AVG 9 Internet Security

Manuel de l'utilisateur

Révision du document 90.6 (14.9.2009)

Table des matières

1. Introduction

Ce manuel utilisateur fournit une documentation complète sur **AVG 9 Internet Security**.

Nous vous remercions d'avoir choisi AVG 9 Internet Security.

AVG 9 Internet Security 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 9 Internet Security** a été entièrement repensée, afin de livrer une protection AVG reconnue et certifiée sous une présentation nouvelle, plus conviviale et plus efficace.

Votre tout nouveau produit **AVG 9 Internet Security** bénéficie d'une interface transparente associée à une analyse encore plus approfondie et plus rapide. D'avantage de fonctions de sécurité ont été automatisées pour plus de commodité et des options utilisateur "intelligentes" ont été incluses de manière à adapter les fonctions de sécurité à vos tâches quotidiennes. La convivialité n'a fait aucun compromis à la sécurité !

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 9 Internet Security sert à protéger les stations de travail fonctionnant avec les systèmes d'exploitation suivants :

- Windows 2000 Edition professionnelle SP4 + Correctif cumulatif 1
- Windows XP Edition familiale SP2
- Windows XP Edition professionnelle SP2
- Windows XP Edition professionnelle x64 Edition SP1
- Windows Vista (x86 et x64, toutes éditions confondues)
- Windows 7 (x86 et x64, toutes éditions confondues)

(et éventuellement les service packs de versions ultérieures pour certains systèmes d'exploitation)

***Remarque** : Le composant Identity Protection n'est pas pris en charge par Windows 2000 et XP x64. Vous pouvez installer AVG 9 Internet Security sur ces systèmes d'exploitation, mais sans le composant Identity Protection.*

2.2. Configuration matérielle minimum

La configuration minimale pour **AVG 9 Internet Security** est la suivante :

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

3. Options d'installation

AVG peut être installé à partir du fichier d'installation disponible sur le CD-ROM d'installation. Vous pouvez également télécharger la dernière version du fichier d'installation sur le site Web d'AVG (http://www.avg.com/).

Avant de procéder à l'installation du programme AVG, nous vous recommandons vivement de consulter le site Web d'AVG (http://www.avg.com/) pour vérifier la présence de nouveaux fichiers d'installation. pour vous assurer de posséder le dernier fichier d'installation en date d'AVG 9 Internet Security.

Nous vous recommandons d'utiliser notre nouvel outil AVG Download Manager qui vous aidera à choisir le fichier d'installation approprié !

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 achetez une copie d'AVG en ligne, le numéro de licence vous sera envoyé par mail.

4. Gestionnaire de téléchargement AVG

Gestionnaire de téléchargement AVG est un outil simple qui vous aide à sélectionner le fichier d'installation correspondant à votre produit. Sur la base des données que vous avez fournies, le gestionnaire va sélectionner le produit, le type de licence, les composantes souhaitées et la langue. Après cela, **Gestionnaire de téléchargement AVG** va télécharger et exécuter la procédure d'installation correspondante.

Avertissement: *Sachez que le Gestionnaire de téléchargement AVG ne prend pas en charge le téléchargement des Editions Réseau et SBS ; il fonctionne uniquement sous Windows 2000 SP4 + Pack correctif cumulatif, Windows XP SP2 et version supérieure et Windows Vista (toutes les éditions).*

Gestionnaire de téléchargement AVG disponible en téléchargement sur le site Web d'AVGhttp://www.avg.com/ Vous trouverez ci-dessous une brève description de chaque action que vous devez prendre au cours de la **Gestionnaire de téléchargement AVG** :

4.1. Sélection de la langue

Dans la première étape de **Gestionnaire de téléchargement AVG** , sélectionnez la langue d'installation dans le menu déroulant. Notez que la langue que vous sélectionnez s'applique uniquement au processus d'installation ; une fois l'installation

