options sont disponibles :

- **Ne jamais mettre à jour les composants du programme** : aucune mise à jour des composants du programme n'est effectuée.
- **Toujours mettre à jour les composants du programme** : Les mises à jour des composants du programme sont effectuées automatiquement.
- **Demander avant de télécharger les composants du programme** : Il s'agit de l'option par défaut. Vous êtes invité à confirmer ou à refuser les mises à jour de composants de programme lorsqu'elles sont disponibles.



Après l'installation d'une mise à jour de composants du programme, il est peut-être nécessaire de redémarrer l'ordinateur afin d'obtenir la pleine fonctionnalité de tous les modules. La section **Redémarrer après une mise à jour des composants du programme** vous permet de choisir l'une des trois options suivantes :

- **Ne jamais redémarrer**
- **Proposer le redémarrage de l'ordinateur si nécessaire**
- **Si nécessaire**, **redémarrer l'ordinateur sans avertissement**

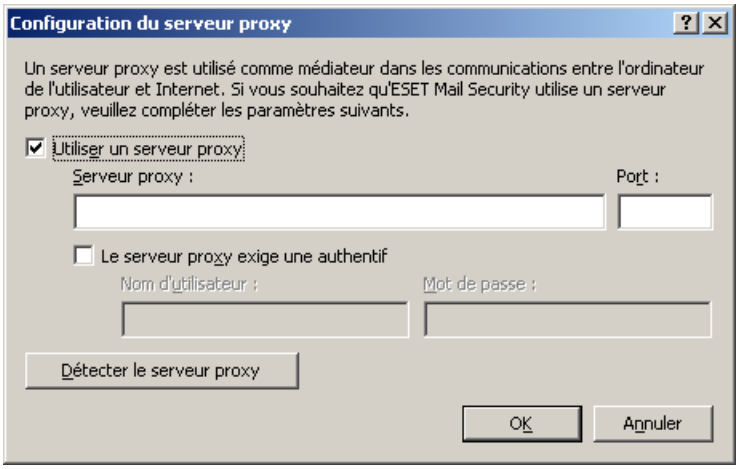
L'option par défaut est **Proposer le redémarrage de l'ordinateur si nécessaire**. La sélection de l'option la plus appropriée dépend du poste de travail sur lequel les paramètres sont appliqués. Notez qu'il existe des différences entre les postes de travail et les serveurs. Par exemple, le redémarrage automatique d'un serveur après une mise à niveau du programme peut causer de sérieux dommages.

4.2.1.2.2 Serveur proxy

Dans ESET Mail Security, la configuration du serveur proxy est disponible dans deux sections de l'arborescence de configuration avancée.

Les paramètres de serveur proxy peuvent être configurés dans **Divers** > **Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour l'intégralité d'ESET Mail Security. Les paramètres définis ici seront utilisés par tous les modules exigeant une connexion à Internet.

Pour spécifier des paramètres de serveur proxy à ce niveau, cochez la case **Utiliser un serveur proxy**, puis entrez l'adresse du serveur proxy dans le champ **Serveur proxy** : , ainsi que le numéro de **port** du serveur proxy.



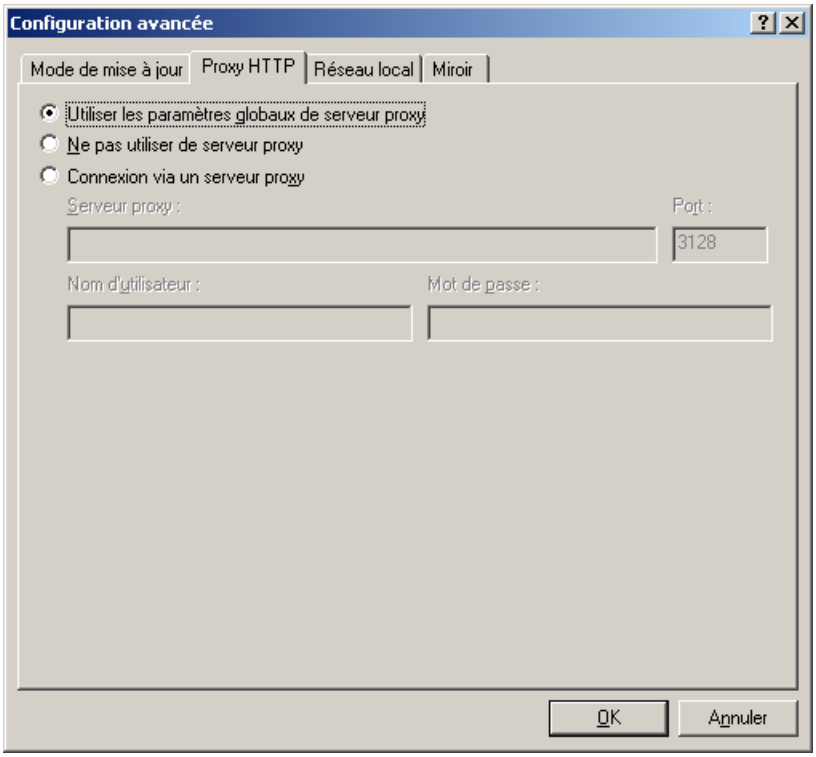
Si la communication avec le serveur proxy exige une authentification, cochez la case **Le serveur proxy nécessite une authentification** et entrez un nom d'utilisateur et un mot de passe valides dans les champs correspondants. Cliquez sur le bouton **Détecter le serveur proxy** pour détecter automatiquement et insérer les paramètres du serveur proxy. Les paramètres indiqués dans Internet Explorer sont copiés.

REMARQUE : cette fonctionnalité ne récupère pas les données d'authentification (nom d'utilisateur et mot de passe) et vous devez les fournir.

Les paramètres de serveur proxy peuvent également être établis dans la configuration avancée de la mise à jour. Ces paramètres s'appliquent au profil de mise à jour donné. Vous pouvez accéder aux options de configuration du serveur proxy pour un profil de mise à jour donné en cliquant sur l'onglet **Proxy HTTP** dans **Configuration avancée des mises à jour**. Vous avez le choix entre ces trois options :

- **Utiliser les paramètres globaux de serveur proxy**
- **Ne pas utiliser de serveur proxy**
- **Connexion via un serveur proxy** (connexion définie par les propriétés de la connexion)

L'option **Utiliser les paramètres globaux de serveur proyx** utilise les options de configuration de serveur proxy déjà indiquées dans la branche **Divers** > **Seveur proxy** de l'arborescence de configuration avancée (comme indiqué précédemment dans le présent article).



Sélectionnez l'option **Ne pas utiliser de serveur proxy** pour indiquer qu'aucun serveur proxy ne sera utilisé pour la mise à jour de ESET Mail Security.

L'option **Connexion via un serveur proxy** doit être sélectionnée si vous souhaitez utiliser un serveur proxy pour mettre à jour ESET Mail Security. Ce serveur proxy doit être différent de celui indiqué dans les paramètres globaux (**Divers** > **Serveur proxy**). Si c'est le cas, des paramètres supplémentaires doivent être spécifiés : **l'adresse du serveur** proxy, le **Port** de communication, ainsi que le **Nom d'utilisateur** et le **Mot de passe** du serveur proxy, si nécessaire.

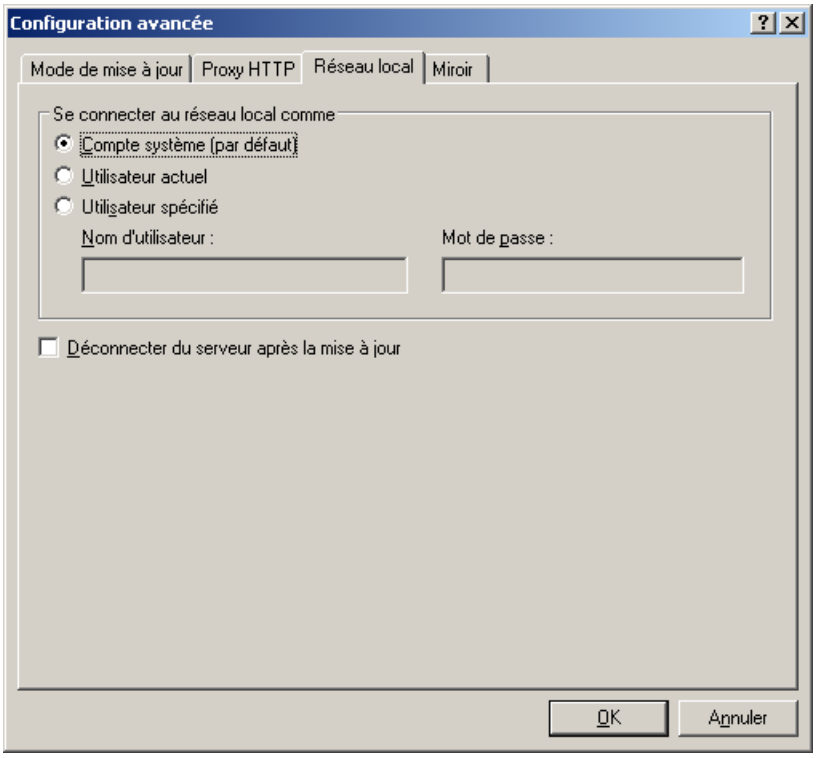
Cette option doit également être sélectionnée si les paramètres de serveur proxy n'ont pas été définis globalement, mais ESET Mail Security se connecte à un serveur proxy pour les mises à jour.

L'option par défaut pour le serveur proxy est **Utiliser les paramètres globaux de serveur proxy**.

4.2.1.2.3 Connexion au réseau local

Lors de mise à jour depuis un serveur local sur un système d'exploitation NT, une authentification est par défaut exigée pour chaque connexion réseau. Dans la plupart des cas, un compte système local n'a pas suffisamment de droits pour accéder au dossier miroir (ce dossier contient des copies des fichiers de mise à jour). Dans ce cas, entrez un nom d'utilisateur et un mot de passe dans la section de configuration des mises à jour ou spécifiez un compte avec lequel le programme peut accéder au serveur de mise à jour (miroir).

Pour configurer un compte de ce type, cliquez sur l'onglet **Réseau local**. La section **Se connecter au réseau local comme** propose les options **Compte système** (**par défaut**), **Utilisateur actuel** et **Utilisateur spécifié**.



Sélectionnez l'option **Compte système** (**par défaut**) pour utiliser le compte système pour l'authentification. Normalement, aucun traitement d'authentification n'a lieu si des données d'authentification ne sont pas fournies dans la section de configuration des mises à jour.

Pour s'assurer que le programme s'authentifie avec le compte de l'utilisateur actuellement connecté, sélectionnez **Utilisateur actuel**. L'inconvénient de cette solution est que le programme est dans l'impossibilité de se connecter au serveur de mise à jour si aucun utilisateur n'est connecté.

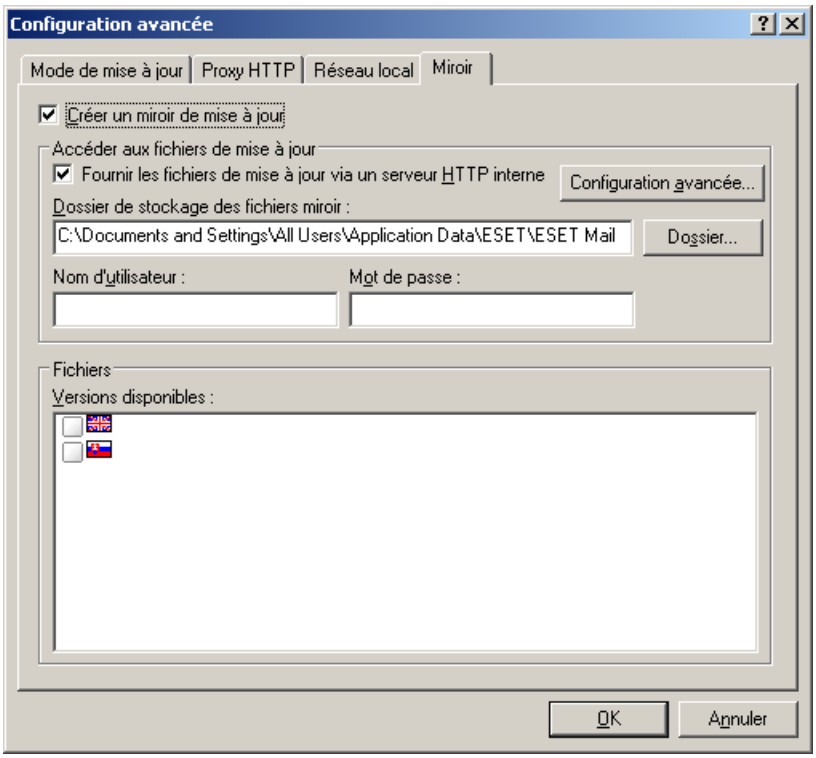
Sélectionnez **Utilisateur spécifié** si vous voulez que le programme utilise un compte utilisateur spécifié pour l'authentification.

Avertissement : Si l'une des options **Utilisateur actuel** ou **Utilisateur spécifié** est sélectionnée, une erreur peut se produire en cas de changement de l'identité du programme pour l'utilisateur souhaité. C'est pour cela que nous recommandons d'entrer les données d'authentification du réseau local dans la section de configuration des mises à jour. Dans cette section de configuration des mises à jour, les données d'authentification doivent être entrées comme suit : nom_de_domaine\utilisateur (dans le cas d'un groupe de travail, entrez nom_de_groupe_de_travail\utilisateur) et le mot de passe de l'utilisateur. La mise à jour de la version HTTP du serveur local n'exige aucune authentification.

4.2.1.2.4 Création de copies de mises à jour : miroir

ESET Mail Security vous permet de créer des copies des fichiers de mises à jour qui peuvent être utilisées pour la mise à jour d'autres postes de travail du réseau. La mise à jour de postes de travail à partir d'un miroir optimise l'équilibre de la charge réseau et libère les bandes passantes des connexions Internet.

Les options de configuration du serveur miroir local sont accessibles (après l'ajout d'une clé de licence valide dans le gestionnaire de licences dans la section Configuration d'avancée de ESET Mail Security) dans la section **Configuration avancée des mises à jour** : . Pour accéder à cette section, appuyez sur la touche F5 et cliquez sur **Mettre à jour** dans l'arborescence de configuration avancée, puis cliquez sur le bouton **Configuration...** situé à côté de **Configuration avancée des mises à jour** : , puis sélectionnez l'onglet **Miroir**).



La première étape de configuration du miroir consiste à sélectionner l'option Créer un miroir de mise à jour. La sélection de cette option active d'autres options de configuration du miroir, telles que la manière d'accéder aux fichiers de mise à jour et le chemin des fichiers miroir.

Les méthodes d'activation du miroir sont décrites en détail dans la section Mise à jour à partir du miroir 91. Pour le moment, notez qu'il existe deux méthodes de base pour accéder au miroir : le dossier des fichiers de mise à jour peut être considéré comme un dossier réseau partagé ou comme un serveur HTTP.

Le dossier dédié aux fichiers de mise à jour du miroir peut être défini dans la section **Dossier de stockage des fichiers miroir**. Cliquez sur **Dossier...** pour naviguer jusqu'au dossier souhaité sur un ordinateur local ou un dossier réseau partagé. Si une autorisation pour le dossier spécifié est requise, les données d'authentification doivent être entrées dans les champs **Nom d'utilisateur** et **Mot de passe**. Le nom d'utilisateur et le mot de passe doivent être entrés sous le format *Domaine/Utilisateur* ou *Workgroup/Utilisateur*. N'oubliez pas de fournir les mots de passe correspondants.

Lors de la configuration du miroir, vous pouvez également spécifier les différentes langues des copies de mises à jour à télécharger. La configuration de la langue de version est accessible dans la section **Fichiers** - **Versions disponibles** :.

REMARQUE : La base de données antispam ne peut pas être mise à jour depuis le miroir. Pour plus d'informations sur les mises à jour de base de données antispam correctes, cliquez ici 37.

4.2.1.2.4.1 Mise à jour à partir du miroir

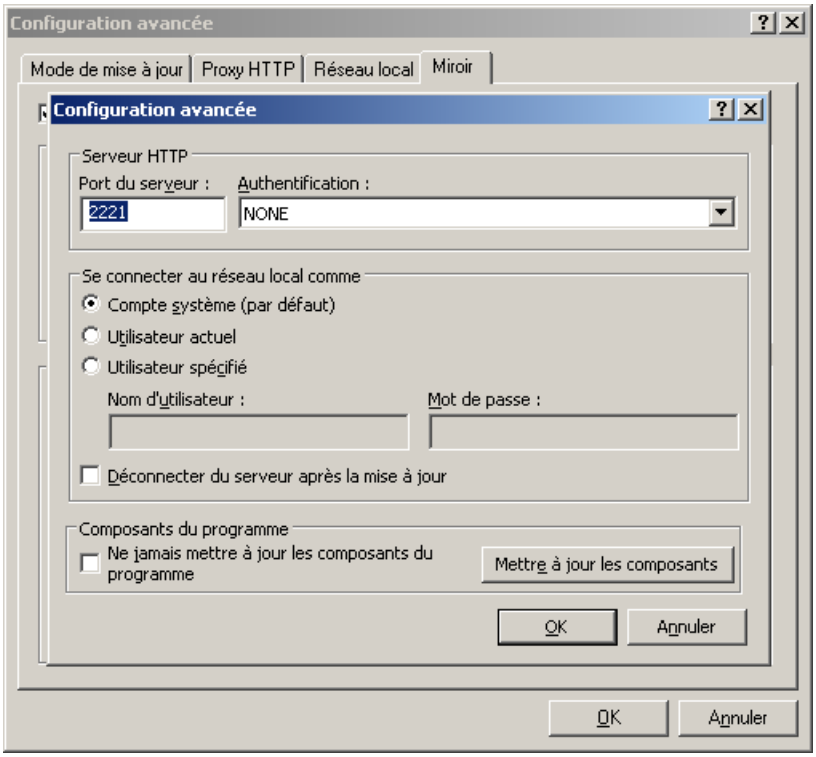
Il existe deux méthodes de base pour configurer le miroir : le dossier des fichiers de mise à jour peut être considéré comme un dossier réseau partagé ou comme un serveur HTTP.

Accès au miroir au moyen d'un serveur HTTP interne

Cette configuration est l'option par défaut ; elle est indiquée dans la configuration du programme prédéfinie. Afin de permettre l'accès au miroir à l'aide du serveur HTTP, accédez aux options **Configuration avancée des mises à jour** (onglet **Miroir**) et sélectionnez l'option **Créer un miroir de mise à jour**.

Dans la section **Configuration avancée** de l'onglet **Miroir**, vous pouvez indiquer le **Port du serveur** sur lequel le serveur HTTP écoute, ainsi que le type d'**Authentification** utilisé par le serveur HTTP. Par défaut, cette option est configurée sur **2221**. L'option **Authentification** définit la méthode d'authentification utilisée pour accéder aux fichiers de mise à jour. Les options disponibles sont les suivantes : **AUCUNE**, **De base** et **NTLM**. Sélectionnez **De base** pour utiliser le codage base64 avec l'authentification de base du nom d'utilisateur et mot de passe. L'option **NTLM** fournit un codage utilisant une méthode de codage fiable. L'utilisateur créé sur le poste de travail partageant les fichiers de mise à jour est utilisé pour l'authentification. L'option par défaut est **AUCUNE**. Elle autorise l'accès aux fichiers des mises à jour sans exiger d'authentification.

Avertissement : l'accès aux fichiers des mises à jour au moyen du serveur HTTP exige que le dossier miroir soit sur le même ordinateur que l'instance ESET Mail Security qui l'a créé.



Une fois la configuration du miroir terminée, ajoutez aux postes de travail un nouveau serveur de mise à jour dans le format **http://adresse_IP_de_votre_serveur:2221**. Pour ce faire, procédez comme suit :

- Ouvrez **Configuration avancée** de ESET Mail Security et cliquez sur la branche **Mise à jour**.
- Cliquez sur **Modifier...** à droite du menu contextuel **Serveur de mise à jour** et ajoutez un nouveau serveur en respectant le format suivant : http://IP_adresse_de_votre_serveur:2221.
- Sélectionnez dans la liste des serveurs de mise à jour le serveur nouvellement ajouté.

Accès au miroir via le partage des systèmes

Un dossier partagé doit d'abord être créé sur un lecteur local ou réseau. Lors de la création du dossier pour le miroir, il est nécessaire d'octroyer le droit d'écriture à l'utilisateur qui va sauvegarder les fichiers de mise à jour dans le dossier et le droit de lecture aux utilisateurs qui vont utiliser le dossier miroir pour la mise à jour de ESET Mail Security.

Continuez ensuite la configuration d'accès au miroir dans la section **Configuration avancée des mises à jour** (onglet **Miroir**) en désactivant l'option **Fournir les fichiers de mise à jour via un serveur HTTP interne**. Cette

option est activée par défaut lors de l'installation du programme.

Si le dossier partagé se trouve sur un autre ordinateur du réseau, une authentification est nécessaire pour accéder à l'autre ordinateur. Pour spécifier les données d'authentification, ouvrez Configuration avancée d'ESET Mail Security (F5) et cliquez sur la branche **Mise à jour**. Cliquez sur le bouton **Configuration...**, puis cliquez sur l'onglet **Réseau local**. Ce paramètre est le même que celui de la mise à jour, comme l'indique la section Connexion au réseau local 89.

Une fois la configuration du miroir terminée, continuez avec les postes de travail en spécifiant \\UNC\CHEMIN comme serveur de mise à jour. Cette opération peut s'effectuer comme suit :

- Ouvrez Configuration avancée de ESET Mail Security et cliquez sur **Mise à jour**
- Cliquez sur **Modifier...** en regard de Serveur de mise à jour et ajoutez un nouveau serveur au *format* *UNC**PATH*.
- Sélectionnez dans la liste des serveurs de mise à jour le serveur nouvellement ajouté.

REMARQUE : pour un fonctionnement correct, le chemin du dossier miroir doit être spécifié comme un chemin UNC. Les mises à jour à partir de lecteurs mappés peuvent ne pas fonctionner.

4.2.1.2.4.2 Dépannage des problèmes de miroir de mise à jour

Dans la plupart des cas, les problèmes de mise à jour depuis un serveur miroir proviennent des raisons suivantes : mauvaise spécification des options du dossier miroir, données d'authentification incorrectes pour l'accès au dossier miroir, mauvaise configuration des postes de travail qui cherchent à télécharger des fichiers de mise à jour du miroir ou combinaison des raisons citées précédemment. Nous donnons ici un aperçu des problèmes les plus fréquents qui peuvent se produire lors d'une mise à jour depuis le miroir :

ESET Mail Security **signale une erreur de connexion au serveur miroir** : l'erreur est probablement causée par une spécification incorrecte du serveur de mise à jour (chemin réseau du dossier miroir) à partir duquel les postes de travail locaux téléchargent les mises à jour. Pour vérifier le dossier, cliquez sur (Windows) **Démarrer > Exécuter** entrez le nom du dossier et cliquez sur **OK**. Le contenu du dossier doit s'afficher.

ESET Mail Security **exige un nom d'utilisateur etun mot de passe** : l'erreur est probablement causée par l'entrée dans la section mise à jour de données d'authentification incorrectes (Nom d'utilisateur et Mot de passe). Le nom d'utilisateur et le mot de passe donnent accès au serveur de mise à jour, à partir duquel le programme se télécharge. Assurez-vous que les données d'authentification sont correctes et entrées dans le bon format. Par exemple, *Domaine/Nom d'utilisateur* ou *Workgroup/Nom d'utilisateur*, en plus des mots de passe correspondants. Si le serveur miroir est accessible à Tous, cela ne veut pas dire que tout utilisateur est autorisé à y accéder. « Tous » ne veut pas dire tout utilisateur non autorisé, cela veut tout simplement dire que le dossier est accessible à tous les utilisateurs du domaine. Par conséquent, si le dossier est accessible à Tous, un nom d'utilisateur du domaine et un mot de passe sont toujours nécessaires et doivent être entrés dans la configuration des mises à jour.

ESET Mail Security **signale une erreur de connexion au serveur miroir** - Le port de communication défini pour l'accès au miroir via HTTP est bloqué.

4.2.2 Comment créer des tâches de mise à jour

Vous pouvez déclencher les mises à jour manuellement en cliquant sur **Mettre à jour la base des signatures de virus** dans la fenêtre principale qui s'affiche lorsque vous cliquez sur Mettre à jour dans le menu principal.

