AVG 8.5 Email Server Edition

Guide de l'utilisateur

Révision du document 85.4 (30.4.2009)

Sommaire

1. Introduction

Ce manuel utilisateur fournit une documentation complète sur **AVG 8.5 Email Server Edition**.

Nous vous remercions d'avoir choisi AVG 8.5 Email Server Edition.

AVG 8.5 Email Server Edition figure parmi les produits AVG primés et a été conçu pour assurer la sécurité de votre ordinateur et vous permettre de travailler en toute sérénité. Comme toute la gamme des produits AVG, **AVG 8.5 Email Server Edition** a été entièrement repensée, afin de livrer une protection AVG reconnue et certifiée sous une présentation nouvelle, plus conviviale et plus efficace.

AVG a été conçu et développé pour protéger vos activités en local et en réseau. Nous espérons que vous profiterez pleinement de la protection du programme AVG et qu'elle vous donnera entière satisfaction.

2. Pré-requis à l'installation d'AVG

2.1. Systèmes d'exploitation pris en charge

AVG 8.5 Email Server Edition est prévu pour protéger les serveurs de messagerie fonctionnant avec les systèmes d'exploitation suivants :

- Windows 2008 Edition Serveur (x86 et x64)
- Windows 2003 Server (x86, x64 et Itanium) SP1
- Windows 2000 Server SP4 + Correctif cumulatif 1

(et éventuellement les service packs de version ultérieure pour certains serveurs de messagerie)

2.2. Serveurs de messagerie pris en charge

Les serveurs de messagerie suivants sont pris en charge :

- ***Version MS Exchange 2000 Server (avec Service Pack 1 ou version supérieure)***

  Remarque : pour Exchange 2000 Server, il faut appliquer le Service Pack 1 (ou supérieur) avant d'utiliser le moteur AVG ; **AVG for MS Exchange 2000/2003 Server** recourt à l'interface VSAPI 2.0 (ou 2.5 pour Exchange 2003 Server) intégrée à ce Service Pack.

- ***Version MS Exchange 2003 Server***
- ***Version MS Exchange 2007 Server***
- ***AVG for Kerio MailServer*** –version 5.x/6.x et supérieure

2.3. Configuration matérielle minimum

Voici la configuration matérielle minimale pour **AVG 8.5 Email Server Edition** :

- Processeur Intel Pentium 1,2 GHz
- 250 Mo d'espace disque dur (pour l'installation)

- 256 Mo libres de RAM

2.4. Désinstallation des versions précédentes

Si une version plus ancienne du programme AVG Serveur de mail est installée, vous devrez la désinstaller manuellement avant de procéder à l'installation d'**AVG 8.5 Email Server Edition**. Pour la désinstallation manuelle de la version précédente, servez-vous de la fonctionnalité standard proposée par Windows.

- Dans le menu Démarrer ***Démarrer/Paramètres/Panneau de configuration/ Ajout/Suppression de programmes***, sélectionnez le programme dans la liste des logiciels installés. Prenez garde à sélectionner le programme AVG qui convient. Vous devez désinstaller AVG Edition Serveur de mail avant de désinstaller AVG Edition Serveur de Fichiers.

- Après la désinstallation de l'édition Serveur de Mail, procédez à la désinstallation de la version précédente d'AVG Edition Serveur de Fichiers. Pour cela, cliquez sur le menu Démarrer ***Démarrer/Tous les programmes/AVG/ Désinstaller AVG***

2.5. Service Packs pour MS Exchange

Etant donné qu'**AVG for MS Exchange 2000/2003 Server** utilise l'interface d'analyse VSAPI 2.0/2.5, vous devez appliquer le Service Pack 1 (ou supérieur) de MS Exchange 2000 Server à votre système. Cliquez sur le lien situé en dessous pour obtenir le dernier Service Pack pour MS Exchange 2000 Server :

Service Pack pour MS Exchange 2000 Server :

http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2000/sp3/default.mspx

Pour MS Exchange 2003 Server, aucun service pack supplémentaire n'est nécessaire ; cependant, il est recommandé de conserver votre système le plus à jour possible en lui appliquant les service packs et les correctifs de manière à garantir une sécurité maximale.

Service Pack pour MS Exchange 2003 Server (facultatif) :

http://www.microsoft.com/exchange/evaluation/sp2/overview.mspx

Au début de l'installation, toutes les versions de bibliothèques système seront examinées. S'il doit installer de nouvelles bibliothèques, le programme renomme les anciennes, en leur attribuant l'extension .delete. Elles seront supprimées au prochain

redémarrage système.

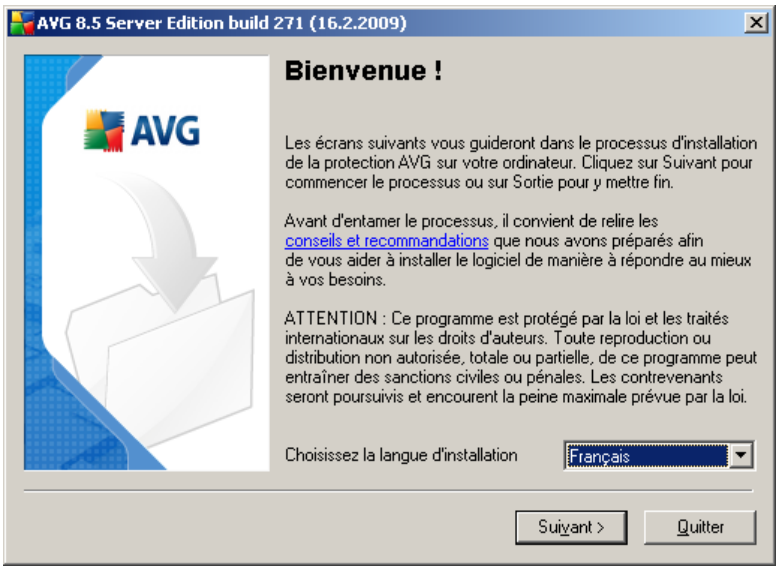
3. Processus d'installation d'AVG

Pour installer AVG sur l'ordinateur, il est nécessaire d'obtenir le dernier fichier d'installation disponible. Vous pouvez utiliser le fichier d'installation figurant sur le CD et fourni avec votre édition, mais il est fort probable qu'il soit déjà périmé. En conséquence, nous vous recommandons de bien vouloir télécharger de dernier fichier d'installation, depuis Internet. Vous pouvez télécharger le fichier à partir du site Web d'AVG (à l'adresse http://www.avg.com/download?prd=msw).

Vous serez invité à saisir votre numéro d'achat/licence au cours du processus d'installation. Vous devez être en possession de ce numéro avant de commencer l'installation. Le numéro d'achat figure sur le coffret du CD-ROM. Si vous avez commandé AVG en ligne, le numéro de licence vous sera envoyé par mail.

Après avoir téléchargé le fichier d'installation et l'avoir enregistré sur le disque dur, lancez la procédure d'installation. L'installation consiste à réaliser une série de tâches décrites à l'intérieur de boîtes de dialogue. Dans la suivante, vous trouverez une explication de chaque boîte de dialogue :

3.1. Lancement de l'installation



Le processus d'installation démarre dans la fenêtre de ***Bienvenue***. Dans cette fenêtre, vous sélectionnez la langue qui sera utilisée au cours de l'installation. Dans la partie inférieure de la fenêtre, localisez l'option ***Choisissez la langue d'installation*** et sélectionnez la langue désirée dans la liste déroulante. Cliquez ensuite sur le bouton ***Suivant*** pour confirmer votre choix et passer à la boîte de dialogue suivante.

Attention : *vous choisissez la langue qui sera utilisée pour l'installation uniquement. Vous ne choisissez pas la langue utilisée dans l'interface AVG ; vous serez amené à le faire ultérieurement, au cours du processus d'installation.*

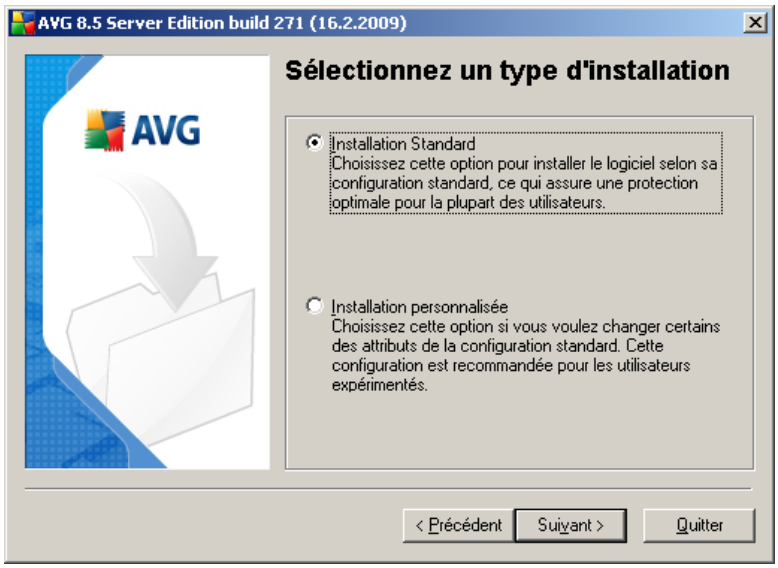
3.2. Contrat de licence

Le ***composant Licence*** affiche le texte complet de l'accord de licence avec AVG. Veuillez le lire attentivement et confirmer que vous l'avez lu, compris et accepté en cliquant sur le bouton ***Oui***. Si vous n'acceptez pas les conditions de l'accord de licence, cliquez sur le bouton ***Je refuse*** ; le processus d'installation prendra fin immédiatement.

3.3. Vérification de l'état du composant

Après avoir accepté les termes de l'accord de licence, vous êtes redirigé vers la boîte de dialogue de ***vérification de l'état du système***. Cette boîte de dialogue ne requiert aucune intervention de votre part : le système est vérifié avant le démarrage de l'installation du programme AVG. Merci de patienter jusqu'à la fin du processus, qui passe automatiquement à la boîte de dialogue suivante.

3.4. Sélection du type d'installation



La boîte de dialogue ***Sélectionnez un type d'installation*** propose deux options d'installation : installation ***standard*** et installation ***personnalisée***.

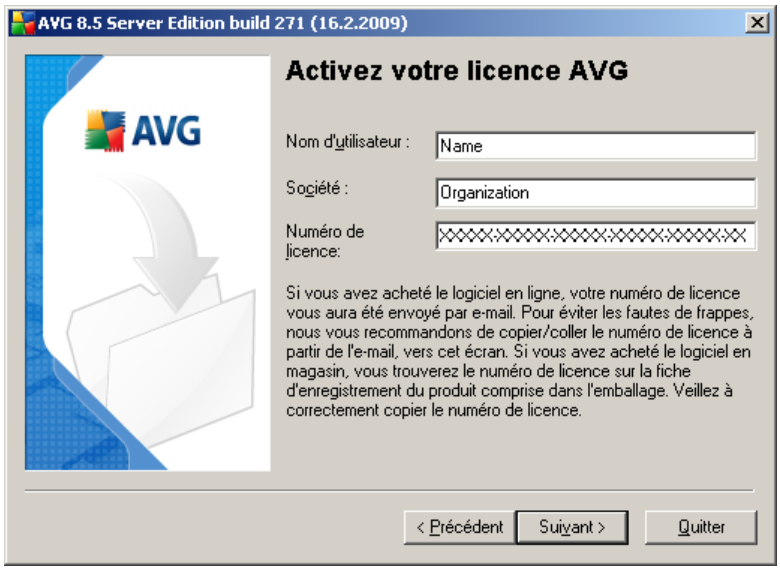
Dans la majorité des cas, il est recommandé d'adopter l'***installation standard*** qui installe automatiquement le programme AVG selon les paramètres prédéfinis par le distributeur du logiciel. Cette configuration allie un maximum de sécurité et une utilisation optimale des ressources. Si besoin est, vous avez toujours la possibilité de modifier directement la configuration dans l'application AVG.

L'installation personnalisée est réservée aux utilisateurs expérimentés qui ont une raison valable d'installer AVG selon des paramètres non standard. Cela leur permet notamment d'adapter le programme à une configuration système spécifique.

3.5. Activer AVG

Dans la boîte de dialogue ***Activer votre licence AVG***, vous devez indiquer vos coordonnées d'enregistrement. Saisissez votre nom (champ ***Nom d'utilisateur***) et le nom de votre (champ ***Société***).

Saisissez ensuite votre numéro de licence/d'achat dans le champ ***Numéro de licence*** . Le numéro de licence figure dans le message de confirmation que vous avez reçu après avoir acheté AVG par Internet. Vous devez saisir le numéro tel qu'il apparaît. Si le numéro de licence est disponible au format électronique (par exemple, dans un e-mail), il est recommandé de l'insérer en faisant appel à la méthode copier-coller.

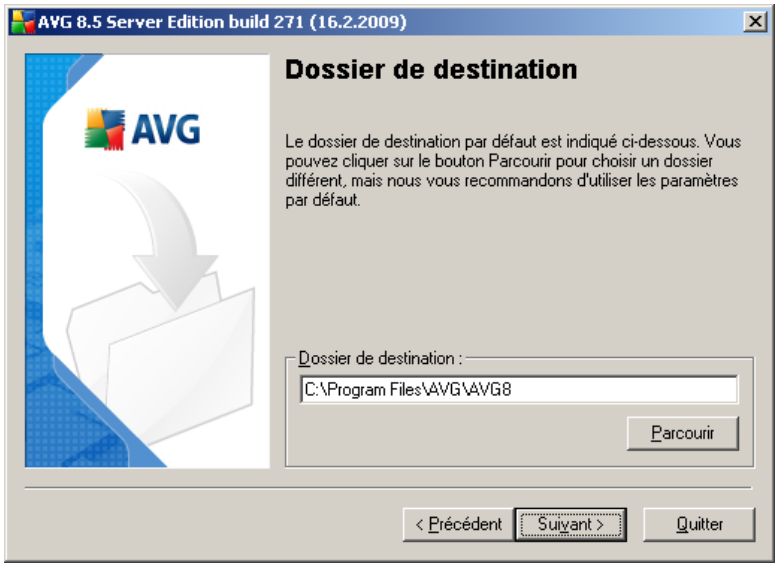


Cliquez sur le bouton ***Suivant*** pour continuer le processus d'installation.

Si vous avez opté pour l'installation standard à l'étape précédente, vous serez amené directement à la boîte de dialogue ***Résumé de l'installation*** . En revanche, si vous

avez opté pour l'installation personnalisée, la boîte de dialogue ***Dossier de destination*** s'affiche.

3.6. Installation personnalisée - Dossier de destination



La boîte de dialogue ***Dossier de destination*** permet d'indiquer le dossier dans lequel les fichiers d'installation AVG sont enregistrés. Par défaut, AVG est installé dans le dossier contenant les fichiers de programme sur le lecteur C:. Si vous optez pour un autre emplacement, cliquez sur le bouton ***Parcourir*** pour consulter la structure du lecteur, puis sélectionnez le dossier souhaité. Cliquez sur le bouton ***Suivant*** pour confirmer votre choix.

3.7. Installation personnalisée - Sélection des composants

La boîte de dialogue ***Sélection des composants*** présente tous les composants AVG qui peuvent être installés. Si les paramètres par défaut ne vous satisfont pas, vous pouvez supprimer ou ajouter certains composants.

Notez que vous pouvez seulement choisir des composants inclus dans l'édition AVG dont vous avez acquis les droits. Seule l'installation de ces composants sera proposée dans la boîte de dialogue Sélection des composants.