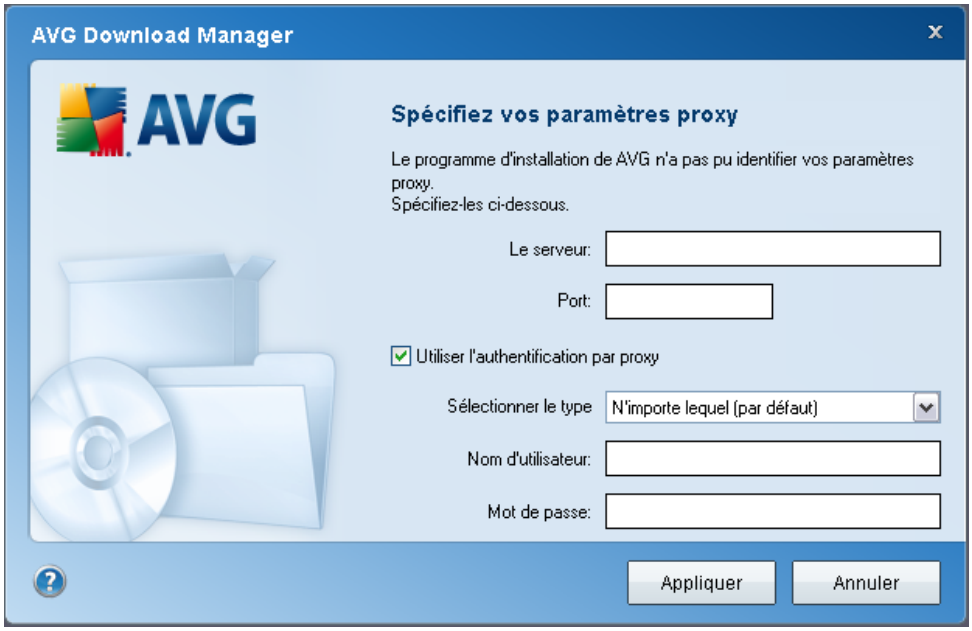
terminée, vous pourrez changer la langue directement à partir des paramètres du programme. Cliquez ensuite sur le bouton ***Suivant*** pour passer à l'écran suivant.

4.2. Vérification de la connectivité

A l'étape suivante, **Gestionnaire de téléchargement AVG** vous allez vous connecter à Internet afin que les mises à jour puissent être localisées. Vous ne pourrez poursuivre la procédure de téléchargement que lorsque le **Gestionnaire de téléchargement AVG** aura fini de tester la connectivité.

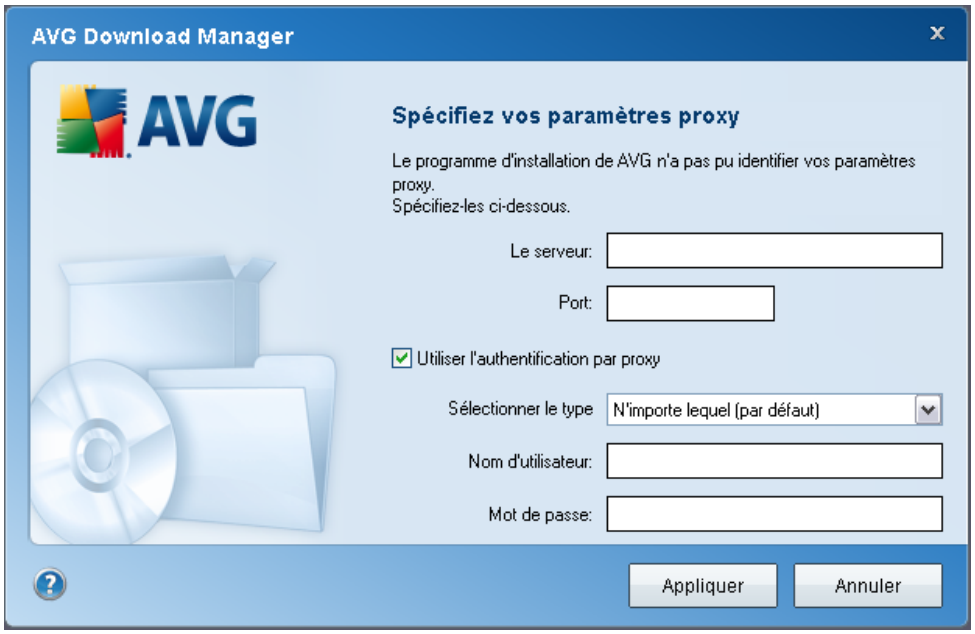
- Si le test de connexion n'aboutit pas, assurez vous que vous êtes effectivement connecté à Internet. Puis cliquez sur le bouton ***Réessayer***

- Si vous utilisez une connexion proxy pour accéder à Internet, cliquez sur le bouton ***Paramètres proxy*** afin de spécifier les informations appropriées.