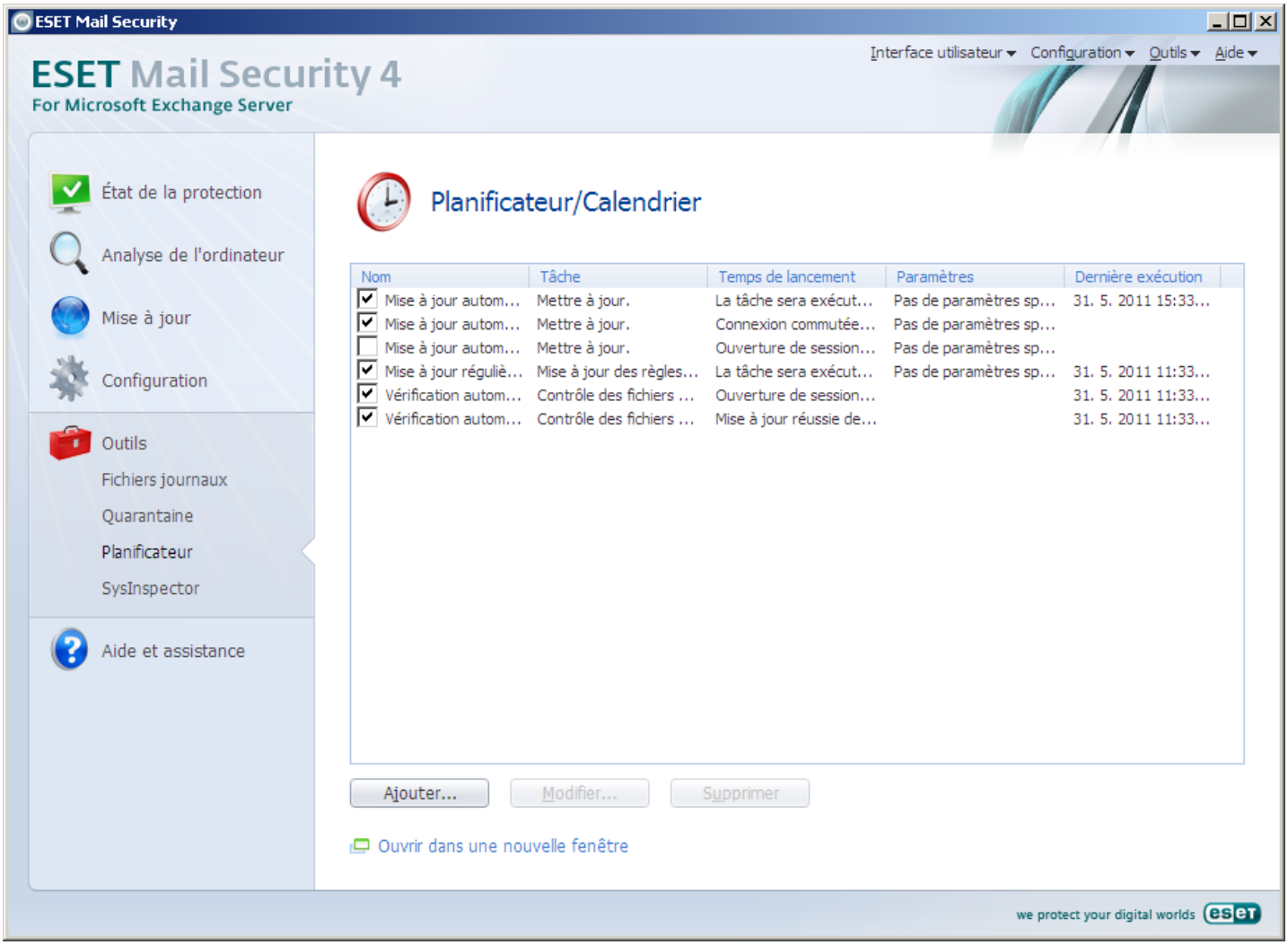
Les mises à jour peuvent également être exécutées sous forme de tâches planifiées. Pour configurer une tâche planifiée, cliquez sur **Outils** > **Planificateur**. Par défaut, les tâches suivantes sont activées dans ESET Mail Security :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**

Chaque tâche de mise à jour peut être modifiée selon les besoins de l'utilisateur. Outre les tâches de mise à jour par défaut, vous pouvez en créer des nouvelles avec vos propres paramètres. Pour plus d'informations sur la création et la configuration des tâches de mise à jour, reportez-vous à la section Planificateur 93.

4.3 Planificateur

Le planificateur est disponible si l'option Mode avancé dans ESET Mail Security est activée. Le **Planificateur** est accessible depuis le menu principal d'ESET Mail Security, dans **Outils**. Le planificateur contient la liste de toutes les tâches planifiées et des propriétés de configuration telles que la date et l'heure prédéfinies, ainsi que le profil d'analyse utilisé.



Par défaut, les tâches planifiées suivantes sont affichées dans le **Planificateur** :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**
- **Vérification automatique des fichiers de démarrage**
- **Vérification automatique des fichiers de démarrage après la mise à jour réussie de la base des signatures de virus**

Pour modifier la configuration d'une tâche planifiée existante (par défaut ou définie par l'utilisateur), cliquez avec le bouton droit sur la tâche et cliquez sur **Modifier...** Vous pouvez également sélectionner la tâche à modifier et cliquer sur le bouton **Modifier...**

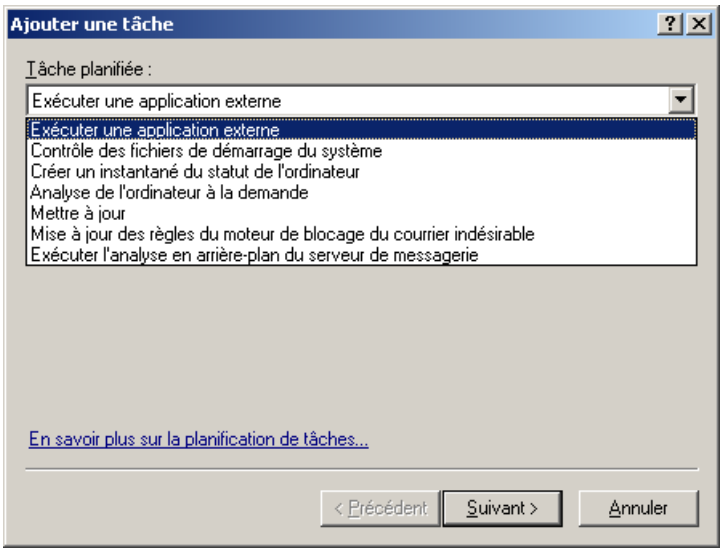
4.3.1 Pourquoi planifier des tâches ?

Le planificateur gère et lance les tâches planifiées qui ont été préalablement définies et configurées. La configuration et les propriétés comprennent des informations telles que la date et l'heure, ainsi que des profils spécifiques à utiliser pendant l'exécution de la tâche.

4.3.2 Création de nouvelles tâches

Pour créer une nouvelle tâche dans le planificateur, cliquez sur le bouton **Ajouter...** ou cliquez avec le bouton droit sur la tâche et sélectionnez **Ajouter...** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter une application externe**
- **Contrôle des fichiers de démarrage du système**
- **Créer un instantané du statut de l'ordinateur**
- **Analyse de l'ordinateur à la demande**
- **Mettre à jour**



La tâche planifiée la plus fréquente étant la **mise à jour**, nous allons expliquer comment ajouter une nouvelle tâche de mise à jour.

Dans le menu déroulant **Tâche planifiée** : , sélectionnez **Mettre à jour**. Cliquez sur **Suivant** et saisissez le nom de la tâche dans le champ **Nom de la tâche** : . Sélectionnez la fréquence de la tâche. Les options disponibles sont les suivantes : **Une fois**, **Plusieurs fois**, **Quotidiennement**, **Hebdo** et **Déclenchée par un événement**. Selon la fréquence sélectionnée, vous serez invité à choisir différents paramètres de mise à jour. Vous pouvez définir ensuite l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les trois options suivantes sont disponibles :

- **Attendre le prochain moment planifié**
- **Exécuter la tâche dès que possible**
- **Exécuter la tâche immédiatement si le temps écoulé depuis la dernière exécution dépasse l'intervalle spécifié** (l'intervalle peut être défini à l'aide de la zone de liste déroulante Intervalle minimal entre deux tâches)

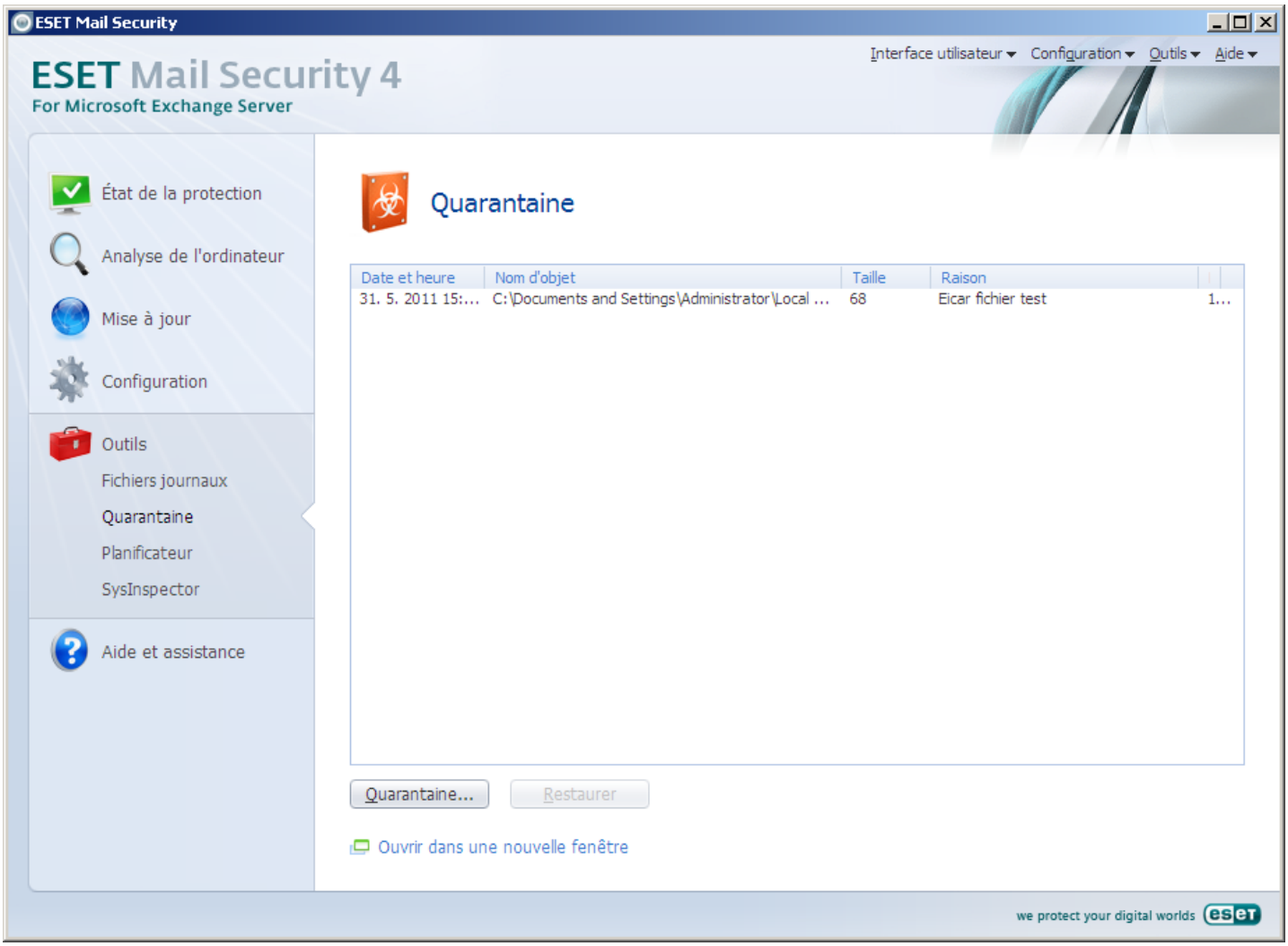
L'étape suivante affiche un résumé complet de la tâche planifiée courante ; l'option **Exécuter la tâche avec des paramètres spécifiques** doit être automatiquement activée. Cliquez sur le bouton **Terminer**.

La boîte de dialogue qui apparaît permet de sélectionner les profils à utiliser pour la tâche planifiée. L'utilisateur peut spécifier un profil principal et un profil secondaire qui sera utilisé si la tâche ne peut s'exécuter à l'aide du profil principal. Confirmez en cliquant sur **OK** dans la fenêtre **Profils de mise à jour**. La nouvelle tâche planifiée est ajoutée à la liste des tâches planifiées.

4.4 Quarantaine

La principale fonction de la quarantaine est le stockage en toute sécurité des fichiers infectés. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés erronément par ESET Mail Security.

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine. Cette action est conseillée si un fichier se comporte de façon suspecte mais n'a pas été détecté par l'analyseur antivirus. Les fichiers de la quarantaine peuvent être soumis pour analyse au laboratoire de recherche sur les menaces d'ESET.



Les fichiers du dossier de quarantaine peuvent être visualisés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin de l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (**ajouté par l'utilisateur...**), ainsi que le nombre de menaces (s'il s'agit par exemple d'une archive contenant plusieurs infiltrations).

4.4.1 Mise en quarantaine de fichiers

ESET Mail Security déplace automatiquement les fichiers supprimés en quarantaine (si vous n'avez pas annulé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur le bouton **Quarantaine...** Dans ce cas, le fichier d'origine n'est pas supprimé de son emplacement initial. Il est également possible d'utiliser le menu contextuel à cette fin : cliquez avec le bouton droit dans la fenêtre **Quarantaine** et sélectionnez l'option **Ajouter...**

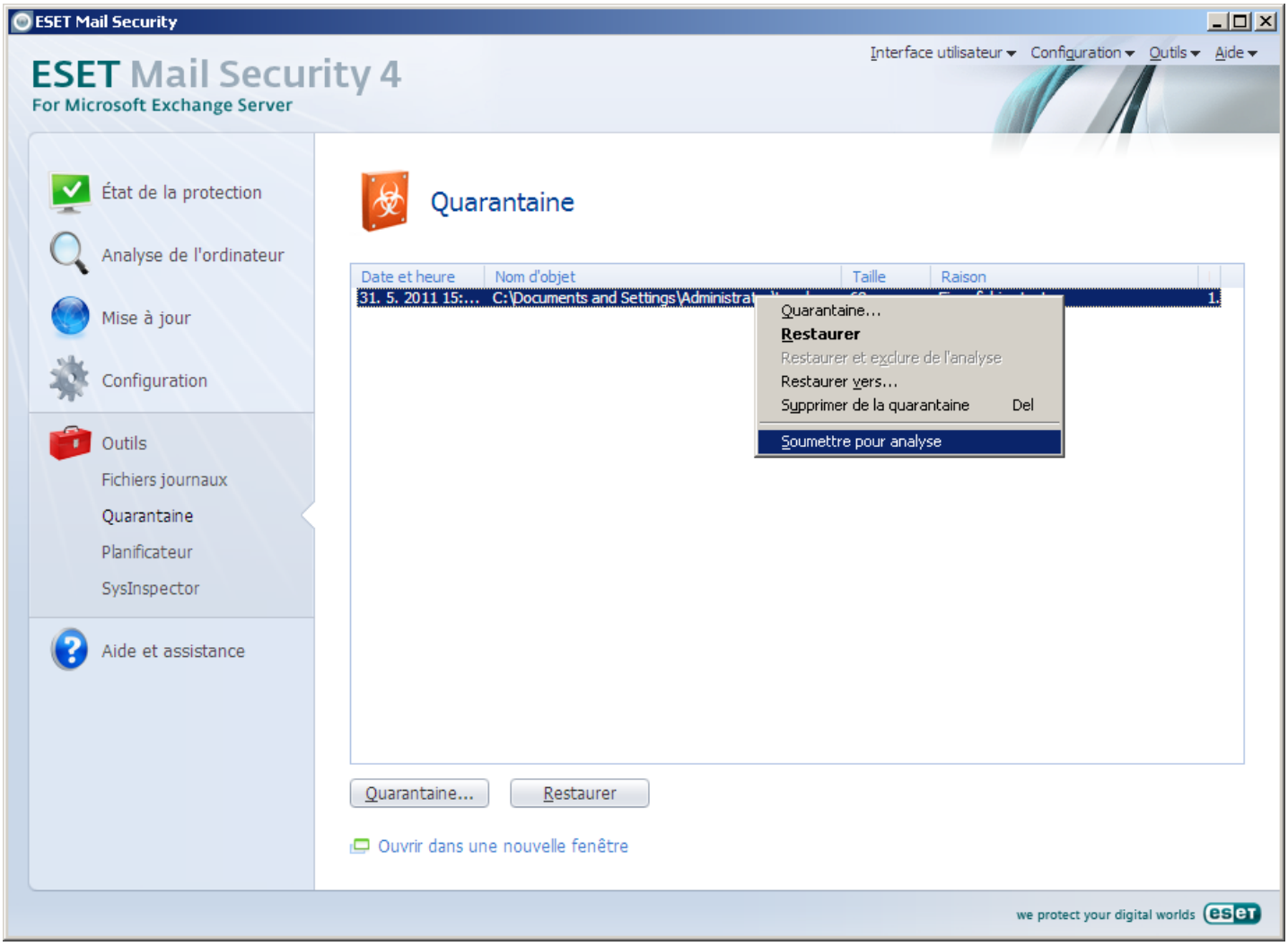
4.4.2 Restauration depuis la quarantaine

Les fichiers mis en quarantaine peuvent aussi être restaurés à leur emplacement d'origine. Utilisez la fonction **Restaurer** à cette fin. L'option **Restaurer** est disponible dans le menu contextuel accessible en cliquant avec le bouton droit sur le fichier dans le fenêtre Quarantaine. Le menu contextuel offre également l'option **Restaurer vers** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

REMARQUE: si le programme place en quarantaine, par erreur, un fichier inoffensif, il convient de le restaurer, de l'exclure de l'analyse et de l'envoyer au service d'assistance d'ESET

4.4.3 Soumission de fichiers de quarantaine

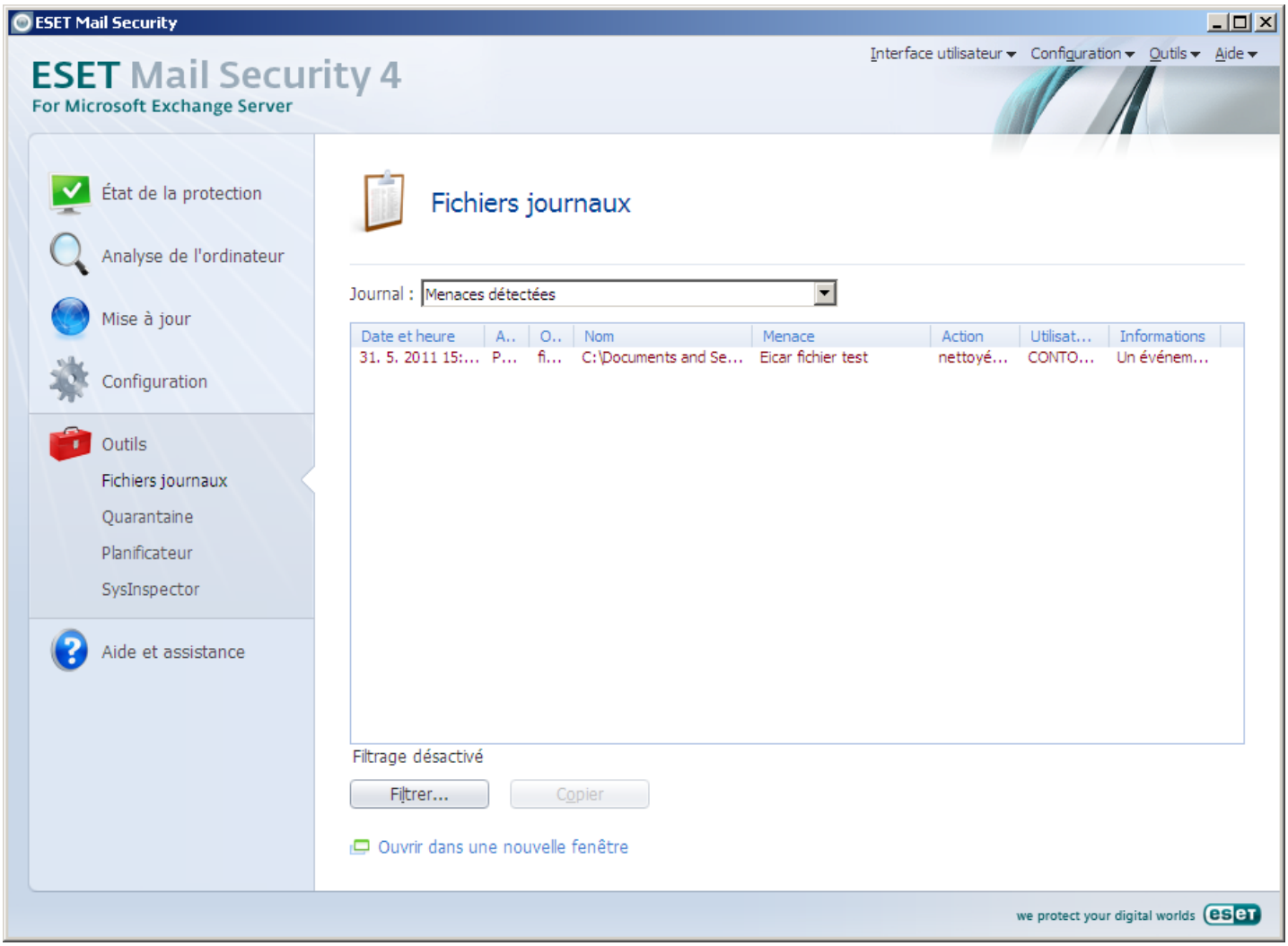
Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré par erreur comme étant infecté (par exemple par l'analyse heuristique du code) et placé en quarantaine, envoyez ce fichier au laboratoire de recherche sur les menaces d'ESET. Pour soumettre un fichier de la quarantaine, cliquez avec le bouton droit sur le fichier et sélectionnez l'option **Soumettre pour analyse** dans le menu contextuel.



4.5 Fichiers journaux

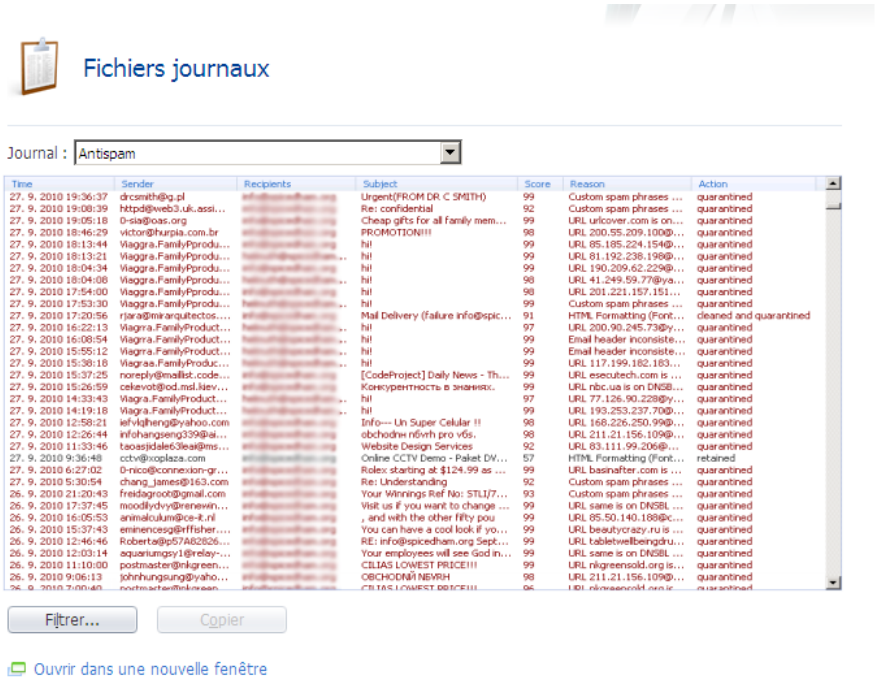
Les journaux stockent les informations des événements importants : infiltrations détectées, journaux des analyseurs à la demande et résident, et informations système.

Les journaux de protection antispam et de mise en liste grise (stockés dans d'autres journaux dans **Outils** > **Fichiers journaux**) contiennent des informations détaillées sur les messages faisant l'objet d'une analyse, ainsi que les actions effectuées sur ces messages. Les journaux peuvent être très utiles si vous recherchez des messages non remis, essayez de savoir pourquoi un message est marqué comme courrier indésirable, etc.



Antispam

Tous les messages classés par ESET Mail Security comme courrier indésirable ou courrier indésirable probable sont enregistrés ici.



Description des colonnes :

Date et heure : heure de l'entrée dans le journal du courrier indésirable

Expéditeur : adresse de l'expéditeur

Destinataire : adresse du destinataire

Objet : objet du message

Score : score de courrier indésirable attribué au message (dans la plage comprise entre 0 et 100)

Raison : indicateur expliquant la raison pour laquelle le message est classé comme courrier indésirable. L'indicateur affiché est le plus élevé. Si vous souhaitez voir les autres indicateurs, double-cliquez sur l'entrée. La fenêtre **Raison** qui apparaît contient les autres indicateurs, classés par ordre décroissant d'importance.

L'URL est réputée pour envoyer du courrier indésirable	Les adresses URL figurant dans les messages peuvent souvent être une indication de courrier indésirable.
Formatage HTML (polices, couleurs, etc.)	Le formatage des éléments figurant dans la partie HTML du message indique les signes caractéristiques de courrier indésirable (type, taille et couleur de la police, etc.)
Astuces de courrier indésirable : obscurcissement	Les mots classiques de courrier indésirable sont généralement masqués par d'autres caractères. Par exemple, le mot « Viagra » est souvent écrit « V1agra » afin de tromper la détection de courrier indésirable.
Courrier indésirable de type image HTML	Les messages de courrier indésirable prennent souvent la forme d'images ; il s'agit d'une autre stratégie qui permet d'éviter les méthodes de détection de courrier indésirable. Ces images contiennent généralement des liens interactifs vers des pages Internet.
Domaine de service d'hébergement du formatage URL	L'adresse URL contient le domaine du service d'hébergement.
Mot-clé évocateur de courrier indésirable...	Le message contient des mots typiques des courriers indésirables.
Incohérence d'en-tête de courrier	Les informations figurant dans l'en-tête sont modifiées pour faire croire à

électronique	une autre source que celle de l'expéditeur d'origine.
Virus	Le message contient une pièce jointe suspecte.
Hameçonnage	Le message contient un texte typique des messages de hameçonnage.
Réplique	Le message contient un texte typique du courrier indésirable visant à proposer des répliques.
Indicateur générique de courrier indésirable	Le message contient des mots/caractères typiques du courrier indésirable, par exemple « Cher ami », « Vous avez gagné ! », etc.
Indicateur de courrier souhaité	Cet indicateur a une fonction opposée à celle des autres indicateurs répertoriés. Il analyse les éléments caractéristiques des messages sollicités classiques. Il diminue le score global de courrier indésirable.
Indicateur de courrier indésirable non spécifique	Le message contient d'autres éléments de courrier indésirable, le codage base64 par exemple.
Expressions personnalisées de courrier indésirable	Autres expressions typiques de courrier indésirable.
URL mise en liste noire	L'URL figurant dans le message se trouve sur une liste noire.
L'IP %s est sur RBL	L'adresse IP... se trouve sur une liste RBL.
L'URL %s est sur DNSBL	L'adresse IP... se trouve sur une liste DNSBL.
L'URL %s est sur RBL ou le serveur n'est pas autorisé à envoyer des messages	L'adresse URL... se trouve sur une liste RBL ou le serveur ne dispose pas des privilèges requis pour envoyer des messages. Les différentes adresses de transfert du message sont comparées à la liste RBL. La dernière adresse fait l'objet de tests concernant ses droits de connectivité aux serveurs de messagerie publics. S'il est impossible de détecter des droits de connectivité valides, l'adresse se trouve dans la liste LBL. Si les messages sont marqués comme courrier indésirable en raison d'un indicateur LBL, le champ **Raison** affiche le message suivant : le serveur n'est pas autorisé à envoyer des messages.

