AVG Edition Serveur de Mail 2011

Manuel de l'utilisateur

Révision du document 2011.01 (22. 9. 2010)

Table des matières

1. Introduction

Ce manuel de l'utilisateur constitue la documentation complète du produit **AVG Edition Serveur de Mail 2011**.

Nous vous remercions d'avoir choisi le programme AVG Edition Serveur de Mail 2011.

AVG Edition Serveur de Mail 2011·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, la solution **AVG Edition Serveur de Mail 2011** 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.

Remarque :*cette documentation contient une description des fonctions spécifiques à l'Edition Serveur de Mail. Si vous avez besoin de plus d'informations sur d'autres fonctions AVG, consultez le manuel utilisateur de l'Edition Internet Security, plus exhaustive. Vous pouvez télécharger ce manuel du site Web d'AVG à l'adresse http://www.avg.com.*

2. Pré-requis à l'installation d'AVG

2.1. Systèmes d'exploitation pris en charge

AVG Edition Serveur de Mail 2011 sert à protéger les postes de travail fonctionnant avec les systèmes d'exploitation suivants :

- Windows 2008 Server Edition (x86 et x64)
- Windows 2003 Server (x86, x64) SP1

2.2. Serveurs de messagerie pris en charge

Les serveurs de messagerie suivants sont pris en charge :

- Version MS Exchange 2003 Server
- Version MS Exchange 2007 Server
- Version MS Exchange 2010 Server
- AVG pour Kerio MailServer – 6.7.2 et version ultérieure

2.3. Configuration matérielle

Voici la configuration matérielle minimale pour **AVG Edition Serveur de Mail 2011** :

- Processeur Intel Pentium 1,5 GHz
- 500 Mo d'espace disque dur (pour l'installation)
- 512 Mo libres de RAM

Voici la configuration matérielle minimale pour **AVG Edition Serveur de Mail 2011** :

- Processeur Intel Pentium 1,8 GHz
- 600 Mo d'espace disque dur (pour l'installation)
- 512 Mo libres de RAM

2.4. Désinstallation des versions précédentes

Si une version plus ancienne du programme AVG pour Serveur de Mail est installée, vous devrez la désinstaller manuellement avant de procéder à l'installation d'**AVG Edition Serveur de Mail 2011**. 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 AVG pour 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***

- Si vous avez déjà utilisé la version 8.x ou une version précédente du programme AVG, n'oubliez pas de désinstaller également les plug-ins de serveur.

  Remarque : *il sera nécessaire de redémarrer la banque d'informations durant la désinstallation.*

  Plug-in Exchange - exécutez setupes.exe avec le paramètre /uninstall dans le dossier d'installation du plug-in.

  Exemple : C:\AVG4ES2K\setupes.exe /uninstall

  Plug-in Lotus Domino/Notes - exécutez setupln.exe avec le paramètre / uninstall dans le dossier d'installation du plug-in.

  Exemple : C:\AVG4LN\setupln.exe /uninstall

2.5. Service Packs pour MS Exchange

Aucun Service Pack supplémentaire n'est nécessaire pour MS Exchange 2003 Server. 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 appliquant l'extension .delete. Elles seront supprimées au prochain redémarrage système.

Service Pack pour MS Exchange 2007 Server (facultatif) :

http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en

3. Processus d'installation d'AVG

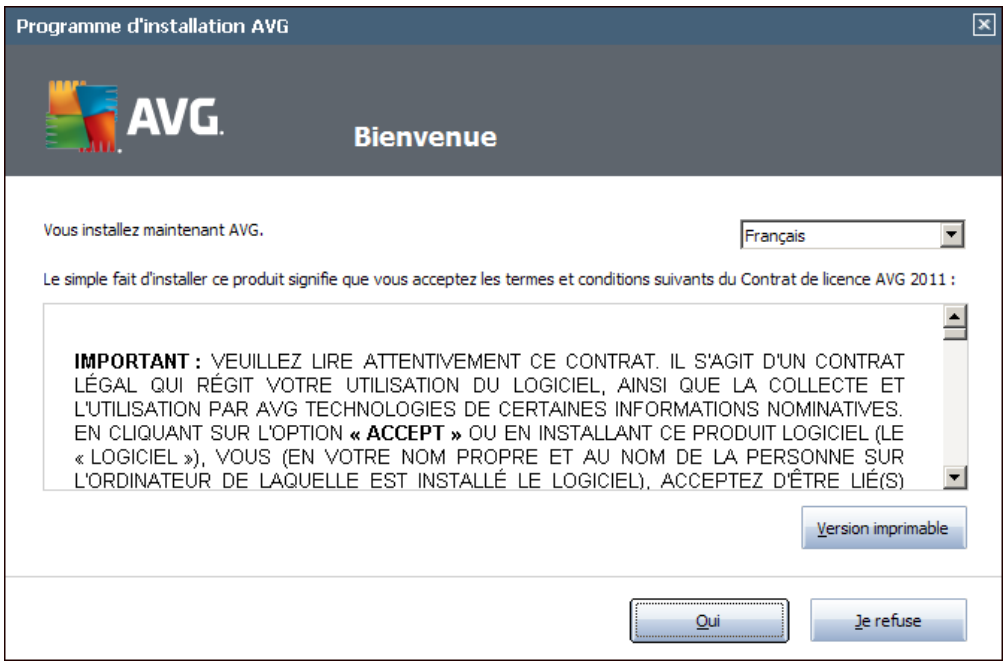
Pour installer AVG sur l'ordinateur, il est nécessaire d'obtenir le dernier fichier d'installation disponible. Vous pouvez utiliser le fichier d'installation figurant sur le CD et fourni avec votre édition, mais il est fort probable qu'il soit déjà périmé. En conséquence, nous vous recommandons de bien 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)

Remarque : *il existe deux fichiers d'installation pour votre produit, un pour les systèmes d'opération 32 bits (x86) et un pour les systèmes 64 bits (x64). Prenez garde d'utiliser le fichier adapté à votre système d'exploitation..*

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 figure dans 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 par l'affichage de l'écran ***Bienvenue***. Dans cet écran, vous choisissez la langue qui sera utilisée tout au long de la procédure d'installation et lisez les termes et conditions de la licence. Cliquez sur le bouton ***Version imprimable*** pour afficher le texte de la licence dans une nouvelle fenêtre.

Cliquez sur le bouton ***Oui*** pour donner votre consentement et passer à la boîte de dialogue suivante.

Attention : *vous aurez la possibilité de choisir des langues supplémentaires plus tard, au cours de l'installation.*

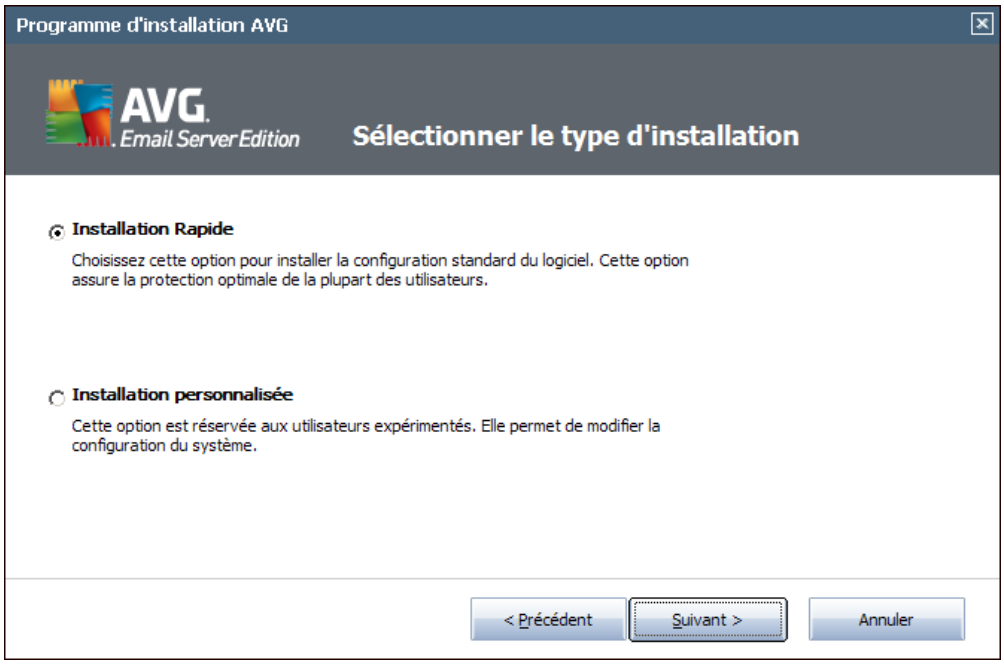
3.2. Activation de la licence

Dans la boîte de dialogue ***Activer votre licence***, vous devez indiquer votre numéro de licence.

Saisissez ensuite votre numéro de licence 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.

3.3. Sélection du type d'installation

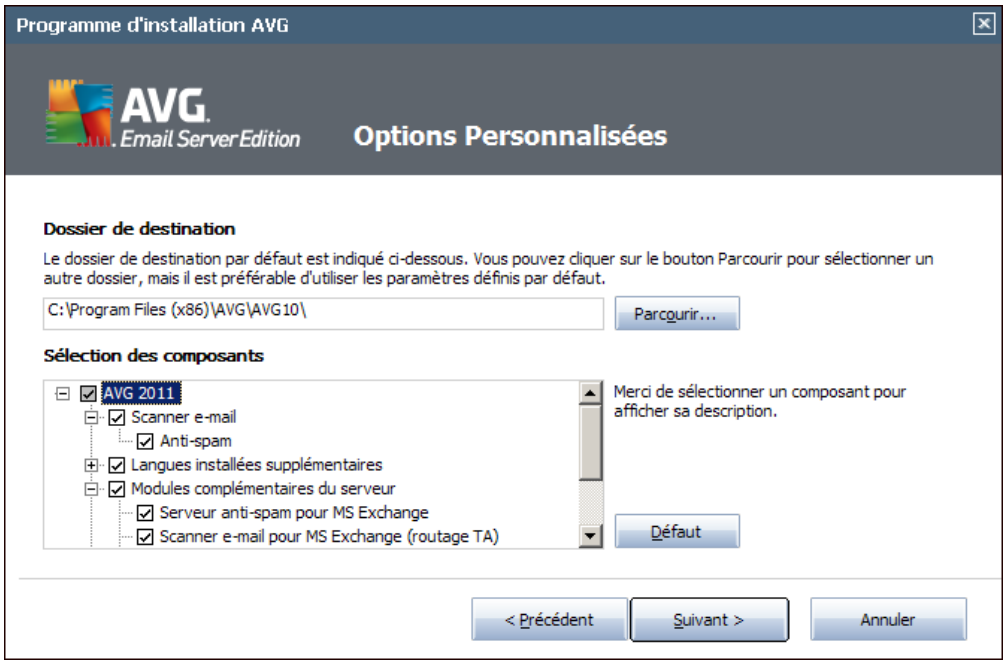


La boîte de dialogue ***Sélectionner le type d'installation*** propose deux modes d'installation : ***Installation rapide*** et ***Installation personnalisée***.

Dans la majorité des cas, il est recommandé d'opter pour l'***installation rapide***, qui installe automatiquement le programme AVG selon les paramètres prédéfinis par l'éditeur 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 exclusivement réservée aux utilisateurs expérimentés qui ont une raison valable d'installer AVG selon des paramètres non standard. Par exemple, cela leur permet d'adapter le programme à une configuration système spécifique.

3.4. Installation personnalisée - Options personnalisées



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 l'arborescence du lecteur, puis sélectionnez le répertoire souhaité.

La catégorie ***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.

- ***Client AVG Remote Admin*** - si vous voulez connecter AVG à une autre instance du Centre de données AVG (AVG Edition Réseau), sélectionnez cette option.

  Remarque : *seuls les composants pour serveurs figurant dans la liste peuvent être contrôlés à distance !*

- ***Gestionnaire des paramètres*** - outil principalement indiqué aux administrateurs réseau afin de copier, modifier et distribuer la configuration d'AVG. Vous pouvez enregistrer cette configuration sur un périphérique amovible (clé USB, etc.) et l'appliquer manuellement ou d'une autre façon aux stations choisies.

- ***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.

Présentation standard des différents composants serveur (***modules complémentaires du serveur***) :

- ***Serveur anti-spam pour MS Exchange***

  Le composant vérifie tous les mails entrants et marque 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.

- ***Scanner e-mail pour MS Exchange (agent de transport de routage)***

  Vérifie tous les messages électroniques entrants et sortants acheminés via le rôle MS Exchange HUB.

  Disponible pour MS Exchange 2007/2010 et peut être installé seulement dans le rôle HUB.

- ***Scanner e-mail pour MS Exchange (Agent de transport SMTP)***

  Vérifie tous les messages électroniques acheminés via l'interface MS Exchange SMTP.

  Disponible pour MS Exchange 2007/2010 seulement ; peut être installé dans les rôles EDGE et HUB.

- ***Scanner e-mail pour MS Exchange (VSAPI)***

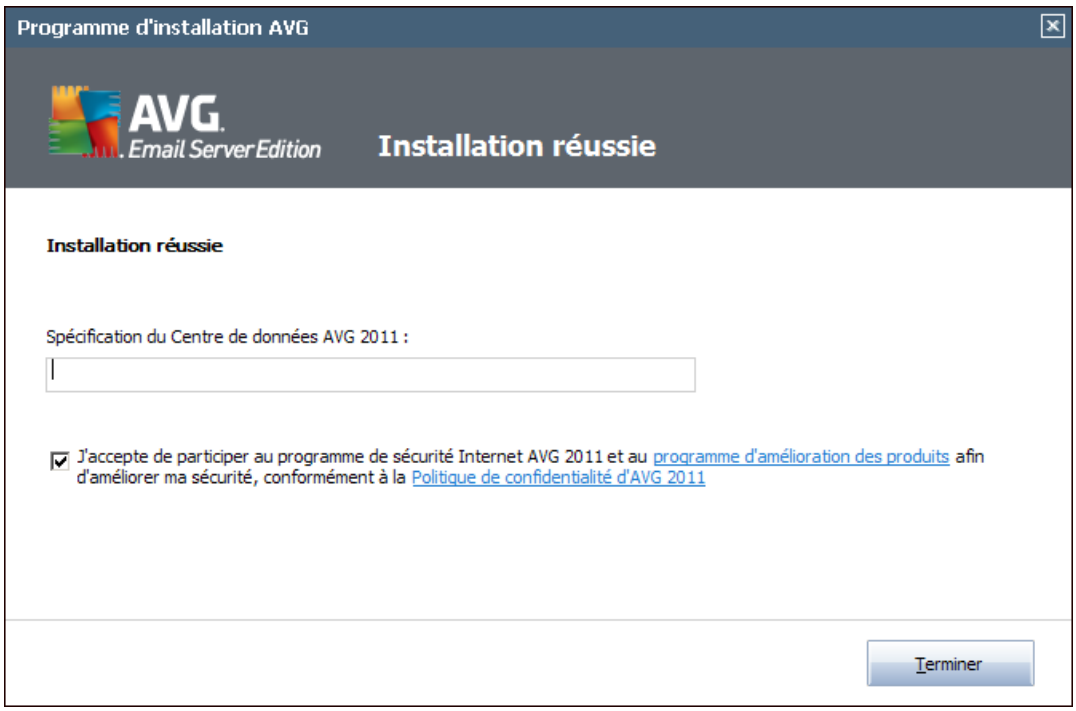
  Vérifie tous les messages électroniques stockés dans les boîtes de réception des utilisateurs. En cas de détection, les virus sont déplacés en quarantaine ou purement et simplement supprimés.