- Si la vérification s'effectue avec succès, cliquez sur le bouton ***Suivant*** pour continuer.

4.3. Paramètres proxy



Si **Gestionnaire de téléchargement AVG** n'a pas pu identifier vos paramètres proxy, vous devez les indiquer manuellement. Indiquez les données suivantes :

- ***Serveur*** : entrez un nom de serveur proxy ou une adresse IP valide
- ***Port*** : fournissez le numéro de port respectif
- ***Utiliser l'authentification proxy*** : si votre serveur proxy exige une authentification, cochez cette case.
- ***Sélectionner l'authentification*** : dans le menu déroulant, sélectionnez le type d'authentification. Nous vous recommandons vivement de conserver les valeurs par défaut (*le serveur proxy vous indiquera alors automatiquement les données requises*). Cependant, si vous êtes un utilisateur chevronné, vous pouvez également choisir l'option Standard (*exigée par certains serveurs*) ou l'option NTLM (*exigée par tous les serveurs ISA*). Saisissez un nom valide ainsi qu'un ***Mot de passe*** (optionnel).

Confirmez les paramètres en cliquant sur le bouton ***Appliquer*** et suivez les indications donnée dans la prochaine étape de **Gestionnaire de téléchargement AVG**.

4.4. Choix du type de licence

Au cours de cette étape, vous êtes invité à choisir le type de licence du produit à télécharger. La description fournie vous aide à sélectionner celui qui vous convient le mieux :

- ***Version complète*** : par exemple ***AVG Anti-Virus***, ***AVG Anti-Virus plus Pare-feu*** ou ***AVG Internet Security***
- ***Version d'évaluation*** : vous donne la possibilité d'utiliser toutes les fonctionnalités du produit AVG complet, pour une durée de 30 jours
- ***Version gratuite*** : fournit une protection gratuite aux particuliers, bien que les fonctionnalités de l'application soient limitées ! En outre, la version gratuite ne comporte pas toutes les fonctionnalités disponibles dans la version payante.

4.5. Télécharger les fichiers à installer

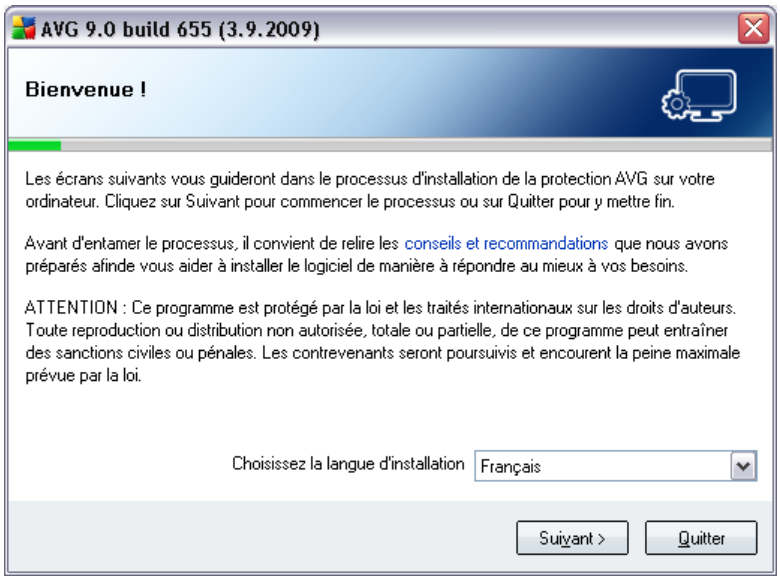
Vous avez maintenant fourni toutes les informations nécessaires pour que le **Gestionnaire de téléchargement AVG** entame le téléchargement du fichier d'installation et lance le processus d'installation. Vous pouvez maintenant passer au Processus d'installation d'AVG.