Action : action effectuée sur le message. Actions possibles :

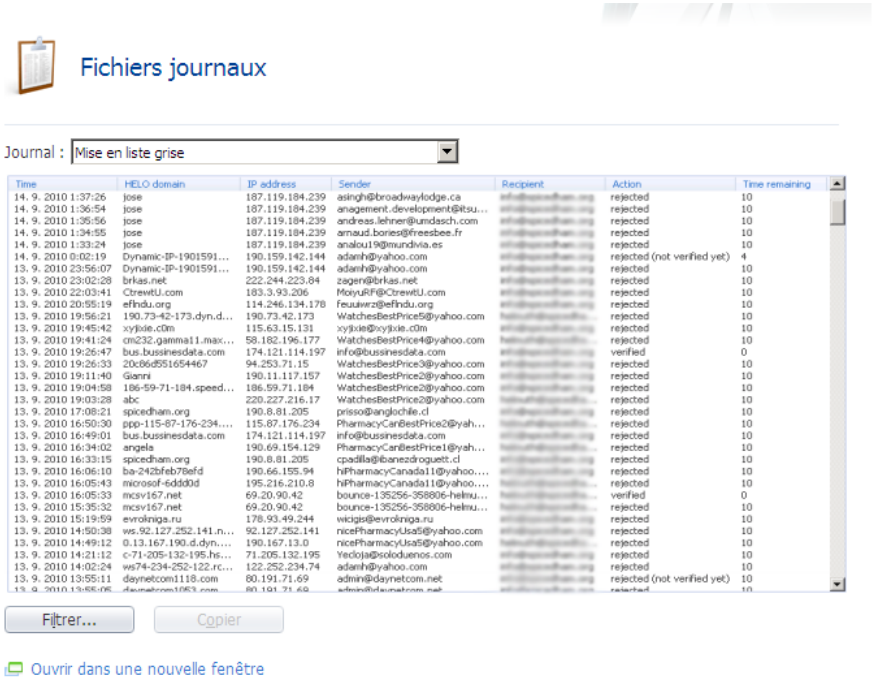
Conservé	Aucune n'a été effectuée sur le message.
Mis en quarantaine	Le message a été placé en quarantaine.
Nettoyé et mis en quarantaine	Le virus a été supprimé du message et le message est mis en quarantaine.
Rejeté	Le message a été refusé et la réponse de rejet SMTP 19 est envoyée à l'expéditeur.
Supprimé	Le message a été supprimé automatiquement 19.

Reçu : heure à laquelle le message a été reçue par le serveur.

REMARQUE : si les messages sont reçus par l'intermédiaire d'un serveur de messagerie, les informations des champs **Date et heure** et **Reçu** sont pratiquement identiques.

Mise en liste grise

Tous les messages qui ont été évalués à l'aide de la méthode de mise en liste grises sont enregistrés dans ce journal.



Description des colonnes :

Date et heure : heure de l'entrée dans le journal du courrier indésirable

Domaine HELO : nom du domaine utilisé par le serveur expéditeur pour s'identifier auprès du serveur de réception

Adresse IP : adresse IP de l'expéditeur

Expéditeur : adresse de l'expéditeur

Destinataire : adresse du destinataire

Action : peut indiquer différents états.

Rejeté	Le message entrant est refusé sur la base du principe de liste grise (première tentative de remise)
Rejeté (pas encore vérifié)	Le message entrant a été remis une nouvelle fois par le serveur expéditeur, mais la durée limite de refus de connexion n'est pas encore atteinte(**Durée limite du refus de connexion initial**).
Vérifié	Le message entrant a été remis plusieurs fois par le serveur d'expédition, la **durée limite du refus de connexion initial** s'est écoulée et le message a été vérifié et remis. Reportez-vous également à l'agent de transport 38.

Temps restant : durée restante jusqu'à la **durée limite du refus de connexion initial**

Menaces détectées

Le journal des menaces contient des informations sur les infiltrations détectées par les modules ESET Mail Security. Ces informations comprennent l'heure de détection, le type de l'analyseur et de l'objet, le nom de l'objet et de l'infiltration, l'emplacement, l'action exécutée et le nom de l'utilisateur connecté au moment où l'infiltration a été détectée. Utilisez le menu contextuel (cliquez avec le bouton droit sur l'élément) pour copier ou supprimer une ou plusieurs lignes du journal, ou encore supprimer tout le journal.

Événements

Le journal d'événements contient des informations sur les événements qui se sont produits dans le programme. Ces informations peuvent souvent contribuer à trouver une solution à un problème qui s'est produit dans le programme.

Analyse de l'ordinateur à la demande

Le journal d'analyse stocke des informations sur les résultats des analyses manuelles et planifiées. Chaque ligne correspond à un seul contrôle d'ordinateur. Il comprend les informations suivantes : date et heure d'analyse, nombre total de fichiers analysés, infectés et nettoyés, et état actuel de l'analyse.

Dans les **journaux d'analyses à la demande**, double-cliquez sur une entrée du journal pour afficher son contenu détaillé dans une fenêtre distincte.
Utilisez le menu contextuel (accessible à l'aide du bouton droit) pour copier une ou plusieurs entrées marquées (dans tous les types de journaux).

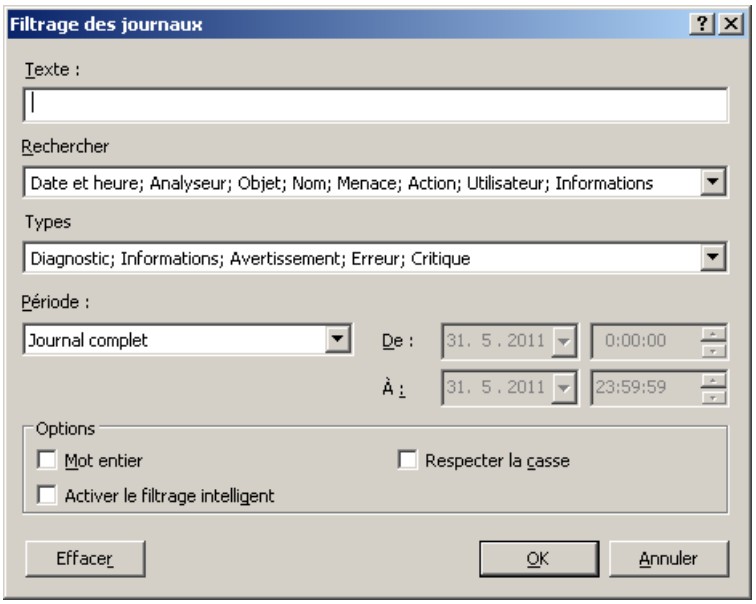
4.5.1 Filtrage des journaux

Le filtrage des journaux est une fonctionnalité très utile qui vous permet de rechercher des enregistrements dans les fichiers journaux, notamment lorsque les enregistrements sont très nombreux et qu'il est difficile de trouver les informations nécessaires.

Lorsque vous utilisez le filtrage, vous pouvez saisir une chaîne des éléments à filtrer dans **Rechercher**, spécifier les colonnes dans lesquelles effectuer la recherche dans **Rechercher dans les colonnes**, sélectionner les types d'enregistrement dans **Types d'enregistrements** et définir une heure dans la zone **Heure** afin de restreindre le nombre d'enregistrements. En indiquant certaines options de filtrage, vous pouvez afficher uniquement les enregistrements pertinents (en fonction de ces options) dans la fenêtre **Fichiers journaux** afin d'y accéder facilement.

Pour ouvrir la fenêtre **Filtrage des journaux**, appuyez une fois sur le bouton **Filtrer...** dans **Outils** > **Fichiers journaux** ou utilisez le raccourci clavier Ctrl + Maj + F.

REMARQUE : pour rechercher un enregistrement donné, utilisez plutôt la fonctionnalité Rechercher dans le journal 102, seule ou avec le filtrage des journaux.



En indiquant certaines options de filtrage, vous pouvez afficher uniquement les enregistrements pertinents (en fonction de ces options) dans la fenêtre Fichiers journaux. Le nombre d'enregistrements affichés est alors restreint, ce qui facilite la recherche des informations nécessaires. Plus vous utilisez d'options de filtrage, plus les résultats sont restreints.

Rechercher : saisissez une chaîne (mot ou partie de mot). Seuls les enregistrements contenant cette chaîne sont affichés. Les autres enregistrements sont masqués pour une meilleure lisibilité.

Rechercher dans les colonnes : : sélectionnez les colonnes à prendre en compte lors du filtrage. Vous pouvez cocher une ou plusieurs colonnes en tant que critères de filtrage. Par défaut, toutes les colonnes sont cochées :

- **Heure**
- **Module**
- **Événement**
- **utilisateur**

Types d'enregistrements : : vous permet de choisir le type d'enregistrements à afficher. Vous pouvez choisir un type d'enregistrement en particulier, plusieurs types simultanément ou tous les types (option par défaut) :

- **Diagnostic**
- **Informations**
- **Avertissement**
- **Erreur**
- **Critique**

Période : : utilisez cette option pour filtrer les enregistrements par période. Vous pouvez choisir l'une des options suivantes :

- **Journal complet** (option par défaut) : aucun filtrage par période n'est effectué et l'intégralité du journal est affiché.
- **Jour antérieur**
- **Dernière semaine**
- **Dernier mois**
- **Intervalle** : en sélectionnant un intervalle, vous pouvez indiquer la période exacte (date et heure) afin de n'afficher que les enregistrements correspondant à la période indiquée.

Outre les paramètres de filtrage ci-dessus, vous disposez également plusieurs **Options** :

Mot entier : affiche uniquement les enregistrements qui correspondent à la chaîne sous forme de mot entier indiquée dans la zone de **recherche**.

Respecter la casse : affiche uniquement les enregistrements qui correspondent à l'utilisation des majuscules et des minuscules indiquée dans la zone de **recherche**.

Activer le filtrage intelligent : utilisez cette option pour qu'ESET Mail Security puisse effectuer le filtrage à l'aide de ses propres méthodes.

Lorsque la configuration des options de filtrage est terminée, appuyez sur le bouton **OK** pour appliquer le filtrage. La fenêtre **Fichiers journaux** n'affiche que les enregistrements correspondants en fonction des options de filtre.

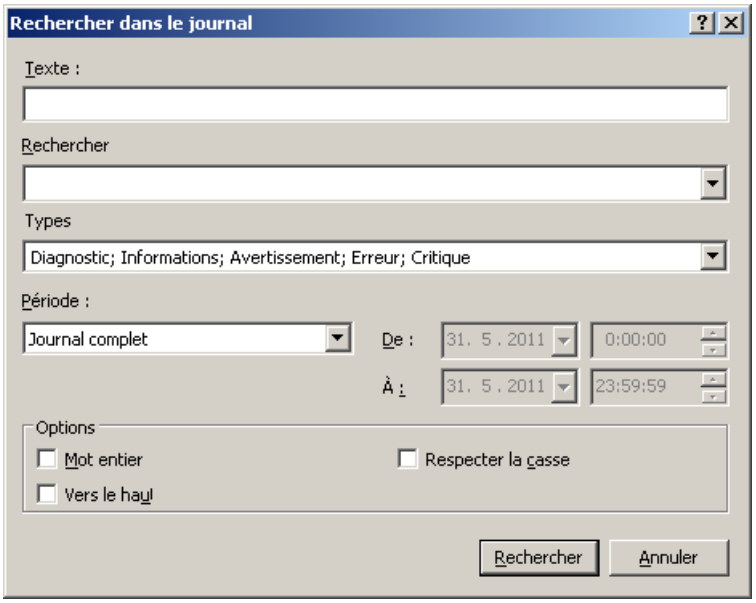
4.5.2 Rechercher dans le journal

Outre le filtrage des journaux 101, vous pouvez utiliser la fonctionnalité de recherche dans les fichiers journaux. Toutefois, vous pouvez également l'utiliser indépendamment du filtrage des journaux. Ce procédé est utile lorsque vous recherchez des enregistrements précis dans les journaux. Tout comme le filtrage des journaux, cette fonctionnalité de recherche permet de trouver les informations que vous recherchez, notamment lorsque les enregistrements sont très nombreux.

Lorsque vous utilisez la fonction de recherche dans le journal, vous pouvez saisir une chaîne des éléments à filtrer dans **Rechercher**, spécifier les colonnes dans lesquelles effectuer la recherche dans **Rechercher dans les colonnes**, sélectionner les types d'enregistrement dans **Types d'enregistrement** et définir une heure dans **Heure** afin de ne rechercher que les enregistrements correspondant à la période indiquée. En indiquant certaines options de recherche, vous pouvez afficher uniquement les enregistrements pertinents (en fonction de ces options) dans la fenêtre Fichiers journaux.

Pour effectuer des recherches dans les journaux, ouvrez la fenêtre **Rechercher dans le journal** en appuyant sur les touches Ctrl + F.

REMARQUE : vous pouvez utiliser la fonctionnalité Rechercher dans le journal avec le filtrage des journaux 101. Vous pouvez d'abord restreindre le nombre d'enregistrements à l'aide du filtrage des journaux, puis effectuer une recherche uniquement dans les enregistrements filtrés.



Rechercher : saisissez une chaîne (mot ou partie de mot). Seuls les enregistrements contenant cette chaîne sont trouvés. Les autres enregistrements sont ignorés.

Rechercher dans les colonnes : : sélectionnez les colonnes à prendre en compte lors de la recherche. Vous pouvez cocher une ou plusieurs colonnes à utiliser pour la recherche. Par défaut, toutes les colonnes sont cochées :

- **Heure**
- **Module**
- **Événement**
- **utilisateur**

Types d'enregistrements : : vous permet de choisir le type d'enregistrements à rechercher. Vous pouvez choisir un type d'enregistrement en particulier, plusieurs types simultanément ou tous les types (option par défaut) :

- **Diagnostic**
- **Informations**
- **Avertissement**
- **Erreur**
- **Critique**

Période : : utilisez cette option pour rechercher des enregistrements correspondant à une période. Vous pouvez choisir l'une des options suivantes :

- **Journal complet** (option par défaut) : n'effectue aucune recherche dans la période ; effectue une recherche dans l'intégralité du journal.
- **Jour antérieur**
- **Dernière semaine**
- **Dernier mois**
- **Intervalle** : en sélectionnant un intervalle, vous pouvez indiquer la période exacte (date et heure) afin de ne rechercher que les enregistrements correspondant à la période indiquée.

Outre les paramètres de recherche ci-dessus, vous disposez également plusieurs **Options** :

Mot entier : recherche uniquement les enregistrements qui correspondent à la chaîne sous forme de mot entier indiquée dans la zone de **recherche**.

Respecter la casse : recherche uniquement les enregistrements qui correspondent à l'utilisation des majuscules et des minuscules indiquée dans la zone de **recherche**.

Vers le haut : lance la recherche vers le haut.

Après avoir configuré les options de recherche, cliquez sur le bouton **Rechercher** pour lancer la recherche. La recherche s'arrête au premier enregistrement correspondant. Cliquez de nouveau sur le bouton **Rechercher** pour poursuivre la recherche. La recherche dans les fichiers journaux s'effectue de haut en bas, à partir de la position actuelle (de l'enregistrement sélectionné).

4.5.3 Maintenance des journaux

La configuration de la consignation d'ESET Mail Security est accessible à partir de la fenêtre principale du programme. Cliquez sur **Configuration** > **Accéder à la configuration avancée complète...** > **Outils** > **Fichiers journaux**. Les options suivantes peuvent être spécifiées pour les fichiers journaux :

- **Supprimer automatiquement les entrées** : les entrées journaux plus anciennes que le nombre de jours spécifié sont automatiquement supprimées.
- **Optimiser automatiquement les fichiers journaux** : permet la défragmentation automatique des fichiers journaux si le pourcentage spécifié d'enregistrements inutilisés est dépassé.
- **Verbosité minimale des journaux** : indique la verbosité minimale des journaux. Les options disponibles sont les suivantes :

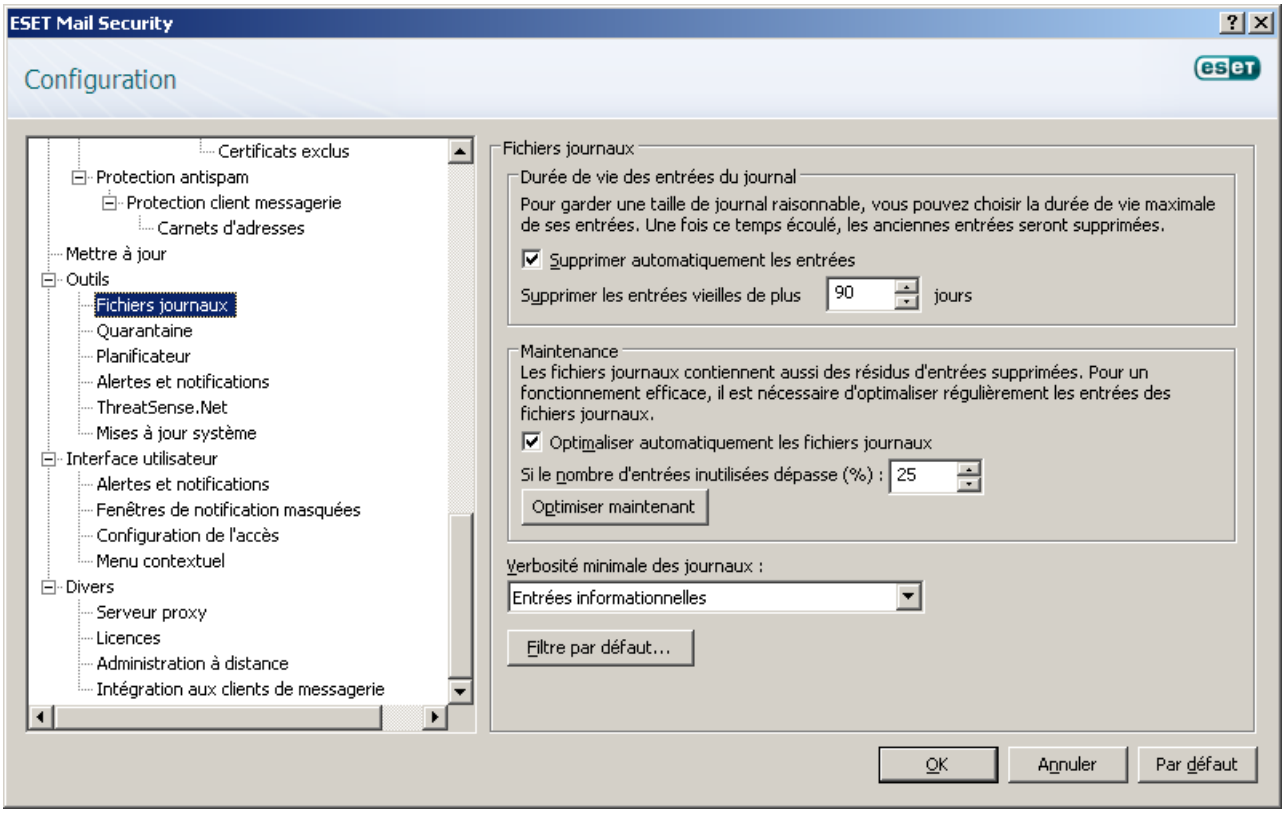
- **Entrées diagnostiques** : consigne toutes les informations nécessaires pour un réglage détaillé du programme et de toutes les entrées ci-dessus.

- **Entrées informatives** : enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.

- **Avertissements** : enregistre les erreurs critiques, les erreurs et les messages d'avertissement.

- **Erreurs** : les erreurs de type « Erreur de téléchargement de fichier » et les erreurs critiques sont enregistrées.

- **Avertissements critiques** : répertorie toutes les erreurs critiques (erreur de démarrage de la protection antivirus, etc.).



4.6 ESET SysInspector

4.6.1 Introduction à ESET SysInspector

ESET SysInspector est une application qui inspecte votre ordinateur en profondeur et qui affiche en détail toutes les données obtenues. Des informations telles que les pilotes et applications installés, les connexions réseau ou les entrées de registre importantes peuvent vous aider à élucider un comportement suspect du système, qu'il soit dû à une incompatibilité logicielle ou matérielle, ou à une infection par logiciel malveillant.

Vous pouvez accéder à ESET SysInspector de deux manières : Depuis la version intégrée dans les solutions ESET Security ou en téléchargeant gratuitement la version autonome (SysInspector.exe) depuis le site Internet d'ESET. Les deux versions sont identiques en matière de fonctionnalités et disposent des mêmes contrôles de programme. La seule différence réside dans la façon dont les résultats sont gérés. Les versions autonomes et intégrées vous permettent d'exporter des instantanés du système dans un fichier *.xml* et de les enregistrer sur le disque. Toutefois, la version intégrée vous permet également de stocker vos instantanés système directement dans **Outils** > **ESET SysInspector** (excepté ESET Remote Administrator). Pour plus d'informations, reportez-vous à la section ESET SysInspector en tant que partie de ESET Mail Security 116.

Veuillez patienter pendant que ESET SysInspector analyse votre ordinateur. L'analyse peut prendre entre 10 secondes et quelques minutes, en fonction de la configuration de votre matériel, du système d'exploitation et du nombre d'applications installées sur votre ordinateur.

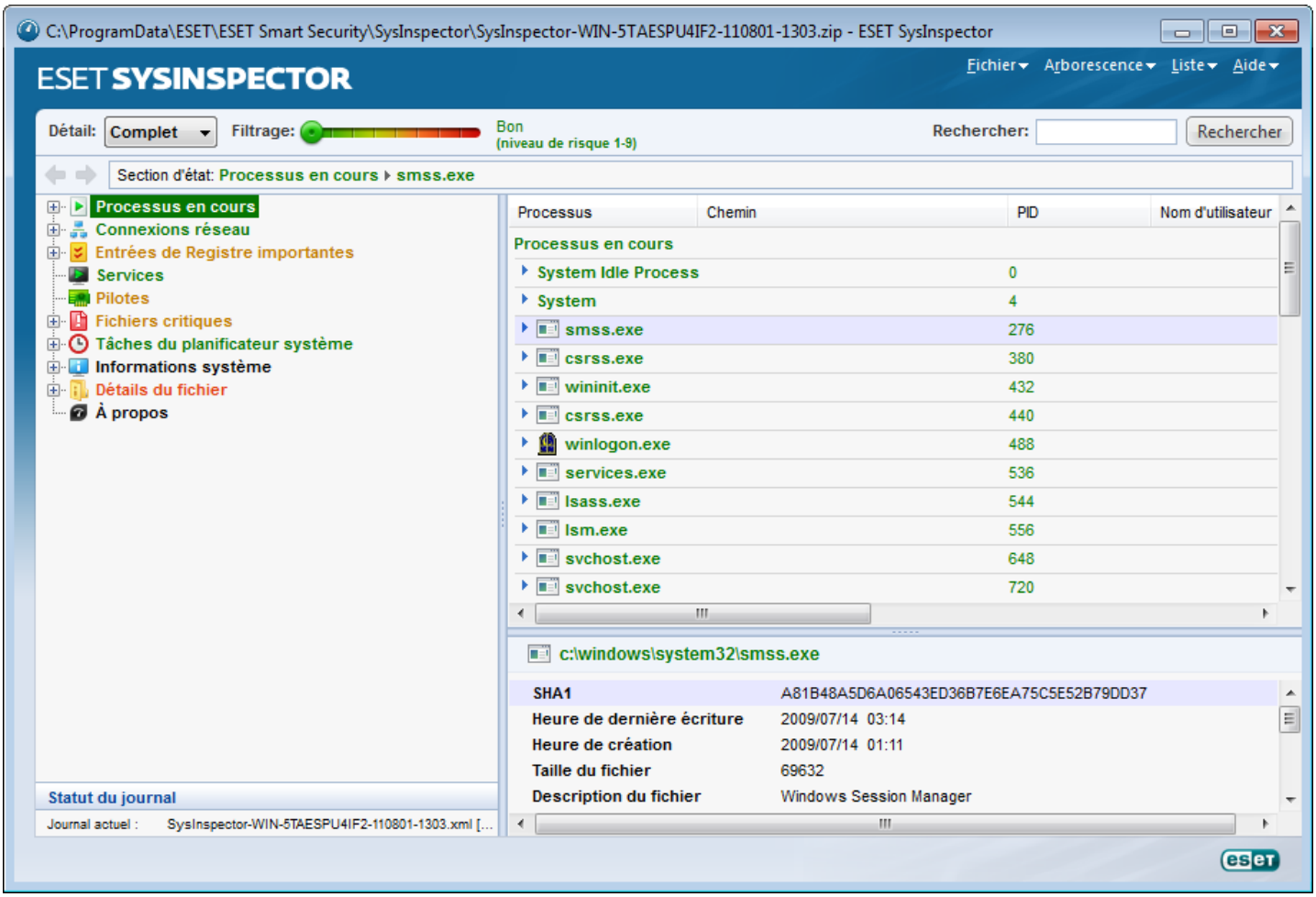
4.6.1.1 Démarrage d'ESET SysInspector

Pour démarrer ESET SysInspector, il suffit de lancer le fichier exécutable *SysInspector.exe* téléchargé depuis le site Web d'ESET. Si vous avez déjà installé une des solutions de sécurité ESET Security, vous pouvez exécuter ESET SysInspector directement depuis le menu Démarrer (**Programmes** > **ESET** > **ESET Mail Security**).