- ***Bibliothèque de communication pour le contrôle à distance*** - si vous voulez connecter AVG à une autre instance d'AVG DataCenter (AVG Edition Réseau), il faut sélectionner cette option.

  Remarque : *Tous les serveurs de messagerie ne sont pas administrables à distance.*

- ***Langues installées supplémentaires***- il est possible de définir la ou les langues dans lesquelles le programme AVG sera installé. Cochez la case ***Langues supplémentaires installées***, puis sélectionnez les langues désirées dans le menu correspondant.

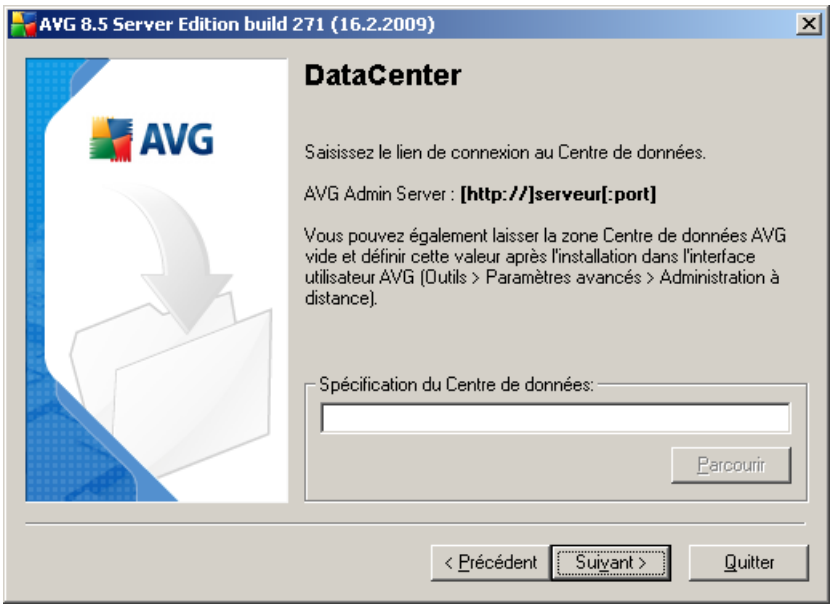
- ***Serveur anti-spam (pour serveur de messagerie)*** - sélectionnez cette option si vous voulez installer la protection anti-spam pour votre serveur de messagerie.

- ***Scanner e-mail (pour serveur de messagerie)*** - sélectionnez cette option si vous voulez installer une protection contre les virus et les codes malveillants.

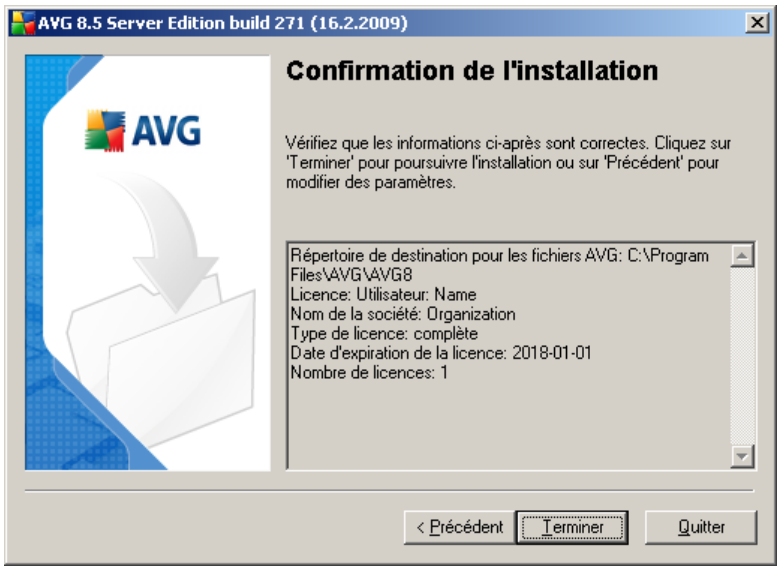
Continuez la procédure en cliquant sur le bouton ***Suivant***.

3.8. Installation personnalisée - Centre de données

Si vous avez sélectionné le module ***Bibliothèque de communication pour le contrôle à distance*** pendant la sélection des modules, vous pouvez définir dans cet écran le lien de connexion pour vous connecter à votre instance d'AVG DataCenter.



3.9. Résumé de l'installation



La boîte de dialogue ***Confirmation de l'installation*** donne des informations générales sur tous les paramètres du processus d'installation. Veuillez vous assurer que toutes ces données sont correctes. Si c'est le cas, cliquez sur le bouton ***Terminer*** pour finaliser l'installation. Sinon, cliquez sur le bouton ***Précédent*** pour revenir dans la boîte de dialogue qui convient et corrigez les informations erronées.

3.10. Installation en cours

La boîte de dialogue ***Installation*** montre la progression du processus d'installation et ne requiert aucune intervention de votre part. Merci de patienter jusqu'à la fin de l'installation. A la fin du processus, la boîte de dialogue ***Installation terminée*** s'affichera.

3.11. Installation terminée

La boîte de dialogue ***Installation terminée*** correspond à la dernière étape du processus d'installation du programme AVG. AVG est maintenant installé sur l'ordinateur et est totalement opérationnel. Le programme s'exécute en arrière-plan en mode automatique.

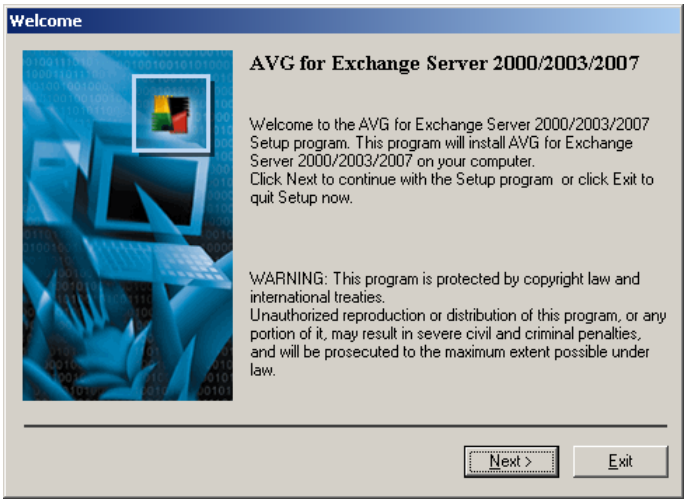
En fonction du serveur de messagerie installé, d'autres boîtes de dialogue d'installation vont s'afficher (voir ci-dessous).

4. Options d'installation d'AVG pour serveurs de mail

Après avoir installé AVG avec succès, l'installation des serveurs de messagerie individuels démarre.

Remarque : *Le mécanisme de protection anti-virus pour Kerio MailServer est directement intégré à l'application Kerio. Des informations supplémentaires sont disponibles au chapitre AVG for Kerio MailServer.*

4.1. Lancement de l'installation



Le processus d'installation démarre dans la fenêtre de ***Bienvenue***. Cliquez sur le bouton ***Suivant*** pour passer à l'écran suivant.

4.2. Contrat de licence

Cette boîte de dialogue contient l'intégralité du texte de l'accord de licence AVG. Lisez-le attentivement et confirmez que vous l'avez lu, puis cliquez sur le bouton ***Oui*** pour accepter l'accord. Si vous n'acceptez pas les termes de la licence, cliquez sur le bouton ***Non*** ; le processus d'installation prendra fin immédiatement.

4.3. Dossier d'installation

Dans la fenêtre suivante, vous êtes invité à sélectionner le dossier d'installation. Cliquez sur le bouton Parcourir pour sélectionner un autre emplacement que celui proposé par défaut. Si vous n'avez pas de raison valable de modifier les paramètres par défaut, il est recommandé de conserver l'emplacement prédéfini. Cliquez sur le

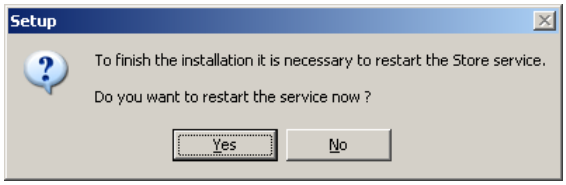
bouton ***Suivant*** pour continuer.

4.4. Lancement de la copie des fichiers

Le programme d'installation vous invite à déclencher la copie des fichiers d'installation pour procéder à l'installation. Pour cela, cliquez sur le bouton ***Suivant***.

4.5. Redémarrage du service Store

Au cours de l'installation ou après la fermeture de la fenêtre du programme d'installation, un message vous invite à redémarrer Exchange Server Store service :



Cliquez sur le bouton ***Yes (Oui)*** pour redémarrer le service Store comprenant tous les composants **AVG pour Exchange** .

Remarque : *le redémarrage du service aura pour effet de rendre votre serveur indisponible pendant quelque temps ! Vous devez avertir les utilisateurs avant de redémarrer le service car tout utilisateur en ligne sera automatiquement déconnecté au moment du redémarrage.*

4.6. Installation achevée

Dès que l'assistant d'installation a copié tous les fichiers nécessaires sur votre disque dur, l'installation est terminée.

Vous pouvez afficher le fichier journal de l'installation en cliquant sur le bouton ***Journal***.

Vous pouvez également consulter le fichier d'installation ultérieurement car il est stocké dans le dossier système temporaire (setup.log).

Cliquez sur ***OK*** dans l'écran Installation achevée pour fermer la boîte de dialogue du programme d'installation .

Après l'installation, l'assistant de configuration d'AVG sera automatiquement exécuté et vous guidera tout au long de la configuration de base d'**AVG 8.5 Email Server Edition**. Bien que la configuration d'AVG soit accessible à n'importe quel moment, nous vous recommandons vivement d'effectuer la configuration de base à l'aide de l'assistant.

Pour configurer la protection de chacun de vos serveurs de messagerie, reportez-vous au chapitre approprié :

- ***AVG pour MS Exchange Server 2007***
- ***AVG pour MS Exchange Server 2000/2003***
- ***AVG pour Kerio MailServer***

5. AVG pour MS Exchange Server 2007

5.1. Configuration

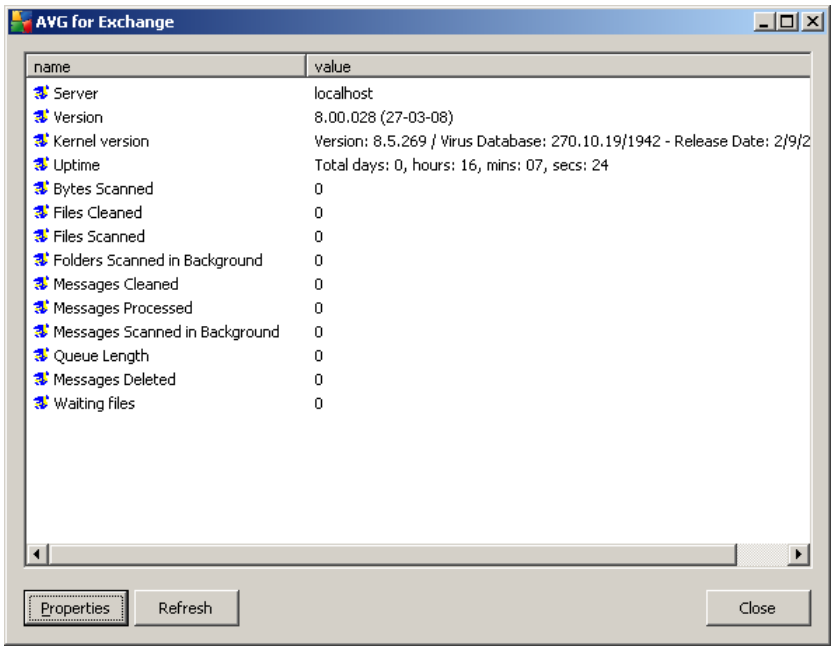
Lorsque vous redémarrez le service Exchange 2007 Server Store après l'installation d'AVG for MS Exchange 2007 Server , aucune autre intervention n'est requise.

5.1.1. Etat

Pour afficher l'état ou la configuration de **AVG**, vous devez d'abord lancer l'application AVG pour Exchange administration. Par défaut, elle se trouve dans le répertoire d'installation.

C:\AVG4ES2K

Accédez à ce répertoire et lancez ***avg4es2kadm.exe***. Une nouvelle fenêtre s'ouvre avec une fenêtre d'information présentant différentes données.



Les informations incluses dans la fenêtre indiquent le nom du serveur, la version de l'application, la version de la base de données, la version du noyau et le temps total d'exécution du programme depuis le dernier démarrage. Des informations sur les performance anti-virus sont également affichées dans la fenêtre *(performance*

monitor counters, compteurs de l'Analyseur de performances).

AVG pour MS Exchange 2007 Server analyse tous les messages figurant dans les bases de données des dossiers publics et privés. Si un virus est détecté, AVG pour MS Exchange 2007 Server écrit un message dans le fichier journal d'AVG ainsi que dans le journal des événements.

5.1.2. VSAPI 2.0

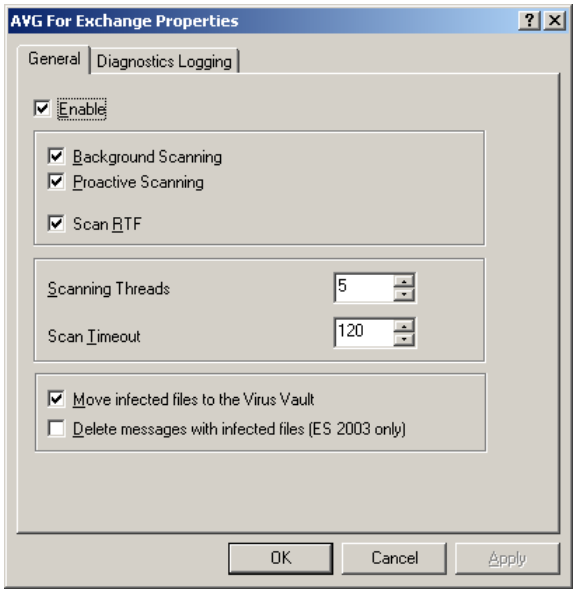
Analyse anti-virale **API 2.5** *(VSAPI 2.5 tel que fourni dans MS Exchange 2003 Server)* permet de supprimer les messages infectés. Cette fonctionnalité peut être configurée dans la boîte de dialogue ***Propriétés*** (voir ci-dessous).

5.1.3. Propriétés générales

La fenêtre de configuration d'AVG pour Exchange 2007 Server s'ouvre lorsque vous cliquez sur le bouton ***Propriétés***.

La fenêtre de configuration ***AVG for Exchange Properties (Propriétés d'AVG pour Exchange)*** comporte deux onglets. Il est possible de modifier les paramètres de l'analyse antivirale des messages et de l'enregistrement des résultats.

Onglet Général



Sous l'onglet ***Général***, vous trouverez plusieurs options liées aux performances de l'analyse antivirale des e-mails effectuée par AVG pour Exchange 2007 Server :

- ***Enable (Activer)*** – elle permet d'activer ou de désactiver l'analyse des messages.
- ***Background Scanning (Analyse en arrière-plan)*** – elle permet d'activer ou de désactiver l'analyse en arrière-plan. L'analyse en arrière-plan est l'une des fonctions clés de l'interface de l'application VSAPI 2.0/2.5. Elle permet l'analyse des threads dans les bases de données de messagerie Exchange. Lorsqu'un élément, pas encore analysé, est trouvé dans les dossiers des boîtes aux lettres de l'utilisateur, il est envoyé à AVG pour Exchange 2007 Server pour analyse. L'analyse et la recherche des objets non examinés s'effectuent en parallèle.