Remarque : *il existe différentes options pour les versions MS Exchange.*

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

3.5. Finalisation de l'installation

Si vous avez sélectionné le ***composant Administration à distance*** pendant la sélection des modules, vous pouvez définir dans cet écran la chaîne de connexion pour vous connecter à votre instance du Centre de données AVG.



AVG est maintenant installé sur l'ordinateur et est totalement opérationnel. Le programme s'exécute en arrière-plan en mode automatique.

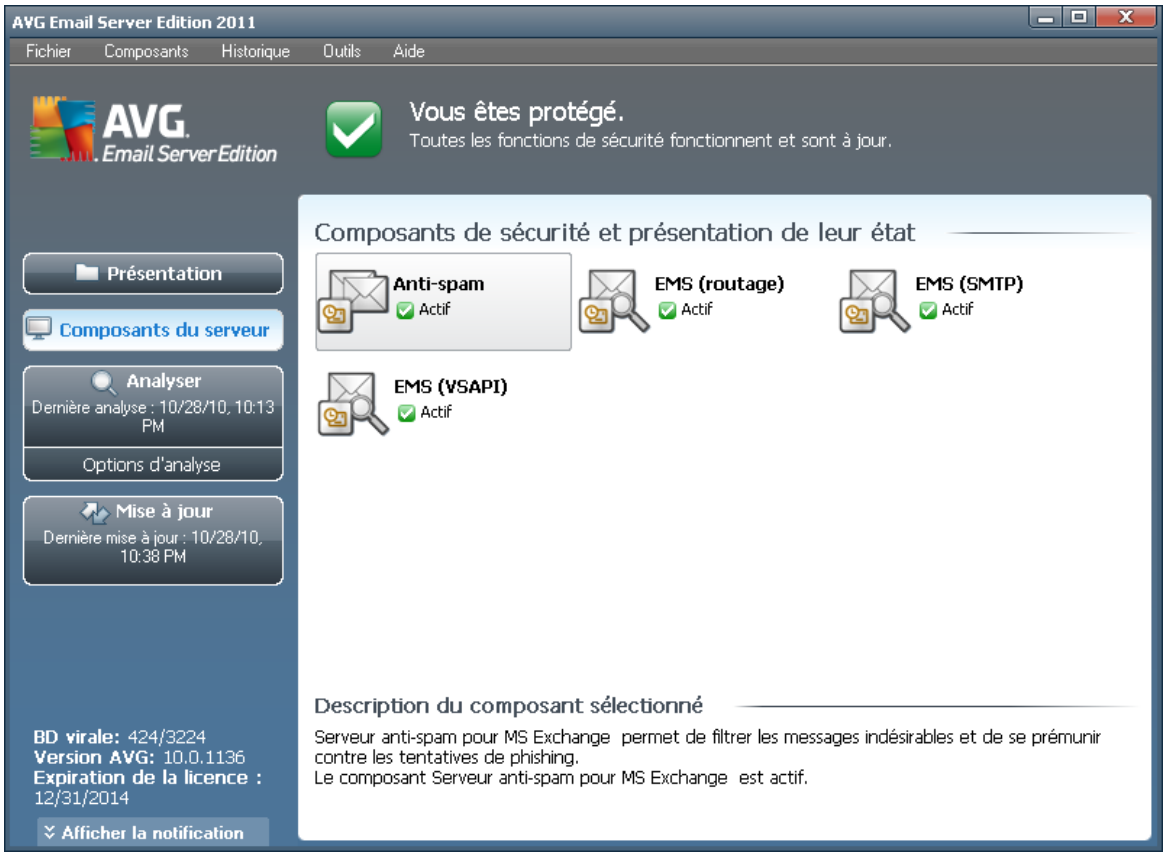
Pour configurer la protection de chacun de vos serveurs de messagerie, reportez-vous au chapitre approprié :

- ***Scanner e-mail pour MS Exchange Server 2007/2010***
- ***Scanner e-mail pour MS Exchange Server 2003***
- ***AVG pour Kerio MailServer***

4. Scanner e-mail pour MS Exchange Server 2007/2010

4.1. Présentation

Les options de configuration d'AVG pour MS Exchange Server 2007/2010 sont intégrées à AVG Edition Serveur de Mail 2011 comme composants du serveur.



Présentation standard des différents composants du serveur :

- ***Anti-Spam - Serveur anti-spam pour MS Exchange***

  Le composant vérifie tous les mails entrants et marque 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.

- ***EMS (routage) - Scanner e-mail pour MS Exchange (agent de transport de routage)***

  Vérifie tous les messages électroniques entrants et sortants acheminés via le rôle MS Exchange HUB.

Disponible pour MS Exchange 2007/2010 et ne peut être installé que dans le rôle HUB.

- ***EMS (SMTP) - Scanner e-mail pour MS Exchange (agent de transport SMTP)***

  Vérifie tous les messages électroniques acheminés via l'interface MS Exchange SMTP.

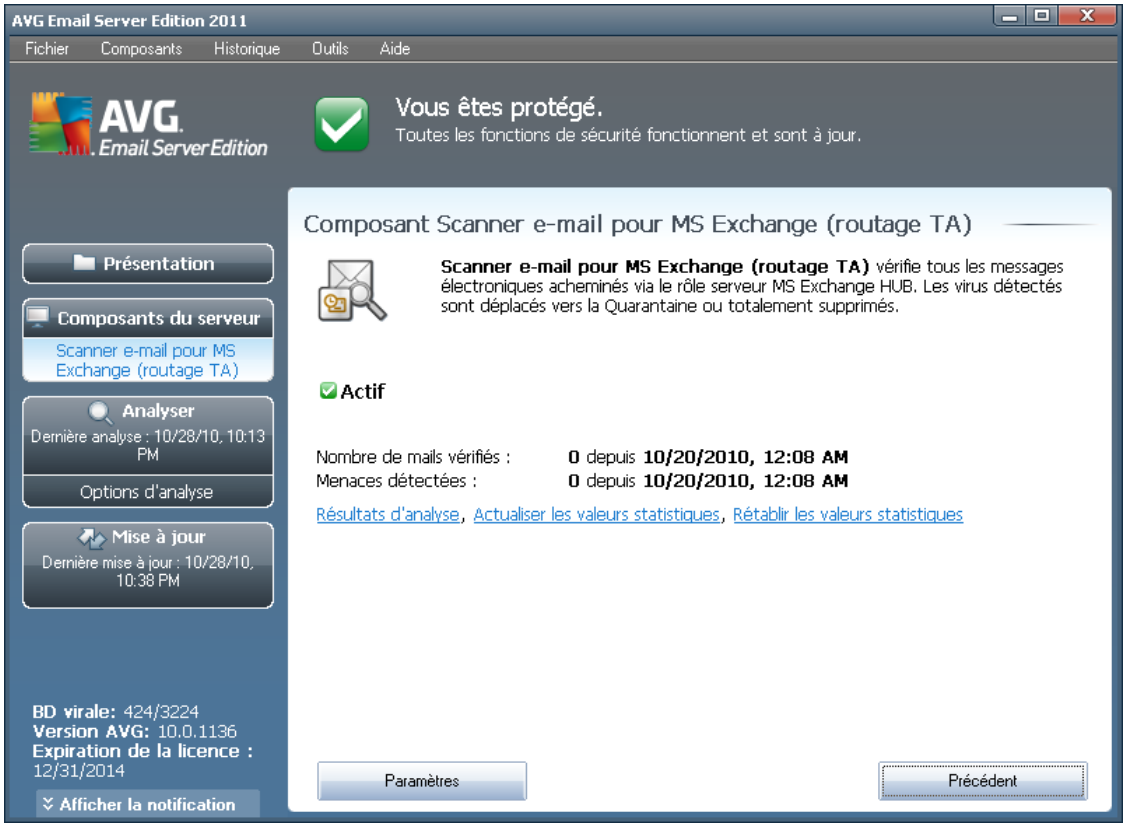
  Disponible pour MS Exchange 2007/2010 seulement ; peut être installé dans les rôles EDGE et HUB.

- ***EMS (VSAPI) - Scanner e-mail pour MS Exchange (VSAPI)***

  Vérifie tous les messages électroniques stockés dans les boîtes de réception des utilisateurs. En cas de détection, les virus sont déplacés en quarantaine ou purement et simplement supprimés.

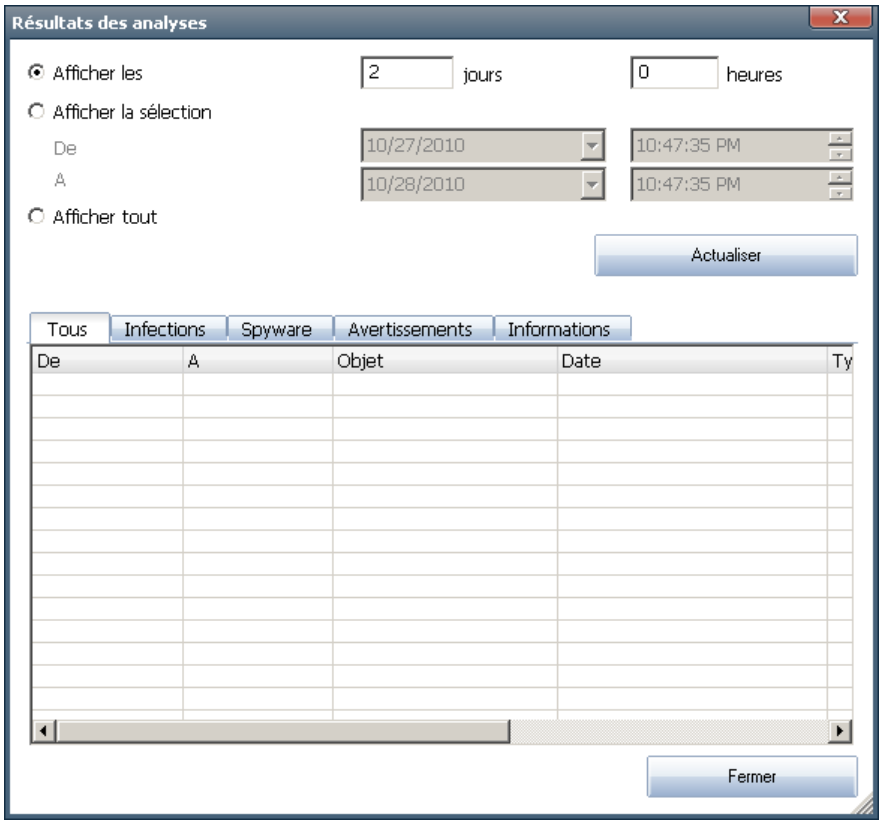
Remarque importante : *si vous décidez d'installer et d'utiliser VSAPI avec l'agent de transport de routage pour un rôle Hub Exchange, vos e-mails seront analysés à deux reprises. Pour éviter ceci, consultez la section* ***Notice technique*** *ci-dessous.*

Double-cliquez sur un composant pour ouvrir son interface. A l'exception de l'anti-spam, tous les composants partagent les boutons de commande et liens suivants :



- ***Résultats des analyses***

Ouvre une nouvelle boîte de dialogue dans laquelle vous pouvez examiner les résultats d'analyse :



Les messages sont classés selon leur gravité sous l'onglet approprié. Consultez la configuration de chaque composant afin de modifier la gravité et le signalement des messages.

Par défaut, seuls les résultats des deux derniers jours s'affichent. Vous pouvez modifier la période d'analyse en choisissant une des options suivantes :

- ***Afficher les*** - indiquez les jours et les heures de votre choix.
- ***Afficher la sélection*** - choisissez une heure et une plage de dates personnalisées.
- ***Afficher tout*** - affiche les résultats pour toute la période.

Utilisez le bouton ***Actualiser*** pour recharger les résultats en fonction des critères définis.

- ***Actualiser les valeurs statistiques*** - met à jour les statistiques affichées ci-dessus.
- ***Rétablir les valeurs statistiques*** - réinitialise toutes les statistiques.

Les boutons qui fonctionnent sont les suivants :

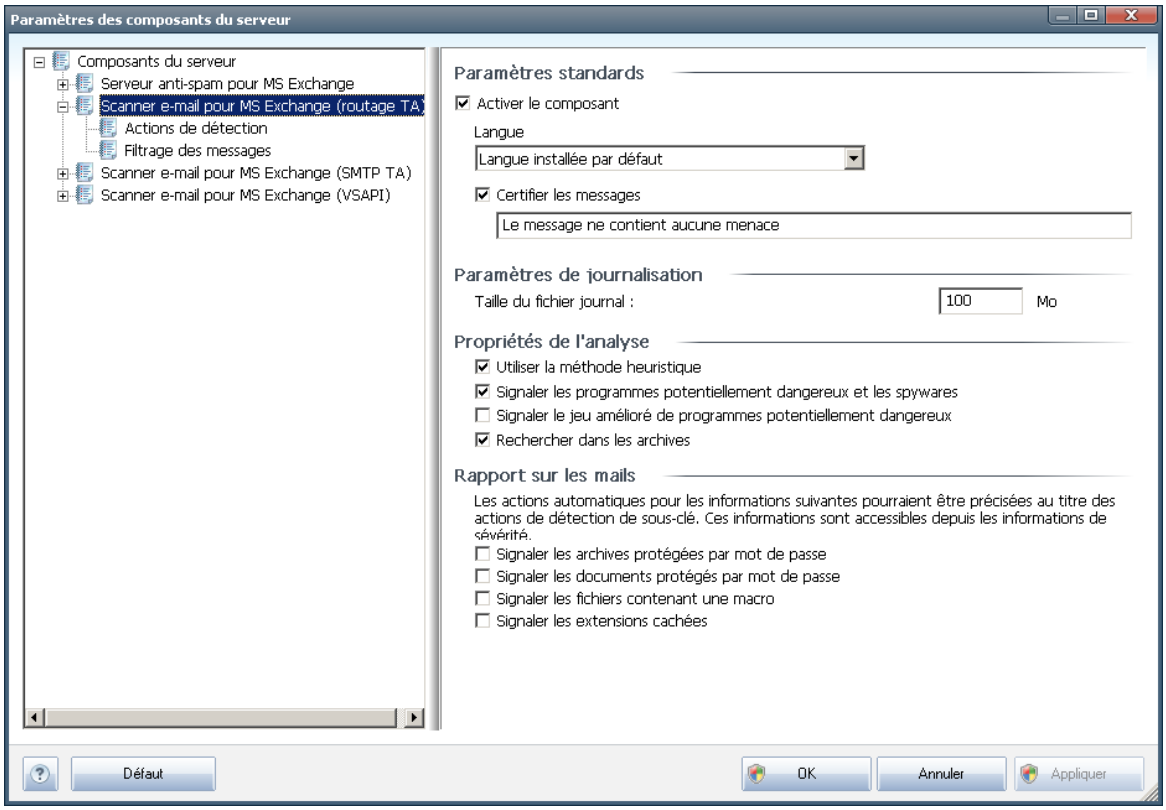
- ***Paramètres*** - ce bouton permet d'ouvrir les paramètres du composant.
- ***Précédent*** - cliquez sur ce bouton pour revenir à l'écran de présentation des composants du serveur.

Vous trouverez davantage d'informations sur les paramètres des composants dans les chapitres suivants.

4.2. Scanner e-mail pour MS Exchange (TA de routage)

Pour ouvrir les paramètres du ***Scanner e-mail pour MS Exchange (agent de transport de routage)***, cliquez le bouton ***Paramètres*** dans l'interface du composant.

Dans la liste ***Composants du serveur***, sélectionnez l'élément ***Scanner e-mail pour MS Exchange (TA de routage)*** :



La section ***Paramètres standard*** contient les options suivantes :

- ***Activer le composant*** - désélectionnez cette case pour désactiver intégralement le composant.
- ***Langue*** - choisissez la langue du composant.