Patientez pendant que l'application vérifie le système, une opération qui pourrait durer plusieurs minutes en fonction du matériel et des données à recueillir.

4.6.2 Interface utilisateur et utilisation de l'application

Pour des raisons de clarté, la fenêtre principale est divisée en quatre principales sections : les Contrôles du programme situés dans le haut de la fenêtre principale, la fenêtre Navigation à gauche, la fenêtre Description à droite au centre et la fenêtre Détails à droite au bas de la fenêtre principale. La section État du journal énumère les paramètres de base d'un journal (filtre utilisé, type de filtre, journal résultat d'une comparaison, etc.).



4.6.2.1 Contrôles du programme

Cette section contient la description de tous les contrôles du programme disponible dans ESET SysInspector.

Fichier

En cliquant sur **Fichier**, vous pouvez enregistrer l'état actuel du système en vue d'une enquête ultérieure ou ouvrir un journal déjà enregistré. Pour la publication, il est conseillé de créer un journal **approprié pour envoi**. Sous cette forme, le journal omet les informations sensibles (nom d'utilisateur, nom d'ordinateur, nom de domaine, privilèges actuels de l'utilisateur, variables d'environnement, etc.).

REMARQUE : vous pouvez ouvrir des rapports enregistrés de ESET SysInspector en les faisant glisser et en les déposant sur la fenêtre principale.

Arborescence

Permet de développer ou de réduire tous les nœuds et d'exporter les sections sélectionnées dans le script de service.

Liste

Contient des fonctions qui simplifient la navigation dans le programme, ainsi que d'autres fonctionnalités comme l'obtention d'informations en ligne.

Aide

Contient des informations sur l'application et ses fonctions.

Détails

Ce paramètre détermine les informations affichées dans la fenêtre principale afin de simplifier l'utilisation des informations. En mode de base, vous avez accès aux informations utilisées pour trouver les solutions aux problèmes communs dans votre système. En mode Moyen, le programme affiche moins de détails. En mode Complet, ESET SysInspector indique toutes les informations requises pour résoudre des problèmes très particuliers.

Filtrage des éléments

Le filtrage des éléments est particulièrement adapté à la recherche de fichiers suspects ou d'entrées de Registre dans le système. En déplaçant le curseur, vous pouvez filtrer les éléments en fonction de leur niveau de risque. Si le curseur est positionné tout à fait à gauche (Niveau de risque 1), tous les éléments sont affichés. En déplaçant le curseur vers la droite, l'application filtre tous les éléments dont le risque est inférieur au niveau de risque actuel et affiche uniquement les éléments qui sont plus suspects que le niveau affiché. Si le curseur est en position maximale à droite, le programme affiche uniquement les éléments nuisibles connus.

Tous les éléments qui appartiennent aux catégories de risque 6 à 9 peuvent poser un risque pour la sécurité. Si vous n'utilisez pas certaines des solutions de sécurité d'ESET, nous vous conseillons d'analyser votre système à l'aide d' ESET Online Scanner dans le cas où ESET SysInspector détecte un élément de ce genre. ESET Online Scanner est un service gratuit.

REMARQUE : le niveau de risque d'un élément peut être rapidement déterminé grâce à la couleur que prend le curseur pour indiquer le niveau de risque.

Rechercher

La fonction de recherche permet de trouver rapidement un élément sur la base de son nom ou d'une partie de son nom. Les résultats de la recherche sont affichés dans la fenêtre Description.

Retour

En cliquant sur la flèche arrière ou avant, vous pouvez revenir aux informations affichées précédemment dans la fenêtre Description. Vous pouvez utiliser la touche de retour arrière et la barre d'espace au lieu de cliquer sur les flèches arrière ou avant.

Section d'état

Affiche le nœud actuel dans la fenêtre Navigation.

Important : les éléments surlignés en rouge sont inconnus et c'est la raison pour laquelle l'application les marque comme potentiellement dangereux. Si un élément est rouge, cela ne signifie pas automatiquement que vous pouvez supprimer le fichier. Avant de le supprimer, assurez-vous que les fichiers sont bel et bien dangereux ou qu'ils ne sont pas nécessaires.

4.6.2.2 Navigation dans ESET SysInspector

ESET SysInspector répartit divers types d'informations en plusieurs sections principales baptisées nœuds. Si des détails supplémentaires sont disponibles, vous pouvez les afficher en développant chaque nœud en sous-nœuds. Pour développer ou réduire un nœud, double-cliquez sur son nom, ou cliquez sur ⊞ ou sur ⊟ en regard du nom du nœud. Quand vous parcourez la structure arborescente des nœuds et des sous-nœuds dans la fenêtre de navigation, vous pouvez voir différents détails pour chaque nœud dans la fenêtre Description. Si vous parcourez les éléments de la fenêtre Description, des détails supplémentaires pour chaque élément peuvent être affichés dans la fenêtre Détails.

Voici les descriptions des principaux nœuds de la fenêtre Navigation et des informations qui s'y rapportent dans les fenêtres Description et Détails.

Processus en cours

Ce nœud comprend les informations sur les applications et les processus en cours d'exécution au moment de la création du journal. La fenêtre Détails comprend des détails complémentaires pour chaque processus tels que les bibliothèques dynamiques utilisées par les processus et leur emplacement dans le système, le nom de l'éditeur de l'application et le niveau de risque du fichier.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

REMARQUE : Un système d'exploitation comprend plusieurs composants noyaux importants fonctionnant 24 h. sur 24/7 j. sur 7 et assurant des fonctions de base et vitales pour d'autres applications utilisateur. Dans certains cas, ces processus sont repris dans l'outil ESET SysInspector avec un chemin d'accès au fichier commençant par \??\. Ces symboles garantissent l'optimisation préalable au lancement pour ce processus ; ils ne présentent aucun danger pour le système.

Connexions de réseau

La fenêtre Description contient la liste des processus et des applications qui communiquent via le réseau à l'aide du protocole sélectionné dans la fenêtre navigation (TCP ou UDP), ainsi que l'adresse distante à laquelle l'application est connectée. Vous pouvez également vérifier les adresses IP des serveurs DNS.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

Entrées de Registre importantes

Contient la liste des entrées de Registre sélectionnées qui sont souvent liées à des problèmes système. Il s'agit des entrées qui indiquent les applications de démarrage, les objets d'application d'assistance du navigateur, etc.

La fenêtre Description peut indiquer les fichiers en rapport avec les entrées de Registre particulières. La fenêtre Détails peut également présenter des détails supplémentaires.

Services

La fenêtre Description contient la liste des fichiers enregistrés en tant que services Windows. Vous pouvez contrôler la manière dont le démarrage du service est paramétré, ainsi que des détails spécifiques du fichier dans la fenêtre Détails.

Pilotes

Liste des pilotes installés sur le système.

Fichiers critiques

La fenêtre Description affiche le contenu des fichiers critiques liés au système d'exploitation Microsoft Windows.

Tâches du planificateur système

Contient une liste de tâches déclenchées par le Planificateur de tâches de Windows à une heure précise ou selon un intervalle spécifié.

Informations système

Contient des informations détaillées sur le matériel et le logiciel, ainsi que des informations sur les variables d'environnement définies, les droits de l'utilisateur et les journaux d'événements du système.

Détails du fichier

Liste des fichiers système importants et des fichiers du dossier Program Files. Des informations complémentaires spécifiques sur les fichiers sont disponibles dans les fenêtres Description et Détails.

À propos de

Informations sur la version de ESET SysInspector et la liste des modules du programme.

4.6.2.2.1 Raccourcis clavier

Voici les raccourcis clavier disponibles dans ESET SysInspector :

Fichier

Ctrl+O	ouvre un journal existant
Ctrl+S	enregistre les journaux créés

Générer

Ctrl+G	génère un instantané standard du statut de l'ordinateur

Ctrl+H	génère un instantané du statut de l'ordinateur qui peut également journaliser des informations sensibles

Filtrage des éléments

1, O	affiche les éléments de niveau de risque 1 à 9 (acceptable)
2	affiche les éléments de niveau de risque 2 à 9 (acceptable)
3	affiche les éléments de niveau de risque 3 à 9 (acceptable)
4, U	affiche les éléments de niveau de risque 4 à 9 (inconnu)
5	affiche les éléments de niveau de risque 5 à 9 (inconnu)
6	affiche les éléments de niveau de risque 6 à 9 (inconnu)
7, B	affiche les éléments de niveau de risque 7 à 9 (risqué)
8	affiche les éléments de niveau de risque 8 à 9 (risqué)
9	affiche les éléments de niveau de risque 9 (risqué)
-	diminue le niveau de risque
+	augmente le niveau de risque
Ctrl+9	mode de filtrage, niveau égal ou supérieur
Ctrl+O	mode de filtrage, niveau égal uniquement

Afficher

Ctrl+5	afficher par éditeur, tous les éditeurs
Ctrl+6	afficher par éditeur, uniquement Microsoft
Ctrl+7	afficher par éditeur, tous les autres éditeurs
Ctrl+3	afficher tous les détails
Ctrl+2	afficher les détails de précision moyenne
Ctrl+1	affichage de base
Retour arrière	revient une étape en arrière
Barre d'espace	avance d'une étape
Ctrl+W	développe l'arborescence
Ctrl+Q	réduit l'arborescence

Autres commandes

Ctrl+T	accède à l'emplacement d'origine de l'élément après la sélection dans les résultats de recherche
Ctrl+P	affiche des informations élémentaires sur un élément
Ctrl+A	affiche des informations complètes sur un élément
Ctrl+C	copie l'arborescence de l'élément
Ctrl+X	copie les éléments
Ctrl+B	trouve des informations sur les fichiers sélectionnés sur Internet
Ctrl+L	ouvre le dossier où se trouve le fichier sélectionné.
Ctrl+R	ouvre l'entrée correspondante dans l'éditeur de registre
Ctrl+Z	copie un chemin d'accès à un fichier (si l'élément est lié à un fichier)
Ctrl+F	passe au champ de recherche
Ctrl+D	ferme les résultats de la recherche
Ctrl+E	exécute le script de service

Comparaison

Ctrl+Alt+O	ouvre le journal d'origine/de comparaison
Ctrl+Alt+R	annule la comparaison
Ctrl+Alt+1	affiche tous les éléments
Ctrl+Alt+2	affiche uniquement les éléments ajoutés ; le journal indique les éléments présents dans le journal actuel
Ctrl+Alt+3	affiche uniquement les éléments supprimés ; le journal indique les éléments présents dans le journal précédent
Ctrl+Alt+4	affiche uniquement les éléments remplacés (fichiers inclus)
Ctrl+Alt+5	affiche uniquement les différences entre les journaux
Ctrl+Alt+C	affiche la comparaison
Ctrl+Alt+N	affiche le journal actuel
Ctrl+Alt+P	ouvre le journal précédent

Divers

F1	afficher l'aide
Alt+F4	quitter l'application
Alt+Maj+F4	quitter l'application sans demander
Ctrl+I	statistiques du journal

4.6.2.3 Comparer

La fonctionnalité Comparer permet de comparer deux journaux. Cette fonctionnalité met en évidence les éléments qui ne sont pas communs aux deux journaux. Cet outil est utile si vous souhaitez assurer le suivi des modifications dans le système. Il vous permettra de détecter l'activité d'un code malveillant.

Après son lancement, l'application crée un journal qui apparaît dans une nouvelle fenêtre. Accédez au menu **Fichier** > **Enregistrer le journal** pour enregistrer le journal dans un fichier. Vous pouvez ouvrir et afficher les fichiers journaux ultérieurement. Pour ouvrir un journal existant, sélectionnez **Fichier** > **Ouvrir le journal**. Dans la fenêtre principale de l'application, ESET SysInspector affiche toujours un journal à la fois.

En comparant deux journaux, vous pouvez afficher un journal actif et un autre journal enregistré dans un fichier. Pour comparer des journaux, choisissez l'option **Fichier** > **Comparer les journaux**, puis choisissez **Sélectionner un fichier**. Le journal sélectionné est comparé au journal actif dans les fenêtres principales de l'application. Le journal comparatif n'indiquera que les différences entre ces deux journaux.

REMARQUE : si vous comparez deux fichiers journaux, choisissez **Fichier** > **Enregistrer le journal** pour l'enregistrer dans un fichier ZIP. Les deux fichiers sont enregistrés. Si vous ouvrez ce fichier ultérieurement, les journaux qu'il contient seront comparés automatiquement.

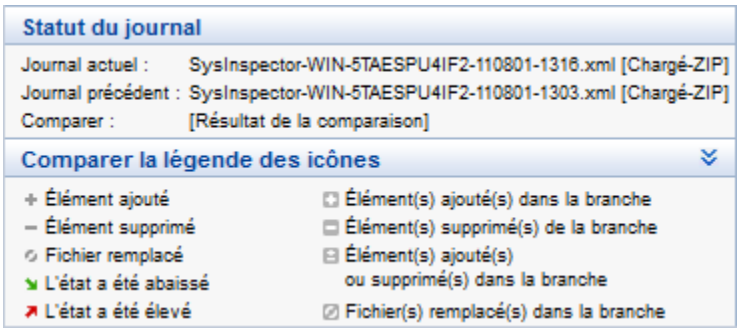
En regard des éléments affichés, ESET SysInspector ajoute des symboles qui identifient les différences entre les journaux comparés.

Les éléments marqués par − se trouvent uniquement dans le journal actif et sont absents du journal de comparaison ouvert. Les éléments marqués du signe + ne figurent que dans le journal ouvert et sont absents du journal actif.

Description de tous les symboles qui peuvent être affichés à côté des éléments :

- + nouvelle valeur, absente du journal précédent.
- cette section de l'arborescence contient de nouvelles valeurs.
- − valeur supprimée, présente uniquement dans le journal précédent.
- cette section de l'arborescence contient des valeurs supprimées.
- valeur/fichier modifié.
- cette section de l'arborescence contient des valeurs/fichiers modifiés.
- le niveau de risque a diminué/était supérieur dans le journal précédent.
- le niveau de risque a augmenté/il était inférieur dans le journal précédent.

La section d'explication affichée dans le coin inférieur gauche décrit tous les symboles et affiche le nom des journaux comparés.



Les journaux de comparaison peuvent être enregistrés dans un fichier et ouverts ultérieurement :

Exemple

Créez un journal reprenant les informations d'origine du système et enregistrez-le dans un fichier appelé précédent.xml. Après avoir modifié le système, ouvrez ESET SysInspector pour qu'il crée un nouveau journal. Enregistrez ce journal sous le nom *actuel.xml*.

Pour voir les différences entre ces deux journaux, utilisez l'option **Fichier** > **Comparer les journaux**. Le programme crée un journal de comparaison qui indique les différences entre les journaux.

Un résultat identique peut être obtenu si vous utilisez l'option de ligne de commande suivante :

SysInspector.exe actuel.xml précédent.xml

4.6.3 Paramètres de la ligne de commande

ESET SysInspector prend en charge la création de rapports via la ligne de commande à l'aide de ces paramètres :

/gen	crée un journal directement depuis la ligne de commande sans exécuter l'interface utilisateur.
/privacy	crée un journal qui exclut les informations sensibles.
/zip	stocke le journal obtenu directement sur le disque dans un fichier compressé.
/silent	supprime l'affichage de la barre de progression de la création du journal.
/help, /?	affiche des informations sur les paramètres de la ligne de commande.

Exemples

Pour charger un journal en particulier directement dans le navigateur, saisissez : *SysInspector.exe "c:\clientlog.xml"*
Pour créer un journal à l'emplacement actuel, saisissez : *SysInspector.exe /gen*
Pour créer un journal dans un dossier en particulier, saisissez : *SysInspector.exe /gen="c:\dossier\"*
Pour créer un journal dans un fichier/dossier en particulier, saisissez : *SysInspector.exe /gen="c:\dossier\monnouveaujournal.xml"*
Pour créer un journal qui exclut les informations sensibles directement dans un fichier compressé, saisissez : *SysInspector.exe /gen="c:\monnouveaujournal.zip"/privacy/zip*
Pour comparer deux journaux, utilisez : *SysInspector.exe "actuel.xml" "original.xml"*

REMARQUE : si le nom du fichier/dossier contient un espace, saisissez-le entre guillemets.

4.6.4 Script de service

Le script de service est un outil qui vise à offrir une aide aux clients qui utilisent ESET SysInspector en supprimant les objets indésirables du système.

Le script de service permet à l'utilisateur d'exporter l'ensemble du journal ESET SysInspector ou des parties sélectionnées uniquement. Après l'exportation, vous pouvez marquer des objets indésirables pour suppression. Vous pouvez ensuite exécuter le journal modifié pour supprimer les objets marqués.

Le script de service convient aux utilisateurs expérimentés qui connaissent les problèmes des systèmes de diagnostic. Des modifications non qualifiées peuvent endommager le système d'exploitation.

Exemple

si vous pensez que votre ordinateur est infecté par un virus qui n'est pas détecté par votre logiciel antivirus, suivez les instructions ci-après :

- Exécutez ESET SysInspector pour obtenir un nouvel instantané du système.
- Sélectionnez le premier élément de la section à gauche (dans l'arborescence), appuyez sur la touche Ctrl, puis sélectionnez le dernier élément afin de marquer tous les éléments.
- Cliquez avec le bouton droit sur les objets sélectionnés, puis sélectionnez l'option du menu contextuel **Exporter les sections sélectionnées dans un script de service**.
- Les objets sélectionnés sont exportés dans un nouveau journal.
- Il s'agit de l'étape la plus importante de toute la procédure : ouvrez le nouveau journal et remplacez l'attribut + par - pour tous les objets que vous souhaitez supprimer. Assurez-vous que vous n'avez sélectionné aucun fichier/objet important du système d'exploitation.
- Ouvrez ESET SysInspector, cliquez sur **Fichier** > **Exécuter le script de services** entrez le chemin d'accès de votre script.
- Cliquez sur **OK** pour lancer le script.

4.6.4.1 Création d'un script de service

Pour créer un script, cliquez avec le bouton droit de la souris sur n'importe quel élément de l'arborescence de menus (dans le volet de gauche) dans la fenêtre principale de ESET SysInspector. Dans le menu contextuel, choisissez l'option **Exporter toutes les sections dans un script de service** ou **Exporter les sections sélectionnées dans un script de service**.

REMARQUE : il est impossible d'exporter le script de service lorsque deux journaux sont comparés.

4.6.4.2 Structure du script de service

La première ligne de l'en-tête du script reprend des informations sur la version du moteur (ev), la version de l'interface utilisateur graphique (gv) et la version du journal (lv). Ces données permettent d'identifier d'éventuelles modifications dans le fichier .xml qui génère le script et d'éviter toute incohérence durant l'exécution. Cette partie du script ne peut pas être modifiée.

Le reste du fichier est scindé en sections dont les éléments peuvent être modifiés (elles indiquent les éléments qui sont traités par le script). Pour marquer un élément à traiter, remplacez le caractère « - » qui le précède par « + ». Les sections du script sont séparées par une ligne vide. Chaque section possède un numéro et un titre.

01) Running processes (processus en cours)

Cette section contient la liste de tous les processus en cours d'exécution dans le système. Chaque processus est identifié par son chemin UNC, puis par son code de hachage CRC16 entre astérisques (*).

Exemple :

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Dans cet exemple, un processus, à savoir module32.exe, a été sélectionné (marqué par le caractère « + ») ; le processus s'arrête à l'exécution du script.

02) Loaded modules (modules chargés)

Cette section répertorie la liste des modules système en cours d'utilisation :

Exemple :

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Dans cet exemple, le module khbekhb.dll a été marqué par un « + ». Quand le script est exécuté, il reconnaît les processus qui utilisent ce module et les arrête.

03) TCP connections (connexions TCP)

Cette section contient des informations sur les connexions TCP existantes.

Exemple :

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner: System
[...]
```

Lorsque le script est exécuté, il localise le propriétaire du socket dans les connexions TCP marquées et arrête le socket, ce qui libère des ressources système.

04) UDP endpoints (points de terminaison UDP)

Cette section contient des informations sur les points de terminaison UDP existants.

Exemple :

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Lorsque le script est exécuté, il isole le propriétaire du socket aux points de terminaison UDP marqués et arrête le socket.

O5) DNS server entries (entrées du serveur DNS)

Cette section contient des informations sur la configuration actuelle du serveur DNS.

Exemple :

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Les entrées du serveur DNS marquées sont supprimées à l'exécution du script.

O6) Important registry entries (entrées de Registre importantes)

Cette section contient des informations relatives aux entrées de Registre importantes.

Exemple :

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Les entrées marquées sont supprimées, réduites à des valeurs de 0 octet ou réinitialisées sur leur valeur par défaut lors de l'exécution du script. L'action à appliquer à chaque entrée dépend de la catégorie de l'entrée et de la valeur de la clé dans ce Registre.

O7) Services (services)

Cette section répertorie les services enregistrés dans le système.

Exemple :

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running, startup:
Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running, startup:
Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped, startup:
Manual
[...]
```

Les services marqués et les services dépendants sont arrêtés et désinstallés après l'exécution du script.

O8) Drivers (pilotes)

Cette section répertorie les pilotes installés.

Exemple :

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Lorsque vous exécutez le script, les pilotes sélectionnés sont arrêtés. Notez que certains pilotes n'autoriseront pas leur arrêt.

09) Critical files (fichiers critiques)

Cette section contient des informations sur les fichiers essentiels au système d'exploitation.

Exemple :

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Les éléments sélectionnés sont soit supprimés, soit restaurés sur leur valeur d'origine.

4.6.4.3 Exécution des scripts de services

Marquez tous les éléments souhaités, puis enregistrez et fermez le script. Exécutez le script modifié directement depuis la fenêtre principale ESET SysInspector en choisissant l'option **Exécuter le script de services** dans le menu Fichier. Lorsque vous ouvrez un script, le programme affiche le message suivant : **Voulez-vous vraiment exécuter le script de service « %Scriptname% » ?** Une fois que vous avez confirmé votre sélection, un autre avertissement peut apparaître pour vous indiquer que le script de service que vous essayez d'exécuter n'a pas été signé. Cliquez sur **Exécuter** pour lancer le script.

Une boîte de dialogue confirmera l'exécution du script.

Si le script n'a pu être traité que partiellement, une boîte de dialogue avec le message suivant apparaît : **Le script de service n'a été exécuté que partiellement. Voulez-vous afficher le rapport d'erreurs ?** Choisissez **Oui** pour afficher un rapport des erreurs complexe qui répertorie les opérations qui n'ont pas été exécutées.

Si le script n'a pas été reconnu, une boîte de dialogue apparaîtra avec le message suivant : **Le script de service sélectionné n'est pas signé. L'exécution de scripts non signés et inconnus peut endommager gravement les données de votre ordinateur. Voulez-vous vraiment exécuter le script et ses actions ?** Ceci peut être le résultat d'incohérences au sein du script (en-tête endommagé, titre de section endommagé, ligne vide manquante entre les sections, etc.). Vous pouvez soit rouvrir le fichier de script et corriger les erreurs qu'il contient, soit créer un autre script de service.

4.6.5 FAQ

L'exécution d'ESET SysInspector requiert-elle des privilèges d'administrateur ?

Bien que ESET SysInspector puisse être exécuté sans privilèges d'administrateur, certaines des informations qu'il recueille peuvent être consultées uniquement via un compte administrateur. Une exécution en tant qu'utilisateur standard ou utilisateur disposant d'un accès restreint entraîne la collecte d'un volume inférieur d'informations sur l'environnement d'exploitation.

ESET SysInspector crée-t-il un fichier journal ?

ESET SysInspector peut créer un fichier journal sur la configuration de votre ordinateur. Pour en enregistrer un, dans le menu principal, sélectionnez **Fichier** > **Enregistrer le journal**. Les journaux sont enregistrés au format XML. Par défaut, les fichiers sont enregistrés dans le répertoire *%USERPROFILE%\Mes documents*\, conformément à la convention de dénomination de fichier SysInspector-%COMPUTERNAME%-YYMMDD-HHMM.XML. Vos pouvez changer l'emplacement et le nom du fichier avant la sauvegarde si vous le souhaitez.

Comment puis-je consulter le fichier journal d'ESET SysInspector ?

Pour consulter un fichier journal créé par ESET SysInspector, exécutez le programme et choisissez **Fichier** > **Ouvrir le journal** dans le menu principal. Vous pouvez également faire glisser les fichiers journaux et les déposer sur l'application ESET SysInspector. Si vous devez consulter fréquemment les fichiers journaux ESET SysInspector, il est conseillé de créer un raccourci vers le fichier SYSINSPECTOR.exe sur le Bureau ; vous pourrez ensuite faire glisser les

fichiers et les déposer sur ce raccourci. Pour des raisons de sécurité, Windows Vista/7 peuvent désactiver la fonction glisser-déposer entre des fenêtres dont les autorisations diffèrent.