  Un thread de basse priorité est utilisé spécifiquement pour chaque base de données, ce qui garantit que les autres tâches (par exemple le stockage des messages dans la base de données Microsoft Exchange) sont toujours réalisées en priorité.

- ***Proactive Scanning (Analyse proactive)*** – elle permet d'activer ou de désactiver l'analyse proactive de VSAPI 2.0/2.5. L'analyse proactive repose sur la gestion dynamique des priorités des éléments placés dans la file d'attente en vue de leur analyse. Les éléments de faible priorité ne sont pas analysés tant que tous les éléments dont la priorité est plus grande n'ont pas été traités (placés le plus souvent à la demande dans la file d'attente). Si la priorité d'un élément augmente lorsqu'un client essaie de l'utiliser, la priorité d'un élément change en fonction de l'activité des utilisateurs.
- ***Scan RTF (Analyser RTF)*** – la case permet de spécifier si les fichiers de type RTF doivent être analysés ou non.
- ***Scanning Threads (Analyse des threads)*** – par défaut, le processus d'analyse s'effectue par threads, afin d'augmenter les performances globales de l'analyse et établir un certain niveau de parallélisme. Dans ce champ, vous pouvez modifier le nombre de threads. Le nombre de threads par défaut est calculé comme étant 2 fois le 'nombre_de_processeurs' + 1.
- ***Scan Timeout (Délai d'analyse)*** – intervalle maximal continu (exprimé en secondes) pendant lequel un thread tente d'accéder au message à analyser.
- ***Mettre les fichiers infectés en quarantaine*** – Si cette case est cochée, tout e-mail infecté est placé dans le composant **Quarantaine** .
- ***Supprimer les messages contenant des fichiers infectés (Exchange Server 2003/2007 uniquement)*** – Après avoir activé cette option, tout message détecté comme porteur de virus est supprimé. Si cette option est désactivée le message infecté est transmis au destinataire, mais la pièce jointe infectée est remplacée par un texte d'information sur le virus détecté. Cette option n'est disponible que pour VSAPI 2.5, fourni avec Exchange 2007 Server.

En général, toutes les fonctions contenues dans cet onglet sont des extensions utilisateur des services d'interface de l'application Microsoft VSAPI 2.0/2.5. Pour

obtenir des informations détaillées sur VSAPI 2.0/2.5, servez-vous des liens suivants (et des liens accessibles à partir de ces liens de référence) :

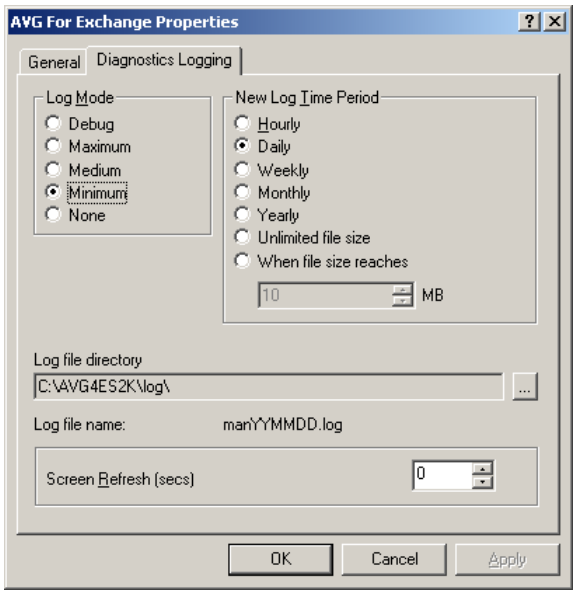
- http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP pour obtenir des informations générales sur VSAPI 2.0 dans Exchange 2000 Server Service Pack

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - pour obtenir des informations sur l'interaction entre Exchange et le logiciel antivirus

- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 pour obtenir des informations sur les fonctions supplémentaires de VSAPI 2.5, dans l'application Exchange 2003 Server.

Remarque : *Le comportement de l'analyse est contrôlé depuis l'application AVG. Dans le menu principal de l'application, sélectionnez Outils/Paramètres avancés. (Voir le chapitre Scanner e-mail).*

5.1.4. Enregistrement des diagnostics



Dans cet onglet, vous pouvez définir la fréquence d'enregistrement de l'analyse antivirale et le comportement général. Plusieurs champs sont prédéfinis sous l'onglet Diagnostics Logging (Journaux de diagnostic) :

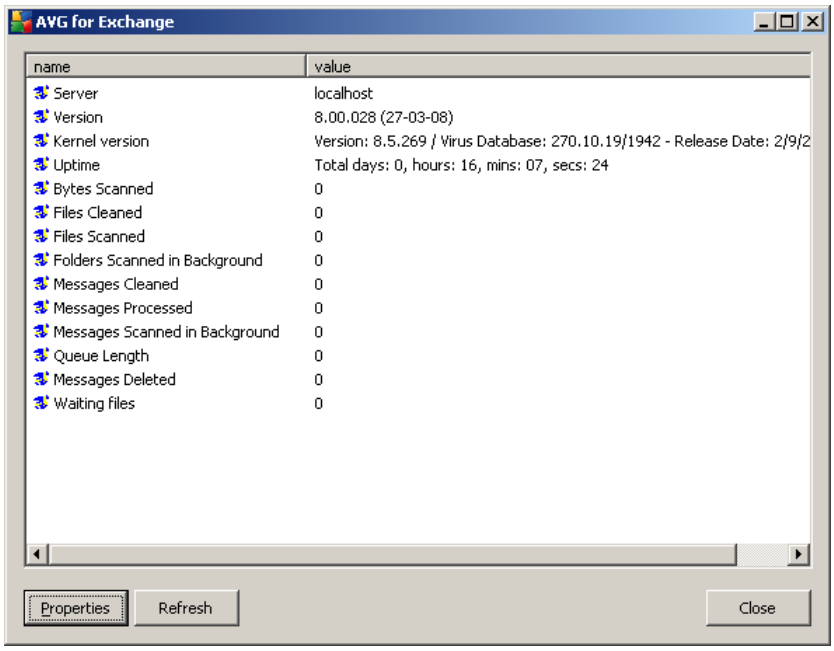
- ***Log Mode (Mode d'enregistrement)*** – vous pouvez ajuster le type

d'informations à enregistrer.

- ***New Log Time Period (Nouvel intervalle d'enregistrement)*** – vous pouvez définir la période de création du fichier journal et éventuellement la taille du fichier journal.
- ***Log file directory (Répertoire des fichiers journaux)*** – modifiez ici l'emplacement par défaut du fichier journal.
- ***Log file name (Nom du fichier journal)*** – modifiez ici l'emplacement par défaut du fichier journal.
- ***Screen Refresh (Actualisation de l'écran)*** – vous pouvez spécifier la fréquence (en secondes) selon laquelle l'écran de contrôle en ligne (affiché dans la fenêtre d'informations sur AVG pour Exchange Server) est mis à jour.

5.2. Surveillance du serveur

5.2.1. Surveillance en ligne



Dans la fenêtre d'information AVG pour Exchange Server - *Reportez-vous à la section Configuration/Etat pour savoir comment y accéder.*), plusieurs champs s'affichent :

Les quatres premiers éléments fournissent des informations générales sur le serveur et sur l'état d'AVG pour Exchange 2007 Server :

- ***Server (serveur)*** – nom du serveur
- ***Version*** – version d'AVG pour Exchange 2007 Server
- ***Kernel version (version du noyau)*** – version du noyau anti-virus et de sa base de données interne
- ***Temps écoulé*** – durée depuis le dernier redémarrage d'Exchange Server

Les autres éléments représentent les compteurs de l'Analyseur de performances de VSAPI 2.0/2.5 relatifs à l'analyse antivirale d'Exchange 2007 Server. Les compteurs sont décrits comme suit :

- ***Bytes Scanned (Octets analysés)*** – nombre total d'octets, dans tous les fichiers, traités par l'outil d'analyse antivirale.
- ***Files Cleaned (Fichiers nettoyés)*** – nombre total de fichiers individuels désinfectés par l'outil d'analyse antivirale.
- ***Files scanned (Fichiers analysés)*** – nombre total de fichiers analysés par l'outil de recherche de virus.
- ***Folders Scanned in Background (Dossiers analysés en arrière-plan)*** – nombre total de dossiers traités par l'analyse en arrière-plan.
- ***Messages Cleaned (Messages nettoyés)*** – nombre total de messages de haut niveau désinfectés par l'outil d'analyse antivirale.
- ***Messages Processed (Messages traités)*** - valeur cumulative du nombre total des messages de haut niveau traités par l'outil d'analyse antivirale.
- ***Messages Scanned in Background (Messages analysés en arrière-plan)*** – nombre total de messages traités par l'analyse en arrière-plan.
- ***Queue Length (Longueur de la file d'attente)*** – nombre actuel de requêtes en attente de traitement par l'outil d'analyse antivirale.
- ***Messages Deleted (Messages supprimés)*** – nombre total de messages suspects supprimés par l'analyse antivirale (disponible seulement dans VSAPI 2.5)
- ***Waiting Files (Fichiers en attente)*** – nombre de fichiers en attente

d'analyse.

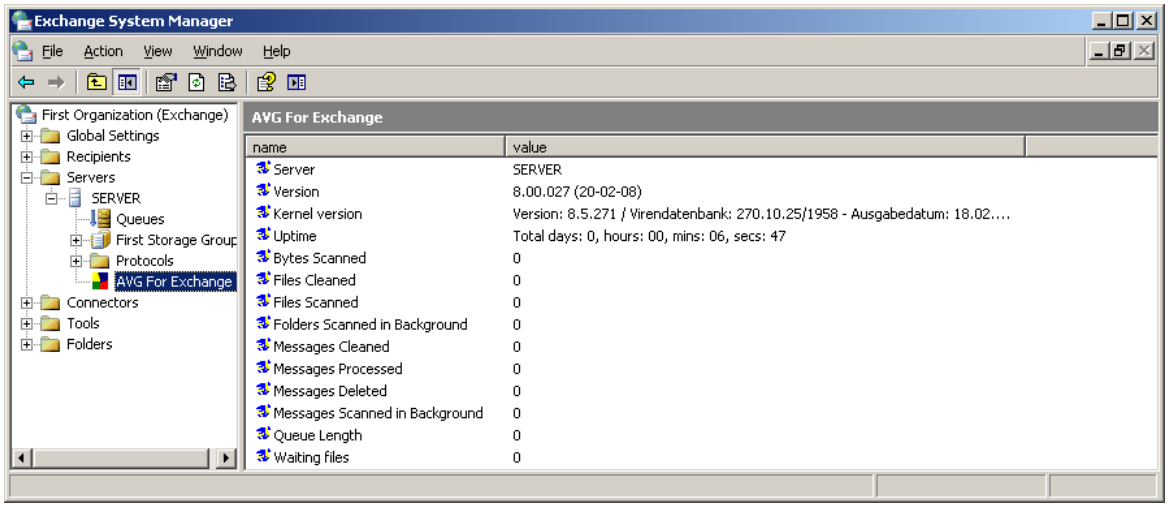
6. AVG pour MS Exchange Server 2000/2003

6.1. Configuration

Lorsqu'Exchange 2000/2003 Server Store service est relancé après l'installation d' **AVG for MS Exchange 2000/2003 Server** , aucune autre intervention n'est requise.

6.1.1. Etat

Pour afficher le statut d'**AVG**, lancez le Gestionnaire système Exchange. Dans la catégorie Servers (Serveurs) de l'arborescence *(à gauche de la fenêtre principale)*, sélectionnez un serveur particulier. La catégorie AVG for Exchange (AVG pour Exchange) figure dans l'arborescence secondaire du serveur. Le fait de sélectionner cette catégorie ouvre la fenêtre d'informations présentant différentes données.



Les informations incluses dans la fenêtre indiquent le nom du serveur, la version de l'application, la version de la base de données, la version du noyau et le temps total d'exécution du programme depuis le dernier démarrage. Des informations sur les performance anti-virus sont également affichées dans la fenêtre *(performance monitor counters, compteurs de l'Analyseur de performances)*.

AVG pour MS Exchange 2000/2003 Server analyse tous les messages figurant dans les bases de données des dossiers publics et privés. Si un virus est détecté, AVG pour MS Exchange 2000/2003 Server écrit un message dans le fichier journal et également dans le journal des événements.

6.1.2. VSAPI 2.0

L'analyse des virus **API 2.0** (VSAPI 2.0 est livré avec MS Exchange 2000 Server) ne permet pas la suppression des messages infectés. Etant donné que la pièce jointe au message infecté ne peut être supprimée, son nom de fichier sera modifié : AVG pour Exchange 2000/2003 Server ajoute l'extension .virusinfo.txt au nom du fichier d'origine. Le contenu du fichier est remplacé par un message concernant le virus connu. Si un virus est détecté directement dans le message, le corps entier du message est remplacé par une note indiquant qu'un virus a été trouvé à l'intérieur de ce message.

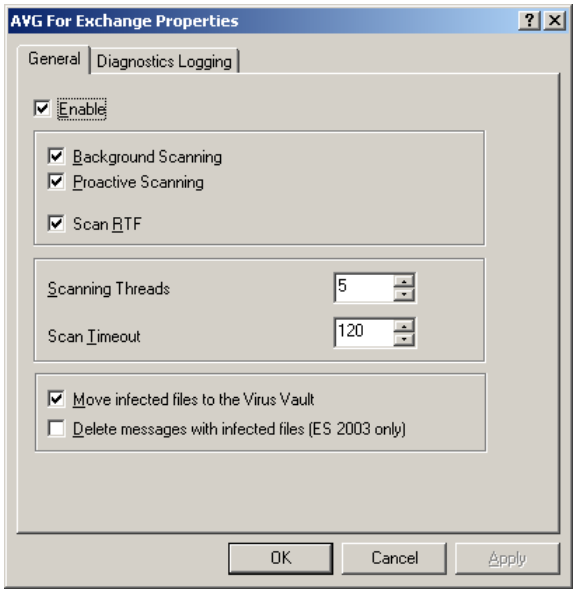
L'analyse anti-virale **API 2.5** *(VSAPI 2.5 est livré avec MS Exchange 2003 Server)* permet également la suppression des messages infectés. Cette fonction peut être configurée dans la boîte de dialogue de configuration AVG pour MS Exchange 2000/2003 Server.

6.1.3. Propriétés générales

Pour ouvrir la fenêtre de configuration AVG pour Exchange 2000/2003 Server, cliquez avec le bouton droit de la souris sur la catégorie ***AVG for Exchange (AVG pour Exchange)*** et sélectionnez l'élément ***Properties (Propriétés)***. Une autre solution consiste à cliquer sur le bouton ***Action*** situé dans le menu supérieur.

La fenêtre de configuration ***AVG for Exchange Properties (Propriétés d'AVG pour Exchange)*** comporte deux onglets. Il est possible de modifier les paramètres de l'analyse antivirale des messages et de l'enregistrement des résultats.

Onglet Général



Sous l'onglet ***General (Général)*** se trouvent plusieurs options liées aux performances de l'analyse antivirale d'AVG pour Exchange 2000/2003 Server :

- ***Enable (Activer)*** – elle permet d'activer ou de désactiver l'analyse des messages.
- ***Background Scanning (Analyse en arrière-plan)*** – elle permet d'activer ou de désactiver l'analyse en arrière-plan. L'analyse en arrière-plan est l'une des fonctions clés de l'interface de l'application VSAPI 2.0/2.5. Elle permet l'analyse des threads dans les bases de données de messagerie Exchange. Lorsqu'un élément, pas encore analysé, est trouvé dans les dossiers des boîtes aux lettres de l'utilisateur, il est envoyé à AVG pour Exchange 2000/2003 Server pour analyse. L'analyse et la recherche des objets non examinés s'effectuent en parallèle.