- ***Certifier les messages*** - cochez cette option pour ajouter une note de certification à tous les messages analysés. Vous pouvez personnaliser le message dans le champ suivant.

La section ***Paramètres de journalisation*** :

- ***Taille du fichier journal*** - choisissez la taille du fichier journal. Valeur par défaut : 100 Mo.

La section ***Propriétés de l'analyse*** :

- ***Utiliser la méthode heuristique*** - cochez cette case pour activer la méthode heuristique lors de l'analyse.
- ***Signaler les programmes potentiellement dangereux et les spywares*** - cochez cette option pour signaler la présence de programmes potentiellement dangereux et de spywares.
- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** - cette option permet de détecter le jeu étendu des spywares : ces programmes ne posent aucun problème et sont parfaitement sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais peuvent ensuite être utilisés à des fins malveillantes. Il peut aussi s'agir de programmes absolument inoffensifs, mais qui sont inopportuns (barres d'outils, etc.). Il s'agit d'une mesure de sécurité et de convivialité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut. Remarque : cette fonction de détection complète l'option précédente. Aussi, si vous souhaitez bénéficiez d'une protection contre des types de spywares standards, veillez à toujours cocher la case précédente.
- ***Analyser les archives*** - cochez cette option afin que le scanner analyse également le contenu des fichiers archivés (zip, rar, etc.)

La section ***Rapports sur les pièces jointes*** vous permet de choisir les éléments à signaler lors de l'analyse. Si elle est cochée, tout message accompagné d'un tel élément contiendra l'étiquette [INFORMATION] dans l'objet du message. C'est la configuration par défaut qui peut être facilement modifiée dans la ***section Actions de détection***, partie ***Informations*** (voir ci-dessous).

Vous avez le choix entre les options suivantes :

- ***Signaler les archives protégées par mot de passe***
- ***Signaler les documents protégés par mot de passe***
- ***Signaler les fichiers contenant une macro***
- ***Signaler les extensions cachées***

L'arborescence suivante contient également ces sous-éléments :

- ***Actions de détection***
- ***Filtrage des messages***

4.3. Scanner e-mail pour MS Exchange (TA SMTP)

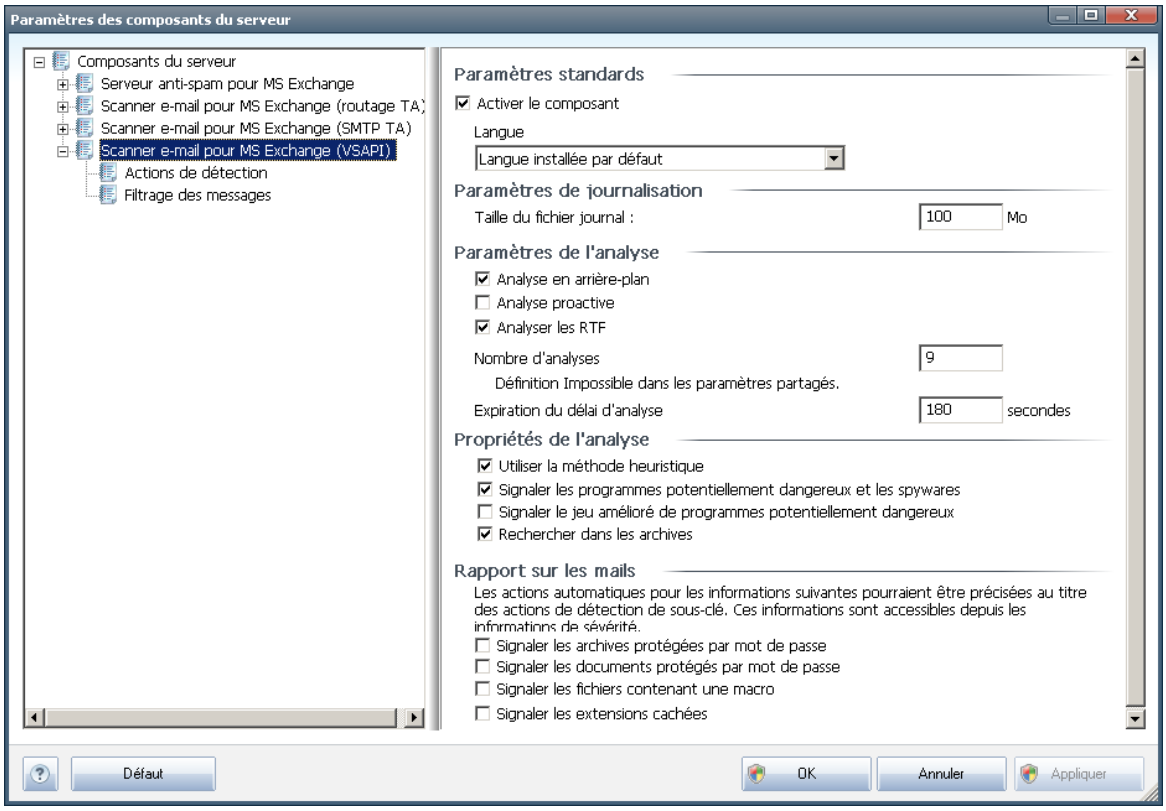
La configuration du composant ***Scanner e-mail pour MS Exchange (Agent de transport SMTP)*** est typiquement identique à celle de l'agent de transport de routage. Pour plus d'informations, reportez-vous au chapitre ci-dessus ***Scanner e-mail pour MS Exchange (TA de routage)***.

L'arborescence suivante contient également ces sous-éléments :

- ***Actions de détection***
- ***Filtrage des messages***

4.4. Scanner e-mail pour MS Exchange (VSAPI)

Cet élément contient les paramètres du composant ***Scanner e-mail pour MS Exchange (VSAPI)***.



La section ***Paramètres standard*** contient les options suivantes :

- ***Activer le composant*** - désélectionnez cette case pour désactiver intégralement le composant.

- ***Langue*** - choisissez la langue du composant.

La section ***Paramètres de journalisation*** :

- ***Taille du fichier journal*** - choisissez la taille du fichier journal. Valeur par défaut : 100 Mo.

Section ***Paramètres de l'analyse*** :

- ***Analyse en arrière-plan*** – 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 non encore analysé avec la dernière mise à jour de la base de données virale AVG est détecté dans les dossiers de courrier de l'utilisateur, il est envoyé à AVG pour Exchange 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.

- ***Analyse proactive (messages entrants)***

  Elle permet d'activer ou de désactiver l'analyse proactive de VSAPI 2.0/2.5. Cette analyse est lancée lorsqu'un élément est envoyé vers un dossier, mais elle s'exécute sans qu'un client n'en fasse la demande.

  Lorsque des messages sont transmis au service Exchange Store, ils sont placés dans la file d'attente globale en vue de leur analyse et sont considérés comme des éléments de faible priorité (nombre maximal : 30 éléments). Ils sont analysés en fonction de la méthode FIFO (premier arrivé, premier servi). Si un client accède à un élément de la file d'attente, la priorité de celui-ci augmente.

  Remarque : *les messages en surnombre resteront non analysés dans le service Store.*

Remarque :*même si vous désactivez les deux options, à savoir* ***Analyse en arrière-plan****et* ***Analyse proactive****, l'analyse sur accès reste toujours active lorsqu'un utilisateur tente de télécharger un message via le client MS Outlook.*

- ***Analyser RTF*** - permet de spécifier si les fichiers de type RTF doivent être analysés ou non.
- ***Nombre de threads d'analyse*** - par défaut, le processus d'analyse s'effectue par threads afin d'augmenter les performances globales de l'analyse et d'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.

Le nombre minimum de threads est calculé comme suit : ('nombre de processeurs'+1) divisé par 2.

Le nombre maximum de threads est calculé comme suit : 'Nombre de processeurs' multiplié par 5 + 1.

Si la valeur est minimale (moins importante) ou maximale (plus importante), la valeur par défaut est utilisée.

- ***Délai d'analyse*** - intervalle maximal continu (exprimé en secondes) durant lequel un thread tente d'accéder au message à analyser (la valeur par défaut est 180 secondes).

La section ***Propriétés de l'analyse*** :

- ***Utiliser la méthode heuristique*** - cochez cette case pour activer la méthode heuristique lors de l'analyse.
- ***Signaler les programmes potentiellement dangereux et les spywares*** - cochez cette option pour signaler la présence de programmes potentiellement dangereux et de spywares.
- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** - cette option permet de détecter le jeu étendu des spywares : ces programmes ne posent aucun problème et sont parfaitement sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais peuvent ensuite être utilisés à des fins malveillantes. Il peut aussi s'agir de programmes absolument inoffensifs, mais qui sont inopportuns (barres d'outils, etc.). Il s'agit d'une mesure de sécurité et de convivialité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut. Remarque : cette fonction de détection complète l'option précédente. Aussi, si vous souhaitez bénéficiez d'une protection contre des types de spywares standards, veillez à toujours cocher la case précédente.
- ***Analyser les archives*** - cochez cette option afin que le scanner analyse également le contenu des fichiers archivés (zip, rar, etc.)

La section ***Rapports sur les pièces jointes*** vous permet de choisir les éléments à signaler lors de l'analyse. La configuration par défaut peut être facilement modifiée dans la ***section Actions de détection***, partie ***Informations*** (voir ci-dessous).

Vous avez le choix entre les options suivantes :

- ***Signaler les archives protégées par mot de passe***
- ***Signaler les documents protégés par mot de passe***
- ***Signaler les fichiers contenant une macro***

- ***Signaler les extensions cachées***

En général, certaines fonctions 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, utilisez les liens suivants (et les liens accessibles à partir de ces liens de référence) :

  - 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.

L'arborescence suivante contient également ces sous-éléments :

- ***Actions de détection***

- ***Filtrage des messages***

4.5. Notice technique

Ces informations traitent de l'installation et de l'utilisation simultanée de VSAPI et d'un agent de transport de routage sur un rôle Hub Exchange. En pareille situation, vos e-mails sont analysés à deux reprises (par le scanner à la demande VSAPI, puis par l'agent de transport de routage).

En raison des modalités de fonctionnement de l'interface VSAPI, cela risque d'entraîner des incohérences au niveau des résultats d'analyses ainsi qu'une charge inutile. Ainsi, il est recommandé d'apporter une correction (voir procédure ci-dessous) pour remédier instantanément à ce problème de double analyse.

Remarque : *seuls les utilisateurs expérimentés peuvent ajuster le Registre. Avant toute modification du registre, il est recommandé d'en faire une copie de sauvegarde et de connaître les modalités de restauration dans l'éventualité d'un problème lié à sa modification.*

Ouvrez l'éditeur de Registre (dans Windows, menu ***Démarrer/Exécuter***, tapez ***regedit*** et appuyez sur la touche Entrée). Parcourez l'arborescence pour accéder à l'entrée suivante :

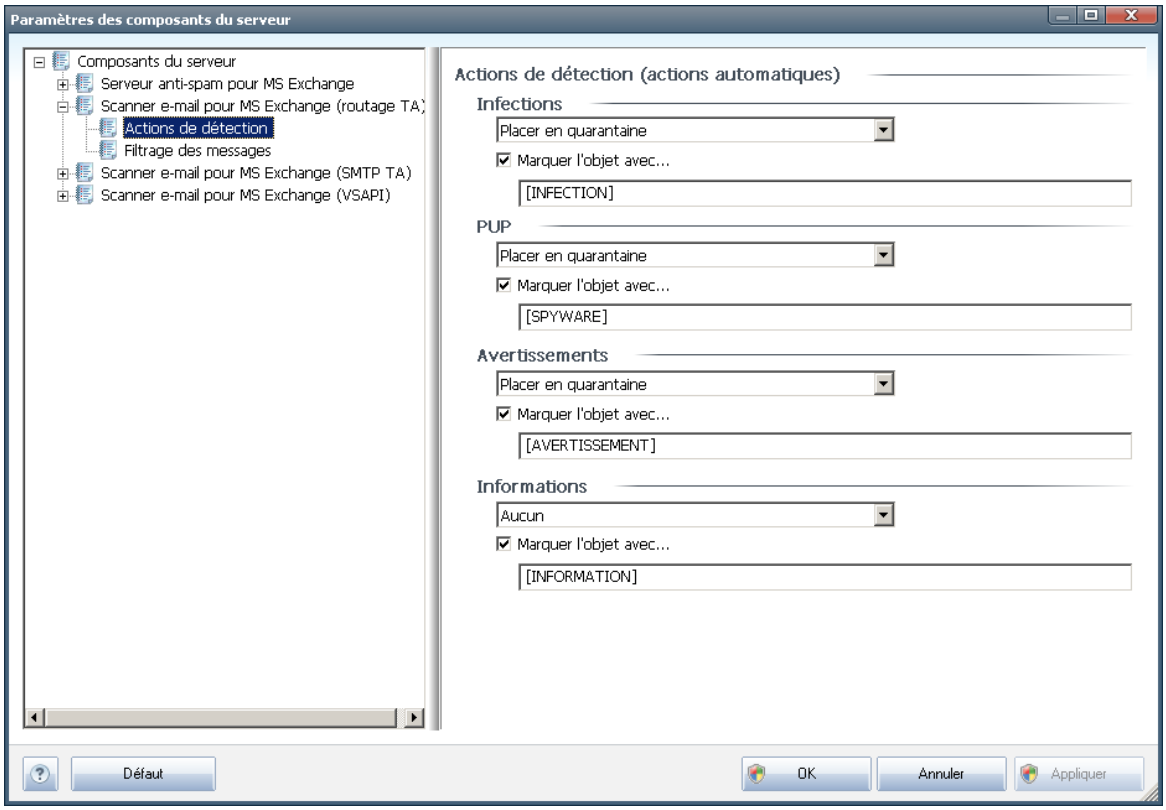
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan

Cliquez avec le bouton droit dans la partie droite de la fenêtre et, dans le menu contextuel, choisissez ***Nouveau/Valeur DWORD (32 bits)***. Nommez la nouvelle valeur ***TransportExclusion***. Double-cliquez dessus, puis remplacez sa valeur par ***1***.

Enfin, pour répercuter ce changement dans le serveur MS Exchange, définissez la valeur de ***ReloadNow*** sur 1. Pour ce faire, cliquer dessus et changez sa valeur.

Vous avez à présent désactivé l'analyse en sortie, par le scanner VSAPI. Cette modification doit prendre effet au bout de quelques minutes.

4.6. Actions de détection



Dans le sous-élément ***Actions de détection***, vous pouvez choisir les actions automatiques qui doivent se produire lors de la procédure d'analyse.