Existe-t-il une spécification pour le format de fichier journal ? Existe-t-il un kit de développement logiciel (SDK) ?

Pour l'instant, il n'existe ni spécifications pour le fichier journal, ni SDK car le programme en est toujours au stade du développement. Après la diffusion du programme, nous fournirons ces éléments sur la base des commentaires et des demandes des clients.

Comment ESET SysInspector évalue-t-il le risque que pose un objet en particulier ?

Dans la majorité des cas, ESET SysInspector attribue des niveaux de risque aux objets (fichiers, processus, clés de Registre, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis qui évaluent le potentiel d'activité malveillante. Sur la base de cette heuristique, un niveau de risque de 1 - Bon (vert) à 9 - Risqué (rouge) est attribué aux objets. Dans le volet de navigation gauche, la couleur des sections est définie par le niveau de risque le plus élevé d'un des objets qu'elles contiennent.

Un niveau de risque « 6 - Inconnu (rouge) » signifie-t-il que l'objet est dangereux ?

Les évaluations d'ESET SysInspector ne garantissent pas qu'un objet est malveillant. Cette réponse doit être apportée par l'expert en sécurité. ESET SysInspector a été développé pour fournir aux experts en sécurité une évaluation rapide afin qu'ils puissent identifier les objets d'un système qui doivent faire l'objet d'un examen plus approfondi en cas de comportement étrange.

Pourquoi ESET SysInspector se connecte-t-il à Internet ?

À l'instar de nombreuses applications, ESET SysInspector possède un « certificat » avec une signature numérique qui permet de garantir que le logiciel a bien été diffusé par ESET et qu'il n'a pas été modifié. Afin de vérifier le certificat, le système d'exploitation contacte une autorité de certification pour confirmer l'identité de l'éditeur de logiciels. Il s'agit d'un comportement normal pour tous les programmes avec signature numérique sous Microsoft Windows.

Qu'est-ce que la technologie Anti-Stealth ?

La technologie Anti-Stealth offre une détection efficace des rootkits.

Quand un système est attaqué par un code malveillant qui se comporte comme un rootkit, l'utilisateur risque une perte ou un vol de données. Sans outil spécial de lutte contre les rootkits, il est pratiquement impossible de les détecter.

Pourquoi y a-t-il parfois des fichiers marqués comme « Signé par MS » avec une valeur différente dans le champ « Nom de la société » ?

Lorsqu'il tente d'identifier la signature numérique d'un fichier exécutable, ESET SysInspector recherche d'abord une signature numérique intégrée au fichier. Si une signature numérique est détectée, le fichier est validaté à l'aide de ces informations. En revanche, si aucune signature numérique n'est détectée, ESI lance la recherche du fichier CAT correspondant (Catalogue de sécurité - *%systemroot%\system32\catroot*) qui contient les informations relatives au fichier exécutable traité. Si le fichier CAT pertinent est trouvé, la signature numérique du fichier CAT est appliquée dans la procédure de validation du fichier exécutable.

Voilà pourquoi des fichiers sont parfois marqués « Signé par MS » mais ont un « Nom de la société » différent.

Exemple :

Windows 2000 comprend l'application HyperTerminal qui se trouve dans *C:\Program Files\Windows NT*. Le fichier exécutable principal de l'application n'a pas de signature numérique, mais ESET SysInspector l'indique comme étant un fichier signé par Microsoft. Ceci s'explique par une référence dans *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* qui pointe vers *C:\Program Files\Windows NT\hypertrm.exe* (le fichier exécutable principal de l'application HyperTerminal) et *sp4.cat* qui possède une signature numérique de Microsoft.

4.6.6 ESET SysInspector en tant que partie de ESET Mail Security

Pour ouvrir la section ESET SysInspector de ESET Mail Security, cliquez sur **Outils** > **ESET SysInspector**. Le système de gestion de la fenêtre ESET SysInspector est semblable à celui des journaux d'analyse des ordinateurs ou des tâches planifiées. Toutes les opérations effectuées avec des instantanés système (création, affichage, comparaison, suppression et exportation) sont accessibles en un ou deux clics.

La fenêtre ESET SysInspector contient les informations élémentaires concernant les instantanés créés : heure de création, bref commentaire, nom de l'utilisateur auteur de l'instantané et statut de l'instantané.

Pour comparer, créer ou supprimer des instantanés, utilisez les boutons correspondants situés en dessous de la liste des instantanés dans la fenêtre ESET SysInspector. Ces options sont également disponibles dans le menu contextuel. Pour afficher l'instantané du système sélectionné, utilisez l'option **Afficher** du menu contextuel. Pour exporter l'instantané sélectionné dans un fichier, cliquez dessus avec le bouton droit de la souris et sélectionnez **Exporter...**

Voici la description détaillée des options disponibles :

- **Comparer** - permet de comparer deux journaux. Elle est particulièrement adaptée si vous souhaitez effectuer le suivi des modifications entre le journal actuel et un ancien journal. Pour que cette option entre en vigueur, vous devez sélectionner deux instantanés à comparer.
- **Créer...** - Crée un enregistrement. Au préalable, vous devez entrer un bref commentaire sur l'enregistrement. Pour consulter le pourcentage de progression de la création de l'instantané en cours, consultez la colonne **Statut**. Tous les instantanés terminés ont le statut **Créé**.
- **Effacer/Effacer tout** - Supprime les entrés de la liste.
- **Exporter...** - Cette option enregistre l'entrée sélectionnée dans un fichier XML (également dans une version compressée).

4.7 ESET SysRescue

ESET SysRescue est un utilitaire qui vous permet de créer un disque amorçable contenant une des solutions ESET Security - il peut s'agir de ESET NOD32 Antivirus, ESET Smart Security, ou d'un des produits orientés serveur. Le principal avantage de ESET SysRescue réside dans le fait que la solution ESET Security s'exécute indépendamment du système d'exploitation hôte, tout en ayant un accès direct au disque et à l'ensemble du système de fichiers. Il est par conséquent possible de supprimer les infiltrations qui ne pourraient normalement pas être supprimées, par exemple lorsque le système d'exploitation est en cours d'exécution.

4.7.1 Configuration minimale requise

ESET SysRescue fonctionne dans l'environnement de préinstallation Microsoft Windows (Windows PE) version 2.x basé sur Windows Vista.

Windows PE fait partie du Kit d'installation automatisée de Windows (Windows AIK) ou du Kit d'évaluation et de déploiement de Windows (Windows ADK). Windows AIK ou ADK doit donc être installé avant la création d'ESET SysRescue (<%http://go.eset.eu/AIK%>) ou (<%http://go.eset.eu/ADK%>). Le kit à installer sur votre système dépend de la version du système d'exploitation utilisé. Windows PE prenant en charge la version 32 bits, le package d'installation d'ESET Security 32 bits doit être installé lors de la création d'ESET SysRescue sur des systèmes 64 bits. ESET SysRescue prend en charge Windows AIK 1.1 et versions ultérieures, ainsi que Windows ADK.

REMARQUE : Étant donné que la taille de Windows AIK est de plus de 1 Go et celle de Windows ADK de 1,3 GO, une connexion Internet rapide est nécessaire pour un téléchargement efficace.

ESET SysRescue est disponible dans les ESET Security version 4.0 et suivantes.

ESET SysRescue prend en charge les systèmes d'exploitation suivants :

- Windows Server 2003 Service Pack 1 avec KB926044
- Windows Server 2003 Service Pack 2
- Windows Server 2008
- Windows Server 2012

Windows AIK prend en charge :

- Windows Server 2003
- Windows Server 2008

Windows ADK prend en charge :

- Windows Server 2012

4.7.2 Procédure de création d'un CD de dépannage

Pour lancer l'Assistant ESET SysRescue, cliquez sur **Démarrer** > **Programmes** > **ESET** > **ESET Mail Security** > **ESET SysRescue**.

Tout d'abord, l'Assistant vérifie si Windows AIK ou Windows ADK est installé et si un périphérique adapté pour la création du support d'amorçage est présent. Si Windows AIK ou Windows ADK n'est pas installé sur l'ordinateur (ou si l'installation est endommagée ou incorrecte), l'Assistant vous propose de l'installer ou de saisir le chemin d'accès à votre dossier Windows AIK (<%http://go.eset.eu/AIK%>) ou Windows ADK (<%http://go.eset.eu/ADK%>).

REMARQUE : Étant donné que la taille de Windows AIK est de plus de 1 Go et celle de Windows ADK de 1,3 GO, une connexion Internet rapide est nécessaire pour un téléchargement efficace.

Au cours de l'étape suivante 117, sélectionnez le support cible où ESET SysRescue est créé.

4.7.3 Sélection de la cible

Outre la sauvegarde sur un CD/DVD/périphérique USB, vous pouvez enregistrer ESET SysRescue dans un fichier ISO. Ensuite, vous pouvez graver l'image ISO sur un CD/DVD, ou l'utiliser d'une autre manière (dans un environnement virtuel tel que VmWare ou Virtualbox par exemple).

Si vous choisissez USB en tant que support cible, le démarrage peut ne pas fonctionner sur certains ordinateurs. Certaines versions du BIOS peuvent signaler des problèmes de communication entre le BIOS et le gestionnaire de démarrage (par exemple sous Windows Vista) et le démarrage s'arrête sur l'erreur suivante :

```
file : \boot\bcd
status : 0xc000000e
info : an error occurred while attemping to read the boot configuration data (une erreur s'est produite pendant la ten
```

Si ce message s'affiche, il est conseillé de sélectionner CD au lieu d'USB en tant que support.

4.7.4 Paramètres

Avant de commencer la création d'ESET SysRescue, l'Assistant d'installation affiche les paramètres de compilation à la dernière étape de l'assistant ESET SysRescue. Cliquez pour ce faire sur le bouton **Changer...** Les options disponibles sont les suivantes :

- Dossiers 118
- ESET Antivirus 118
- Paramètres avancés 118
- Protocole Internet 119
- Périphérique USB amorçable 119 (lorsque le périphérique USB cible est sélectionné)
- Gravure 119 (lorsque le CD/DVD cible est sélectionné)

Le bouton **Créer** est inactif si aucun package d'installation MSI n'a été défini ou si aucune solution ESET Security n'est installée sur l'ordinateur. Pour sélectionner un package d'installation, cliquez sur le bouton **Modifier**, puis accédez à l'onglet **Antivirus ESET**. Si vous ne saisissez pas le nom d'utilisateur et le mot de passe (**Modifier** > **Antivirus ESET**), le bouton **Créer** est inactif.

4.7.4.1 Dossiers

Le **dossier temporaire** est un dossier de travail dans lequel sont stockés les fichiers nécessaires à la compilation d'ESET SysRescue.

Le **dossier ISO** est un dossier dans lequel est enregistré le fichier ISO après la compilation.

La liste dans cet onglet répertorie tous les disques de réseau locaux et mappés, ainsi que l'espace disponible. Si certains des dossiers sont stockés sur un lecteur ne disposant pas de l'espace suffisant, il est conseillé de sélectionner un autre lecteur avec plus d'espace disponible. Dans le cas contraire, la compilation pourrait s'arrêter prématurément en raison d'un manque d'espace sur le disque.

Applications externes : vous permet d'indiquer des programmes supplémentaires qui seront exécutés ou installés après l'amorçage depuis un support ESET SysRescue.

Inclure les applications externes : permet d'ajouter des programmes externes à la compilation ESET SysRescue.

Dossier sélectionné : dossier dans lequel se trouvent les programmes à ajouter au disque ESET SysRescue.

4.7.4.2 ESET Antivirus

Pour créer le CD ESET SysRescue, vous pouvez sélectionner deux sources de fichiers ESET à utiliser par le compilateur.

Dossier ESS/EAV : fichiers déjà contenus dans le dossier dans lequel la solution ESET Security est installée sur l'ordinateur.

Fichier MSI : les fichiers contenus dans le programme d'installation MSI sont utilisés.

Vous pouvez choisir de mettre à jour l'emplacement des fichiers (.nup). Normalement, l'option par défaut **Dossier ESS/EAV/Fichier MSI** doit être définie. Dans certains cas, il est possible de choisir un **dossier de mise à jour**, par exemple pour utiliser une version de base des signatures de virus plus ancienne ou plus récente.

Vous pouvez utiliser l'une des deux sources suivantes pour le nom d'utilisateur et le mot de passe :

ESS/EAV installé - Le nom d'utilisateur et le mot de passe sont copiés depuis la version installée de la solution ESET Security.

De l'utilisateur - Le nom d'utilisateur et le mot de passe saisis dans les zones de texte correspondantes sont utilisés.

REMARQUE : La solution ESET Security sur le CD ESET SysRescue est mise à jour soit via Internet, soit par l'intermédiaire de la solution ESET Security installée sur l'ordinateur sur lequel le CD ESET SysRescue est exécuté.

4.7.4.3 Paramètres avancés

L'onglet **Avancé** permet d'optimiser le CD ESET SysRescue en fonction de la quantité de mémoire disponible sur l'ordinateur. Sélectionnez **576 Mo et plus** pour écrire le contenu du CD dans la mémoire vive (RAM). Si vous choisissez **moins de 576 Mo**, l'accès au CD de récupération aura lieu en permanence lorsque WinPE est en exécution.

Dans la section **Pilotes externes**, vous pouvez installer les pilotes de votre matériel (en général, une carte de réseau). Bien que WinPE repose sur Windows Vista PS1 qui prend en charge une large gamme de matériel, il arrive parfois que le matériel ne soit pas reconnu. Dans ce cas, un pilote doit être ajouté manuellement. L'installation du pilote dans la compilation ESET SysRescue peut s'effectuer de deux manières : manuellement (à l'aide du bouton **Ajouter**) et automatiquement (par l'intermédiaire du bouton **Recherche auto**). En cas d'installation manuelle, vous devez choisir le chemin d'accès au fichier .inf correspondant (le fichier *.sys applicable doit se trouver également dans le dossier). En cas d'installation automatique, le pilote est détecté automatiquement dans le système d'exploitation de l'ordinateur. Il est conseillé d'utiliser l'introduction automatique uniquement si ESET SysRescue est utilisé sur un ordinateur qui possède la même carte de réseau que l'ordinateur sur lequel le CD ESET SysRescue a été créé. Lors de la création d'ESET SysRescue, le pilote est installé dans la compilation, ce qui évite à l'utilisateur d'avoir à le rechercher ultérieurement.

4.7.4.4 Protocole Internet

Cette section vous permet de configurer les informations réseau de base et de définir les connexions prédéfinies en fonction d'ESET SysRescue.

Sélectionnez **Adresse IP privée automatique** pour obtenir l'adresse IP automatiquement depuis le serveur DHCP (Dynamic Host Configuration Protocol).

Cette connexion réseau peut également utiliser une adresse IP spécifiée manuellement (appelée également adresse IP statique). Sélectionnez **Personnalisé** pour configurer les paramètres IP appropriés. Si vous sélectionnez cette option, vous devez indiquer une **adresse IP** et, pour les connexions Internet grande vitesse, un **masque de sous-réseau**. Dans **Serveur DNS préféré** et **Serveur DNS de rechange**, saisissez les adresses principale et secondaire de serveur DNS.

4.7.4.5 Périphérique USB d'amorçage

Si vous avez choisi le périphérique USB en tant que support cible, vous pouvez choisir l'un des périphériques USB disponibles dans l'onglet **Périphérique USB d'amorçage** (si plusieurs périphériques USB existent).

Sélectionnez le **périphérique** cible approprié sur lequel ESET SysRescue va être installé.

Avertissement : le périphérique USB sélectionné est formaté lors de la création d'ESET SysRescue. Toutes les données du périphérique sont supprimées.

Si vous choisissez l'option **Format rapide**, le formatage supprime tous les fichiers de la partition, mais ne recherche pas les secteurs endommagés du disque. Utilisez cette option si votre périphérique USB a été déjà formaté et que vous êtes certain qu'il n'est pas endommagé.

4.7.4.6 Graver

Si vous avez choisi CD/DVD en tant que support cible, vous pouvez définir les paramètres de gravure complémentaires dans l'onglet **Graver**.

Supprimer fichier ISO - Cochez cette case pour supprimer le fichier ISO temporaire après la création du CD ESET SysRescue.

Suppression activée - Permet de choisir entre la suppression rapide et la suppression complète.

Graveur - Choisissez le lecteur à utiliser pour la gravure.

Avertissement : il s'agit de l'option par défaut. En cas d'utilisation d'un CD/DVD réinscriptible, toutes les données sur le CD/DVD sont supprimées.

La section Support contient des informations sur le support dans le lecteur de CD/DVD.

Vitesse de gravure : sélectionnez la vitesse souhaitée dans le menu déroulant. Les capacités du périphérique de gravure et le type de CD/DVD utilisé doivent être pris en compte lors de la sélection de la vitesse de gravure.

4.7.5 Utilisation d'ESET SysRescue

Pour que le CD/DVD/USB de récupération fonctionne efficacement, l'ordinateur doit être démarré depuis le support d'amorçage ESET SysRescue. La priorité d'amorçage peut être modifiée dans le BIOS. Vous pouvez également utiliser le menu d'amorçage au démarrage de l'ordinateur (généralement à l'aide de l'une des touches F9 à F12) en fonction de la version de la carte mère ou du BIOS.

Une fois l'amorçage depuis le support d'amorçage terminé, la solution ESET Security démarre. Comme ESET SysRescue n'est utilisé que dans des situations spécifiques, certains modules de protection et fonctionnalités de programme présents dans la version standard de ESET Security ne sont pas nécessaires ; leur liste est limitée à l' **Analyse de l'ordinateur**, à la **Mise à jour** et à certaines sections de la **Configuration**. ESET SysRescue peut mettre à jour la base des signatures de virus. C'est la principale fonctionnalité de cette application et nous vous recommandons d'effectuer cette mise à jour avant de lancer l'analyse de l'ordinateur.

4.7.5.1 Utilisation d'ESET SysRescue

En supposant que des ordinateurs du réseau aient été infectés par un virus modifiant des fichiers exécutables (.exe). La solution ESET Security est capable de nettoyer tous les fichiers infectés, à l'exception d'*explorer.exe* qui ne peut pas être nettoyé, même en mode sans échec. Cela est dû au fait que le fichier *explorer.exe*, c'est-à-dire l'un des principaux processus de Windows, est également lancé en mode sans échec. La solution ESET Security n'exécute aucune opération et le fichier reste infecté.

Dans ce type de scénario, vous pouvez utiliser ESET SysRescue pour résoudre le problème. ESET SysRescue ne requiert aucun composant du système d'exploitation hôte et peut traiter (nettoyer, supprimer) n'importe quel fichier sur le disque.

4.8 Options d'interface utilisateur

La configuration de l'interface utilisateur d'ESET Mail Security peut être modifiée de manière à pouvoir ajuster l'environnement de travail selon vos besoins. Ces options de configuration sont accessibles depuis la branche **Interface utilisateur** de l'arborescence de configuration avancée de ESET Mail Security.

Dans la section **Éléments de l'interface utilisateur**, l'option **Mode avancé** permet aux utilisateurs de passer au mode avancé. Le mode avancé affiche des paramètres détaillés et des commandes supplémentaires pour ESET Mail Security.

L'**interface utilisateur graphique** doit être désactivée si les éléments graphiques ralentissent les performances de l'ordinateur ou causent d'autres problèmes. De la même manière, il est peut-être nécessaire de désactiver l'interface utilisateur graphique pour les utilisateurs malvoyants, car elle peut créer un conflit avec des applications spéciales utilisées pour la lecture de textes affichés à l'écran.

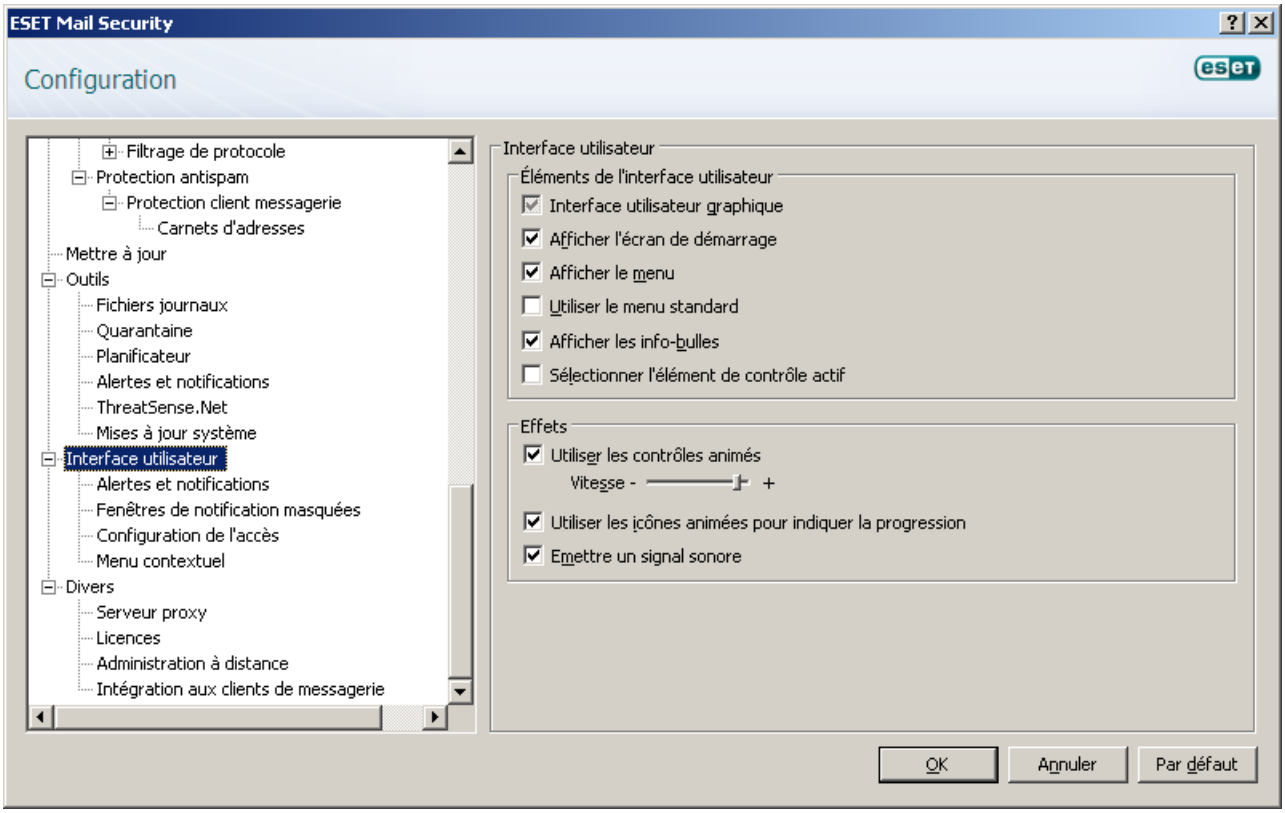
Pour désactiver l'écran de démarrage de ESET Mail Security, désélectionnez l'option **Afficher l'écran de démarrage**.

En haut de la fenêtre principale de programme de ESET Mail Security figure un menu standard qui peut être activé ou désactivé en fonction de l'option **Utiliser le menu standard**.

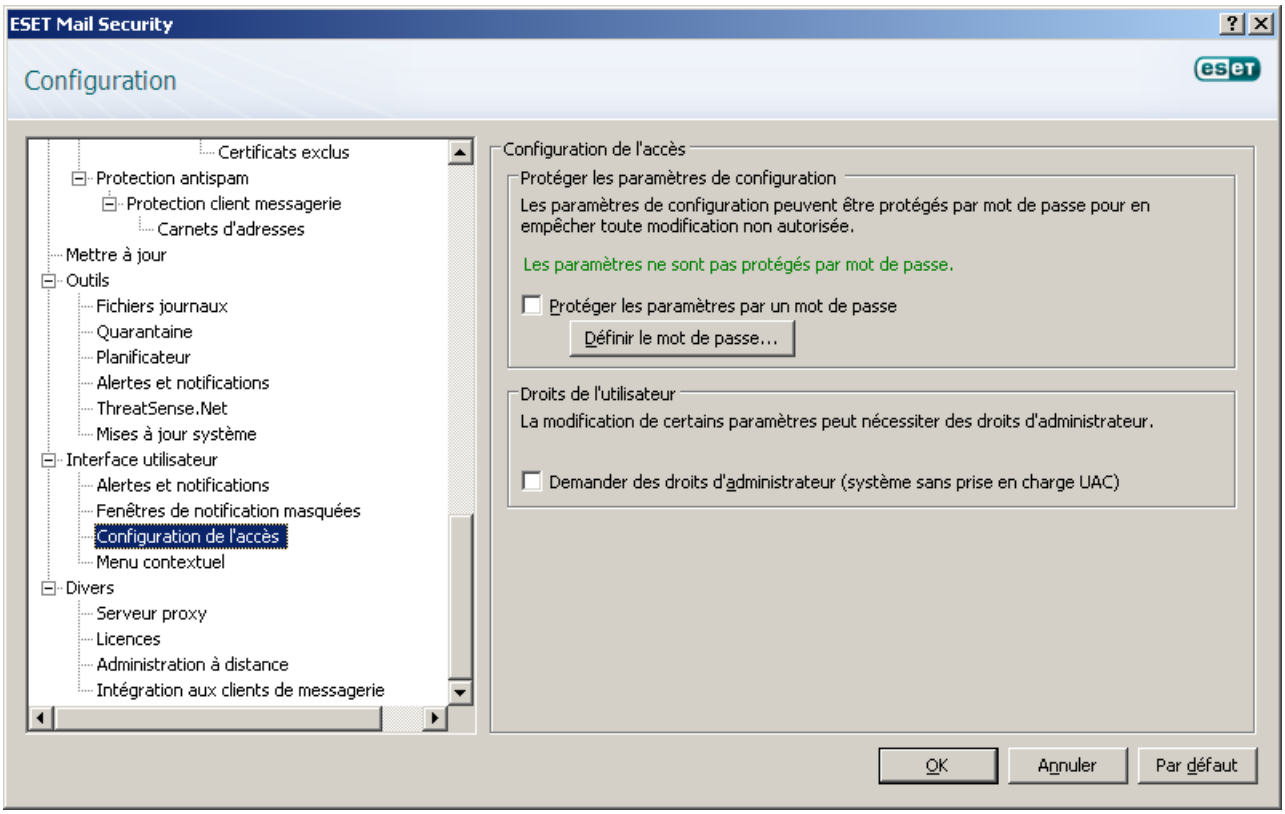
Si l'option **Afficher les info-bulles** est activée, une courte description apparaît si le curseur est immobilisé sur une option. Lorsque l'option **Sélectionner l'élément de contrôle actif** est sélectionnée, le système met en évidence tout élément situé dans la zone active du curseur de la souris. L'élément mis en évidence est activé si l'utilisateur clique dessus.