  Un thread de basse priorité est utilisé spécifiquement pour chaque base de données, ce qui garantit que les autres tâches (par exemple le stockage des messages dans la base de données Microsoft Exchange) sont toujours réalisées en priorité.

- ***Proactive Scanning (Analyse proactive)*** – elle permet d'activer ou de désactiver l'analyse proactive de VSAPI 2.0/2.5. L'analyse proactive repose sur la gestion dynamique des priorités des éléments placés dans la file d'attente en vue de leur analyse. Les éléments de faible priorité ne sont pas analysés tant que tous les éléments dont la priorité est plus grande n'ont pas été traités (placés le plus souvent à la demande dans la file d'attente). Si la priorité d'un élément augmente lorsqu'un client essaie de l'utiliser, la priorité d'un élément

change en fonction de l'activité des utilisateurs.

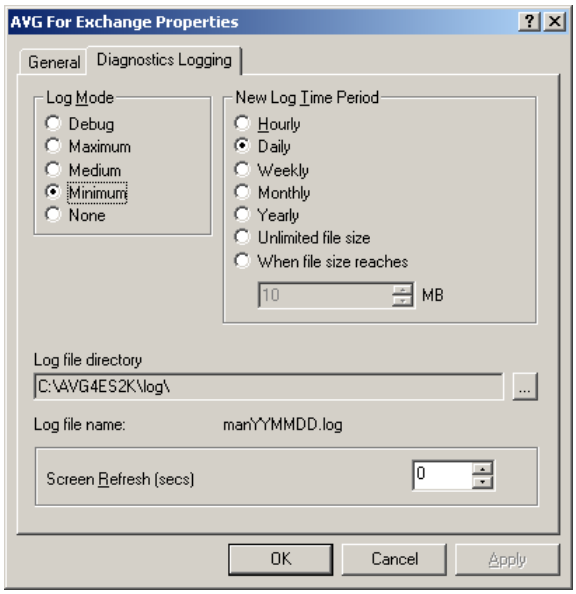
- ***Scan RTF (Analyser RTF)*** – la case permet de spécifier si les fichiers de type RTF doivent être analysés ou non.
- ***Scanning Threads (Analyse des threads)*** – par défaut, le processus d'analyse s'effectue par threads, afin d'augmenter les performances globales de l'analyse et établir un certain niveau de parallélisme. Dans ce champ, vous pouvez modifier le nombre de threads. Le nombre de threads par défaut est calculé comme étant 2 fois le 'nombre_de_processeurs' + 1.
- ***Scan Timeout (Délai d'analyse)*** – intervalle maximal continu (exprimé en secondes) pendant lequel un thread tente d'accéder au message à analyser.
- ***Move infected files to the Virus Vault (Déplace les fichiers infectés dans la quarantaine)*** – si la case est cochée, tout message infecté est confiné dans le composant **Quarantaine AVG**.
- ***Delete messages with infected files (Exchange Server 2003 uniquement) (Supprimer les messages contenant des fichiers infectés)*** - après activation de cette option tout message, dans lequel un virus est détecté, est supprimé. Si cette option est désactivée le message infecté est transmis au destinataire, mais la pièce jointe infectée est remplacée par un texte d'information sur le virus détecté. Cette option n'est disponible que pour VSAPI 2.5, fourni avec Exchange 2003 Server.

En général, toutes les fonctions contenues dans cet onglet sont des extensions utilisateur des services d'interface de l'application Microsoft VSAPI 2.0/2.5. Pour obtenir des informations détaillées sur VSAPI 2.0/2.5, servez-vous des liens suivants (et des liens accessibles à partir de ces liens de référence) :

- http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP pour obtenir des informations générales sur VSAPI 2.0 dans Exchange 2000 Server Service Pack
- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - pour obtenir des informations sur l'interaction entre Exchange et le logiciel antivirus
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 pour obtenir des informations sur les fonctions supplémentaires de VSAPI 2.5, dans l'application Exchange 2003 Server.

Remarque : *Le comportement du moteur d'analyse est contrôlé par l'application AVG Serveur de messagerie. Dans le menu principal de l'application, sélectionnez Outils/ Paramètres avancés. (Voir le chapitre Scanner e-mail).*

6.1.4. Enregistrement des diagnostics

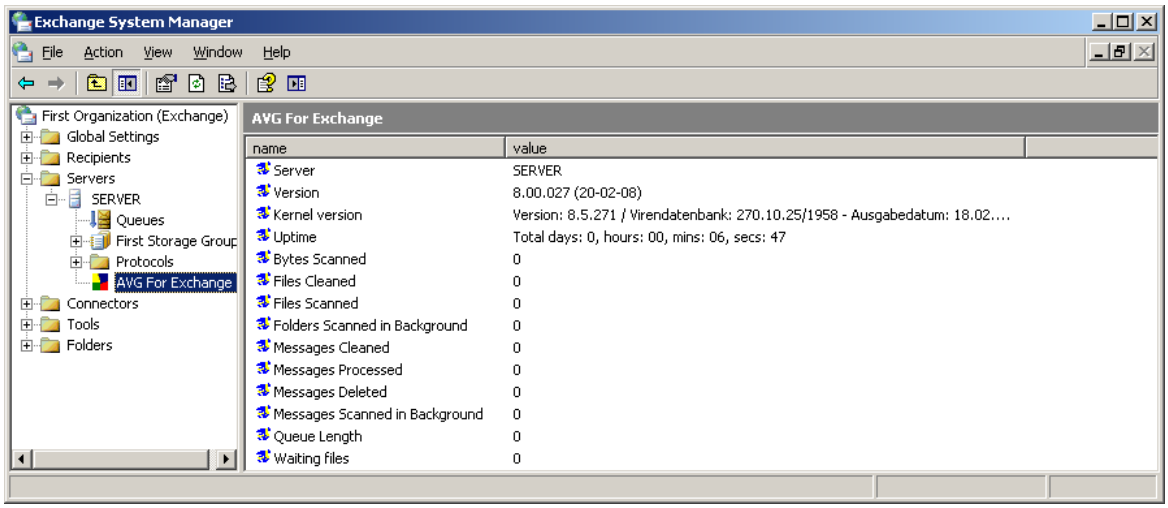


Dans cet onglet, vous pouvez définir la fréquence d'enregistrement de l'analyse antivirale et le comportement général. Plusieurs champs sont prédéfinis sous l'onglet Diagnostics Logging (Journaux de diagnostic) :

- ***Log Mode (Mode d'enregistrement)*** – vous pouvez ajuster le type d'informations à enregistrer.
- ***New Log Time Period (Nouvel intervalle d'enregistrement)*** – vous pouvez définir la période de création du fichier journal et éventuellement la taille du fichier journal.
- ***Log file directory (Répertoire des fichiers journaux)*** – modifiez ici l'emplacement par défaut du fichier journal.
- ***Log file name (Nom du fichier journal)*** – modifiez ici l'emplacement par défaut du fichier journal.
- ***Screen Refresh (Actualisation de l'écran)*** – vous pouvez spécifier la fréquence (en secondes) selon laquelle l'écran de contrôle en ligne (affiché dans la fenêtre d'informations sur AVG pour Exchange 2000/2003 Server) est mis à jour.

6.2. Surveillance du serveur

6.2.1. Surveillance en ligne



Dans la fenêtre d'information AVG pour MS Exchange 2000/2003 Server, *reportez-vous à la section Configuration/Etat pour savoir comment y accéder.*), plusieurs champs s'affichent :

Les quatre premiers éléments fournissent des informations générales sur le serveur et l'état d'AVG pour Exchange 2000/2003 Server :

- ***Server (serveur)*** – nom du serveur
- ***Version*** – version d'AVG pour Exchange 2000/2003 Server
- ***Kernel version (version du noyau)*** – version du noyau anti-virus et de sa base de données interne
- ***Uptime (temps écoulé)*** – laps de temps total depuis la dernière exécution d'Exchange Server
- ***Waiting Files (Fichiers en attente)*** – nombre de fichiers en attente d'analyse.

Les autres éléments représentent des compteurs de l'Analyseur de performances particuliers de VSAPI 2.0/2.5 relatifs à l'analyse antivirale d'Exchange 2000/2003 Server et ils ne sont pas nécessairement toujours visibles. Les compteurs sont décrits

comme suit :

- ***Bytes Scanned (Octets analysés)*** – nombre total d'octets, dans tous les fichiers, traités par l'outil d'analyse antivirale.
- ***Files Cleaned (Fichiers nettoyés)*** – nombre total de fichiers individuels désinfectés par l'outil d'analyse antivirale.
- ***Files Cleaned/sec (Fichiers nettoyés/sec)*** – taux de désinfection des fichiers individuels par l'outil d'analyse antivirale.
- ***Files Quarantined (Fichiers déplacés en quarantaine)*** – nombre total de fichiers individuels placés en quarantaine par l'outil d'analyse antivirale.
- ***Files Quarantined/sec (Fichiers en quarantaine/sec)*** – taux de mise en quarantaine des fichiers individuels par l'outil d'analyse antivirale.
- ***Folders Scanned in Background (Dossiers analysés en arrière-plan)*** – nombre total de dossiers traités par l'analyse en arrière-plan.
- ***Messages Cleaned (Messages nettoyés)*** – nombre total de messages de haut niveau désinfectés par l'outil d'analyse antivirale.
- ***Messages Cleaned/sec (Messages nettoyés/sec)*** – taux de nettoyage des messages de haut niveau par l'outil d'analyse antivirale.
- ***Messages Quarantined (Messages déplacés en quarantaine)*** – nombre total de messages de haut niveau placés en quarantaine par l'outil d'analyse antivirale.
- ***Messages Quarantined/sec (Messages déplacés en quarantaine/sec)*** – taux de mise en quarantaine des messages de haut niveau par l'outil d'analyse antivirale.
- ***Messages Processed (Messages traités)*** - valeur cumulative du nombre total des messages de haut niveau traités par l'outil d'analyse antivirale.
- ***Messages Processed/sec (Messages traités/sec)*** – taux de traitement des messages de haut niveau par l'outil d'analyse antivirale.
- ***Messages Scanned in Background (Messages analysés en arrière-plan)*** – nombre total de messages traités par l'analyse en arrière-plan.
- ***Messages Deleted (Messages supprimés)*** – nombre total de messages suspects supprimés par l'analyse antivirale (disponible seulement dans

VSAPI 2.5)

- ***Messages Deleted/sec (Messages supprimés/sec)*** – taux de suppression des messages suspects par l'analyse antivirale (disponible seulement dans VSAPI 2.5)

- ***Queue Length (Longueur de la file d'attente)*** – nombre actuel de requêtes en attente de traitement par l'outil d'analyse antivirale.

6.2.2. Journal des évènements

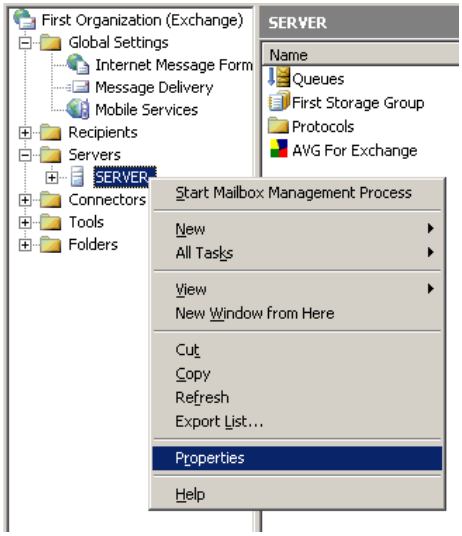
Hormis la surveillance en ligne d'AVG pour MS Exchange 2000/2003 Server, vous pouvez configurer l'analyse antivirale en vue de l'enregistrement des événements dans le **journal des événements**. Un évènement peut représenter divers éléments : des commentaires liés au chargement de bibliothèques de programme, la détection d'un virus, un avertissement lié à la résolution d'un problème, etc.

Vous pouvez configurer le niveau de consignation d'Exchange VSAPI 2.0/2.5 dans la fenêtre principale du *Gestionnaire du système Exchange (comme indiqué dans la section Configuration/Consignation des diagnostics)*.

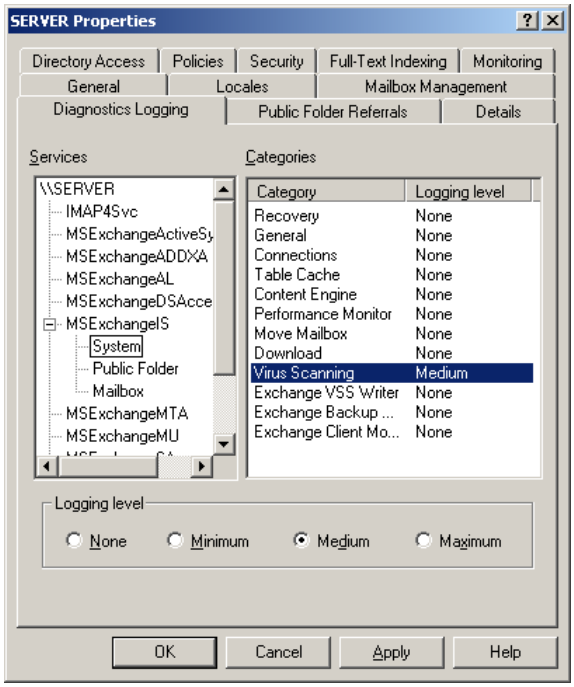
- Double-cliquez sur la catégorie ***Servers (Serveurs)*** dans l'arborescence.

- Sélectionnez le serveur (voir l'exemple du nom du serveur dans la capture d'écran ci-dessous).

- Cliquez avec le bouton droit de la souris sur le nom du serveur et choisissez ***Properties (Propriétés)*** dans le menu contextuel.