Ces actions sont disponibles pour les éléments suivants :

- ***Infections***
- ***PUP (programmes potentiellement dangereux)***
- ***Avertissements***
- ***Informations***

A partir du menu déroulant, choisissez l'action à effectuer pour chaque élément :

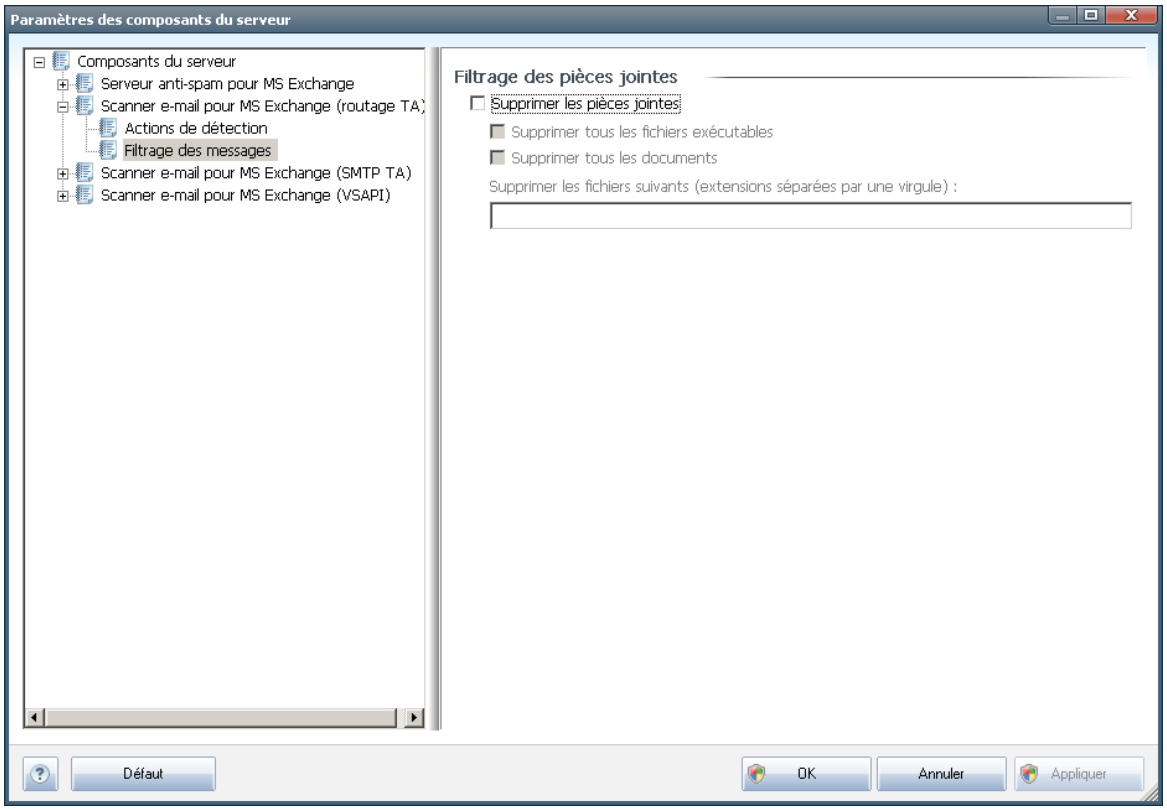
- ***Aucune*** - aucune action n'est effectuée.
- ***Placer en quarantaine*** - la menace est placée en Quarantaine.

- ***Supprimer*** - la menace est supprimée.

Pour sélectionner l'objet d'un message personnalisé contenant l'élément ou la menace donnée, cochez la case ***Marquer l'objet avec...***, puis entrez la valeur voulue.

Remarque :*La dernière fonction mentionnée n'est pas disponible pour Scanner e-mail pour MS Exchange VSAPI.*

4.7. Filtrage des messages



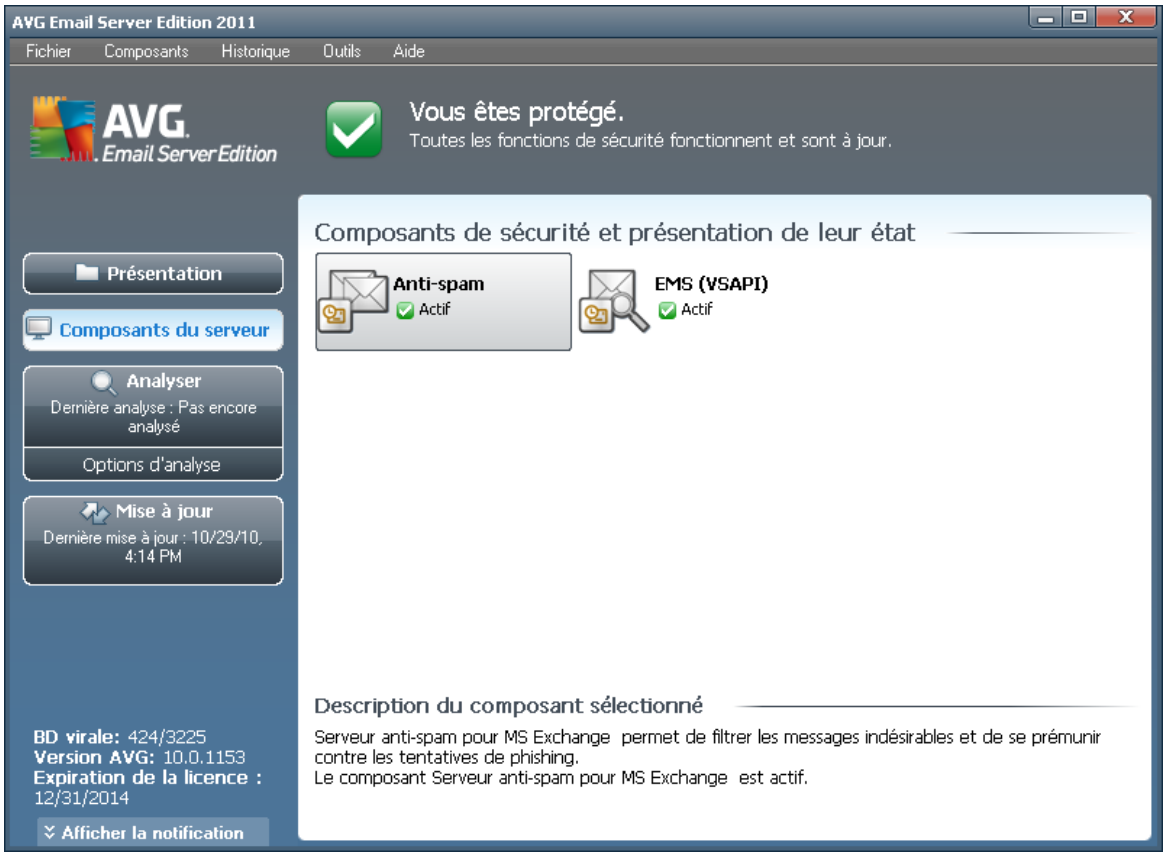
Dans le sous-élément ***Filtrage des messages***, vous pouvez choisir les pièces jointes à supprimer de façon automatique (le cas échéant). Vous avez le choix entre les options suivantes :

- ***Supprimer les pièces jointes*** - cochez cette case pour activer la fonction.
- ***Supprimer tous les fichiers exécutables*** - permet de supprimer tous les fichiers exécutables.
- ***Supprimer tous les documents*** - permet de supprimer tous les fichiers.
- ***Supprimer les fichiers suivants (extensions séparées par une virgule)*** - saisissez dans la case les extensions des fichiers à supprimer automatiquement. Séparez les extensions par une virgule.

5. Scanner e-mail pour MS Exchange Server 2003

5.1. Présentation

Les options de configuration du Scanner e-mail pour MS Exchange Server 2003 sont intégrées à AVG Edition Serveur de Mail 2011 comme composants du serveur.



Les composants du serveur sont les suivants :

Présentation standard des différents composants du serveur :

- ***Anti-Spam - Serveur anti-spam pour MS Exchange***

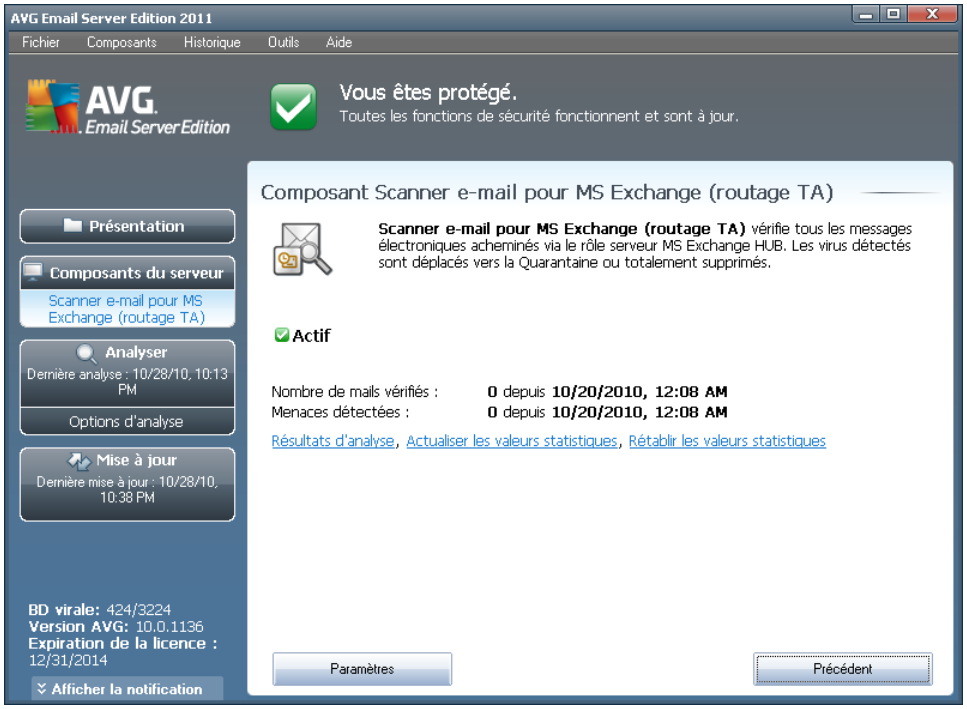
  Le composant vérifie tous les mails entrants et marque les courriers indésirables comme SPAM. Le composant utilise plusieurs méthodes d'analyse pour traiter chaque mail afin d'offrir un niveau de protection maximal contre les messages indésirables.

- ***EMS (VSAPI) - Scanner e-mail pour MS Exchange (VSAPI)***

  Vérifie tous les messages électroniques stockés dans les boîtes de réception des utilisateurs. En cas de détection, les virus sont mis en quarantaine ou purement

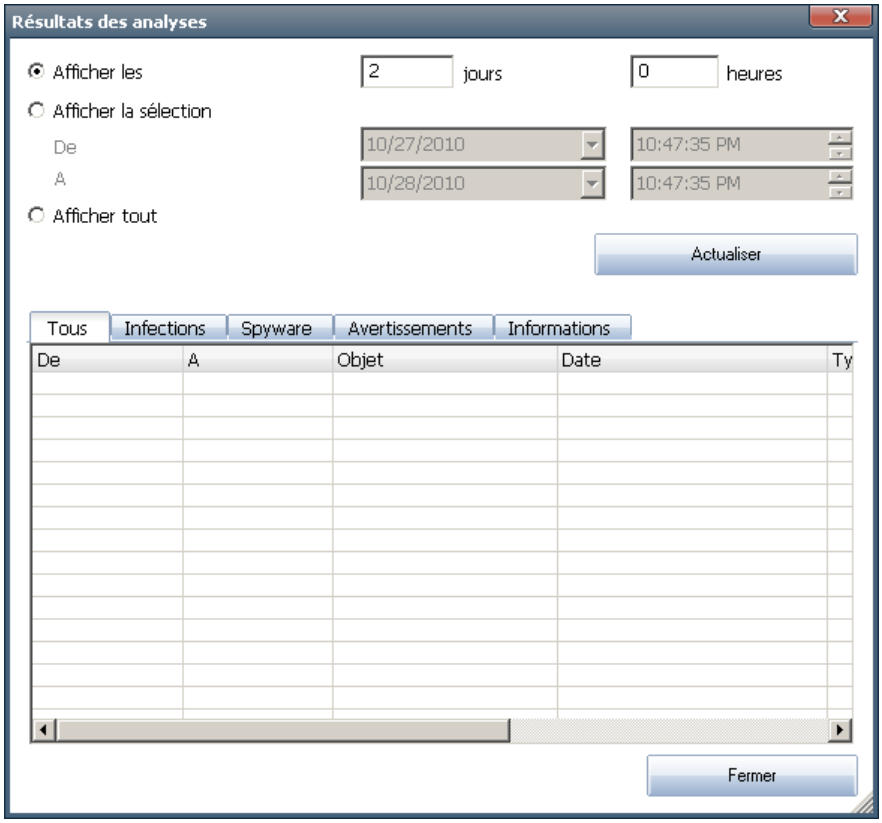
et simplement supprimés.

Double-cliquez sur un composant pour ouvrir son interface. A l'exception de l'anti-spam, tous les composants partagent les boutons de commande et liens suivants :



- ***Résultats des analyses***

  Ouvre une nouvelle boîte de dialogue dans laquelle vous pouvez examiner les résultats d'analyse :



Les messages sont classés selon leur gravité sous l'onglet approprié. Consultez la configuration de chaque composant afin de modifier la gravité et le signalement des messages.

Par défaut, seuls les résultats des deux derniers jours s'affichent. Vous pouvez modifier la période d'analyse en choisissant une des options suivantes :

- ***Afficher les*** - indiquez les jours et les heures de votre choix.
- ***Afficher la sélection*** - choisissez une heure et une plage de dates personnalisées.
- ***Afficher tout*** - affiche les résultats pour toute la période.

Utilisez le bouton ***Actualiser*** pour recharger les résultats en fonction des critères définis.

- ***Actualiser les valeurs statistiques*** - met à jour les statistiques affichées ci-dessus.
- ***Rétablir les valeurs statistiques*** - réinitialise toutes les statistiques.

Les boutons qui fonctionnent sont les suivants :

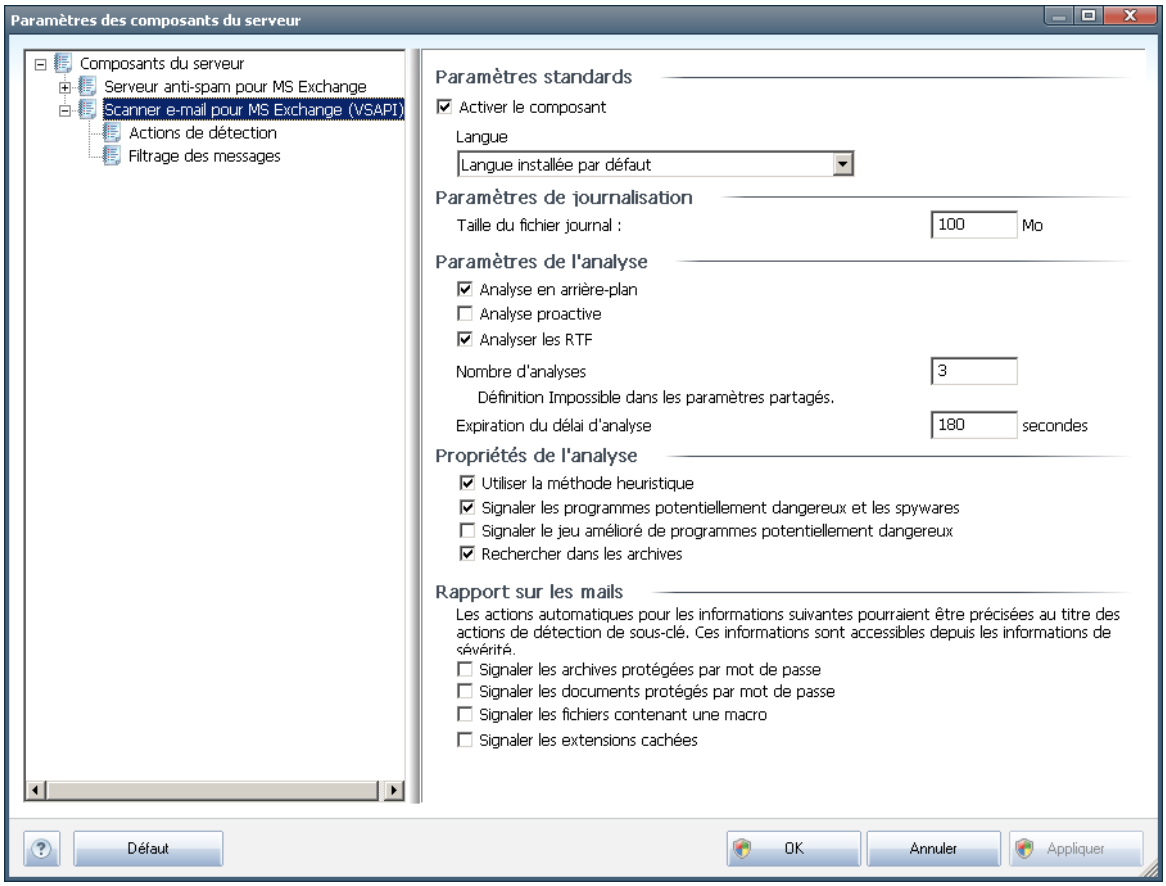
- ***Paramètres*** - ce bouton permet d'ouvrir les paramètres du composant.