Pour diminuer ou augmenter la vitesse des effets animés, sélectionnez l'option **Utiliser les contrôles animés** et déplacez le curseur **Vitesse** vers la gauche ou vers la droite.

Pour activer l'utilisation des icônes animées afin d'afficher la progression des différentes opérations, sélectionnez l'option **Utiliser les icônes animées pour indiquer la progression**. Si vous souhaitez que le programme émette un son d'avertissement si un événement important se produit, sélectionnez l'option **Émettre un signal sonore**.



Les fonctionnalités d'**interface utilisateur** permettent également de protéger les paramètres de configuration de ESET Mail Security par mot de passe. Cette option se trouve dans le sous-menu **Protection des paramètres** dans **Interface utilisateur**. Il est essentiel que le programme soit correctement configuré pour garantir le maximum de sécurité au système. Tout changement non autorisé peut provoquer la perte de données importantes. Pour définir un mot de passe visant à protéger les paramètres de configuration, cliquez sur **Définir le mot de passe...**



4.8.1 Alertes et notifications

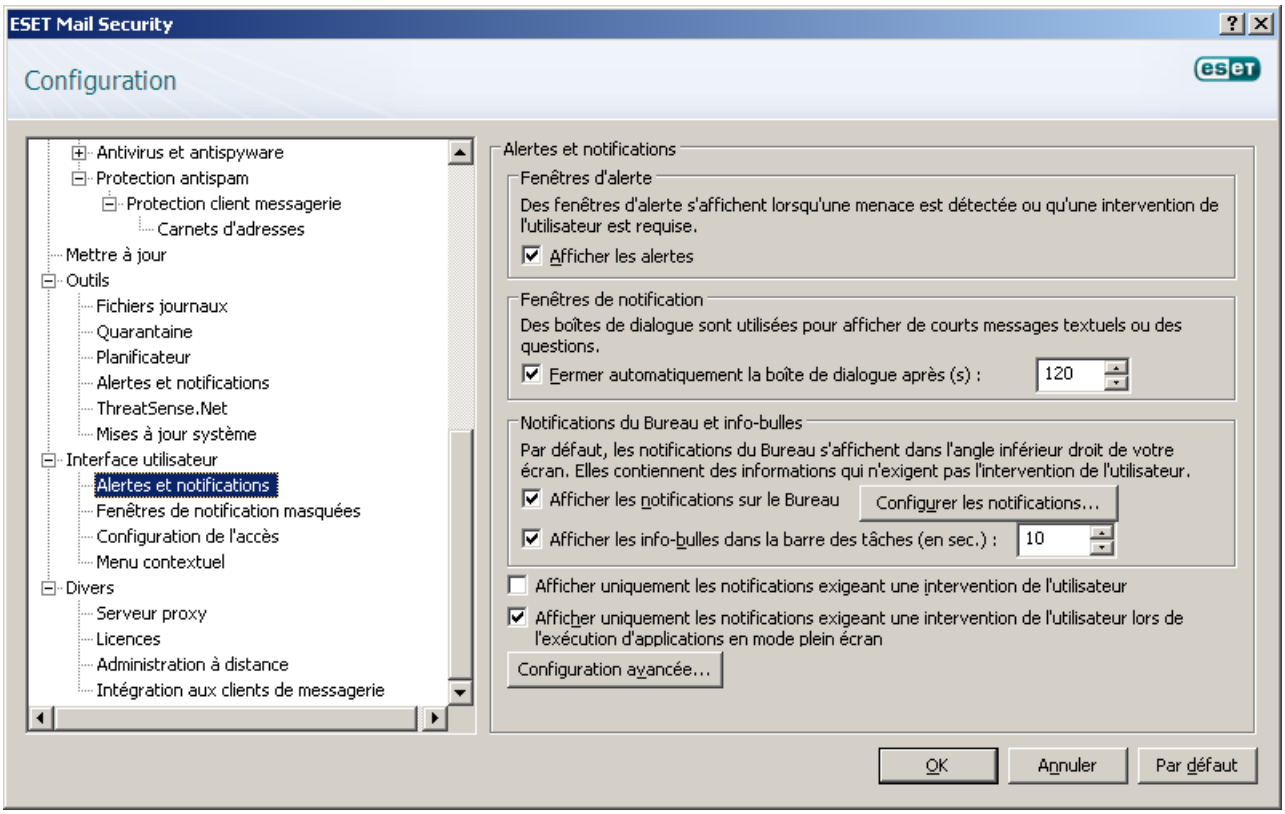
La section **Configurer les alertes et notifications** dans **Interface utilisateur** vous permet de configurer le mode de traitement des alertes en cas de menace et des notifications système dans ESET Mail Security.

La première option est **Afficher les alertes**. Lorsqu'elle est désactivée, aucune fenêtre d'alerte ne s'affiche, ce qui ne convient qu'à un nombre limité de situations particulières. Nous recommandons à la majorité des utilisateurs de conserver l'option par défaut (activée).

Pour fermer automatiquement les fenêtres d'alerte après un certain délai, sélectionnez l'option **Fermer automatiquement la boîte de dialogue après (s)**. Si les fenêtres d'alerte ne sont pas fermées manuellement, le système les ferme automatiquement une fois le laps de temps écoulé.

Les notifications sur le bureau et les infobulles sont fournies à titre d'information uniquement et ne permettent ni n'exigent aucune interaction avec l'utilisateur. Elles s'affichent dans la partie système de la barre d'état, dans l'angle inférieur droit de l'écran. Pour activer l'affichage des notifications sur le bureau, activez l'option **Afficher les notifications sur le bureau**. Vous pouvez modifier d'autres options détaillées (la durée d'affichage des notifications et la transparence de la fenêtre) en cliquant sur le bouton **Configurer les notifications...**

Pour prévisualiser le comportement des notifications, cliquez sur le bouton **Aperçu**. Pour configurer la durée d'affichage des infobulles, utilisez l'option **Afficher les infos-bulles dans la barre des tâches (s)**.



Cliquez sur **Configuration avancée...** pour indiquer des options de configuration supplémentaires **Alertes et notifications**, notamment l'option **Afficher uniquement les notifications exigeant une intervention de l'utilisateur**. Cette option vous permet d'activer/de désactiver l'affichage des alertes et des notifications qui n'exigent aucune interaction de l'utilisateur. Sélectionnez **Afficher uniquement les notifications exigeant une intervention de l'utilisateur lors de l'exécution d'applications en mode plein écran** pour supprimer toutes les notifications non interactives. Dans le menu déroulant **Verbosité minimale des événements à afficher**, vous pouvez sélectionner le niveau de gravité de démarrage des alertes et notifications à afficher.

La dernière fonctionnalité de cette section permet de configurer la destination des notifications dans un environnement multi-utilisateur. **Sur les systèmes multi-utilisateurs, afficher les notifications sur l'écran de l'utilisateur suivant** : permet de définir l'utilisateur qui recevra les notifications importantes d'ESET Mail Security. Normalement, il doit s'agir de l'administrateur système ou de l'administrateur réseau. Cette option est particulièrement utile pour les serveurs Terminal Server, pour autant que toutes les notifications système soient envoyées à l'administrateur.

4.8.2 Désactivation de l'interface utilisateur graphique sur Terminal Server

Ce chapitre indique comment désactiver l'interface utilisateur graphique d'ESET Mail Security sur Windows Terminal Server pour les sessions utilisateur.

Normalement, l'interface utilisateur graphique d'ESET Mail Security démarre chaque fois qu'un utilisateur distant se connecte au serveur et crée une session de terminal. Cet affichage n'est généralement pas conseillé sur les serveurs Terminal Server. Si vous souhaitez désactiver l'interface utilisateur graphique pour les sessions de terminal, procédez comme suit :

1. Exécutez *regedit.exe*
2. Accédez à *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
3. Cliquez avec le bouton droit sur la valeur *egui* et sélectionnez *Modifier...*
4. Ajoutez un paramètre `/terminal` à la fin d'une chaîne existante

Voici un exemple des données de valeur *egui* :

```
"C:\Program Files\ESET\ESET Mail Security\egui.exe" /hide /waitservice /terminal
```

Si vous souhaitez rétablir ce paramètre et activer le démarrage automatique de l'interface utilisateur graphique d'ESET Mail Security, supprimez le paramètre `/terminal` . Pour accéder à la valeur de registre *egui*, répétez les étapes 1 à 3.

4.9 eShell

eShell (abréviation d'ESET Shell) est une interface à ligne de commande pour ESET Mail Security. eShell s'utilise en remplacement de l'interface utilisateur graphique et dispose de toutes les fonctionnalités et options proposées normalement par cette interface. eShell vous permet de configurer et d'administrer l'intégralité du programme sans avoir à utiliser l'interface utilisateur graphique.

Outre les fonctions et fonctionnalités disponible dans l'interface graphique, l'interface à ligne de commande vous permet d'automatiser l'exécution de scripts afin de configurer et de modifier la configuration, ou encore d'effectuer une opération. eShell est également utile pour les utilisateurs qui préfèrent les lignes de commande aux interfaces graphiques.

REMARQUE : Un manuel eShell peut être téléchargé ici. Il répertorie toutes les commandes, avec leur syntaxe et une description.

Cette section indique comment parcourir et utiliser le système eShell. Elle répertorie également toutes les commandes et décrit chaque commande, ainsi que l'opération qu'elle effectue.

Le système eShell peut être exécuté de deux manières :

- Mode interactif : ce mode est utile lorsque vous souhaitez utiliser régulièrement eShell (pas simplement exécuter une seule commande), par exemple lorsque vous modifiez la configuration, affichez des journaux, etc. Vous pouvez également utiliser le mode interactif si vous ne connaissez pas encore toutes les commandes. Le mode interactif simplifie la navigation dans eShell. Il affiche également les commandes que vous pouvez utilisez dans un contexte défini.
- Commande unique/mode de traitement par lots : vous pouvez utiliser ce mode si vous avez uniquement besoin d'exécuter une commande sans passer au mode interactif eShell. Pour ce faire, saisissez dans l'invite de commande Windows `eShell` et ajoutez les paramètres appropriés. Par exemple :

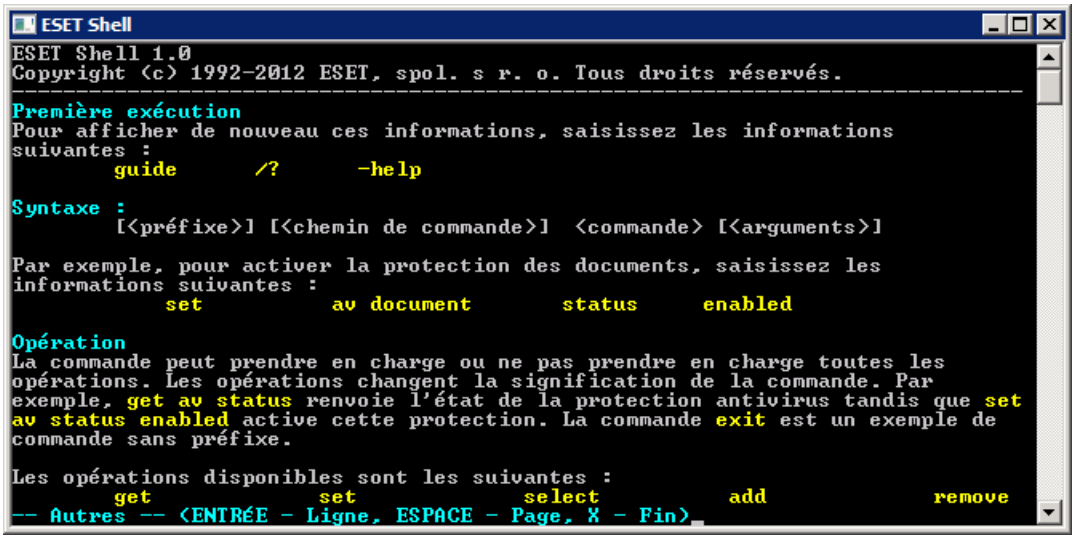
```
eshell set av document status enabled
```

REMARQUE : afin d'exécuter les commandes eShell depuis l'invite de commande Windows ou d'exécuter les fichiers en mode de traitement par lots, cette fonction doit d'abord être activée (la commande `set general access batch always` doit être exécutée en mode interactif). Pour plus d'informations sur la commande set batch, cliquez ici 127.

Pour passer au mode interactif eShell, vous pouvez utiliser l'une des deux méthodes suivantes :

- Par l'intermédiaire du menu Démarrer de Windows : **Démarrer** > **Tous les programmes** > **ESET** > **ESET File Security** > **ESET shell**
- Depuis l'invite de commande Windows en tapant `eShell` et en appuyant sur la touche Entrée.

Lorsque vous exécutez eShell en mode interactif pour la première fois, l'écran de première exécution s'affiche.



Il présente des exemples de base concernant l'utilisation d'eShell avec une syntaxe, un préfixe, un chemin d'accès à une commande, des formes abrégées, des alias, etc. Il constitue un guide rapide d'utilisation d'eShell.

REMARQUE : Si vous souhaitez afficher ultérieurement cet écran de première exécution, tapez la commande `guide` .

REMARQUE : les commandes ne font pas la distinction entre les majuscules et les minuscules : que vous saisissiez les noms de commande en majuscules ou en minuscules, les commandes s'exécutent de la même manière.

4.9.1 Utilisation

Syntaxe
Pour qu'elles fonctionnent correctement, les commandes doivent avec une syntaxe correcte. Elles peuvent être composées d'un préfixe, d'un contexte, d'arguments, d'options, etc. Voici la syntaxe générale utilisée dans eShell :

[<préfixe>] [<chemin de la commande>] <commande> [<arguments>]

Exemple (cette commande active la protection des documents) :
`SET AV DOCUMENT STATUS ENABLED`

`SET` - préfixe
`AV DOCUMENT` - chemin vers une commande particulière, contexte auquel la commande appartient
`STATUS` - commande proprement dite
`ENABLED` - argument de la commande

L'utilisation de la valeur `HELP` ou `?` avec une commande affiche la syntaxe de cette commande. Par exemple, la commande `CLEANLEVEL HELP` affiche la syntaxe de la commande `CLEANLEVEL` :

SYNTAXE :
```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

Vous pouvez constater que `[get]` est entre crochets. Cela indique que le préfixe `get` est l'option par défaut de la commande `cleanlevel` . En d'autres termes, lorsque vous exécutez la commande `cleanlevel` sans indiquer de préfixe, la commande utilise le préfixe par défaut (dans ce cas `get cleanlevel`). Vous gagnerez du temps en n'indiquant pas de préfixe. La valeur `get` est généralement le préfixe par défaut pour la plupart des commandes, mais vous devez effectuer cette vérification pour chaque commande et vous assurer qu'il correspond bien à l'instruction que vous souhaitez exécuter.

REMARQUE : Les commandes ne font pas la distinction entre les majuscules et les minuscules : que vous saisissiez les noms de commande en majuscules ou en minuscules, les commandes s'exécutent de la même manière.

Préfixe/Opération
Un préfixe est une opération. L'option `GET` fournit des informations sur la configuration d'une fonctionnalité d'ESET Mail Security ou indique l'état (`GET AV STATUS` affiche l'état de la protection en cours). L'option `SET` (préfixe) configure la fonctionnalité ou change son état (`SET AV STATUS ENABLED` active la protection).

eShell vous permet d'utiliser ces préfixes. Les commandes peuvent prendre en charge ou ne pas prendre en charge les préfixes :

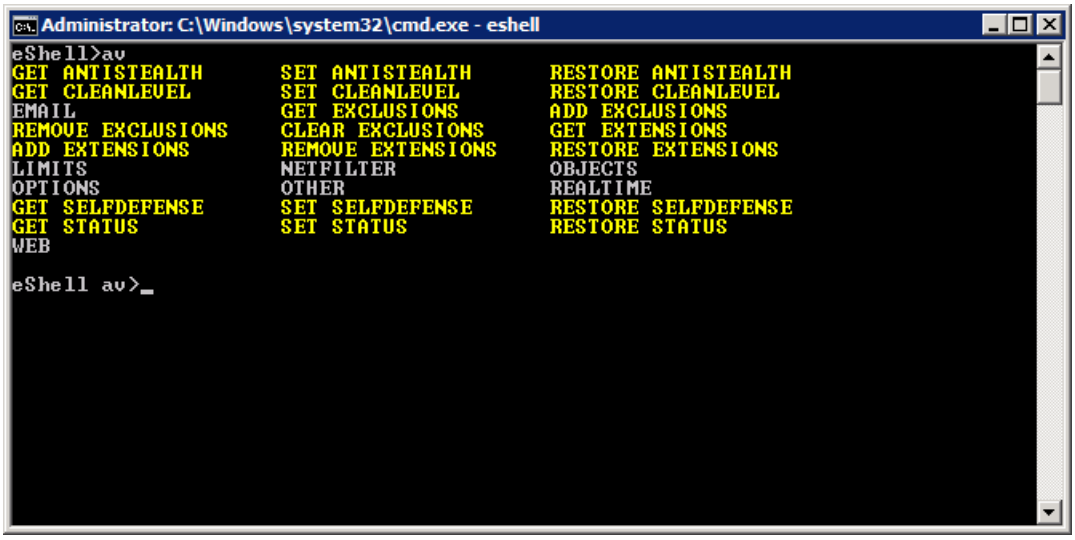
`GET` - renvoie le paramètre/l'état en cours.
`SET` - définit la valeur/l'état.
`SELECT` - sélectionne un élément.
`ADD` - ajoute un élément.
`REMOVE` - supprime un élément.
`CLEAR` - supprime tous les éléments/fichiers.
`START` - démarre une action.
`STOP` - arrête une action.
`PAUSE` - interrompt une action.
`RESUME` - reprend une action.
`RESTORE` - restaure les paramètres/l'objet/le fichier par défaut.
`SEND` - envoie un objet/fichier.
`IMPORT` - importe d'un fichier.
`EXPORT` - exporte dans un fichier.

Les préfixes tels que `GET` et `SET` sont utilisés avec de nombreuses commandes (certaines commandes telles que `EXIT`) n'utilisent pas de préfixe.

Chemin/Contexte de la commande
Les commandes sont placées dans des contextes qui constituent une arborescence. Le niveau supérieur de l'arborescence est la racine. Lorsque vous exécutez eShell, vous vous trouvez au niveau racine :

```
eShell>
```

Vous pouvez exécuter la commande depuis cet emplacement ou saisir le nom du contexte dans l'arborescence pour y accéder. Par exemple, lorsque vous saisissez le contexte `TOOLS` , toutes les commandes et sous-contextes disponibles depuis cet emplacement sont répertoriés.



Les éléments en jaune correspondent aux commandes que vous pouvez exécuter et les éléments en gris sont des sous-contextes que vous pouvez saisir. Un sous-contexte contient des commandes supplémentaires.

Si vous devez remonter d'un niveau, utilisez `..` (deux points). Par exemple, imaginons que vous vous trouvez à ce niveau :

```
eShell av options>
```

saisissez `..` et vous remontez d'un niveau :

```
eShell av>
```

Si vous souhaitez retourner au niveau racine depuis `eShell av options>` (soit deux niveaux en dessous de la racine), tapez simplement `..  ..` (deux points et deux points séparés par un espace). Vous remontez alors de deux niveaux, ce qui correspond dans ce cas à la racine. Vous pouvez utiliser cette méthode, quel que soit le niveau auquel vous vous trouvez dans l'arborescence. Utilisez le nombre de `..` correspondant au niveau auquel vous souhaitez accéder.

Le chemin est relatif au contexte en cours. Si la commande est contenue dans le contexte en cours, n'indiquez pas de chemin. Par exemple, pour exécuter `GET AV STATUS` , saisissez :

`GET AV STATUS` - si vous êtes dans le contexte racine (la ligne de commande indique `eShell>`)
`GET STATUS` - si vous êtes dans le contexte `AV` (la ligne de commande indique `eShell av>`)
`.. GET STATUS` - si vous êtes dans le contexte `AV OPTIONS` (la ligne de commande indique `eShell av options>`)

Argument
Un argument est une action qui peut être réalisée pour une commande particulière. Par exemple, la commande `CLEANLEVEL` peut être utilisée avec les arguments suivants :

`none` - Ne pas nettoyer
`normal` - Nettoyage standard
`strict` - Nettoyage strict

Les arguments `ENABLED` ou `DISABLED`permettent d'activer ou de désactiver une fonctionnalité.

Forme abrégée/Commandes raccourcies
eShell vous permet de raccourcir les contextes, les commandes et les arguments (à condition que l'argument soit un paramètre ou une autre option). Il n'est pas possible de raccourcir un préfixe ou un argument s'il s'agit d'une valeur concrète telle qu'un nombre, un nom ou un chemin.

Voici des exemples de forme raccourcie :

`set status disabled` => `set stat en`
`add av exclusions C:\path\file.ext` => `add av exc C:\path\file.ext`

Si deux commandes ou contextes commencent par la même lettre, `ABOUT` et `AV`par exemple, et que vous saisissez la commande raccourcie `A` , eShell ne parvient pas à déterminer laquelle de ces deux commandes vous souhaitez exécuter. Un message d'erreur s'affiche et répertorie les commandes commençant par un « A » pour que vous puissiez sélectionner celle à exécuter :

```
eShell>a
La commande suivante n'est pas unique : a

Les commandes suivantes sont disponibles dans ce contexte :
ABOUT - Affiche les informations sur le programme
AV - Passe au contexte av
```

Ensuite, l'ajout d'une ou de plusieurs lettres (`AB` au lieu de `A`) eShell exécute la commande `ABOUT` car cette commande est unique.

REMARQUE : afin d'avoir la garantie qu'une commande s'exécute comme vous le souhaitez, il est recommandé de ne pas abréger les commandes, les arguments, etc. et d'utiliser plutôt la forme complète. La commande s'exécute alors exactement comme vous le souhaitez et vous évite de commettre des erreurs. Ce conseil s'applique notamment pour les fichiers et les scripts de traitement par lots.

Alias
Un alias est un autre nom qui peut être utilisé pour exécuter une commande (à condition que la commande dispose d'un alias). Voici quelques alias par défaut :

`(global) help` - ?
`(global) close` - exit
`(global) quit` - exit
`(global) bye` - exit
`warnlog` - tools log events
`virlog` - tools log detections

"(global)" signifie que la commande peut être utilisée dans tous les emplacements, quel que soit le contexte actuel. Une commande peut comporter plusieurs alias. Par exemple, la commande `EXIT` comporte les alias `CLOSE`, `QUIT` et `BYE` . Si vous souhaitez quitter eShell, vous pouvez utiliser la commande `EXIT` proprement dite ou l'un de ses alias. L'alias `VIRLOG` est attribué à la commande `DETECTIONS` qui se trouve dans le contexte `TOOLS LOG` . Les détections de commande sont ainsi disponibles depuis le contexte `ROOT` , ce qui facilite l'accès (vous n'avez plus à saisir `TOOLS` puis le contexte `LOG` et l'exécutez directement depuis `ROOT`).

eShell vous permet de définir vos propres alias.

Commandes protégées
Certaines commandes sont protégées et ne peuvent être exécutées qu'après la saisie d'un mot de passe.

Guide
Lorsque vous exécutez la commande `GUIDE` , l'écran de première exécution apparaît et vous explique comment utiliser eShell. Cette commande est disponible dans le contexte `ROOT` (`eShell>`).

Help
Lorsque la commande `HELP` est utilisée seule, elle répertorie toutes les commandes disponibles, avec les préfixes et les sous-contextes du contexte actuel. Elle décrit également brièvement chaque commande/sous-contexte. Lorsque vous exécutez la commande `HELP` en tant qu'argument avec une commande spécifique (par exemple `CLEANLEVEL HELP`), vous obtenez tous les détails de cette commande. Le système affiche la SYNTAXE, les OPÉRATIONS, les ARGUMENTS et les ALIAS de la commande, ainsi qu'une brève description.

Historique de commande
eShell conserve un historique des commandes exécutées. Cet historique s'applique uniquement à la session interactive eShell en cours. Lorsque vous quittez eShell, l'historique des commandes est supprimé. Utilisez les flèches Haut et Bas de votre clavier pour parcourir l'historique. Lorsque vous avez localisé la commande que vous recherchiez, vous pouvez la réexécuter ou la modifier sans avoir à saisir l'intégralité de la commande depuis le début.

CLS/Effacement de l'écran
La commande `CLS` peut être utilisée pour effacer le contenu de l'écran. Cette commande fonctionne de la même manière que l'invite de commande Windows ou que toute autre interface à ligne de commande.

EXIT/CLOSE/QUIT/BYE
Pour fermer ou quitter eShell, vous pouvez utiliser l'une de ces commandes (`EXIT`, `CLOSE`, `QUIT` ou `BYE`).

4.9.2 Commandes

Cette section répertorie toutes les commandes eShell disponibles, ainsi qu'une description en guise d'exemple. Pour obtenir la liste complète des commandes, reportez-vous au manuel eShell. Vous pouvez le télécharger ici.

REMARQUE : les commandes ne font pas la distinction entre les majuscules et les minuscules : que vous saisissiez les noms de commande en majuscules ou en minuscules, les commandes s'exécutent de la même manière.

Commandes contenues dans le contexte **ROOT** :

ABOUT

Répertorie les informations sur le programme. Cette commande indique le nom du produit installé, son numéro de version, les composants installés (notamment le numéro de version de chaque composant), ainsi que des informations de base sur le serveur et le système d'exploitation sur lesquels s'exécute ESET Mail Security.

CHEMIN DE CONTEXTE :