- La fenêtre ***Properties (Propriétés)*** s'affiche.
- Cliquez sur l'onglet ***Diagnostics Logging (Journaux de diagnostic)***.
- Dans l'arborescence ***Services***, sélectionnez le dossier MSExchangeIS / System (MSExchangeIS / Système).
- Dans la liste ***Categories (Catégories)*** ouverte, sélectionnez l'élément ***Virus Scanning (Analyse anti-virus)*** et choisissez le niveau d'enregistrement pour le journal d'évènements du système d'exploitation. Vous avez le choix entre les niveaux suivants :
  - ***Aucun***
  - ***Minimal***
  - ***Moyen***
  - ***Maximal***



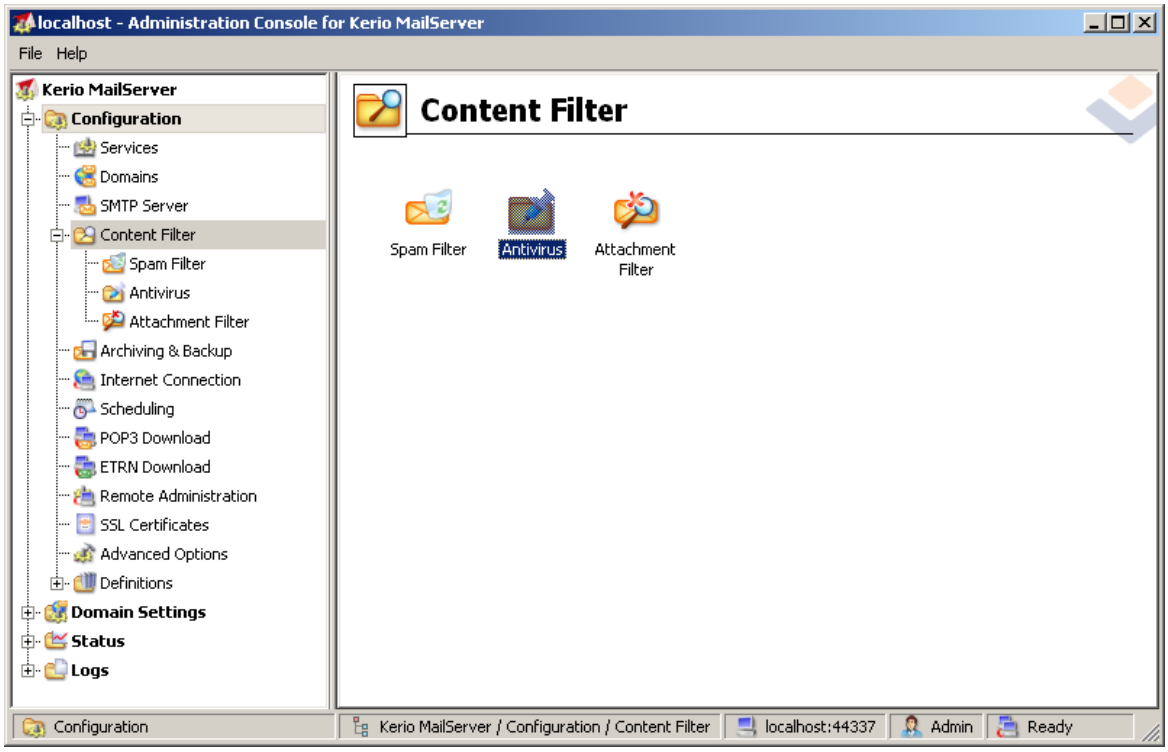
Remarque : *Pour obtenir la description complète des évènements VSAPI 2.0/2.5, activez ce lien :*

http://support.microsoft.com/default.aspx?scid=kb;EN-US;294336.

7. AVG for Kerio MailServer

7.1. Configuration

Le mécanisme de protection antivirale est intégré directement à l'application Kerio MailServer. Pour activer la protection de messagerie de Kerio MailServer par le moteur d'analyse AVG, lancez l'application Kerio Administration Console. Dans l'arborescence située à gauche de la fenêtre de l'application, choisissez le sous-groupe Content Filter (Filtrage du contenu) dans la catégorie Configuration:

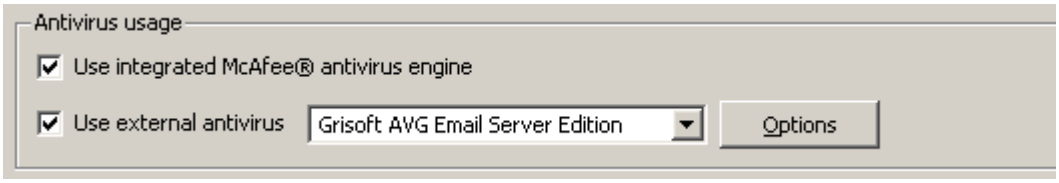


Cliquer sur l'élément Content Filter (Filtrage du contenu) ouvre une boîte de dialogue contenant trois options :

- ***Spam Filter (Filtre anti-spam)***
- ***Antivirus*** (voir la section ***Antivirus***)
- ***Attachment Filter (Filtrage des pièces jointes)*** (voir la section ***– Filtrage des pièces jointes***)

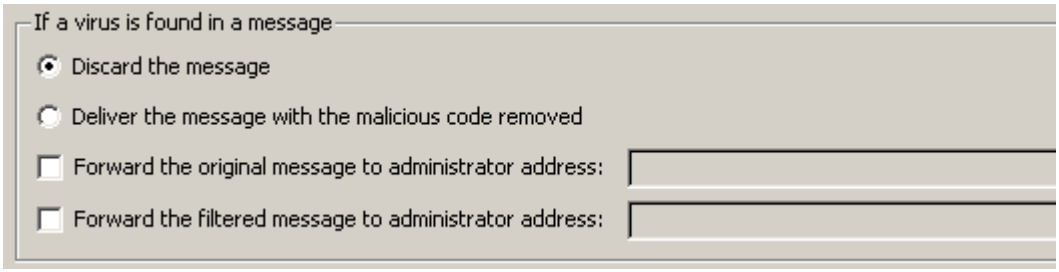
7.1.1. Anti-virus

Pour activer AVG for Kerio MailServer, cochez la case Use external antivirus (Utiliser un anti-virus externe) et choisissez la commande AVG Email Server Edition (AVG Edition Serveur de mail) dans le menu logiciel externe situé dans la zone Antivirus usage (Utilisation de l'anti-virus) de la fenêtre de configuration :



Dans la section suivante, vous avez la possibilité d'indiquer la procédure à appliquer en présence d'un message infecté ou filtré :

- ***If a virus is found in a message (Si un virus est trouvé dans un message)***

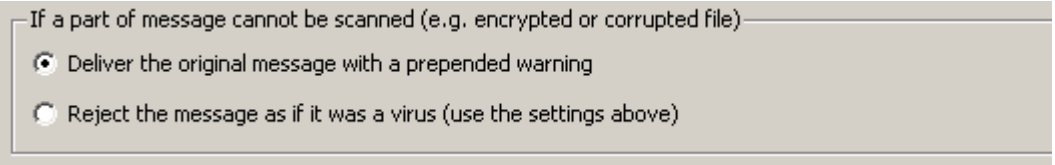


Cette zone précise l'action à effectuer si un virus est trouvé dans un message ou si un message est isolé par le filtrage des pièces jointes :

  - ***Discard the message (Ignorer le message)*** – cette option permet de supprimer le message infecté ou filtré.
  - ***Deliver the message with the malicious code removed (Distribuer le message sans le code malveillant)*** – cette option permet de transmettre le message au destinataire, sans la pièce jointe potentiellement dangereuse.
  - ***Forward the original message to administrator address (Transférer le message d'origine à l'adresse de l'administrateur)***¬– avec cette option, le message infecté est transféré à l'adresse indiquée dans le champ d'adresse.

- ***Forward the filtered message to administrator address (Transférer le message filtré à l'adresse de l'administrateur)***¬– avec cette option, le message filtré est transféré à l'adresse indiquée dans la zone d'adresse.

- ***If a part of message cannot be scanned (Si une partie du message ne peut être analysée), par exemple, en cas de corruption de fichier.***



Cette zone précise l'action à réaliser lorsqu'une partie ou la pièce jointe du message ne peut être analysée :

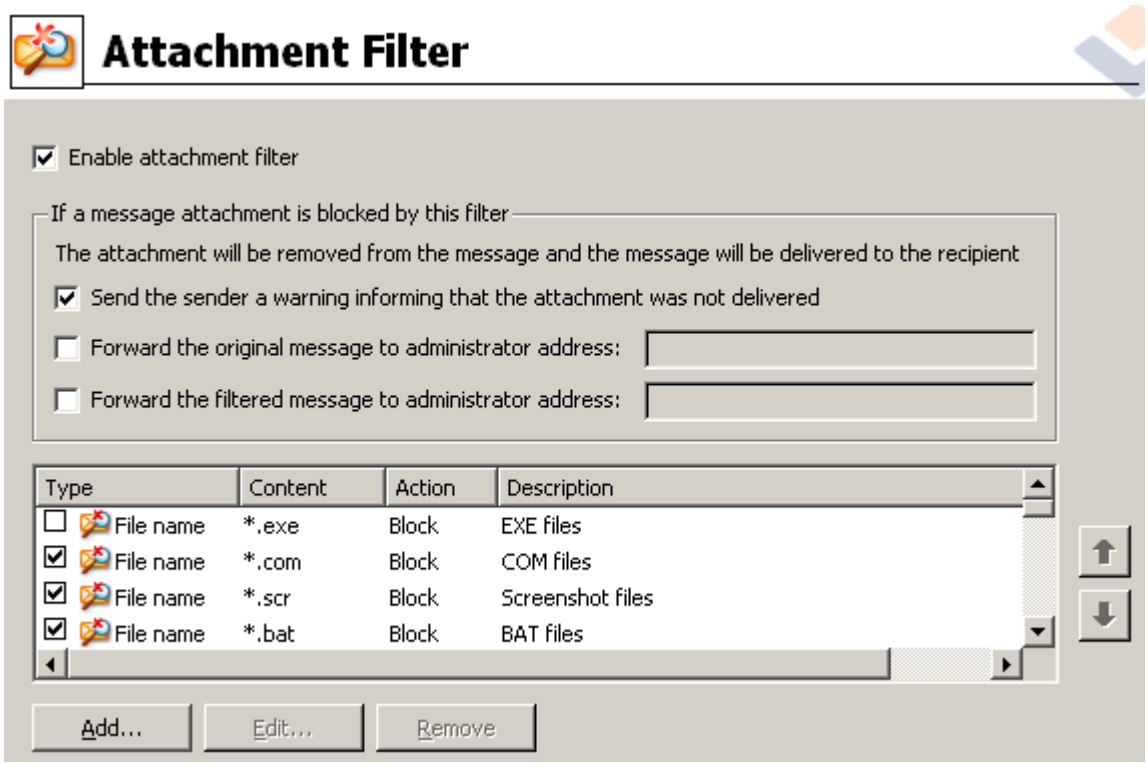
- ***Deliver the original message with a prepared warning (Distribuer le message d'origine accompagné de l'avertissement préparé)*** - le message (ou la pièce jointe) sera envoyé sans vérification. L'utilisateur sera averti que le message est susceptible de contenir des virus.

- ***Reject the message as if it was virus (Refuser le message comme s'il s'agissait d'un virus)*** - le système se comporte de la même manière que s'il s'agissait d'un virus (c'est-à-dire que le message est distribué sans pièce jointe ou est refusé). Cette option est sans danger, mais rend quasi impossible l'envoi d'archives protégées par un mot de passe.

Remarque : *Le comportement du moteur d'analyse est contrôlé par l'application AVG Serveur de messagerie. Dans le menu principal de l'application, sélectionnez Outils/ Paramètres avancés. (Voir le chapitre Scanner e-mail).*

7.1.2. Filtrage des pièces jointes

Dans le menu Attachment Filter (Filtrage des pièces jointes) figure une liste de diverses définitions de pièces jointes :



Vous pouvez activer/désactiver le filtrage les pièces jointes des messages en cochant la case Enable attachment filter (Activer le filtrage des pièces jointes). Vous pouvez également modifier les paramètres suivants :

- ***Send a warning to sender that the attachment was not delivered (Envoyer un avertissement à l'expéditeur pour signaler que la pièce jointe n'a pas été distribuée)***

  L'expéditeur recevra un avertissement du serveur Kerio MailServer indiquant qu'il a envoyé un message avec un virus ou une pièce jointe bloquée.

- ***Forward the original message to administrator address (Transférer le message d'origine à l'adresse de l'administrateur)***

  Le message sera transféré (tel quel, c'est-à-dire avec la pièce jointe infectée ou

interdite) à l'adresse définie qu'il s'agisse d'une adresse locale ou externe.

- ***Forward the filtered message to administrator address (Transférer le message filtré à l'adresse de l'administrateur)***

  Le message, débarrassé de la pièce jointe infectée ou interdite, est transmis (sauf dans le cadre des actions sélectionnées par la suite) à l'adresse définie. Cette option permet de vérifier le fonctionnement correct de l'anti-virus et/ou du filtrage des pièces jointes.

Dans la liste des extensions, chacun des éléments dispose de quatre champs :

- ***Type*** – spécification du genre de pièce jointe déterminé par l'extension attribué dans le champ Content (Contenu). Les types disponibles sont File name (Nom de fichier) ou MIME type (Type MIME). Vous pouvez cocher la case correspondante au champ pour inclure ou exclure l'élément du filtrage des pièces jointes.

- ***Content (Contenu)*** – spécifiez ici l'extension à filtrer. Vous pouvez utiliser les caractères génériques du système d'exploitation (par exemple, la chaîne « *. doc.* » équivaut à tout fichier d'extension .doc et à tout fichier dont l'extension est précédée de .doc).

- ***Action*** – définit l'action à réaliser en cas de pièce jointe spécifique. Les actions possibles sont Accept (accepter la pièce jointe) et Block (bloquer la pièce jointe comme indiqué dans la page de l'onglet Action).

- ***Description*** – la description de la pièce jointe est incluse dans ce champ.

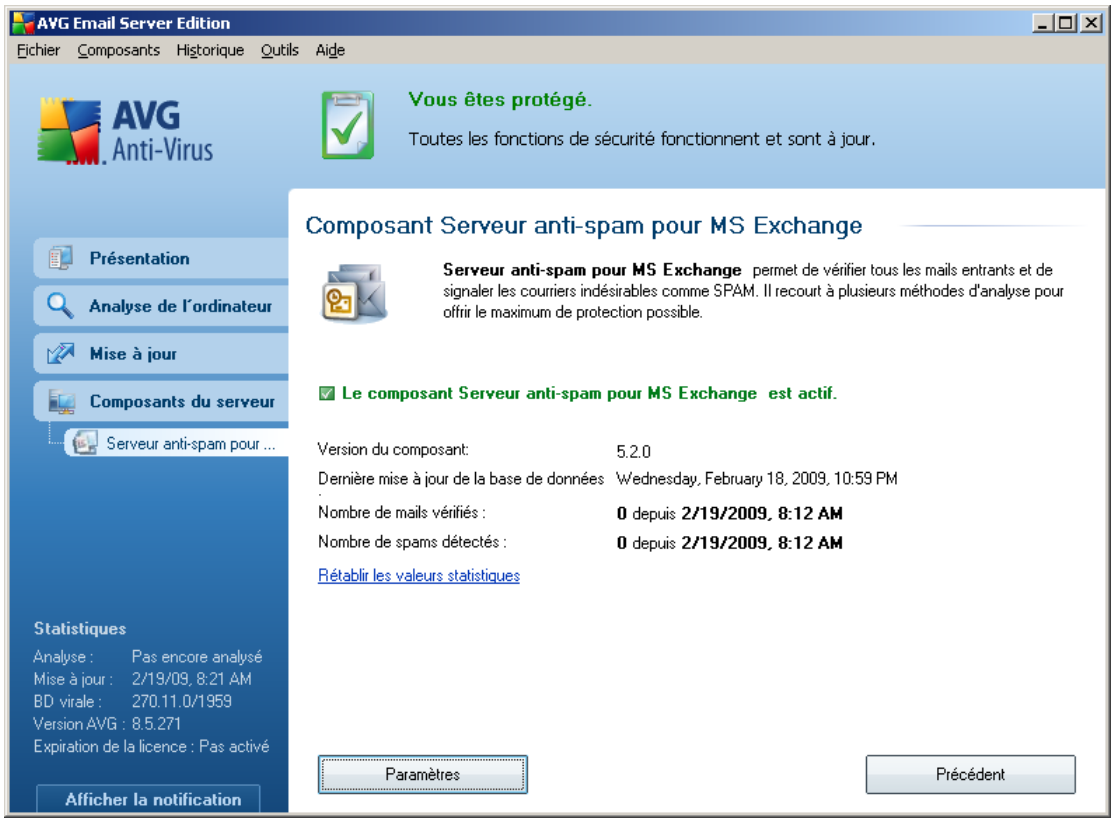
Pour enlever un élément de la liste, cliquez sur le bouton Remove (Supprimer). Vous pouvez insérer un élément dans la liste en cliquant sur le bouton ***Add...*** (Ajouter…). Vous pouvez aussi modifier un enregistrement en cliquant sur le bouton ***Edit...*** (Modifier…). La fenêtre suivante s'affiche alors :

- Dans le champ Description, vous pouvez décrire brièvement la pièce jointe à filtrer.
- Dans le champ If a mail message contains an attachment where (Si un mail contient une pièce jointe avec), vous choisissez le type de pièce jointe (File name ou MIME type). Vous pouvez également choisir une extension particulière dans la liste des extensions proposées ou la saisir directement avec des caractères génériques.