- ***Précédent*** - cliquez sur ce bouton pour revenir à l'écran de présentation des composants du serveur.

Vous trouverez davantage d'informations sur les paramètres des composants dans les chapitres suivants.

5.2. Scanner e-mail pour MS Exchange (VSAPI)

Cet élément contient les paramètres du composant ***Scanner e-mail pour MS Exchange (VSAPI)***.



La section ***Paramètres standard*** contient les options suivantes :

- ***Activer le composant*** - désélectionnez cette case pour désactiver intégralement le composant.

- ***Langue*** - choisissez la langue du composant.

La section ***Paramètres de journalisation*** :

- ***Taille du fichier journal*** - choisissez la taille du fichier journal. Valeur par défaut : 100 Mo.

Section ***Paramètres de l'analyse*** :

- ***Analyse en arrière-plan*** – 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 non encore analysé avec la dernière mise à jour de la base de données virale AVG est détecté dans les dossiers de courrier de l'utilisateur, il est envoyé à AVG pour Exchange 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.

- ***Analyse proactive (messages entrants)***

  Elle permet d'activer ou de désactiver l'analyse proactive de VSAPI 2.0/2.5. Cette analyse est lancée lorsqu'un élément est envoyé vers un dossier, mais elle s'exécute sans qu'un client n'en fasse la demande.

  Lorsque des messages sont transmis au service Exchange Store, ils sont placés dans la file d'attente globale en vue de leur analyse et sont considérés comme des éléments de faible priorité (nombre maximal : 30 éléments). Ils sont analysés en fonction de la méthode FIFO (premier arrivé, premier servi). Si un client accède à un élément de la file d'attente, la priorité de celui-ci augmente.

  Remarque : *les messages en surnombre resteront non analysés dans le service Store.*

Remarque :*même si vous désactivez les deux options, à savoir* ***Analyse en arrière-plan****et* ***Analyse proactive****, l'analyse sur accès reste toujours active lorsqu'un utilisateur tente de télécharger un message via le client MS Outlook.*

- ***Analyser RTF*** - permet de spécifier si les fichiers de type RTF doivent être analysés ou non.
- ***Nombre de threads d'analyse*** - par défaut, le processus d'analyse s'effectue par threads afin d'augmenter les performances globales de l'analyse et d'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.

  Le nombre minimum de threads est calculé comme suit : ('nombre de processeurs'+1) divisé par 2.

  Le nombre maximum de threads est calculé comme suit : 'Nombre de processeurs' multiplié par 5 + 1.

  Si la valeur est minimale (moins importante) ou maximale (plus importante), la

valeur par défaut est utilisée.

- ***Délai d'analyse*** - intervalle maximal continu (exprimé en secondes) durant lequel un thread tente d'accéder au message à analyser (la valeur par défaut est 180 secondes).

La section ***Propriétés de l'analyse*** :

- ***Utiliser la méthode heuristique*** - cochez cette case pour activer la méthode heuristique lors de l'analyse.
- ***Signaler les programmes potentiellement dangereux et les spywares*** - cochez cette option pour signaler la présence de programmes potentiellement dangereux et de spywares.
- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** - cette option permet de détecter le jeu étendu des spywares : ces programmes ne posent aucun problème et sont parfaitement sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais peuvent ensuite être utilisés à des fins malveillantes. Il peut aussi s'agir de programmes absolument inoffensifs, mais qui sont inopportuns (barres d'outils, etc.). Il s'agit d'une mesure de sécurité et de convivialité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut. Remarque : cette fonction de détection complète l'option précédente. Aussi, si vous souhaitez bénéficiez d'une protection contre des types de spywares standard, veillez à toujours cocher la case précédente.
- ***Analyser les archives*** - cochez cette option afin que le scanner analyse également le contenu des fichiers archivés (zip, rar, etc.)

La section ***Rapports sur les pièces jointes*** vous permet de choisir les éléments à signaler lors de l'analyse. La configuration par défaut peut être facilement modifiée dans la ***section Actions de détection***, partie ***Informations*** (voir ci-dessous).

Vous avez le choix entre les options suivantes :

- ***Signaler les archives protégées par mot de passe***
- ***Signaler les documents protégés par mot de passe***
- ***Signaler les fichiers contenant une macro***
- ***Signaler les extensions cachées***

En général, toutes ces fonctions 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, utilisez les liens suivants (et les liens accessibles à partir de ces liens de référence) :

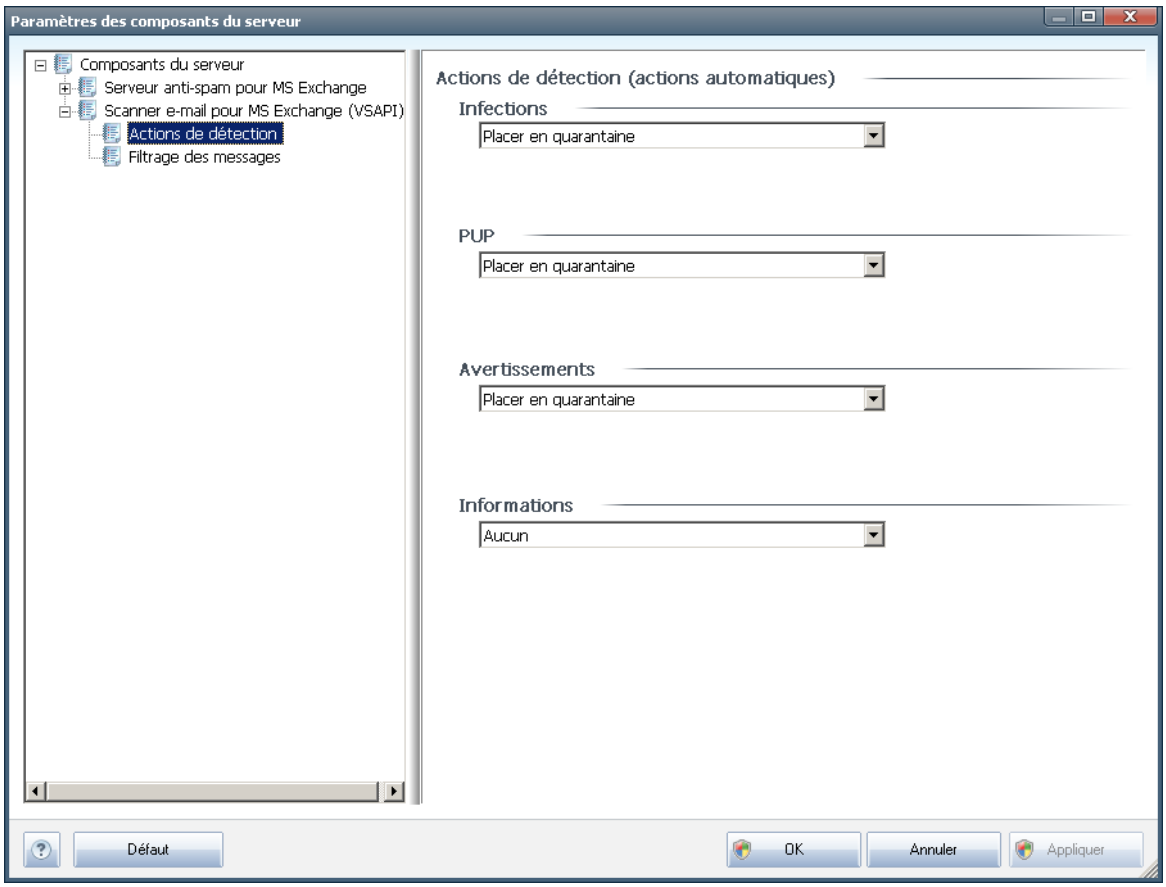
- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k- pour obtenir des informations sur l'interaction entre Exchange et le logiciel antivirus

- 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.

L'arborescence suivante contient également ces sous-éléments :

- ***Actions de détection***
- ***Filtrage des messages***

5.3. Actions de détection



Dans le sous-élément ***Actions de détection***, vous pouvez choisir les actions automatiques qui doivent se produire lors de la procédure d'analyse.

Ces actions sont disponibles pour les éléments suivants :

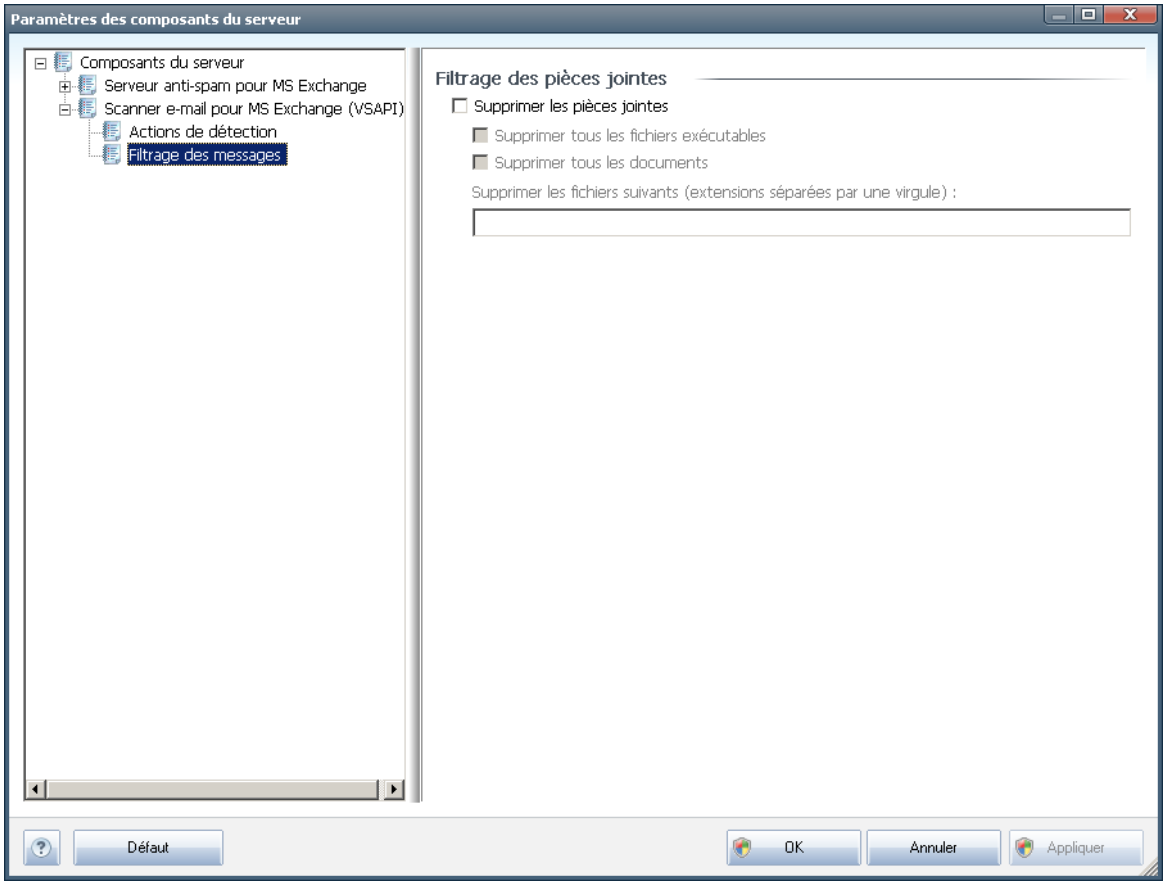
- ***Infections***
- ***PUP (programmes potentiellement dangereux)***
- ***Avertissements***

- ***Informations***

A partir du menu déroulant, choisissez l'action à effectuer pour chaque élément :

- ***Aucune*** - aucune action n'est effectuée.
- ***Placer en quarantaine*** - la menace est placée en Quarantaine.
- ***Supprimer*** - la menace est supprimée.

5.4. Filtrage des messages



Dans le sous-élément ***Filtrage des messages***, vous pouvez choisir les pièces jointes à supprimer de façon automatique (le cas échéant). Vous avez le choix entre les options suivantes :

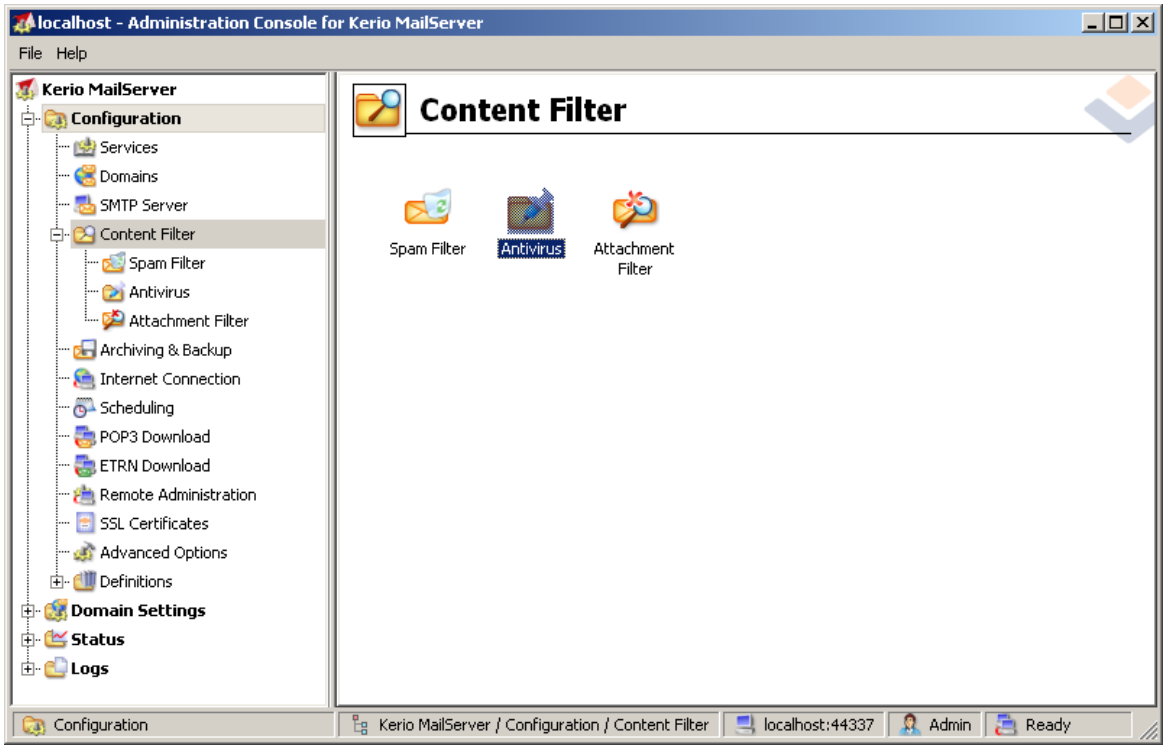
- ***Supprimer les pièces jointes*** - cochez cette case pour activer la fonction.
- ***Supprimer tous les fichiers exécutables*** - permet de supprimer tous les fichiers exécutables.
- ***Supprimer tous les documents*** - permet de supprimer tous les fichiers.