```
root
```

BATCH

Démarre le mode de traitement par lots d'eShell. Ce mode est très utile lors de l'exécution de fichiers/scripts en mode de traitement par lots. Il est recommandé pour les fichiers de traitement par lots. Placez `START BATCH` comme première commande dans le fichier ou le script de traitement par lots pour activer le mode de traitement par lots. Lorsque vous activez cette fonction, aucune entrée interactive (saisie d'un mot de passe par exemple) n'est demandée et les arguments manquants sont remplacés par les options par défaut. Le fichier de traitements par lots ne s'arrête pas au milieu, car eShell atteint une intervention de l'utilisateur. De cette manière, le fichier de traitement par lots s'exécute sans s'arrêter (sauf en cas d'erreur ou si les commandes du fichier de traitement par lots sont incorrectes).

CHEMIN DE CONTEXTE :

```
root
```

SYNTAXE :

```
[start] batch
```

OPÉRATIONS :

`start` - Démarre le mode de traitement par lots d'eShell.

CHEMIN DE CONTEXTE :

`root`

EXEMPLES :

`start batch` - Démarre le mode de traitement par lots d'eShell.

GUIDE

Affiche l'écran de première exécution.

CHEMIN DE CONTEXTE :

`root`

PASSWORD

Normalement, lorsque vous exécutez des commandes protégées par mot de passe, vous êtes invité à taper un mot de passe pour des raisons de sécurité. Il concerne les commandes qui désactivent la protection antivirus et qui peuvent avoir une incidence sur le fonctionnement du produit ESET Mail Security. Vous êtes invité à saisir un mot de passe chaque fois que vous exécutez une commande de ce type. Afin d'éviter d'avoir à saisir un mot de passe à chaque fois, vous pouvez définir ce mot de passe. Il sera mémorisé par eShell et utilisé automatiquement à chaque exécution d'une commande protégée par un mot de passe. De cette manière, vous n'aurez plus à le saisir à chaque fois.

REMARQUE : le mot de passe défini ne fonctionne que pour la session interactive eShell en cours. Lorsque vous quittez eShell, ce mot de passe défini est supprimé. Lorsque vous redémarrez eShell, le mot de passe doit être redéfini.

Ce mot de passe défini est également très utile lorsque vous exécutez des fichiers/scripts de traitement par lots. Voici un exemple de fichier de traitement par lots :