Dans le champ Then (Alors), déterminez si vous bloquez ou acceptez la pièce jointe.

8. Configuration anti-spam

8.1. Interface de l'Anti-Spam



Vous trouverez la boîte de dialogue du composant du ***serveur*** anti-spam dans la section ***Composants du serveur*** (menu de gauche). Celle-ci contient des informations sur la fonctionnalité du composant du serveur et des informations sur son état actuel (Le composant *Anti-Spam Server pour MS Exchange est actif.*) ainsi que des statistiques.

Vous pouvez redéfinir les statistiques en cliquant sur la référence ***Redéfinir les valeurs statistiques***.

Les boutons qui fonctionnent sont les suivants :

- ***Paramètres*** - utilisez ce bouton pour ouvrir l'option Paramètres anti-spam.

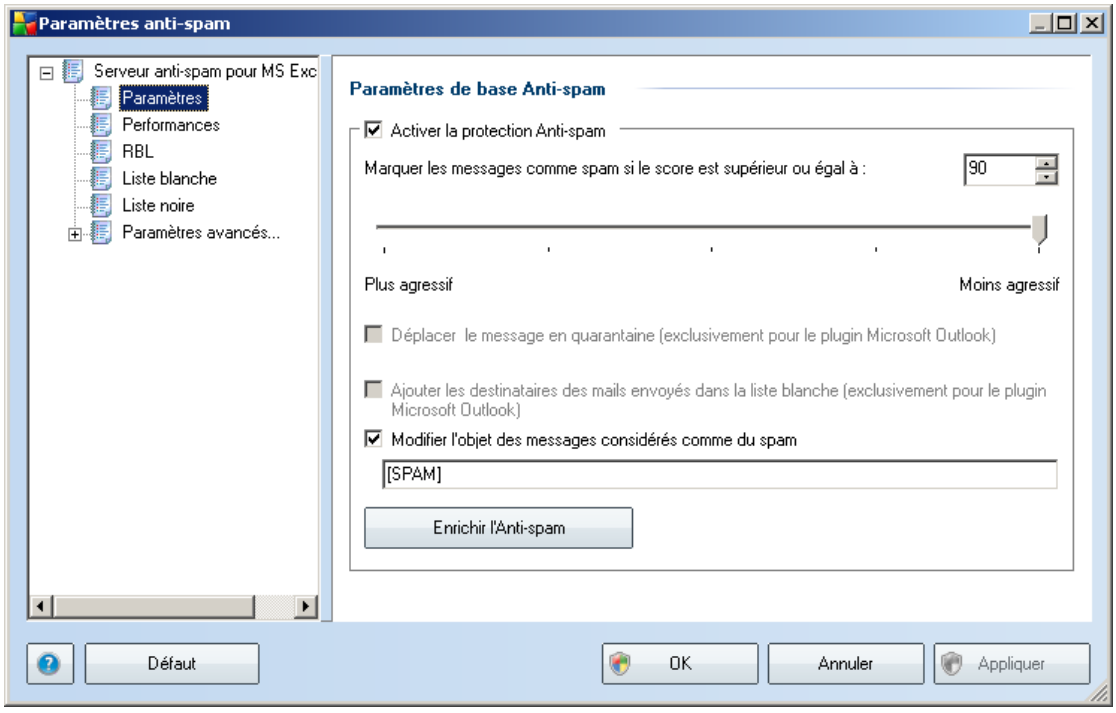
- ***Retour*** - appuyez sur ce bouton pour retourner à Présentation des composants du serveur.

8.2. Principes de l'Anti-Spam

Le terme « spam » désigne un message indésirable ; il s'agit généralement d'un produit ou d'un service à caractère publicitaire envoyé en masse à de nombreuses adresses électroniques ayant pour conséquence d'encombrer les boîtes aux lettres des destinataires. Il faut distinguer le spam des autres messages commerciaux légitimes que les consommateurs consentent à recevoir. Non seulement le spam peut être gênant, mais il est également à l'origine d'escroqueries, de virus ou de contenu pouvant heurter la sensibilité de certaines personnes.

Le composant Anti-Spam vérifie tous les mails entrants et signale les courriers indésirables comme SPAM. Le composant utilise plusieurs méthodes d'analyse pour traiter chaque mail afin d'offrir un niveau de protection maximal contre les messages indésirables.

8.3. Paramètres de l'anti-spam



Dans la boîte de dialogue ***Paramètres de base anti-spam***, cochez la case ***Activer***

la protection anti-spam pour autoriser/interdire l'analyse anti-spam dans les communications par e-mail.

Cette boîte de dialogue permet aussi de sélectionner des mesures de contrôle plus ou moins strictes en matière de contrôle anti-spam. Le composant ***Anti-Spam*** attribue à chaque message un score (*déterminant la présence de SPAM*) éventuel, en recourant à plusieurs techniques d'analyse dynamiques. Pour régler le paramètre ***Marquer les messages comme spams si le score est supérieur ou égal à***, saisissez le score qui convient (*de 0 à 100*) ou faites glisser le curseur vers la gauche ou vers la droite (*de 50 à 90*).

Il est généralement recommandé de choisir un seuil compris entre 50 et 90 et en cas de doute de le fixer à 90. Voici l'effet obtenu selon le score que vous définissez :

- ***Valeur 90-99*** - la plupart des messages entrants parviennent à leur destinataire (sans être considérés comme du spam). Les spams les plus faciles à reconnaître sont filtrés, mais vous risquez de laissez passer une quantité importante de spam.
- ***Valeur 80-89*** - les messages susceptibles d'être du spam sont identifiés par le filtre. Il est possible toutefois que certains messages valides soient détectés à tort comme du spam.
- ***Valeur 60-79*** - ce type de configuration est particulièrement strict. Tous les messages susceptibles d'être du spam sont identifiés par le filtre. Il est fort probable que certains messages anodins soient également rejetés.
- ***Valeur 1-59*** - ce type de configuration est très restrictif. Les messages qui ne sont pas du spam ont autant de chances d'être rejetés que ceux qui en sont vraiment. Ce seuil n'est pas recommandé dans des conditions normales d'utilisation.
- ***Valeur 0*** - dans ce mode, vous recevez uniquement les messages provenant des expéditeurs inscrits dans votre ***liste blanche***. Tout autre message est traité comme du spam. ***Ce seuil n'est pas recommandé dans des conditions normales d'utilisation.***

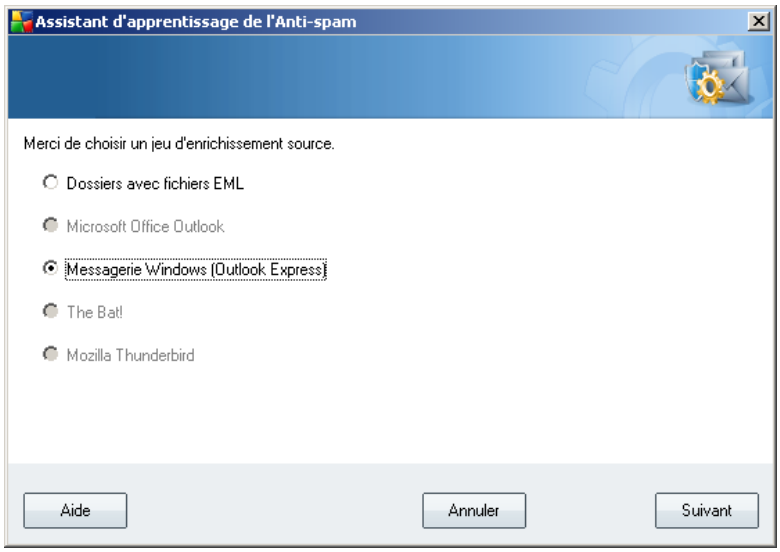
Vous pourrez également définir comment les e-mails spam détectés doivent être traités :

- ***Modifier l'objet des messages considérés comme spam*** - cochez cette case pour que tous les messages détectés comme du spam soient signalés à l'aide d'un mot ou d'un caractère particulier dans l'objet du message. Le texte souhaité doit être saisi dans la zone de texte activée.

Le bouton Enrichir l'anti-spam lance l'***Assistant d'enrichissement anti-spam***, décrit de façon détaillée dans le chapitre suivant.

8.3.1. Assistant d'enrichissement de l'anti-spam

Le premier écran de l'***Assistant d'enrichissement de l'anti-spam*** vous invite à sélectionner l'origine des messages contribuant à l'enrichissement. En général, vous utiliserez des mails signalés par erreur comme spam ou des messages indésirables qui n'ont pas été reconnus comme spam.



Plusieurs choix sont proposés :

- ***un client de messagerie spécifique*** - si vous utilisez un des clients répertoriés (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), sélectionnez l'option correspondante

- ***Dossiers avec fichiers EML*** - si vous utilisez un autre programme de messagerie, commencez par enregistrer les messages dans un dossier (format *.eml*) ou assurez-vous que vous connaissez l'emplacement des dossiers dans lesquels sont stockés les messages du client de messagerie. Sélectionnez ensuite l'option ***Dossiers avec fichiers EML***, qui permet de spécifier le dossier désiré à l'étape suivante

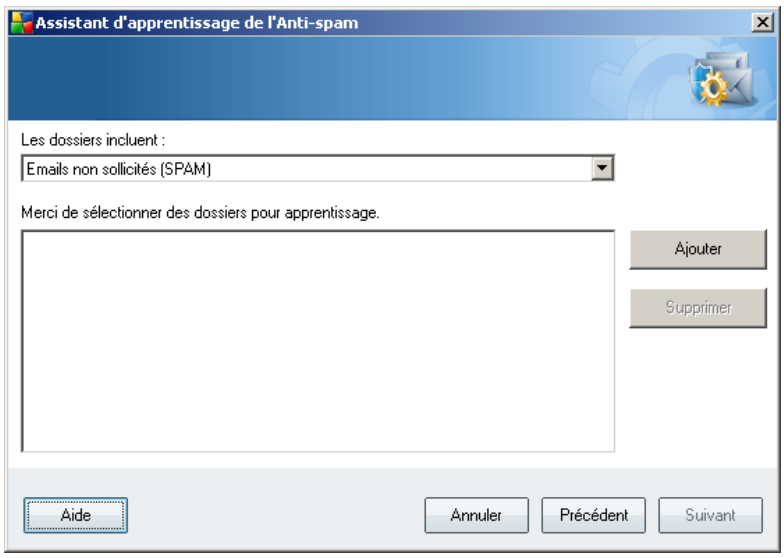
Pour faciliter et accélérer le processus d'enrichissement, il est judicieux de trier préalablement les mails dans les dossiers de façon à ne conserver que les messages pertinents (messages sollicités ou indésirables). Cela n'est toutefois pas absolument nécessaire car vous pourrez filtrer les messages par la suite.

Sélectionnez l'option qui convient, puis cliquez sur le bouton ***Suivant*** pour continuer l'assistant.

8.3.2. Sélection du dossier contenant les messages

La boîte de dialogue qui s'affiche à cette étape dépend de votre précédente sélection.

Dossiers avec fichiers EML



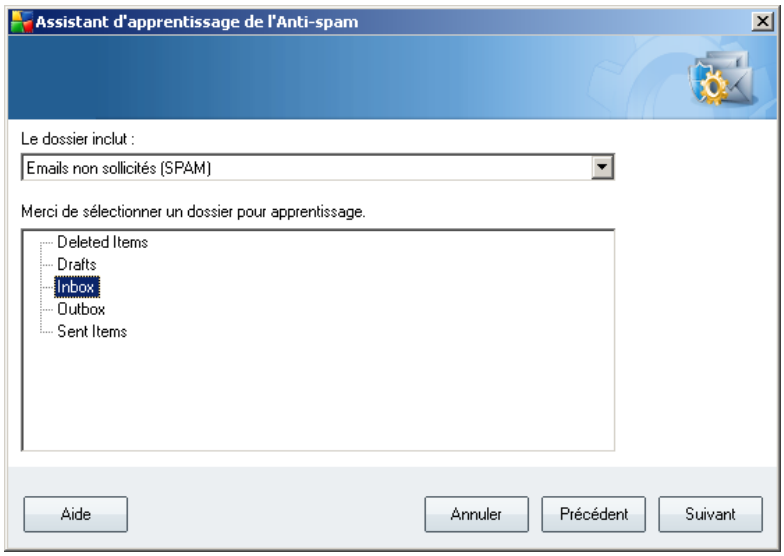
Dans cette boîte de dialogue, sélectionnez le dossier contenant les messages à utiliser pour la procédure d'enrichissement. Cliquez sur le bouton ***Ajouter*** pour localiser le dossier contenant les fichiers .eml (*messages e-mail enregistrés*). Le dossier sélectionné apparaît dans la boîte de dialogue.

Dans la liste déroulante ***Les dossiers incluent***, choisissez l'une des deux options pour préciser si le dossier sélectionné contient des messages sollicités (*HAM*) ou des messages indésirables (*SPAM*). Notez que vous aurez la possibilité de filtrer les messages à l'étape suivante. Il n'est donc pas indispensable que le dossier contienne exclusivement des messages pertinents pour l'enrichissement de la base de données anti-spam. Vous pouvez également enlever de la liste les dossiers qui ne vous intéressent pas en cliquant sur le bouton ***Supprimer***.

Lorsque c'est fait, cliquez sur ***Suivant*** et passez aux ***options de filtrage des messages***.

Client de messagerie spécifique

Lorsque vous avez choisi une option, une nouvelle boîte de dialogue apparaît.

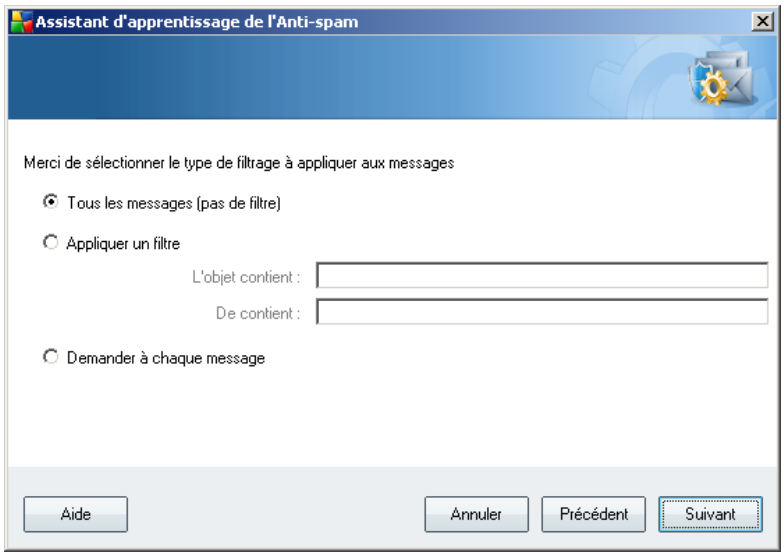


Remarque : *si vous avez opté pour Microsoft Office Outlook, vous devrez d'abord sélectionner le profil MS Office Outlook.*

Dans la liste déroulante ***Les dossiers incluent***, optez pour l'une des options pour préciser si le dossier sélectionné contient des messages valides (*HAM*) ou indésirables (*SPAM*). Notez que vous aurez la possibilité de filtrer les messages à l'étape suivante. Il n'est donc pas indispensable que le dossier contienne exclusivement des messages pertinents pour l'enrichissement de la base de données anti-spam. L'arborescence du client de messagerie sélectionné figure déjà dans la partie centrale de la boîte de dialogue. Localisez le dossier désiré dans l'arborescence et mettez-le en surbrillance.