- ***Supprimer les fichiers suivants (extensions séparées par une virgule)*** - saisissez dans la case les extensions des fichiers à supprimer automatiquement. Séparez les extensions par une virgule.

6. AVG pour Kerio MailServer

6.1. 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 Filtrage du contenu dans la catégorie Configuration:

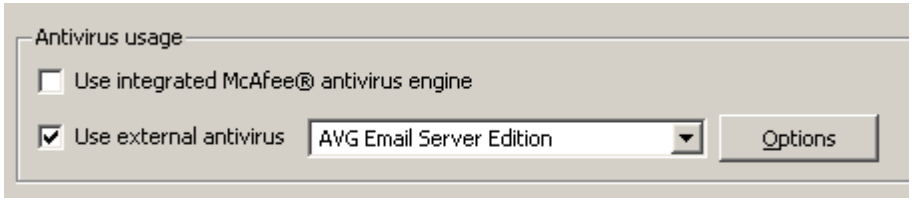


Cliquer sur l'élément Content Filter (Filtrage du contenu) ouvre une boîte de dialogue contenant trois options :

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

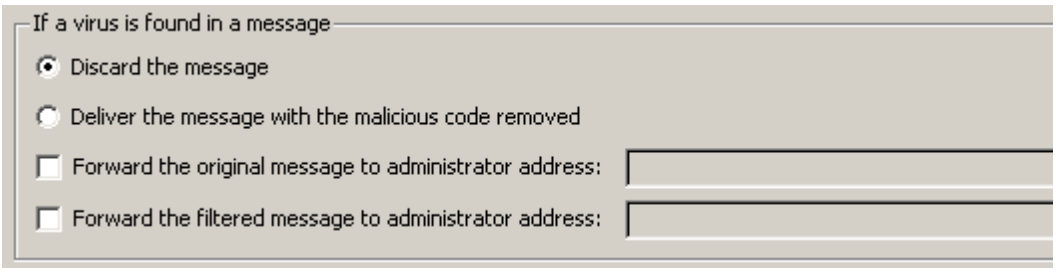
6.1.1. Anti-virus

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 :

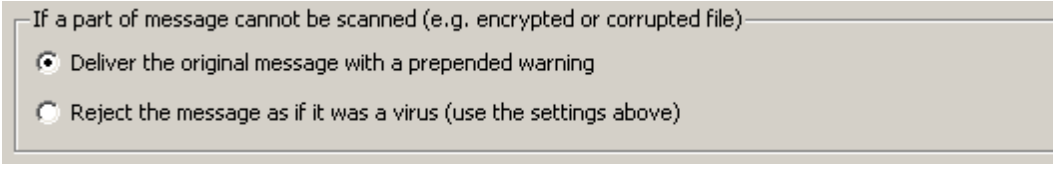
- ***If a virus is found in a message (Si un virus est trouvé dans un message)***



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

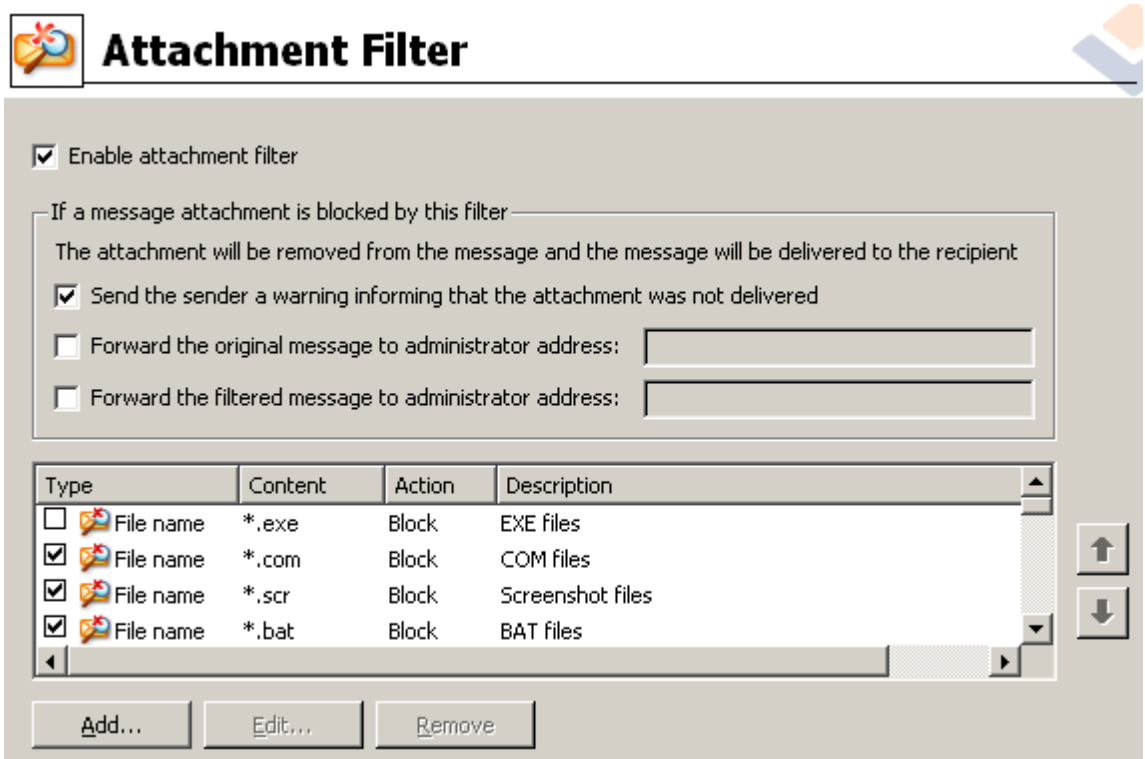
message ne peut être analysée :

- ***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.

6.1.2. Filtrage des pièces jointes

Dans le menu 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 Activer le filtrage des pièces jointes. Vous pouvez également modifier les paramètres suivants :

- ***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.

- ***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.

- ***Transférer le message d'origine 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 :

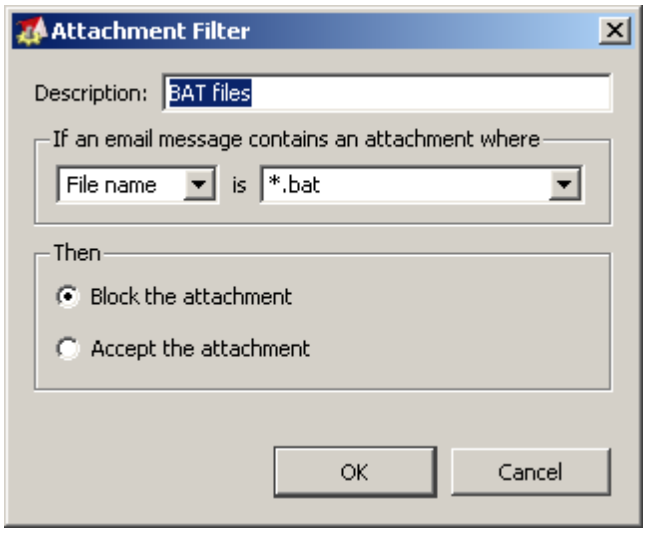
- ***Type*** – spécification du type de pièce jointe, déterminé par l'extension attribué dans le champ Content (Contenu). Les types disponibles sont File name (Nom de fichier) ou MIME type (Type MIME). Vous pouvez cocher la case correspondante au champ pour inclure ou exclure l'élément du filtrage des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

- ***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 pour une pièce jointe spécifique. Les actions possibles sont Accepter (accepter la pièce jointe) et Bloquer (l'action définie au-dessus de la liste des pièces jointes désactivées sera réalisée).

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

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



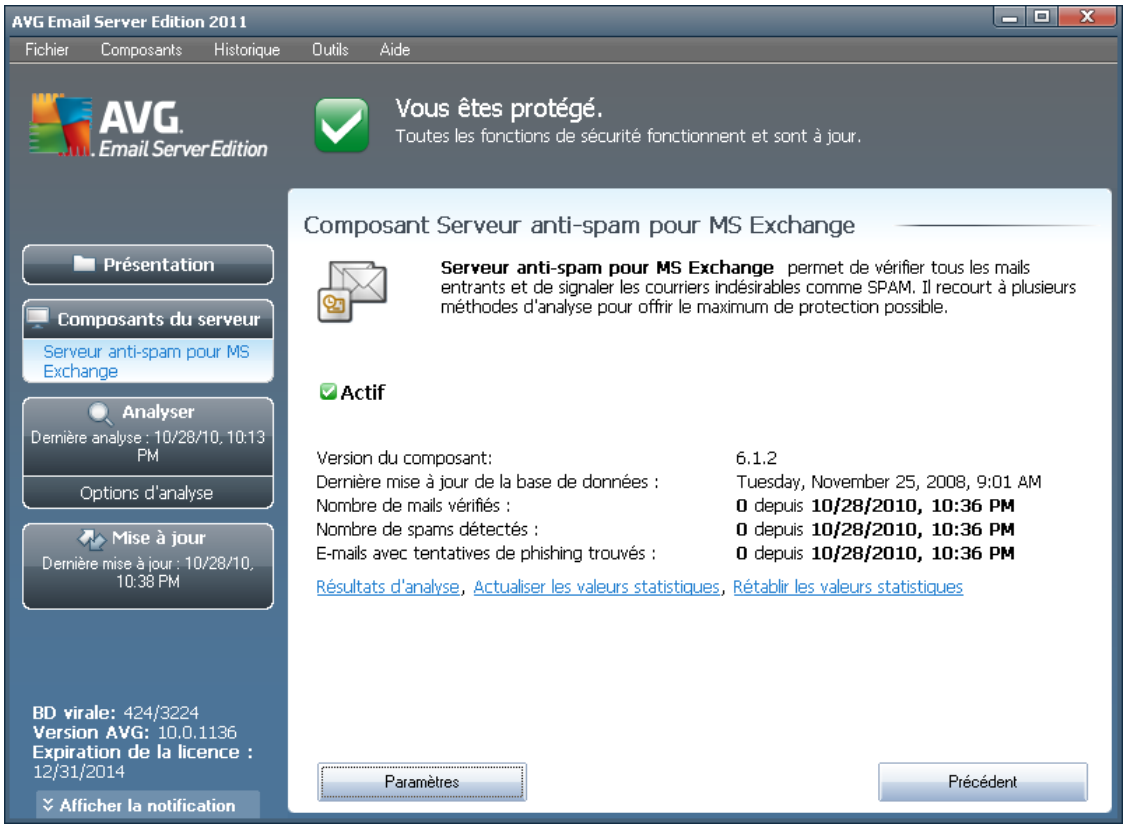
- Dans le champ Description, vous pouvez décrire brièvement la pièce jointe à filtrer.

- 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.

7. Configuration anti-spam

7.1. Interface de l'Anti-Spam

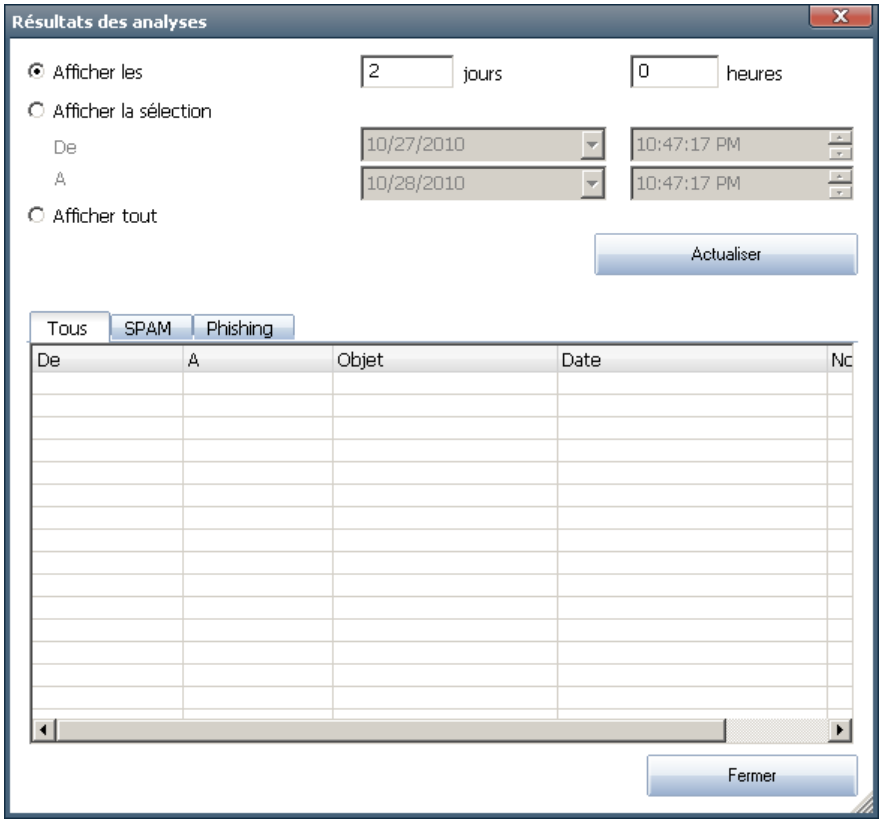


Vous trouverez la boîte de dialogue du composant du ***serveur*** anti-spam dans la section ***Composants du serveur*** (menu de gauche). Celle-ci contient des informations sur la fonctionnalité du composant du serveur et des informations sur son état actuel (*Le composant Anti-Spam Server pour MS Exchange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

Liens disponibles :

- ***Résultats des analyses***

  Ouvre une nouvelle boîte de dialogue dans laquelle vous pouvez examiner les résultats des analyses anti-spam :



vous pouvez y consulter les messages signalés comme du SPAM (messages indésirables) ou comme une tentative d'hameçonnage (toute opération visant à voler des données personnelles, des données bancaires, une identité, etc.). Par défaut, seuls les résultats des deux derniers jours s'affichent. Vous pouvez modifier la période d'analyse en choisissant une des options suivantes :

- ***Afficher les*** - indiquez les jours et les heures de votre choix.
- ***Afficher la sélection*** - choisissez une heure et une plage de dates personnalisées.
- ***Afficher tout*** - affiche les résultats pour toute la période.

Utilisez le bouton ***Actualiser*** pour recharger les résultats en fonction des critères définis.

- ***Actualiser les valeurs statistiques*** - met à jour les statistiques affichées ci-dessus.
- ***Rétablir les valeurs statistiques*** - réinitialise toutes les statistiques.