```
eshell start batch "&" set password plain <votremotdepasse> "&" set status disabled
```

La commande concaténée ci-dessus démarre un mode de traitement par lots, définit le mot de passe qui sera utilisé et désactive la protection.

CHEMIN DE CONTEXTE :

`root`

SYNTAXE :

`[get] | restore password`

`set password [plain <motdepasse>]`

OPÉRATIONS :

`get` - Affiche le mot de passe

`set` - Définit ou efface le mot de passe

`restore` - Efface le mot de passe

ARGUMENTS :

`plain` - Permet d'entrer le mot de passe en tant que paramètre

`password` - Mot de passe

EXEMPLES :

`set password plain <votremotdepasse>` - Définit un mot de passe qui sera utilisé pour les commandes protégées par mot de passe.

`restore password` - Efface le mot de passe.

EXEMPLES :

`get password` - Utilisez cette commande pour définir si le mot de passe est configuré (le mot de passe n'apparaît pas clairement ; il est remplacé par une série d'astérisques *). Si vous ne voyez aucun astérisque, cela signifie qu'aucun mot de passe n'est défini.

`set password plain <votremotdepasse>` - Utilisez cette commande pour configurer le mot de passe défini

`restore password` - Cette commande efface le mot de passe défini.

STATUS

Affiche des informations sur l'état en cours de la protection ESET Mail Security (identique à l'interface utilisateur graphique).

CHEMIN DE CONTEXTE :

`root`

SYNTAXE :

`[get] | restore status`

`set status disabled | enabled`

OPÉRATIONS :

`get` - Affiche l'état de la protection antivirus.

`set` - Désactive/Active la protection antivirus.

`restore` - Restaure les paramètres par défaut

ARGUMENTS :

`disabled` - Désactive la protection antivirus

`enabled` - Active la protection antivirus

EXEMPLES :

`get status` - Affiche l'état de la protection en cours

`set status disabled` - Désactive la protection

`restore status` - Restaure la protection sur le paramètre par défaut (activée)

VIRLOG

Cette commande est un alias de la commande `DETECTIONS` . Elle est utile lorsque vous devez afficher des informations sur les infiltrations détectées.

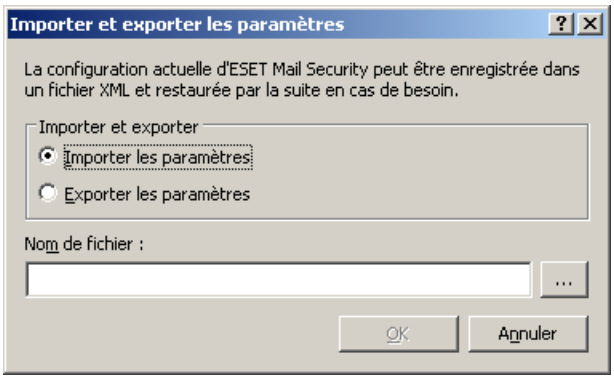
WARNLOG

Cette commande est un alias de la commande `EVENTS` . Elle est utile lorsque vous devez afficher des informations sur différents événements.

4.10 Importer et exporter les paramètres

Les configurations d'importation et d'exportation de ESET Mail Security sont accessibles dans **Configuration** en cliquant sur **Importer** et **exporter les paramètres**.

L'importation et l'exportation utilisent le type de fichier .xml. Ces opérations sont utiles si vous devez sauvegarder la configuration actuelle d'ESET Mail Security pour l'utiliser ultérieurement. L'option Exporter les paramètres est également pratique pour les utilisateurs qui souhaitent utiliser leur configuration ESET Mail Security préférée sur plusieurs systèmes. Il leur suffit d'importer un fichier .xml pour transférer les paramètres souhaités.



4.11 ThreatSense.Net

Le système d'alerte anticipé ThreatSense.Net est un outil qui permet d'informer ESET immédiatement et en permanence de l'existence de nouvelles infiltrations. Le système d'alerte anticipé bidirectionnel ThreatSense.Net n'a qu'un seul objectif : améliorer la protection que nous vous offrons. Le meilleur moyen d'être sûr de détecter les nouvelles menaces dès qu'elles apparaissent est de rester en contact permanent avec le plus grand nombre de nos clients et de les utiliser comme des éclaireurs. Deux options sont possibles :

1. Vous pouvez décider de ne pas activer le système d'alerte anticipé ThreatSense.Net. Vous ne perdez rien de la fonctionnalité du logiciel et vous bénéficiez toujours la meilleure protection que nous offrons.

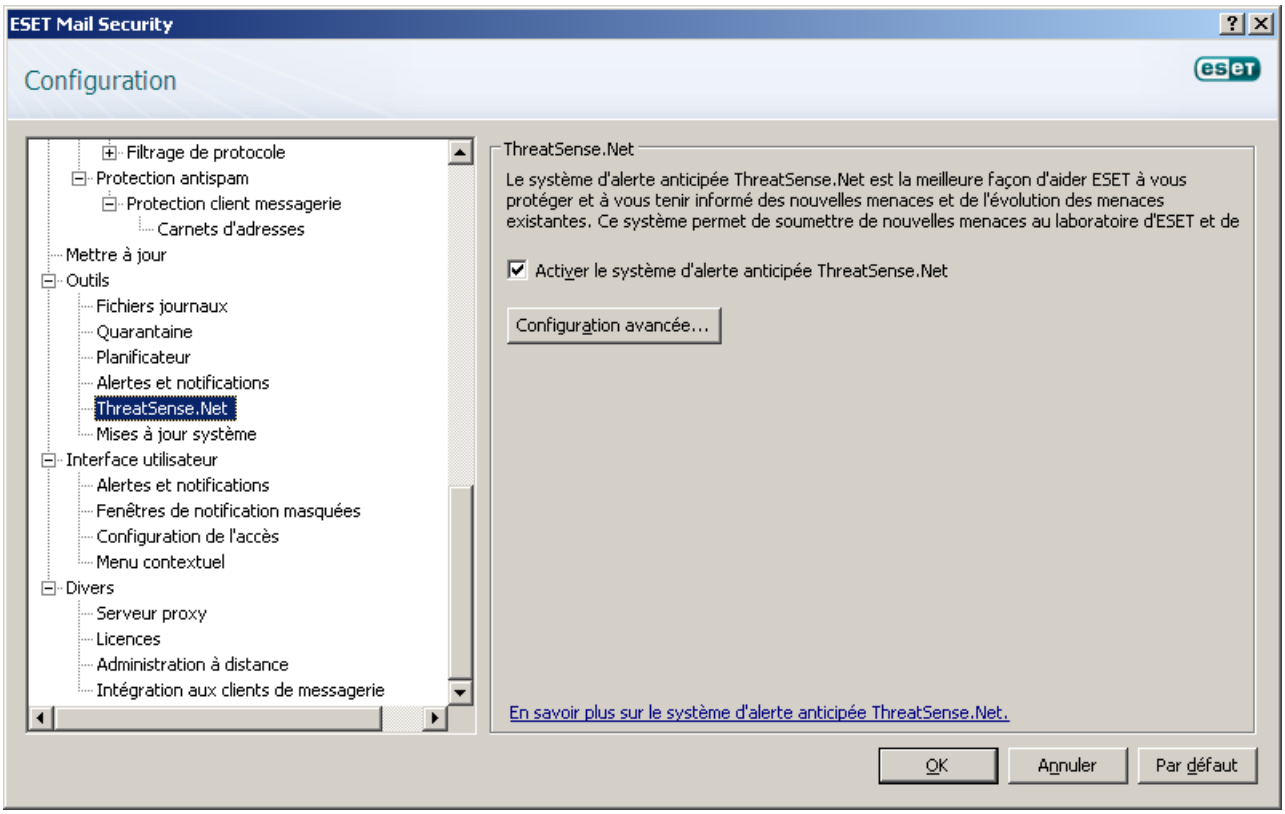
2. Vous pouvez configurer le système d'alerte anticipé ThreatSense.Net afin d'envoyer des informations anonymes qui concernent les nouvelles menaces et indiquent l'endroit où se trouve le code menaçant. Ce fichier peut être envoyé à ESET pour une analyse détaillée. En étudiant ces menaces, ESET améliore ses capacités à détecter les menaces.

Le système d'alerte anticipé ThreatSense.Net collecte sur votre ordinateur des informations concernant les nouvelles menaces détectées. Ces informations comprennent un échantillon ou une copie du fichier dans lequel la menace est apparue, le chemin et le nom du fichier, la date et l'heure, le processus par lequel la menace est apparue sur votre ordinateur et des informations sur le système d'exploitation de votre ordinateur.

Certaines informations vous concernant ou concernant votre ordinateur (noms d'utilisateur dans un chemin de répertoire) sont divulguées au laboratoire de recherche sur les menaces d'ESET, mais ces informations ne sont utilisées à AUCUNE autre fin que pour répondre immédiatement aux nouvelles menaces.

Par défaut, ESET Mail Security est configuré pour demander confirmation avant de soumettre au laboratoire d'ESET les fichiers suspects pour une analyse détaillée. Les fichiers ayant une certaine extension (.doc ou .xls par exemple) sont toujours exclus. Vous pouvez également ajouter d'autres extensions si vous ou votre entreprise souhaitez éviter d'envoyer certains fichiers.

La configuration de ThreatSense.Net est accessible depuis la fenêtre Configuration avancée, dans **Outils** > **ThreatSense.Net**. Sélectionnez l'option **Activer le système d'alerte anticipé ThreatSense** pour activer le système, puis cliquez sur le bouton **Configuration avancée...**.

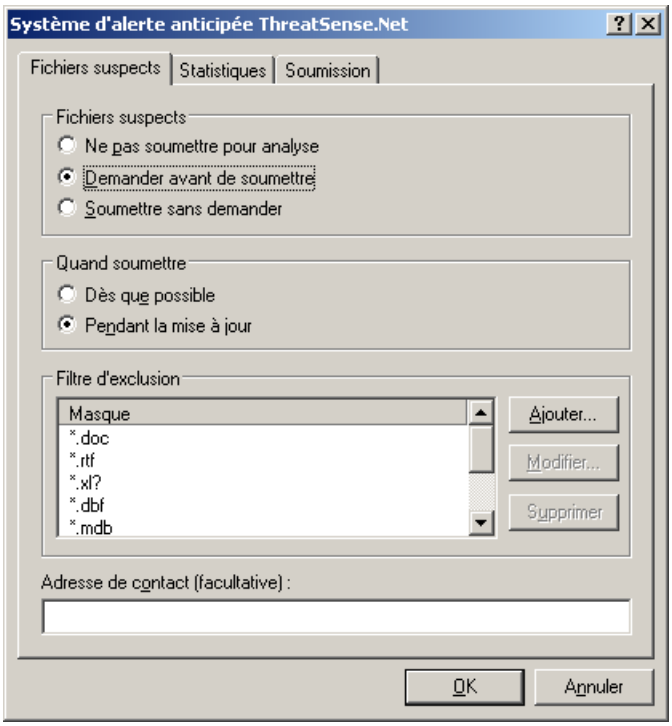


4.11.1 Fichiers suspects

L'onglet **Fichiers suspects** permet de configurer la manière dont les menaces sont soumises pour analyse au laboratoire de recherche sur les menaces d'ESET.

Si vous trouvez un fichier suspect, vous pouvez le soumettre à notre laboratoire de recherche sur les menaces pour analyse. S'il s'agit d'une application malveillante, sa détection est ajoutée à la prochaine mise à jour de la base des signatures de virus.

La soumission des fichiers peut être définie pour avoir lieu automatiquement. Vous pouvez également sélectionner l'option **Demander avant de soumettre** si vous souhaitez connaître les fichiers qui sont envoyés pour analyse et confirmer l'envoi.



Si vous ne souhaitez pas soumettre de fichiers, sélectionnez l'option **Ne pas soumettre pour analyse**. Le fait de choisir de ne pas soumettre les fichiers pour analyse n'a pas d'incidence sur la soumission des informations statistiques qui est configurée indépendamment (reportez-vous à la section Statistiques 133).

Quand soumettre : par défaut, l'option **Dès que possible** est sélectionnée pour que les fichiers suspects soient envoyés au laboratoire de recherche sur les menaces d'ESET. Ceci est recommandé lorsqu'une connexion Internet permanente est disponible et que les fichiers suspects peuvent être livrés très rapidement. Sélectionnez l'option **Pendant la mise à jour** pour que les fichiers suspects soient téléchargés vers ThreatSense.Net pendant la mise à jour suivante.

Filtre d'exclusion : cette option permet d'exclure certains fichiers/dossiers de la soumission. Par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, tels que des documents ou des feuilles de calcul. Les fichiers les plus ordinaires sont exclus par défaut (.doc, etc.). Vous pouvez ajouter des fichiers à la liste des fichiers exclus si vous le souhaitez.

Adresse de contact : votre **adresse de contact [facultative]** peut être envoyée avec les fichiers suspects et peut être utilisée pour vous contacter si des informations complémentaires sont nécessaires pour l'analyse. Notez que vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires s'avèrent nécessaires.

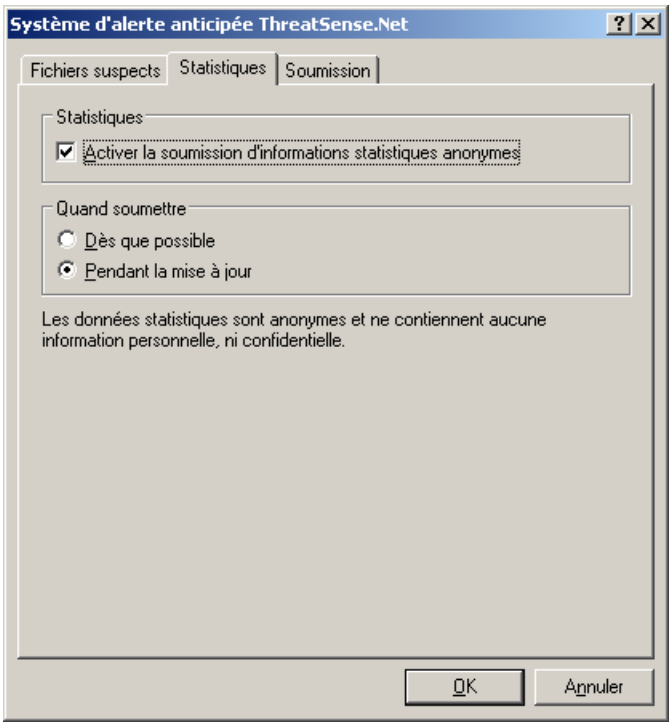
4.11.2 Statistiques

Le système d'alerte anticipé ThreatSense.Net collecte sur votre ordinateur des informations anonymes concernant les nouvelles menaces détectées. Ces informations peuvent inclure le nom de l'infiltration, la date et l'heure de détection, la version du produit de sécurité ESET, ainsi que des informations sur la version du système d'exploitation de votre ordinateur et ses paramètres régionaux. Les statistiques sont normalement fournies aux serveurs ESET une ou deux fois par jour.

Voici un exemple d'informations statistiques envoyées :

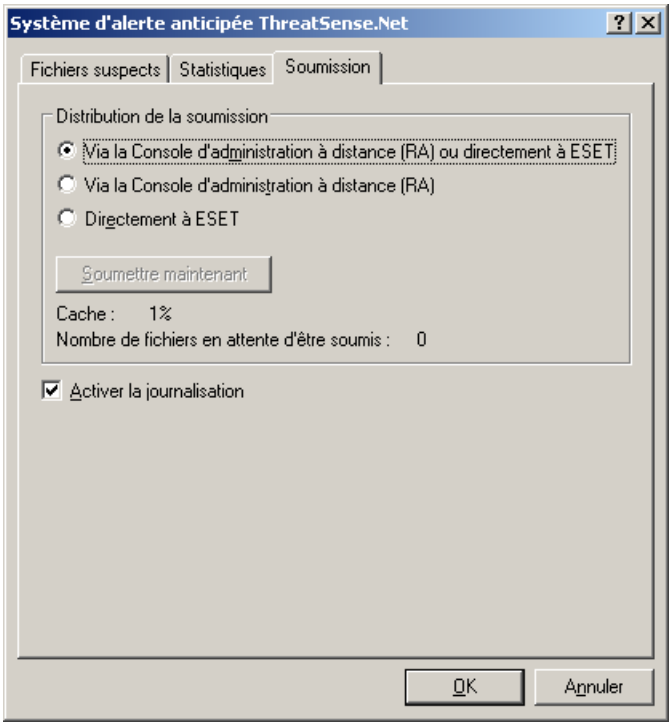
```
# utc_time=2005-04-14 07:21:28
# country="Slovaquie"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8NS7\rdgFR1
```

Quand soumettre : vous pouvez définir le moment de l'envoi des informations statistiques. Si vous choisissez d'envoyer les informations statistiques **Dès que possible**, elles sont envoyées immédiatement après leur création. Ce choix convient si une connexion Internet est disponible en permanence. Si l'option **Pendant la mise à jour** est sélectionnée, toutes les informations statistiques sont envoyées collectivement pendant la mise à jour suivante.



4.11.3 Soumission

Vous pouvez sélectionner le mode d'envoi des fichiers et des informations statistiques à ESET. Sélectionnez l'option **Via la Console d'administration à distance (RA) ou directement à ESET** pour que les fichiers et les statistiques soient envoyés par tout moyen disponible. Sélectionnez l'option **Via la Console d'administration à distance (RA)** pour envoyer les fichiers et les statistiques au serveur d'administration à distance qui les envoie ensuite au laboratoire de recherche sur les menaces d'ESET. Si l'option **Directement à ESET** est sélectionnée, tous les fichiers suspects et les informations statistiques seront livrés directement par le programme au laboratoire d'ESET.



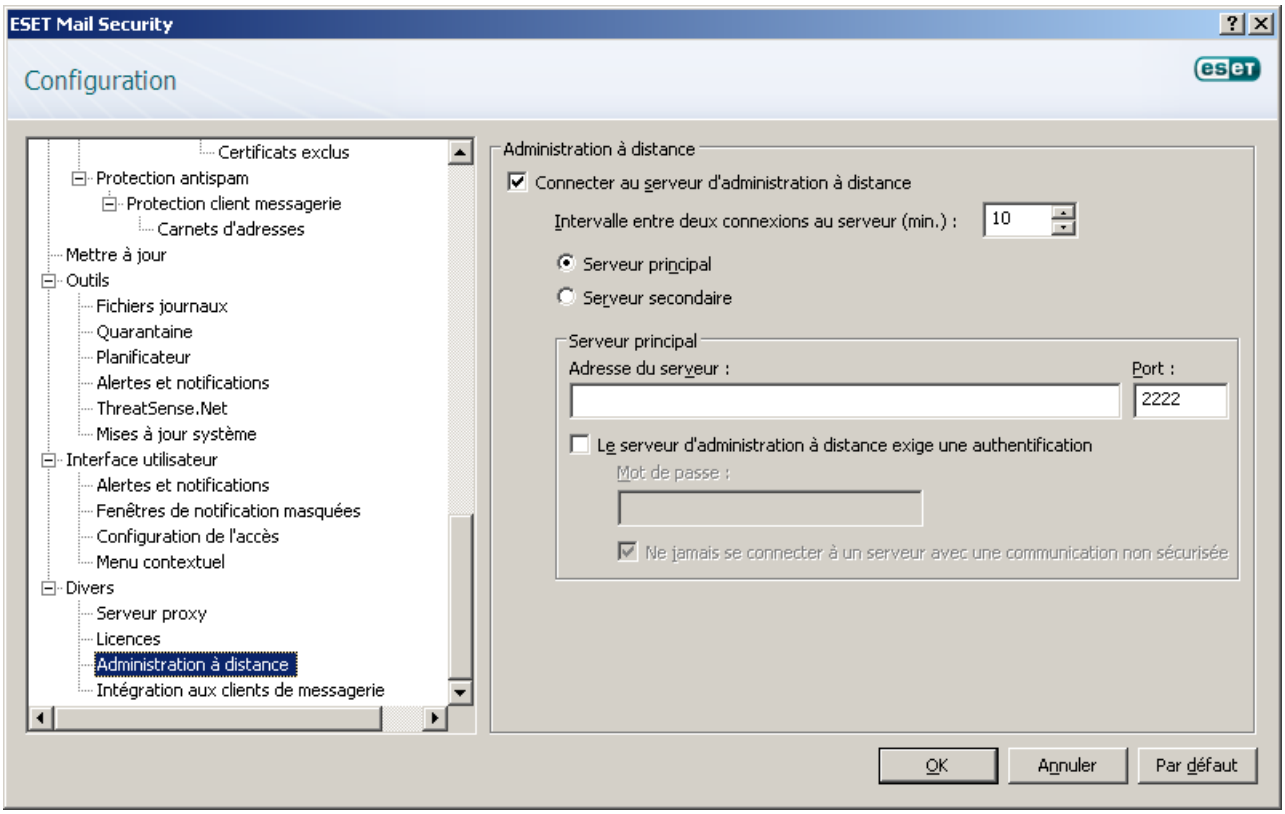
Si des fichiers sont en attente de soumission, le bouton **Soumettre maintenant** est activé. Cliquez sur ce bouton pour soumettre immédiatement les fichiers et les informations statistiques.

Activez l'option **Activer la journalisation** pour créer un journal permettant d'enregistrer les soumissions des fichiers et des informations statistiques.

4.12 Administration à distance

ESET Remote Administrator est un outil puissant permettant de gérer la stratégie de sécurité et qui offre une vision globale de la sécurité du réseau. Cet outil est particulièrement utile pour les grands réseaux. ESET Remote Administrator non seulement augmente le niveau de sécurité, mais permet également de gérer ESET Mail Security très facilement sur les postes de travail client.

Les options de configuration de l'administration à distance sont accessibles à partir de la fenêtre principale d'ESET Mail Security. Cliquez sur **Configuration** > **Accéder à la configuration avancée complète...** > **Divers** > **Administration à distance**.



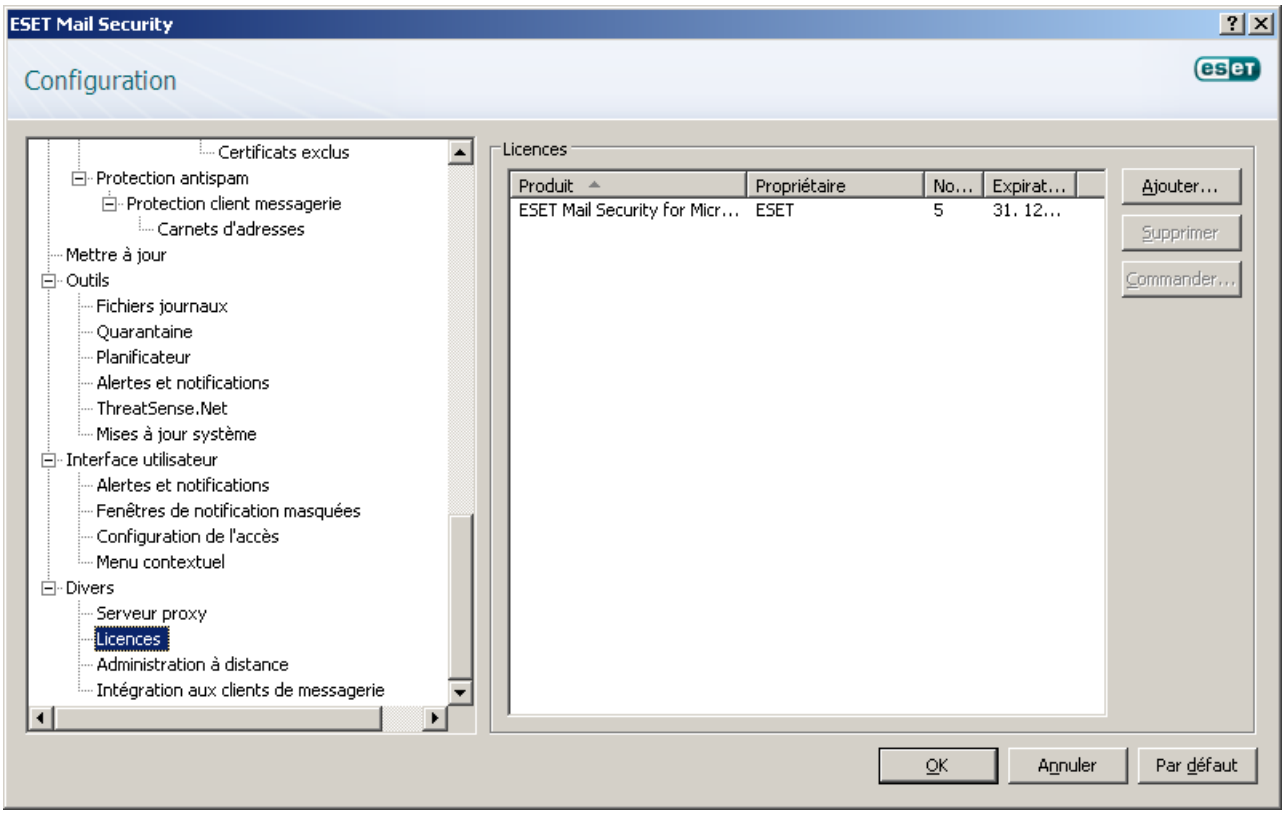
Activez l'administration à distance en sélectionnant l'option **Connecter au serveur d'administration à distance**. D'autres options sont également disponibles :

- **Intervalle entre deux connexions au serveur (min.) :** cette option indique la fréquence à laquelle ESET Mail Security se connecte à ESET Remote Administrator Server. Si la valeur est 0, les informations sont envoyées toutes les 5 secondes.
- **Adresse du serveur :** c'est l'adresse du serveur réseau où le serveur d'administration à distance est installé.
- **Port :** ce champ contient le port du serveur prédéfini utilisé pour la connexion. Il est recommandé de laisser le paramètre de port prédéfini sur 2222
- **Le serveur d'administration à distance exige une authentification :** Le serveur d'administration à distance exige une authentification.

Cliquez sur **OK** pour confirmer les modifications et appliquer les paramètres qu'utilise ESET Mail Security pour se connecter à ESET Remote Administrator Server.

4.13 Licences

La branche **Licences** vous permet de gérer les clés de licence d'ESET Mail Security et d'autres produits ESET tels que ESET Mail Security, etc. Après l'achat, les clés de licence sont fournies en même temps que le nom d'utilisateur et le mot de passe. Pour **ajouter/supprimer** une clé de licence, cliquez sur le bouton correspondant dans la fenêtre du gestionnaire de licences. Le gestionnaire de licences est accessible à partir de Configuration avancée complète sous **Divers** > **Licences**.



Une clé de licence est un fichier texte contenant des informations concernant le produit acheté : son propriétaire, le nombre de licences et la date d'expiration.

La fenêtre du gestionnaire de licences permet à l'utilisateur de charger et de voir le contenu de la clé de licence à l'aide du bouton **Ajouter...** ; les informations contenues sont affichées dans la fenêtre du gestionnaire. Pour supprimer des clés de licence de la liste, cliquez sur **Supprimer**.

Si une clé de licence est expirée et que vous êtes intéressé par le renouvellement de l'achat, cliquez sur le bouton **Commander...** : vous serez dirigé vers le site Web de la boutique en ligne.

5. Glossaire

5.1 Types d'infiltrations

Une infiltration est un élément de logiciel malveillant qui tente de s'introduire dans l'ordinateur d'un utilisateur et/ou de l'endommager.

5.1.1 Virus

Un virus est une infiltration qui endommage les fichiers existants de votre ordinateur. Les virus informatiques sont comparables aux virus biologiques parce qu'ils utilisent des techniques similaires pour se propager d'un ordinateur à l'autre.

Les virus informatiques attaquent principalement les fichiers et documents exécutables. Pour proliférer, un virus attache son « corps » à la fin d'un fichier cible. En bref, un virus informatique fonctionne de la manière suivante : après l'exécution du fichier infecté, le virus s'active lui-même (avant l'application originale) et exécute sa tâche prédéfinie. C'est après seulement que l'application originale peut s'exécuter. Un virus ne peut pas infecter un ordinateur à moins qu'un utilisateur n'exécute ou n'ouvre lui-même (accidentellement ou délibérément) le programme malveillant.

Les virus peuvent varier en fonction de leur gravité et de leur cible. Certains sont extrêmement dangereux parce qu'ils ont la capacité de supprimer délibérément des fichiers du disque dur. D'autres, en revanche, ne causent pas de réels dommages : ils ne servent qu'à gêner l'utilisateur et à démontrer les compétences techniques de leurs auteurs.

Il est important de noter que, contrairement aux chevaux de Troie et aux logiciels espions, les virus sont de plus en plus rares, car d'un point de vue commercial, ils ne sont pas très attrayants pour les auteurs de programmes malveillants. En outre, le terme « virus » est souvent utilisé mal à propos pour couvrir tout type d'infiltrations. On tend à le remplacer progressivement par le terme « logiciel malveillant » ou « malware » en anglais.

Si votre ordinateur est infecté par un virus, il est nécessaire de restaurer les fichiers infectés à leur état original, c'est-à-dire de les nettoyer à l'aide d'un programme antivirus.

Dans la catégorie des virus, on peut citer : OneHalf, Tenga et Yankee Doodle.

5.1.2 Vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. La différence fondamentale entre les virus et les vers réside dans le fait que les vers ont la capacité de se répliquer et de voyager par eux-mêmes. Ils ne dépendent pas des fichiers hôtes (ou des secteurs d'amorçage). Les vers se propagent par l'intermédiaire d'adresses de messagerie de votre liste de contacts ou exploitent les vulnérabilités de sécurité des applications réseau.

Les vers sont ainsi susceptibles de vivre beaucoup plus longtemps que les virus. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois en quelques minutes. Leur capacité à se répliquer indépendamment et rapidement les rend plus dangereux que les autres types de programmes malveillants.

Un ver activé dans un système peut être à l'origine de plusieurs dérèglements : il peut supprimer des fichiers, dégrader les performances du système ou même désactiver certains programmes. Par nature, il peut servir de « moyen de transport » à d'autres types d'infiltrations.

Si votre ordinateur est infecté par un ver, il est recommandé de supprimer les fichiers infectés, car ils contiennent probablement du code malveillant.

Parmi les vers les plus connus, on peut citer : Lovsan/Blaster, Stration/Warezov, Bagle et Netsky.

5.1.3 Chevaux de Troie

Dans le passé, les chevaux de Troie étaient définis comme une catégorie d'infiltrations dont la particularité est de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptent de les exécuter. Il est cependant important de remarquer que cette définition s'applique aux anciens chevaux de Troie. Aujourd'hui, il ne leur est plus utile de se déguiser. Leur unique objectif est de trouver la manière la plus facile de s'infiltrer pour accomplir leurs desseins malveillants. Le terme « cheval de Troie » est donc devenu un terme très général qui décrit toute infiltration qui n'entre pas dans une catégorie spécifique.

La catégorie étant très vaste, elle est souvent divisée en plusieurs sous-catégories :

- **Téléchargeur** : programme malveillant qui est en mesure de télécharger d'autres infiltrations sur Internet.
- **Dropper** : type de cheval de Troie conçu pour déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- **Backdoor** : application qui communique à distance avec les pirates et leur permet d'accéder à un système et d'en prendre le contrôle.
- **Keylogger** (keystroke logger) : programme qui enregistre chaque touche sur laquelle tape l'utilisateur avant d'envoyer les informations aux pirates.
- **Composeur** : programme destiné à se connecter à des numéros surtaxés. Il est presque impossible qu'un utilisateur remarque la création d'une nouvelle connexion. Les composeurs ne peuvent porter préjudice qu'aux utilisateurs ayant des modems par ligne commutée, qui sont de moins en moins utilisés.

Les chevaux de Troie prennent généralement la forme de fichiers exécutables avec l'extension .exe. Si un fichier est identifié comme cheval de Troie sur votre ordinateur, il est recommandé de le supprimer, car il contient sans doute du code malveillant.

Parmi les chevaux de Troie les plus connus, on peut citer : NetBus, Trojandownloader. Small.ZL, Slapper

5.1.4 Rootkits

Les rootkits sont des programmes malveillants qui procurent aux pirates un accès illimité à un système tout en dissimulant leur présence. Après avoir accédé au système (généralement en exploitant une faille), les rootkits utilisent des fonctions du système d'exploitation pour se protéger des logiciels antivirus : ils dissimulent des processus, des fichiers et des données de la base de registre Windows. Pour cette raison, il est presque impossible de les détecter à l'aide des techniques de test ordinaires.

Il existe deux niveaux de détection permettant d'éviter les rootkits :

1) Lorsqu'ils essaient d'accéder au système. Ils ne sont pas encore installés et donc inactifs. La plupart des antivirus sont en mesure d'éliminer les rootkits à ce niveau (en supposant qu'ils détectent effectivement les fichiers comme infectés).
2) Lorsqu'ils sont inaccessibles aux tests habituels. Les utilisateurs ESET Mail Security bénéficient de la technologie Anti-Stealth qui permet de détecter et d'éliminer les rootkits en activité.

5.1.5 Logiciels publicitaires

Le terme anglais « adware » désigne les logiciels soutenus par la publicité. Les programmes qui affichent des publicités entrent donc dans cette catégorie. Les logiciels publicitaires ouvrent généralement une nouvelle fenêtre contextuelle automatiquement dans un navigateur Internet. Cette fenêtre contient de la publicité ou modifie la page de démarrage du navigateur. Ils sont généralement associés à des programmes gratuits et permettent aux développeurs de couvrir les frais de développement de leurs applications (souvent utiles).

Les logiciels publicitaires en tant que tels ne sont pas dangereux ; ils dérangent simplement les utilisateurs en affichant des publicités. Le danger réside dans le fait qu'ils peuvent également avoir des fonctions d'espionnage (comme les logiciels espions).

Si vous décidez d'utiliser un logiciel gratuit, soyez particulièrement attentif au programme d'installation. La plupart des programmes d'installation vous avertissent en effet qu'ils installent également un programme publicitaire. Dans la plupart des cas, vous pourrez désactiver cette installation supplémentaire et installer le programme sans logiciel publicitaire.

Certains programmes refusent de s'installer sans leur logiciel publicitaire ou voient leurs fonctionnalités limitées. Cela signifie que les logiciels publicitaires accèdent souvent au système de manière « légale », dans la mesure où les utilisateurs l'ont accepté. Dans ce cas, il est préférable de procéder avec prudence. Si un logiciel publicitaire est détecté sur votre ordinateur, il est conseillé de le supprimer, car il est fort probable qu'il contienne du code malveillant.

5.1.6 Logiciels espions

Cette catégorie englobe toutes les applications qui envoient des informations confidentielles sans le consentement des utilisateurs et à leur insu. Les logiciels espions utilisent des fonctions de traçage pour envoyer diverses données statistiques telles que la liste des sites Web visités, les adresses e-mail de la liste de contacts de l'utilisateur ou la liste des touches du clavier utilisées.

Les auteurs de ces logiciels espions affirment que ces techniques ont pour but d'en savoir plus sur les besoins et intérêts des utilisateurs afin de mieux cibler les offres publicitaires. Le problème est qu'il n'y a pas de distinction claire entre les applications utiles et les applications malveillantes, et que personne ne peut garantir que les informations récupérées ne sont pas utilisées à des fins frauduleuses. Les données récupérées par les logiciels espions peuvent être des codes de sécurité, des codes secrets, des numéros de compte bancaire, etc. Les logiciels espions sont souvent intégrés aux versions gratuites d'un programme dans le but de générer des gains ou d'inciter à l'achat du logiciel. Les utilisateurs sont souvent informés de la présence d'un logiciel espion au cours de l'installation d'un programme qui vise à les inciter à acquérir la version payante qui en est dépourvue.

Parmi les produits logiciels gratuits bien connus qui contiennent des logiciels espions, on trouve les applications clients de réseaux P2P (poste à poste). Spyfalcon ou Spy Sheriff (et beaucoup d'autres) appartiennent à une sous-catégorie spécifique de logiciels espions : ils semblent être des programmes antispyware alors qu'ils sont en réalité eux-mêmes des logiciels espions.

Si un fichier est détecté comme logiciel espion sur votre ordinateur, il est préférable de le supprimer, car il est fort probable qu'il contienne du code malveillant.

5.1.7 Applications potentiellement dangereuses

Il existe de nombreux programmes authentiques qui permettent de simplifier l'administration des ordinateurs en réseau. Toutefois, s'ils tombent entre de mauvaises mains, ces programmes sont susceptibles d'être utilisés à des fins malveillantes. ESET Mail Security permet de détecter ces menaces.

Les applications potentiellement dangereuses rentrent dans une classification utilisée pour les logiciels commerciaux légitimes. Cette classification comprend les programmes d'accès à distance, les applications de résolution de mot de passe ou les keyloggers 138 (programmes qui enregistrent chaque frappe au clavier de l'utilisateur).

Si vous découvrez qu'une application potentiellement dangereuse est présente et fonctionne sur votre ordinateur (sans que vous l'ayez installée), consultez l'administrateur réseau ou supprimez l'application.

5.1.8 Applications potentiellement indésirables

Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. Ces applications sont habituellement installées après consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Voici les changements les plus significatifs :

- affichage de nouvelles fenêtres ;
- activation et exécution de processus cachés ;
- utilisation plus importante des ressources système ;
- modification des résultats de recherche ;
- communication de l'application avec des serveurs distants.

5.2 Courrier électronique

Le courrier électronique est une forme de communication moderne qui offre beaucoup d'avantages. Adaptable, rapide et direct, il a joué un rôle crucial dans l'expansion d'Internet au début des années 90.

Malheureusement, le grand anonymat des courriers électroniques et Internet a laissé libre champ aux activités illégales telles que le « spamming » (le fait d'envoyer des messages indésirables à un grand nombre de personnes). Les courriers indésirables comprennent les publicités indésirables, les canulars et les logiciels malveillants. Les désagréments et le danger augmentent, car l'envoi de tels messages ne coûte rien et les auteurs de courrier indésirable disposent de nombreux outils qui leur permettent de se procurer facilement de nouvelles adresses de messagerie. Par ailleurs, le volume et la variété du courrier indésirable ne facilitent pas la réglementation. Plus vous utilisez votre adresse de messagerie, plus vous augmentez la possibilité de tomber dans un moteur de base de données de courrier indésirable. Voici quelques conseils de prévention :

- Évitez de publier votre adresse de messagerie sur Internet.
- Ne donnez votre adresse de messagerie qu'à des personnes fiables.
- Évitez d'utiliser des pseudonymes communs : un pseudonyme compliqué est moins susceptible d'être traqué.
- Ne répondez pas au courrier indésirable qui est arrivé dans votre boîte de réception.
- Faites attention lorsque vous remplissez des formulaires sur Internet : soyez particulièrement attentif aux options du type « Oui, je voudrais recevoir des informations concernant … ».
- Utilisez des adresses de messagerie « spécialisées », par exemple une adresse pour votre travail, une autre pour communiquer avec vos amis, etc.
- Changez vos adresses de messagerie de temps en temps.
- Utilisez une solution antispam.

5.2.1 Publicités

La publicité via Internet est une des formes de publicité les plus en vogue. D'un point de vue marketing, la publicité présente plusieurs avantages : ses coûts sont minimes, elle est très directe et les messages sont transmis presque immédiatement. De nombreuses entreprises utilisent des outils de marketing par courrier électronique pour communiquer de manière efficace avec leurs clients et prospects.

Ce mode de publicité est légitime, car vous pourriez être intéressé par la réception d'informations commerciales sur certains produits. Toutefois, de nombreuses entreprises envoient des masses de messages commerciaux non sollicités. La publicité par e-mail dépasse alors les limites et devient du courrier indésirable, ou spam.

La quantité de messages publicitaires non sollicités est devenue un réel problème, car elle ne montre aucun signe de ralentissement. Les auteurs de messages non sollicités tentent souvent de déguiser le courrier indésirable sous des dehors de messages légitimes.

5.2.2 Canulars

Un canular (ou hoax) est message propagé sur Internet. Il est envoyé généralement avec le courrier et parfois par des outils de communication tels que ICQ et Skype. Le message est souvent une blague ou une légende urbaine.

Les canulars essaient de provoquer chez les destinataires de la peur, de l'incertitude et du doute, les amenant à croire qu'un « virus indétectable » supprime tous les fichiers et récupère les mots de passe, ou effectue une activité nuisible sur leur système.

Certains canulars demandent aux destinataires de transmettre des messages à leurs contacts, ce qui a pour conséquence de propager les canulars. Même les téléphones portables reçoivent des canulars et des demandes d'aide (des personnes proposant par exemple de vous envoyer de l'argent depuis l'étranger). Il est souvent impossible de déterminer l'intention du créateur.

Si un message vous demande de le faire suivre à toutes vos connaissances, il peut très bien s'agir d'un canular. Sur Internet, de nombreux sites spécialisés peuvent vérifier la légitimité d'un courrier. Avant de retransmettre un message que vous soupçonnez d'être un canular, faites d'abord une recherche sur Internet à son sujet.

5.2.3 Hameçonnage

Le terme d'hameçonnage (phishing en anglais) désigne une activité frauduleuse utilisant des techniques de piratage psychologique qui consistent à manipuler les utilisateurs pour obtenir des informations confidentielles. Son but est d'accéder à des données sensibles, telles que numéros de comptes bancaires, codes secrets, etc.

La technique consiste généralement à envoyer un message électronique en se faisant passer pour une personne ou une entreprise digne de confiance (institution financière, compagnie d'assurance par exemple). Le message peut sembler tout à fait authentique et contenir des graphiques et contenus qui proviennent véritablement de la source dont il se réclame. Vous êtes invité à entrer, sous divers prétextes (vérification de données, opérations financières), certaines de vos données personnelles : numéros de compte en banque ou noms d'utilisateur et mots de passe. Toutes ces données, si elles sont soumises, peuvent facilement être volées et utilisées à des fins illégales.

Les banques, compagnies d'assurance et autres sociétés légales ne demandent jamais de noms d'utilisateur et de mots de passe dans un message non sollicité.

5.2.4 Reconnaissance du courrier indésirable

Généralement, peu d'indicateurs contribuent à identifier le courrier indésirable (messages non sollicités) dans une boîte à lettres. Si un message remplit au moins l'un des critères suivants, il s'agit probablement de courrier indésirable.

- L'adresse de l'expéditeur ne figure pas dans la liste de vos contacts.
- Le contenu du message concerne une grosse somme d'argent qui vous est offerte, mais vous devez fournir d'abord une petite somme.
- Vous devez entrer, sous divers prétextes (vérification de données, opérations financières), certaines de vos données personnelles : numéros de compte en banque ou noms d'utilisateur et mots de passe.
- Le message est écrit dans une langue étrangère.
- Le message vous propose d'acheter un produit qui ne vous intéresse pas. Si vous décidez d'acheter quand même, vérifiez que l'expéditeur du message est un vendeur sérieux (consultez le fabricant original du produit).
- Quelques mots sont mal écrits pour pouvoir passer à travers le filtre de courrier indésirable. Par exemple, « vaigra » au lieu de « viagra », etc.

5.2.4.1 Règles

Dans le contexte des solutions de protection antispam et des clients de messagerie, les règles sont des outils permettant de manipuler les fonctions de messagerie. Elles se composent de deux parties logiques :

1) La condition (par exemple, un message entrant provenant d'une certaine adresse)

2) L'action (par exemple, la suppression du message ou son déplacement vers un dossier spécifique).

Le nombre de règles et leurs combinaisons varient en fonction de la solution de protection antispam. Ces règles servent de protection antispam (messages non sollicités). Exemples caractéristiques :

- Condition : un message entrant contient des mots habituellement utilisés dans le courrier indésirable. 2. Action : supprimer le message
- Condition : un message entrant contient une pièce jointe comportant l'extension .exe 2. Action : supprimer la pièce jointe et livrer le message dans la boîte aux lettres
- Condition : un message entrant arrive de votre employeur 2. Action : déplacer le message dans le dossier Travail.

Nous vous recommandons d'utiliser une combinaison de règles des programmes de programme antispam afin de faciliter l'administration et d'améliorer le filtrage du courrier indésirable.

5.2.4.2 Filtre bayésien

Le filtrage bayésien est une méthode très efficace de filtrage des messages, utilisée par la plupart des produits de protection antispam. Il permet d'identifier les messages non sollicités avec grande précision et peut s'adapter à chaque utilisateur.

Le principe est le suivant : la première phase est une phase d'apprentissage. L'utilisateur doit désigner un nombre suffisant de messages entrants comme étant des messages légitimes ou du courrier indésirable (normalement 200/200). Le filtre analyse les deux catégories et apprend par exemple que le courrier indésirable contient généralement des mots tels que « rolex » ou « viagra », tandis que les messages légitimes sont envoyés par des parents ou à partir d'adresses figurant dans la liste des contacts de l'utilisateur. Si le nombre de messages traités est suffisant, le filtre bayésien peut affecter un certain « indice de spam » à chaque message et déterminer s'il est ou non un courrier indésirable.

Le principal avantage du filtre bayésien est sa souplesse. Par exemple, si un utilisateur est biologiste, tous les messages entrants concernant la biologie ou des champs d'études apparentés recevront généralement un indice de probabilité moindre. Si un message envoyé par un membre de la liste des contacts de l'utilisateur comprend des mots qui le classeraient normalement dans la catégorie des messages non sollicités, il est marqué comme légitime dans la mesure où les expéditeurs d'une liste de contacts réduisent la probabilité qu'il s'agisse d'un courrier indésirable.

5.2.4.3 Liste blanche

En général, une liste blanche est une liste de personnes ou d'éléments qui ont été acceptés ou ont obtenu une autorisation d'accès. Le terme « liste blanche de messagerie » définit la liste de contacts dont l'utilisateur souhaite recevoir les messages. Ces listes blanches sont basées sur des mots-clés recherchés dans une adresse électronique, des noms de domaines ou des adresses IP.

Si une liste blanche fonctionne en « mode exclusif », les messages de toutes les autres adresses, domaines ou adresses IP sont écartés. Si elle fonctionne en mode non exclusif, ces messages ne sont pas supprimés, mais filtrés d'une autre façon.

Une liste blanche fonctionne sur le principe opposé de la liste noire 142. Les listes blanches sont relativement faciles à maintenir, plus que les listes noires. Pour un meilleur filtrage du courrier indésirable, nous vous recommandons d'utiliser des listes blanches et des listes noires.

5.2.4.4 Liste noire

En général, une liste noire répertorie les personnes ou les éléments non acceptés ou interdits. Dans le monde virtuel, c'est une technique qui permet d'accepter des messages de tous les utilisateurs qui ne figurent pas sur cette liste.

Il existe deux types de listes noires : les listes créées par les utilisateurs dans l'application de protection antispam et les listes professionnelles mises à jour régulièrement. Ces dernières sont créées par des institutions spécialisées et sont disponibles sur Internet.

Il est essentiel d'utiliser les listes noires pour bloquer le courrier indésirable, mais elles sont très difficiles à tenir à jour, car de nouveaux éléments à bloquer apparaissent jour après jour. Nous recommandons d'utiliser à la fois une liste blanche 142 et une liste noire pour mieux filtrer le courrier indésirable.

5.2.4.5 Contrôle côté serveur

Le contrôle côté serveur est une technique permettant d'identifier le courrier indésirable de masse d'après le nombre de messages reçus et les réactions des utilisateurs. Chaque message laisse une empreinte numérique unique en fonction de son contenu. Le numéro d'identification unique ne donne aucune information sur le contenu du message. Deux messages identiques ont une empreinte identique, tandis que des messages différents ont une empreinte différente.

Si un message est marqué comme courrier indésirable, son empreinte est envoyée au serveur. Si le serveur reçoit plusieurs empreintes identiques (correspondant à un certain message de courrier indésirable), cette empreinte est stockée dans la base des empreintes de courrier indésirable. Lorsqu'il analyse des messages entrants, le programme envoie les empreintes de ces messages au serveur. Le serveur renvoie des informations indiquant les empreintes qui correspondent à des messages déjà identifiés comme courrier indésirable par d'autres utilisateurs.