Une fois fait, cliquez sur ***Suivant*** et passez aux ***options de filtrage des messages***.

8.3.3. Options de filtrage des messages



Dans cette boîte de dialogue, vous définissez la manière dont sont filtrés les messages.

Si vous êtes sûr que le dossier sélectionné n'inclut que des messages utiles pour l'enrichissement, sélectionnez l'option ***Tous les messages (sans filtrage)***.

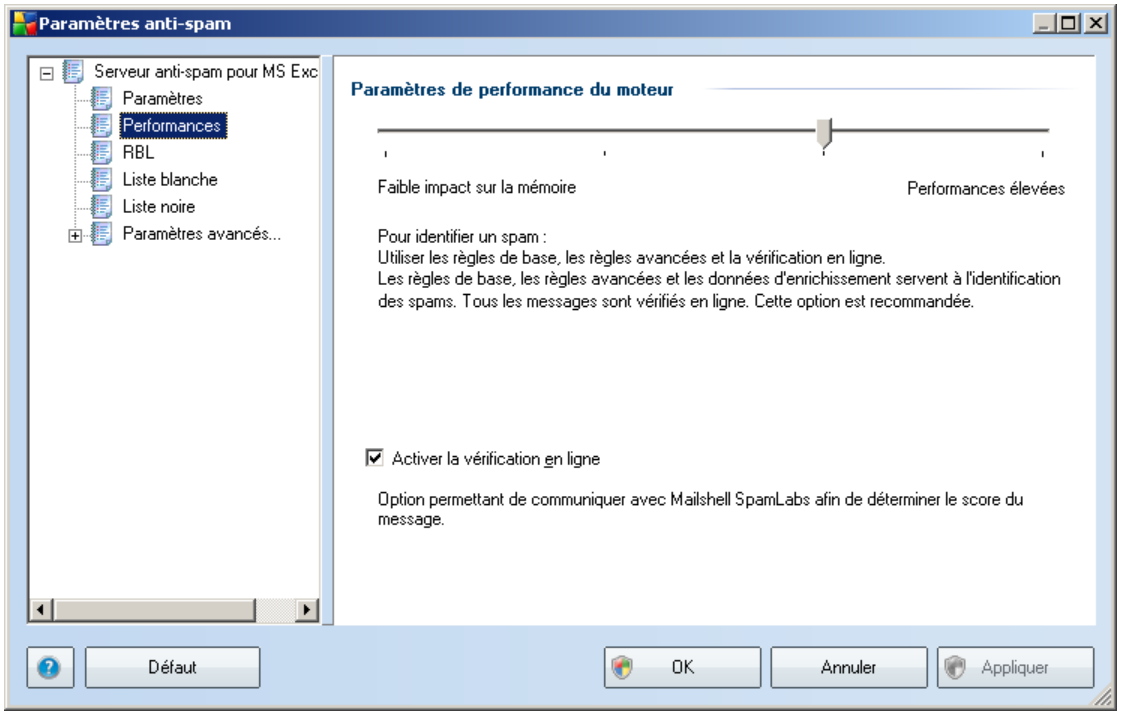
En cas de doute sur les messages contenus dans le dossier ou si vous voulez que l'assistant vous interroge pour chaque message (de manière à décider si le message en question contribue à l'enrichissement ou non de l'anti-spam), sélectionnez l'option ***Demander à chaque message***.

Pour accéder aux options avancées du filtrage, activez l'option ***Utiliser le filtre***. Vous pouvez spécifier un mot (*nom*), une partie d'un mot ou une phrase à rechercher dans l'objet des messages et/ou dans le champ de l'expéditeur. Tous les messages correspondant exactement aux critères définis seront utilisés pour l'enrichissement de la base de données sans autre message de la part du programme.

Attention ! : *Lorsque vous renseignez les deux zones de texte, les adresses correspondant à une seule des conditions sont aussi utilisées.*

Une fois l'option adéquate sélectionnée, cliquez sur ***Suivant***. La boîte de dialogue suivante, fournie à titre d'information uniquement, indique que l'assistant est prêt à traiter les messages. Pour commencer l'enrichissement, cliquez de nouveau sur le bouton ***Suivant***. L'enrichissement est déclenché et fonctionne selon les paramètres sélectionnés.

8.4. Performances



La boîte de dialogue ***Paramètres de performance du moteur*** (*associée à l'entrée* ***Performances*** *de l'arborescence de navigation de gauche*) présente les paramètres de performances du composant ***Anti-Spam***. En faisant glisser le curseur vers la gauche ou la droite, vous faites varier le niveau de performances de l'analyse depuis le mode ***Faible impact sur la mémoire*** jusqu'au mode ***Performances élevées***.

- ***Faible impact sur la mémoire*** - Pendant le processus d'analyse destiné à identifier le spam, aucune règle n'est appliquée. Seules les données d'enrichissement sont utilisées pour l'identification de spam. Ce mode ne convient pas pour une utilisation standard, sauf si votre ordinateur est peu véloce.

- ***Performances élevées*** - Ce mode exige une quantité de mémoire importante. Pendant l'analyse destinée à identifier le spam, les fonctions suivantes seront utilisées : règles et cache de base de données de spam, règles standard et avancées, adresses IP et bases de données de l'expéditeur de spam.

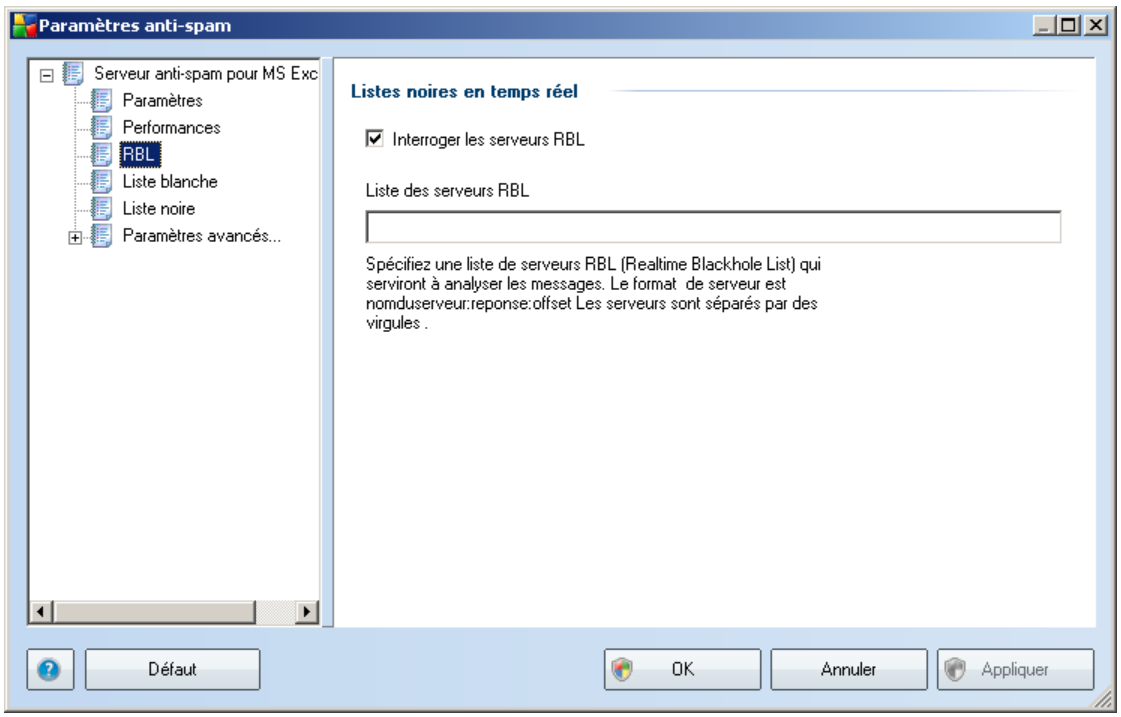
L'option ***Activer la vérification en ligne*** est sélectionnée par défaut. Cette configuration produit une détection plus précise du spam grâce à la communication

avec les serveurs Mailshell. En effet, les données analysées sont comparées aux bases de données en ligne Mailshell.

Il est généralement recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité. Tout changement de configuration ne doit être réalisé que par un utilisateur expérimenté.

8.5. RBL

L'entrée ***RBL*** ouvre une boîte de dialogue d'édition intitulée ***Listes noires en temps réel*** :



Dans cette boîte de dialogue, vous pouvez activer/désactiver la fonction ***Interroger les serveurs RBL***.

Le serveur RBL (*Realtime Blackhole List*) est un serveur DNS doté d'une base de données étendue d'expéditeurs de spam connus. Lorsque cette fonction est activée, tous les mails sont vérifiés par rapport à la base de données du serveur RBL et sont signalés comme du spam dès lors qu'ils sont identiques à une entrée de la base de données.

Les bases de données des serveurs RBL contiennent les signatures de spam les plus actuelles, qui leur permet d'assurer une détection anti-spam la plus exhaustive qui soit. Cette fonction est particulièrement utile pour les utilisateurs qui reçoivent de gros volumes de spams, qui ne sont pas détectés ordinairement par le moteur anti-Spam.

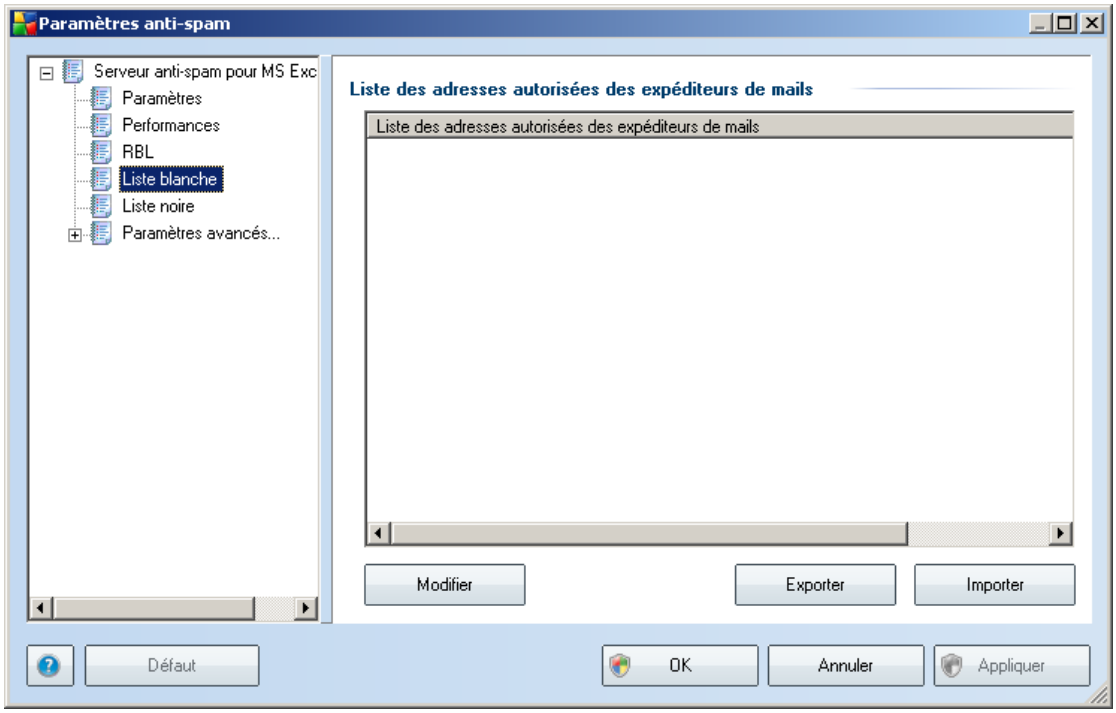
La ***liste des serveurs RBL*** permet de définir les emplacements des serveurs RBL. Par défaut, deux adresses de serveurs RBL sont spécifiées. Nous vous recommandons de conserver les paramètres proposés par défaut sauf si vous avez véritablement besoin de les modifier et si vous êtes un utilisateur expérimenté !

Remarque : *le fait d'activer cette fonction risque de réduire la vitesse de réception des mails sur certains systèmes et configurations, dans la mesure où chaque message est comparé au contenu de la base de données du serveur RBL.*

Notez qu'aucune donnée personnelle n'est transmise au serveur.

8.6. Liste blanche

L'entrée ***Liste blanche*** ouvre une boîte de dialogue contenant la liste globale des adresses d'expéditeurs et des noms de domaine approuvés dont les messages ne seront jamais considérés comme du spam.



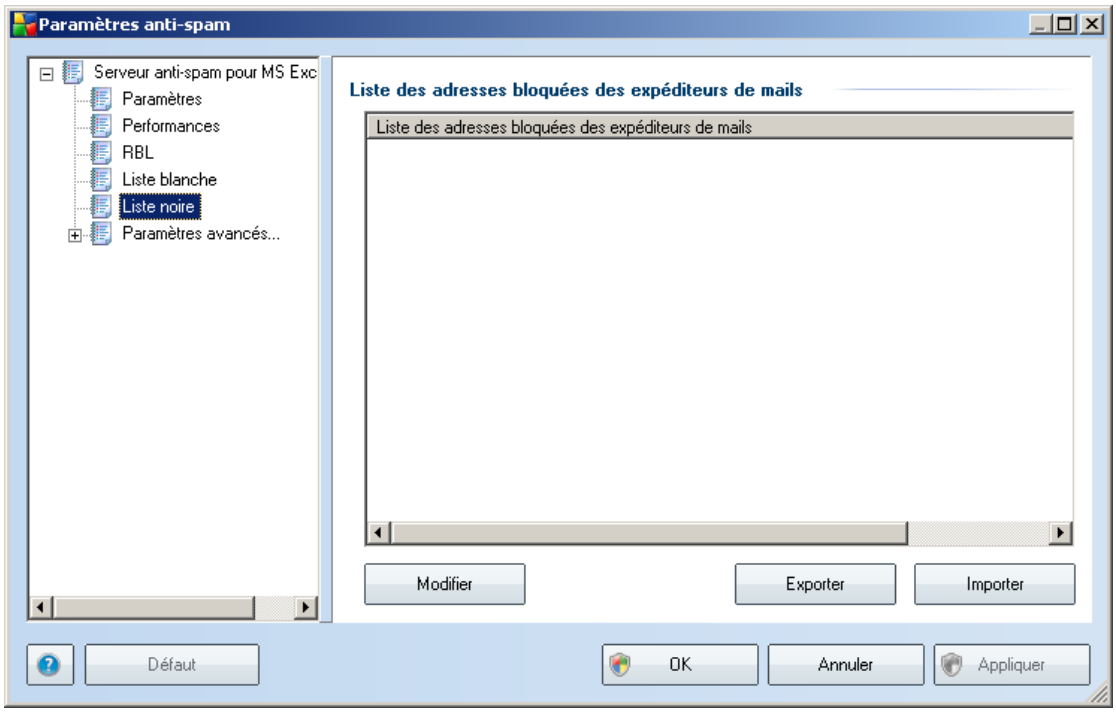
Dans l'interface d'édition, vous avez la possibilité d'établir la liste des expéditeurs qui ne vous enverront pas de messages indésirables(spam). De la même manière, vous pouvez dresser une liste de noms de domaine complets (*avg.fr*, par exemple) dont vous avez la certitude qu'ils ne diffusent pas de messages indésirables.