Les boutons qui fonctionnent sont les suivants :

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

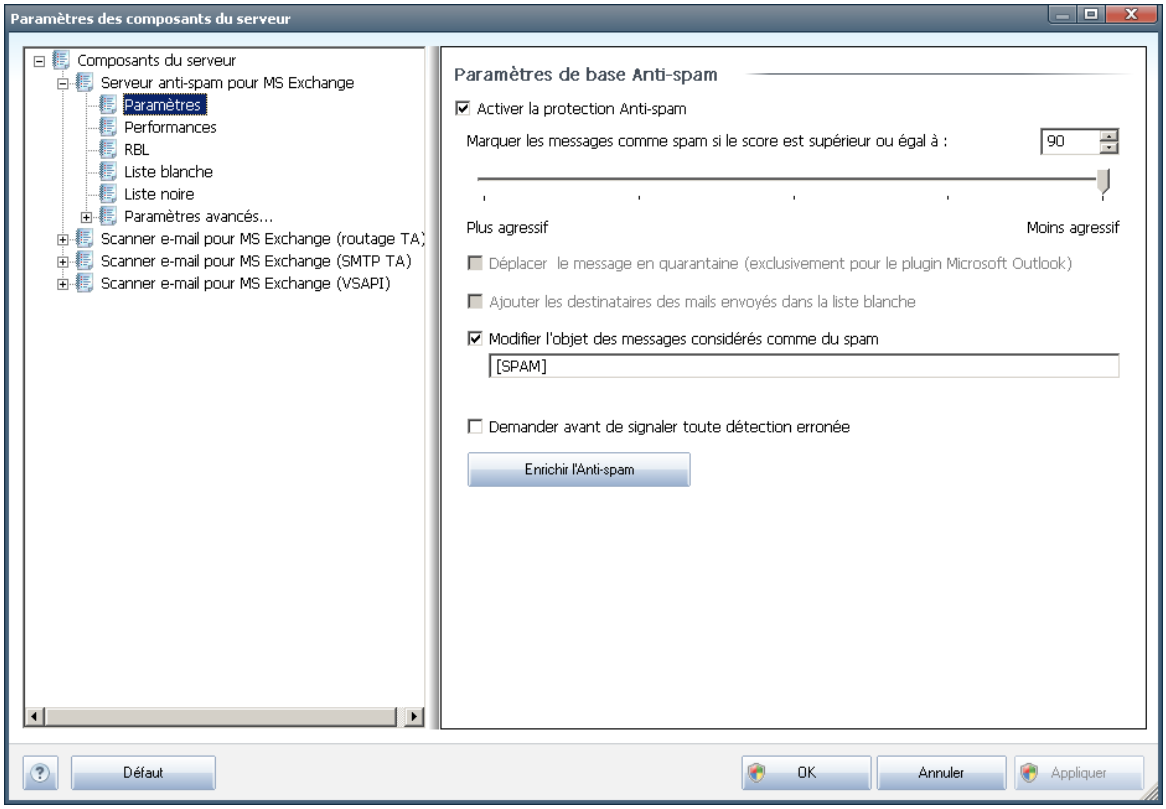
- ***Précédent*** - cliquez sur ce bouton pour revenir à l'écran de présentation des composants du serveur.

7.2. 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 du SPAM. Le composant utilise plusieurs méthodes d'analyse pour traiter chaque mail afin d'offrir un niveau de protection maximal contre les messages indésirables.

7.3. 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 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 spam si le résultat est supérieur ou égal à***, saisissez le score qui convient (entre *50 et 90*) ou faites glisser le curseur vers la gauche ou vers la droite.

Voici l'effet obtenu selon le score que vous définissez :

- ***Valeur 90*** - la plupart des messages entrants parviennent à leur destinataire (sans être considérés comme du spam). Le spam le plus facilement identifiable est stoppé, mais vous risquez de laisser 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 50-59*** - 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.

Vous pourrez également définir comment lesspam détectés doivent être traités :

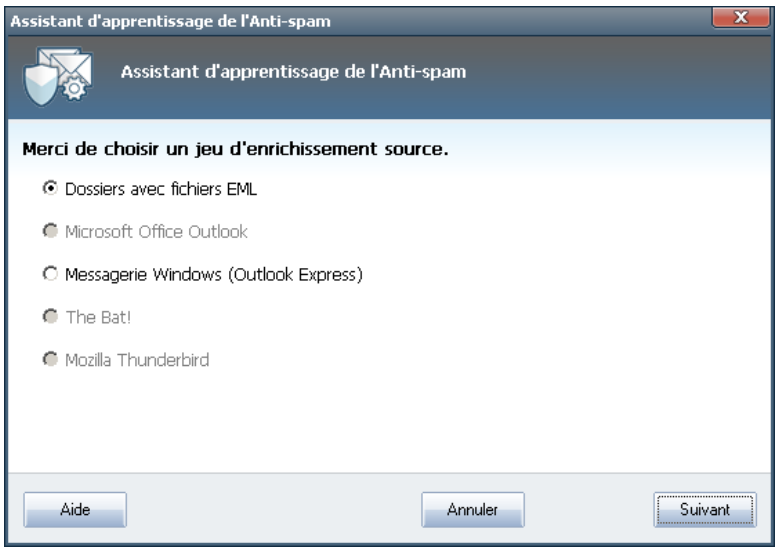
- ***Modifier l'objet des messages considérés comme spam*** - cochez cette case pour que tous les messages détectés comme du spam soient signalés à l'aide d'un mot ou d'un caractère particulier dans l'objet du message. Le texte souhaité doit être saisi dans la zone de texte activée.
- ***Demander avant de signaler toute détection erronée*** - dans la mesure où vous avez donné votre accord pour participer au programme d'amélioration des produits au cours de l'installation, (ce programme permet de recueillir des informations les plus à jour sur les menaces rencontrées par les utilisateurs du monde entier et, en retour, d'améliorer la protection de tous, vous autorisez le signalement des menaces détectées à AVG. La procédure de signalement est entièrement automatisée. Toutefois, vous pouvez cocher cette case pour confirmer que vous voulez être interrogé avant qu'un spam détecté soit signalé à AVG afin de vous assurer que le message en question a bien lieu d'être classé dans la catégorie du spam.

  Remarque : *cette option n'est pas applicable pour AVG Edition Serveur de Mail 2011*

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

7.3.1. Assistant d'enrichissement de l'Anti-Spam

La première boîte de dialogue de l'***Assistant d'enrichissement de l'anti-spam*** vous invite à sélectionner la source des messages que vous souhaitez utiliser pour 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

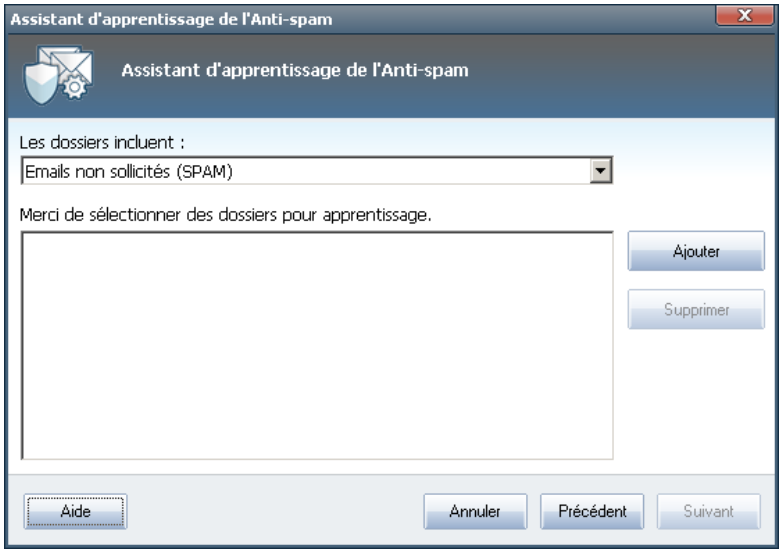
Pour faciliter et accélérer le processus d'enrichissement, il est judicieux de trier préalablement les mails dans les dossiers de façon à ne conserver que les messages pertinents (messages sollicités ou indésirables). Cela n'est toutefois pas absolument nécessaire car vous pourrez filtrer les messages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

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

7.3.2. 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



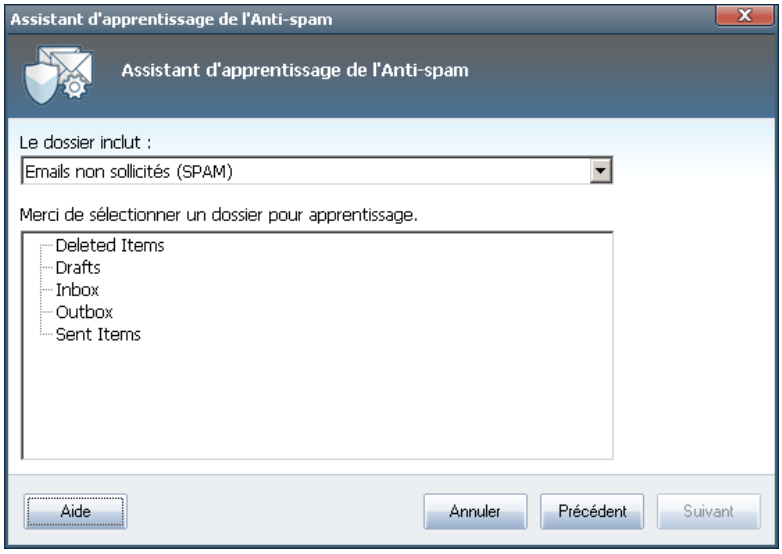
Dans cette boîte de dialogue, sélectionnez le dossier contenant les messages à utiliser pour la procédure d'enrichissement. Cliquez sur le bouton ***Ajouter*** pour localiser le dossier contenant les fichiers .eml (*messages e-mail enregistrés*). Le dossier sélectionné apparaît dans la boîte de dialogue.

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***.

Une fois 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***, 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. L'arborescence du client de messagerie sélectionné figure déjà dans la partie centrale de la boîte de dialogue. Identifiez le dossier souhaité dans l'arborescence, et mettez-le en surbrillance à l'aide de la souris.

Cliquez ensuite sur ***Suivant*** et passez aux ***options de filtrage des messages***.

7.3.3. Options de filtrage des messages

Dans cette boîte de dialogue, vous pouvez définir le filtrage des messages.

Si vous êtes certain que le dossier sélectionné contient uniquement les messages que vous souhaitez utiliser pour l'enrichissement, sélectionnez l'option ***Tous les messages (sans filtrage)***.

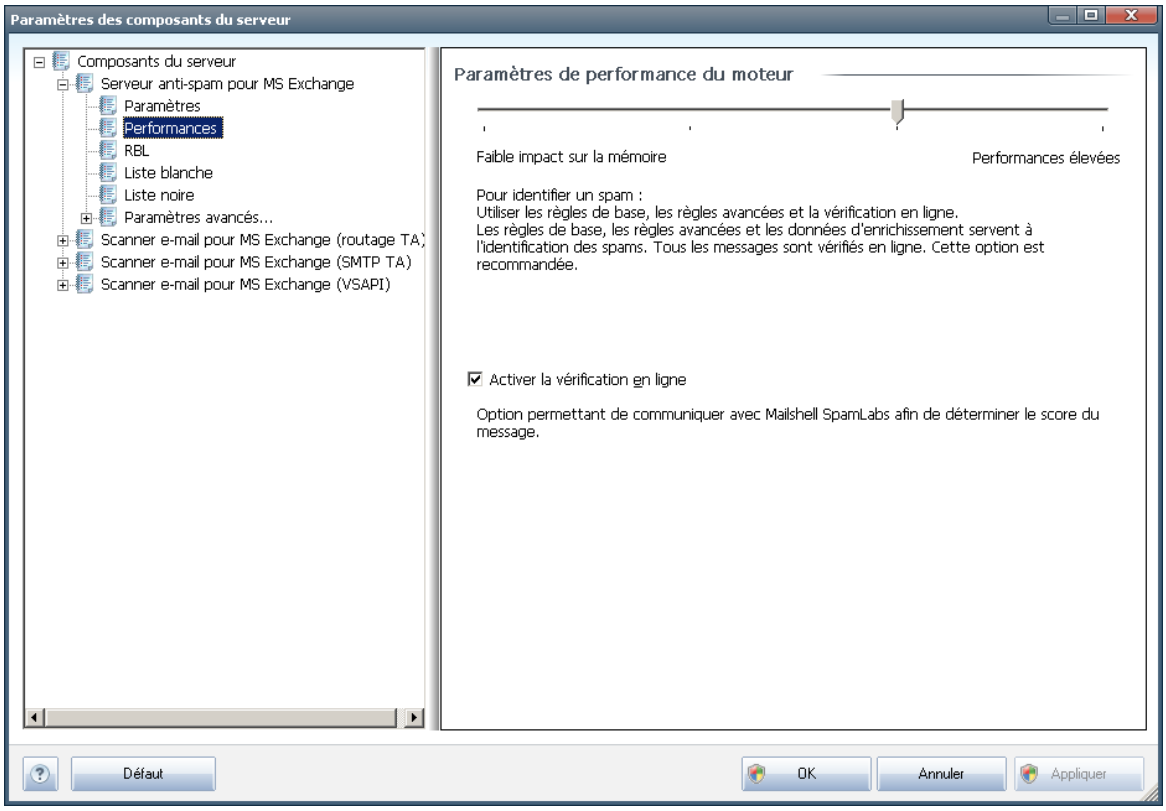
En cas de doute sur les messages contenus dans le dossier ou si vous voulez que l'assistant vous interroge pour chaque message (de manière à décider si le message en question contribue à l'enrichissement ou non de l'anti-spam), sélectionnez l'option ***Demander à chaque message***.

Pour d'autres paramètres avancés de filtrage, sélectionnez l'option ***Utiliser le filtre***. Vous pouvez saisir un mot (nom), une partie d'un mot ou une expression à rechercher dans le champ de l'objet de l'e-mail et/ou 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.

7.4. 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.

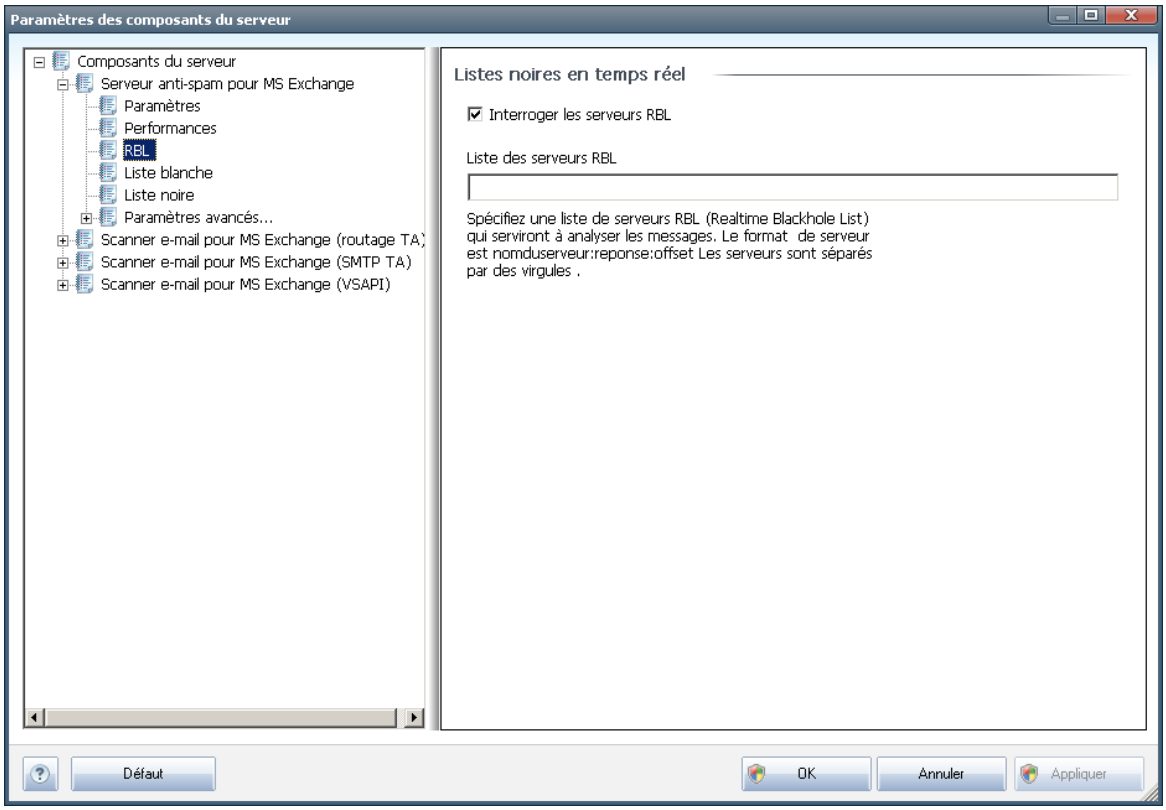
L'option ***Activer la vérification en ligne*** est sélectionnée par défaut. Cette configuration produit une détection plus précise du spam grâce à la communication avec les serveurs Mailshell. En effet, les données analysées sont comparées aux bases de données en ligne Mailshell.