Lorsque vous disposez d'une liste d'expéditeurs et ou de noms de domaines, il ne vous reste plus qu'à l'incorporer selon l'une des méthodes suivantes : vous saisissez directement chaque adresse ou importez la liste entière. Vous avez accès aux boutons de fonction suivants :

- ***Modifier*** - cliquez sur ce bouton pour ouvrir une boîte de dialogue permettant de définir manuellement une liste d'adresses (la méthode *copier-coller* convient également). Insérez un élément (expéditeur, nom de domaine) par ligne.
- ***Importer*** - si vous avez déjà préparé un fichier texte d'adresses électroniques/ de noms de domaines, cliquez simplement sur ce bouton pour l'importer. Le fichier doit être au format texte brut et ne contenir qu'un seul élément (adresse, nom de domaine) par ligne.
- ***Exporter*** - si vous désirez exporter les enregistrements pour une raison quelconque, cliquez sur ce bouton. Tous les enregistrements seront conservés au format texte brut.

8.7. Liste noire

L'entrée ***Liste noire*** ouvre une boîte de dialogue contenant la liste globale des adresses d'expéditeurs et des noms de domaine bloqués dont les messages seront systématiquement considérés comme du spam.



Dans l'interface d'édition, vous avez la possibilité d'établir la liste des expéditeurs que vous jugez enclins à vous envoyer des messages indésirables (spam). De la même manière, vous pouvez dresser une liste de noms de domaine complets (*sociétédespam.com*, par exemple) dont vous avez reçu ou pensez recevoir des messages indésirables. Tous les mails des adresses ou domaines répertoriés seront alors identifiées comme des expéditeurs de spam.

Lorsque vous disposez d'une liste d'expéditeurs et ou de noms de domaines, il ne vous reste plus qu'à l'incorporer selon l'une des méthodes suivantes : vous saisissez directement chaque adresse ou importez la liste entière. Vous avez accès aux boutons de fonction suivants :

- ***Modifier*** - cliquez sur ce bouton pour ouvrir une boîte de dialogue permettant de définir manuellement une liste d'adresses (la méthode *copier-coller* convient également). Insérez un élément (expéditeur, nom de domaine) par ligne.

- ***Importer*** - si vous avez déjà préparé un fichier texte d'adresses électroniques/ de noms de domaines, cliquez simplement sur ce bouton pour l'importer. Le fichier doit être au format texte brut et ne contenir qu'un seul élément (adresse, nom de domaine) par ligne.

- ***Exporter*** - si vous désirez exporter les enregistrements pour une raison quelconque, cliquez sur ce bouton. Tous les enregistrements seront conservés au format texte brut.

8.8. Paramètres avancés

Il est généralement recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité. Tout changement de configuration ne peut être réalisé que par un utilisateur expérimenté.

Si vous pensez devoir modifier la configuration Anti-Spam à un niveau très avancé, conformez-vous aux instructions fournies dans l'interface utilisateur. Généralement, vous trouverez dans chaque boîte de dialogue une seule fonction spécifique que vous pouvez ajuster. Sa description figure toujours dans la boîte de dialogue elle-même :

- ***Cache*** - signature, réputation du domaine, réputation légitime

- ***Enrichissement*** - enrichissement par mots, historique des scores, score Offset, entrées maximales de mots, seuil d'enrichissement, pondération, tampon écriture

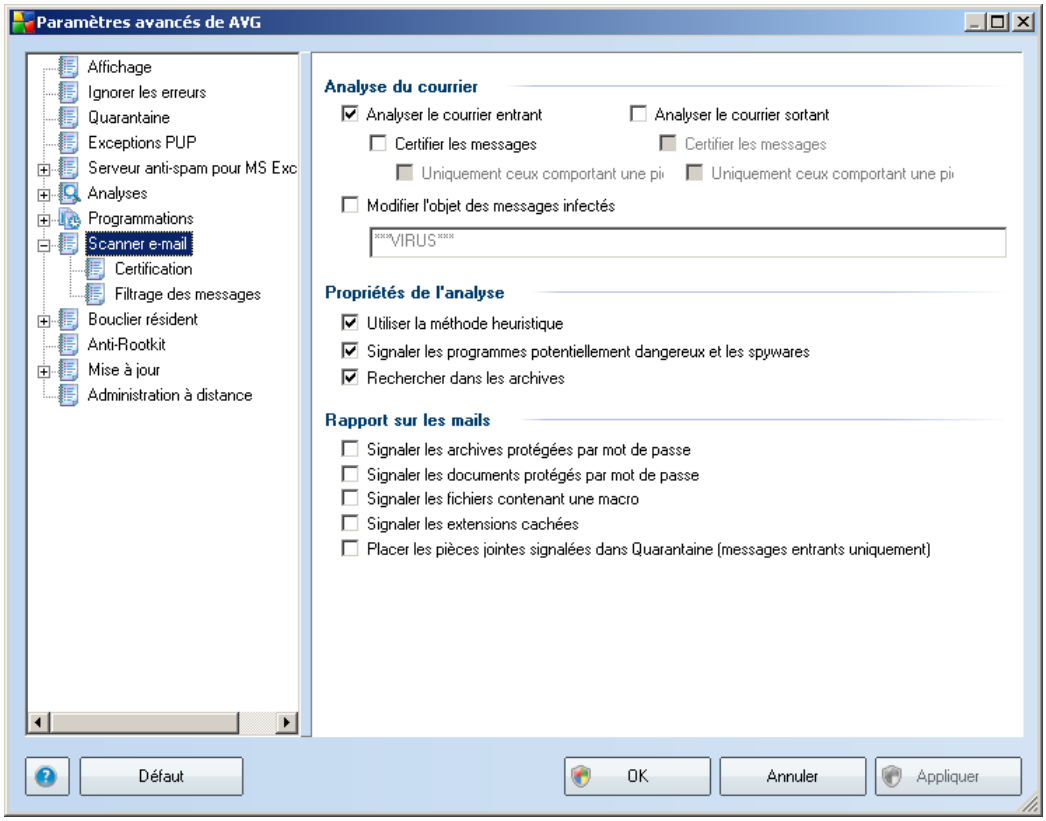
- ***Filtrage*** - liste des langues, liste des pays, adresses IP approuvées, adresses IP bloquées, pays bloqués, caractères bloqués, expéditeurs usurpés

- ***RBL*** - serveurs RBL, résultats multiples, seuil, délai, IP max.

- ***Connexion Internet*** - délai, serveur proxy, authentification du serveur proxy

9. Scanner e-mail

Les paramètres du ***Scanner e-mail*** sont configurés dans AVG Edition Serveur de messagerie. Dans le menu principal de l'application, sélectionnez ***Outils/Paramètres avancés***. Dans le menu gauche de la boîte de dialogue **Paramètres avancés**, cliquez sur **Scanner e-mail**.



La boîte de dialogue ***Scanner e-mail*** est divisée en trois parties :

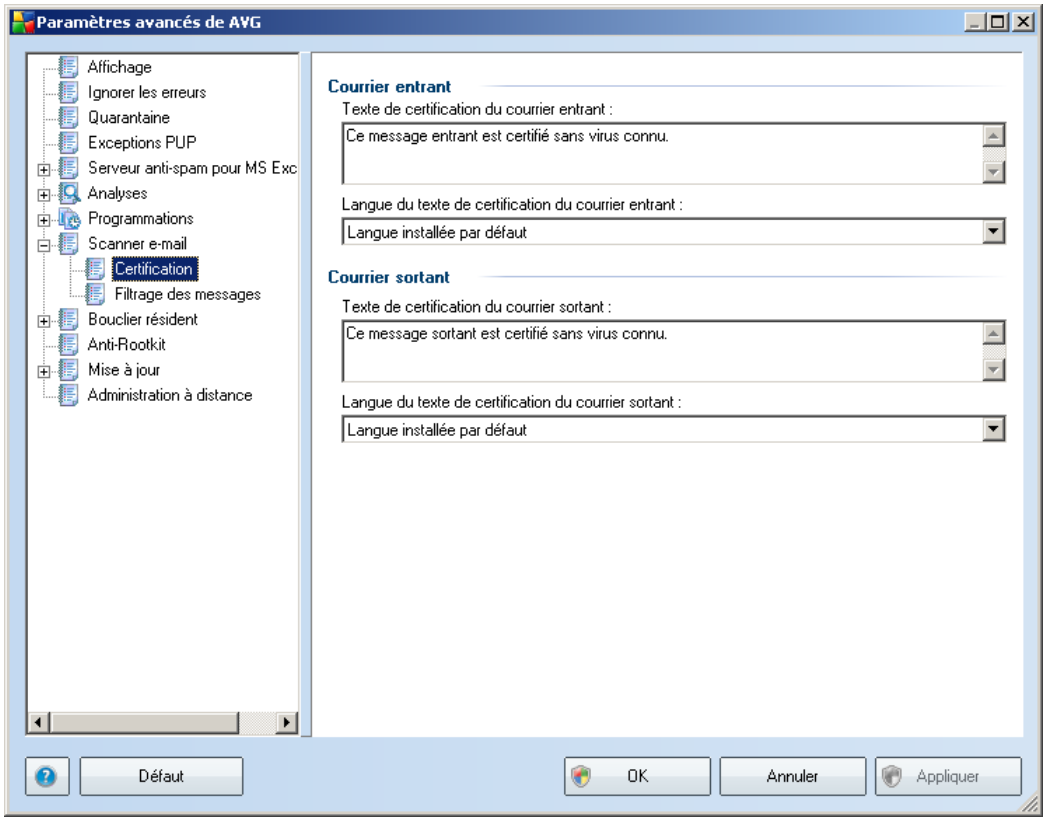
- ***Analyse du courrier*** - dans cette partie, indiquez si vous voulez analyser les messages entrants et/ou sortants et faire certifier tous les messages ou uniquement les messages avec pièces jointes (la *certification "courrier exempt de virus" n'est pas compatible avec le format HTML/RTF*). Vous pouvez aussi demander au programme AVG de modifier l'objet des messages présentant des risques d'infection. Cochez la case ***Modifier l'objet des messages infectés*** et adaptez le texte en conséquence (*le texte par défaut est ***VIRUS****).

- ***Propriétés de l'analyse*** - indiquez si la méthode heuristique doit être utilisée lors de l'analyse (***Utiliser la méthode heuristique***), si vous voulez vérifier la

présence de programmes potentiellement dangereux (***Signaler les programmes potentiellement dangereux et les spywares***) et si le contenu des archives doit être examiné (***Rechercher dans les archives***).

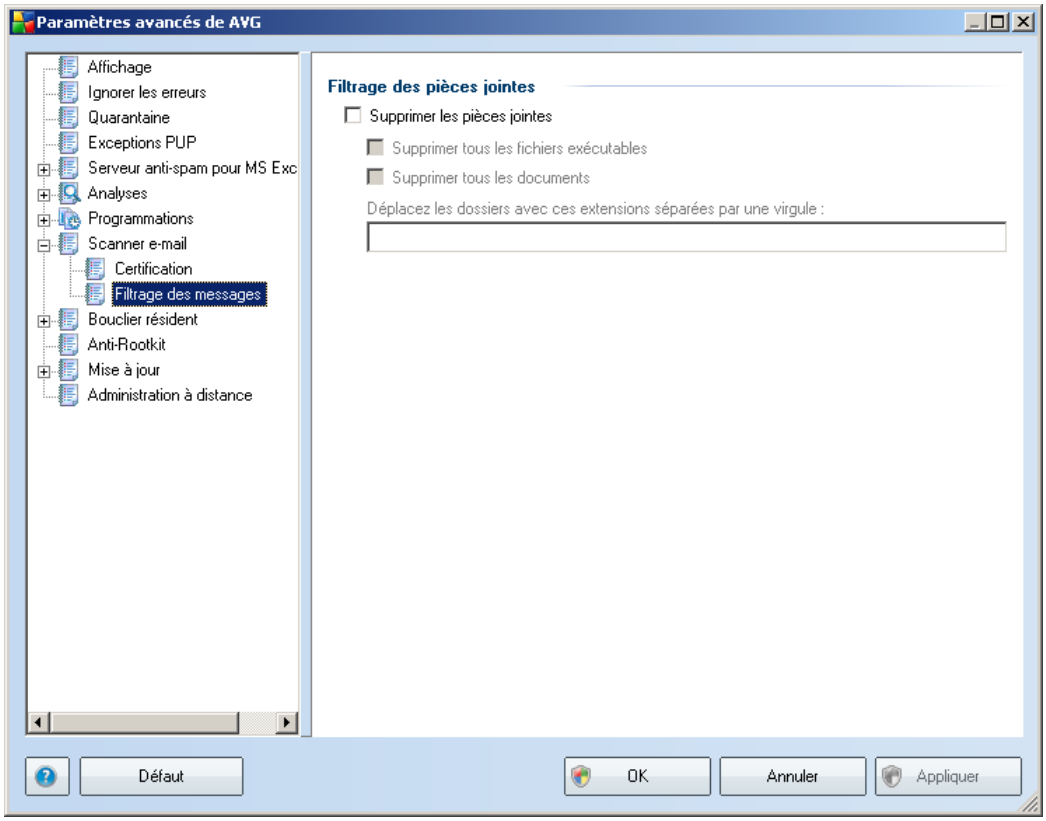
- ***Rapport sur les pièces jointes***- indiquez si vous voulez être averti par e-mail lorsque l'analyse d'un e-mail révèle la présence d'une archive protégée par mot de passe,d'un document protégé par mot de passe, d'une macro contenant un fichier et/ou d'un fichier dont l'extension est masquée. En l'occurrence, définissez si l'objet détecté doit être placé en ***quarantaine***.

9.1. Certification



La boîte de dialogue ***Certification*** vous permet de spécifier le contenu de la note de certification et de préciser la langue utilisée. Ce texte doit être entré séparément pour les ***messages entrants*** et pour les ***messages sortants***.

9.2. Filtrage des messages



La boîte de dialogue ***Filtrage des pièces jointes*** est destinée à vous aider à définir les paramètres de l'analyse des pièces jointes aux mails. Par défaut, l'option ***Supprimer les pièces jointes*** est désactivée. Si vous décidez de l'activer, toutes les pièces jointes signalées comme infectées ou potentiellement dangereuses sont automatiquement supprimées. Pour définir explicitement les types de pièces jointes à supprimer, sélectionnez l'option correspondante :

- ***Supprimer tous les fichiers exécutables*** - tous les fichiers *.exe seront supprimés
- ***Supprimer tous les documents***- tous les fichiers *.doc seront supprimés
- ***Supprimer les fichiers comportant les extensions suivantes séparées par une virgule*** - indiquez toutes les extensions de fichier correspondant aux fichiers à supprimer

10. FAQ et assistance technique

En cas de problème technique ou commercial avec votre produit AVG, vous pouvez consulter la section ***FAQ*** du site Web d'AVG à l'adresse www.avg.fr.

Si vous n'y trouvez pas l'aide dont vous avez besoin, vous pouvez aussi contacter notre service d'assistance technique par e-mail. Merci d'utiliser le formulaire réservé à cet effet, accessible depuis le menu du système, en passant par l'***Aide / Obtenir de l'aide en ligne***.