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.

7.5. 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 spam qui ne sont ordinairement pas détectés par le moteur anti-spam.

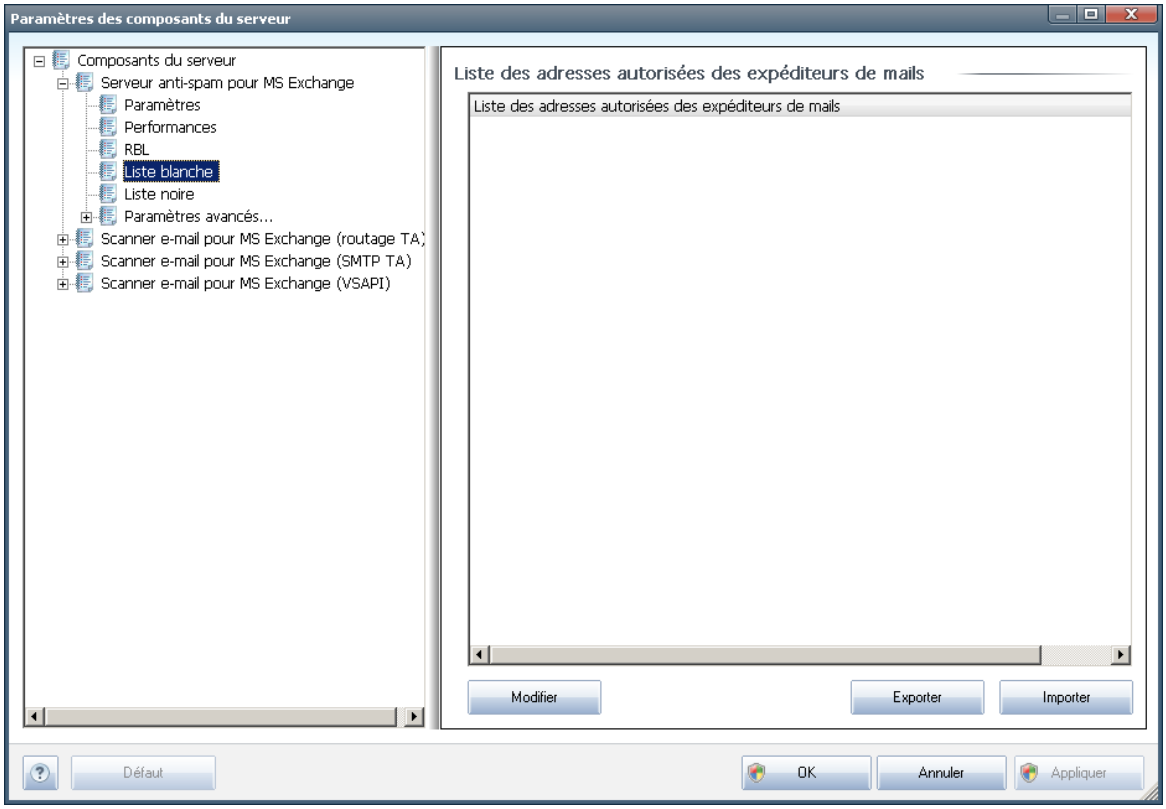
La ***liste des serveurs RBL*** permet de définir les emplacements des serveurs RBL. Par défaut, deux adresses de serveurs RBL sont spécifiées. Nous vous recommandons de conserver les paramètres proposés par défaut sauf si vous avez véritablement besoin de les modifier et si vous êtes un utilisateur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

7.6. 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 (*avgfrance.com*, 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 : saisissez directement chaque adresse ou importez la liste entière. Vous avez accès aux boutons de fonctions suivants :

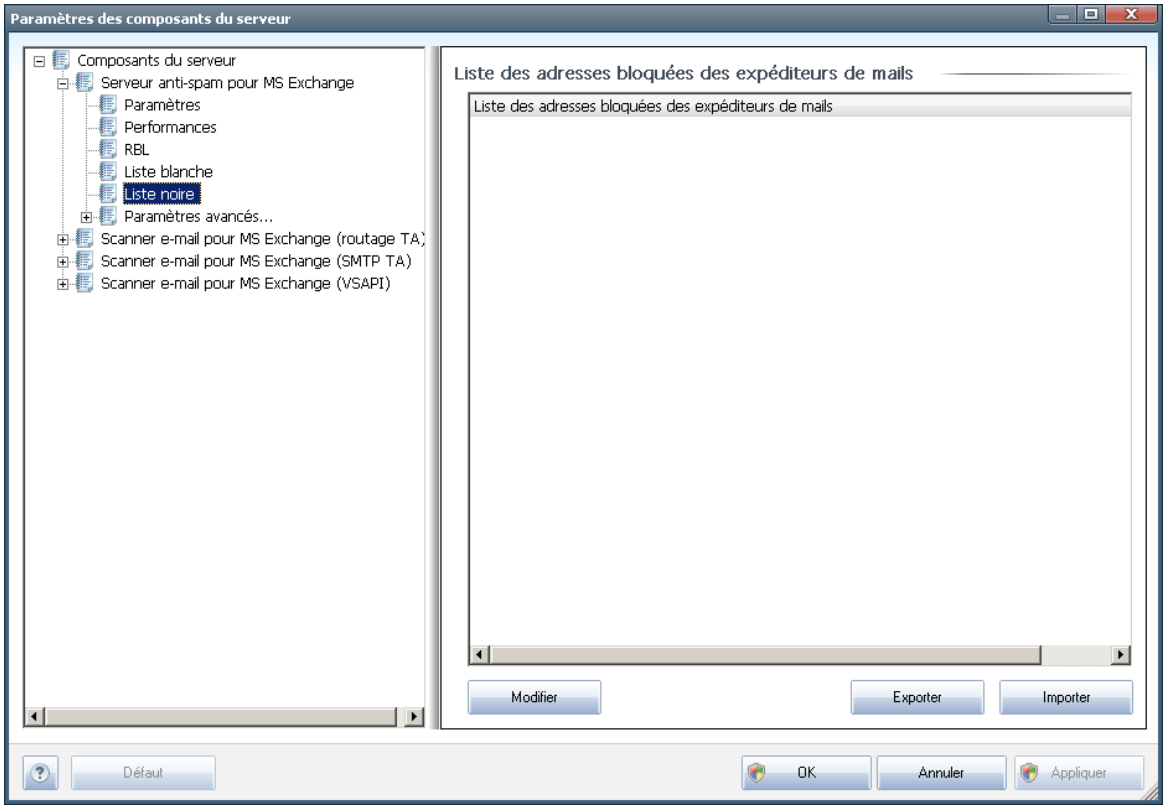
- ***Modifier*** - cliquez sur ce bouton pour ouvrir une boîte de dialogue permettant de définir manuellement une liste d'adresses (la méthode *copier-coller convient également*). Insérez une entrée (expéditeur, nom de domaine) par ligne.

- ***Importer*** - vous pouvez importer vos adresses électroniques en cliquant sur ce bouton. Le fichier d'entrée peut être un fichier texte (au format texte brut, à raison d'un seul élément - adresse, nom de domaine - par ligne), un fichier WAB ; l'importation peut également être réalisée à partir du Carnet d'adresses Windows ou Microsoft Office Outlook.

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

7.7. 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 : saisissez directement

chaque adresse ou importez la liste entière. Vous avez accès aux boutons de fonctions 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 une entrée (expéditeur, nom de domaine) par ligne.

- ***Importer*** - vous pouvez importer vos adresses électroniques en cliquant sur ce bouton. Le fichier d'entrée peut être un fichier texte (au format texte brut, à raison d'un seul élément - adresse, nom de domaine - par ligne), un fichier WAB ; l'importation peut également être réalisée à partir du Carnet d'adresses Windows ou Microsoft Office Outlook.

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

7.8. 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*** - nombre maximum de mots à entrer, seuil d'apprentissage automatique, pondération

- ***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.

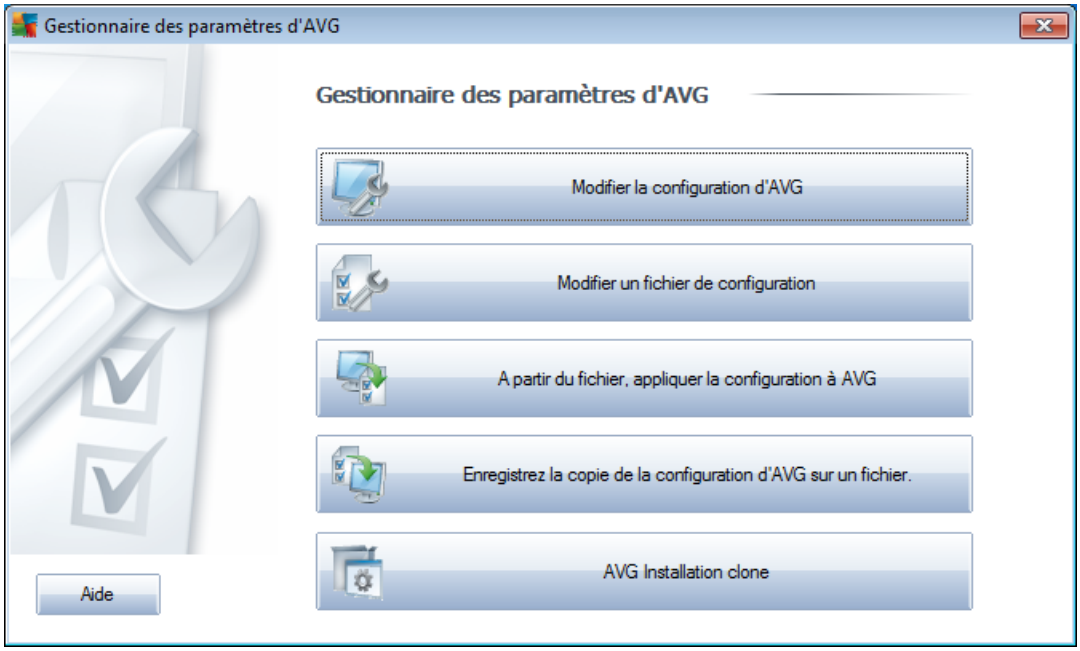
- ***Connexion Internet*** - délai, serveur proxy, authentification du serveur proxy

8. Gestionnaire des paramètres AVG

Principalement indiqué pour les réseaux de petite taille, le ***Gestionnaire des paramètres AVG*** est un outil qui permet de copier, de modifier et de distribuer la configuration d'AVG. Vous pouvez enregistrer cette configuration sur un périphérique amovible (clé USB, etc.) et l'appliquer manuellement aux stations de votre choix.

Cet outil est inclus dans l'installation du programme AVG. Il est accessible via le menu Démarrer de Windows :

Tous les programmes/AVG 2011/Gestionnaire des paramètres AVG



- ***Supprimer la configuration d'AVG de cet ordinateur***

  Utilisez ce bouton pour ouvrir une boîte de dialogue qui propose des paramètres avancés de l'installation locale d'AVG. Toutes les modifications apportées à ce niveau affecteront également l'installation locale d'AVG.

- ***Charger et modifier le fichier de configuration d'AVG***

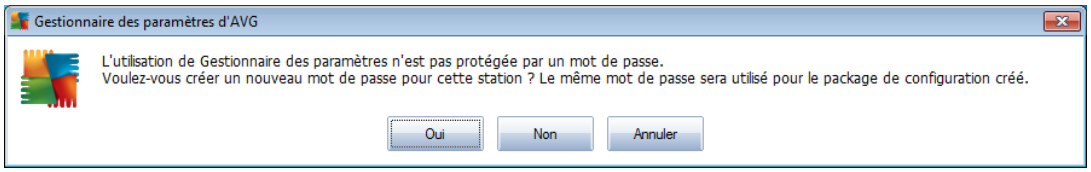
  Si vous disposez déjà d'un fichier de configuration d'AVG (.pck), utilisez ce bouton pour l'ouvrir et y apporter des modifications. Une fois les modifications confirmées à l'aide du bouton ***OK*** ou ***Appliquer***, le fichier est remplacé par les nouveaux paramètres !

- ***Appliquer la configuration depuis le fichier vers AVG sur cet ordinateur***

  Utilisez ce bouton pour ouvrir un fichier de configuration d'AVG (.pck) et appliquez-le à l'installation locale d'AVG.

- ***Conserver la configuration locale d'AVG dans un fichier***

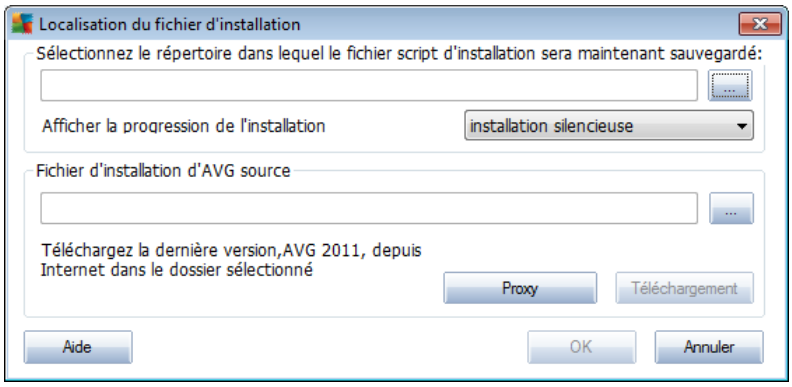
  Utilisez ce bouton pour enregistrer le fichier de configuration (.pck) de l'installation locale d'AVG. Si vous n'avez pas défini de mot de passe pour les Actions autorisées, la boîte de dialogue suivante peut s'afficher :



  Choisissez ***Oui*** pour créer immédiatement le mot de passe d'accès à la Liste des éléments autorisés, puis saisissez les informations requises avant de confirmer votre choix. Choisissez ***Non*** pour ignorer la création d'un mot de passe, puis enregistrez la configuration locale d'AVG dans un fichier.

- ***Cloner l'installation d'AVG***

  Cette option permet de faire une copie de l'installation locale d'AVG en créant un package d'installation qui contient des options personnalisées. Pour ce faire, sélectionnez d'abord le dossier où le script d'installation sera enregistré.



  Ensuite, choisissez l'une des options suivantes à partir du menu déroulant :

  - ***Installation masquée*** - aucune information n'est affichée lors de la procédure d'installation.
  - ***Afficher uniquement la progression de l'installation*** - l'installation ne nécessite pas d'intervention de la part de l'utilisateur, mais la progression est parfaitement visible.
  - ***Afficher l'assistant d'installation*** - l'installation est visible et l'utilisateur devra confirmer manuellement toutes les étapes.

  Utilisez le bouton ***Télécharger*** pour télécharger le dernier fichier d'installation d'AVG, disponible directement sur le site Web d'AVG, dans le dossier sélectionné ou placez manuellement le fichier d'installation d'AVG dans ce dossier.

Vous pouvez utiliser le bouton ***Proxy*** pour définir les paramètres d'un serveur proxy, si le réseau l'exige pour établir une connexion.

Lorsque vous cliquez sur ***OK***, le processus de duplication démarre et prend un peu de temps. Une boîte de dialogue vous invitant à créer un mot de passe pour la liste des éléments autorisés s'affiche (voir ci-dessus). ***AvgSetup.bat*** devrait ensuite être disponible dans le dossier ainsi que d'autres fichiers. Si vous exécutez le fichier ***AvgSetup.bat***, il installe le programme AVG en fonction des paramètres précédemment choisis.

9. 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 http://www.avg.com.

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***.