5. Processus d'installation d'AVG

Pour installer sur l'ordinateur, il est nécessaire d'obtenir le dernier fichier d'installation disponible. **AVG 9 Internet Security** 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. Téléchargez le fichier depuis le site Web d'AVG http://www.avg.com/) / section ***Téléchargements.*** Vous pouvez également utiliser notre nouvel outil ***AVG Download Manager*** qui vous aidera à créer et à télécharger le conditionnement d'installation adapté à vos besoins, puis à lancer le processus de téléchargement.

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 :

5.1. Lancement de l'installation

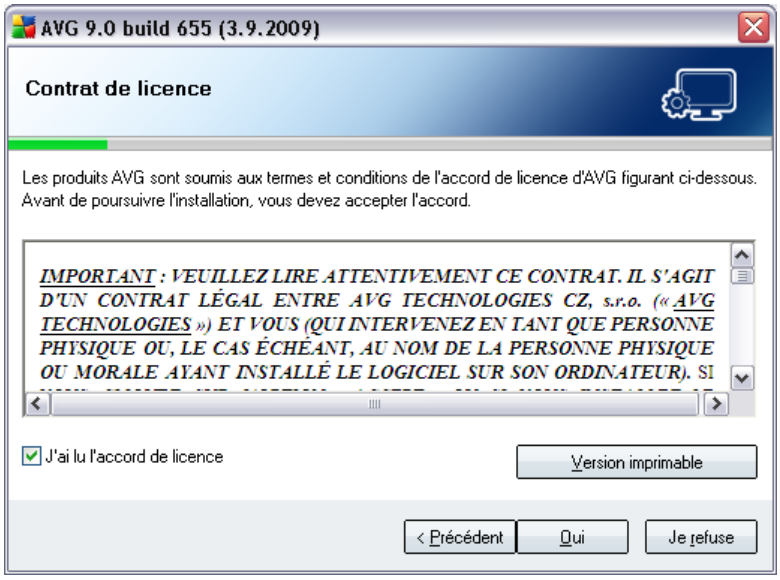


Le processus d'installation commence par l'affichage de la fenêtre ***Bienvenue dans le programme d'installation AVG***. Dans cette fenêtre, vous sélectionnez la langue qui sera utilisée au cours de l'installation. Dans la partie inférieure de la fenêtre, localisez l'option ***Choisissez la langue d'installation*** 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 ici 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.

5.2. Contrat de licence



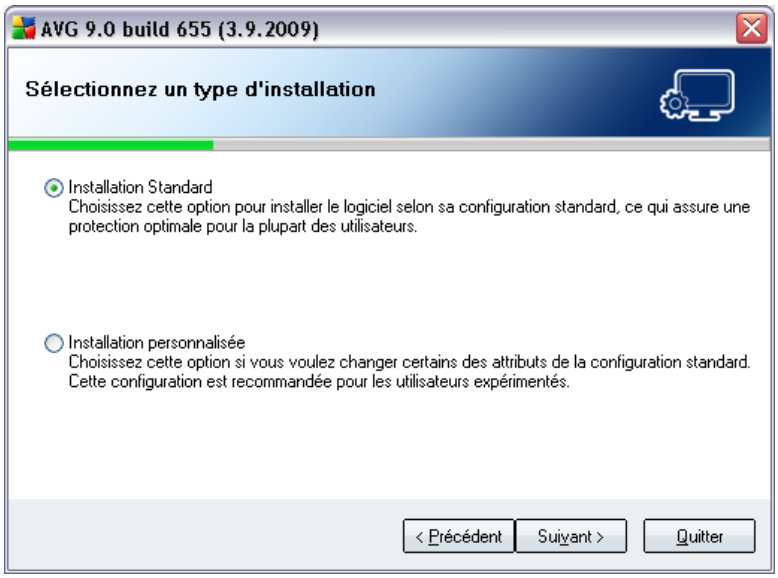
Le ***composant Licence*** affiche le texte complet de l'accord de licence avec AVG. Lisez-le attentivement et confirmez que vous avez lu, compris et accepté le contrat en cochant la case ***J'ai lu les termes du contrat de licence*** avant d'appuyer sur le bouton ***Accepter***.

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.

5.3. 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.

5.4. 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 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.

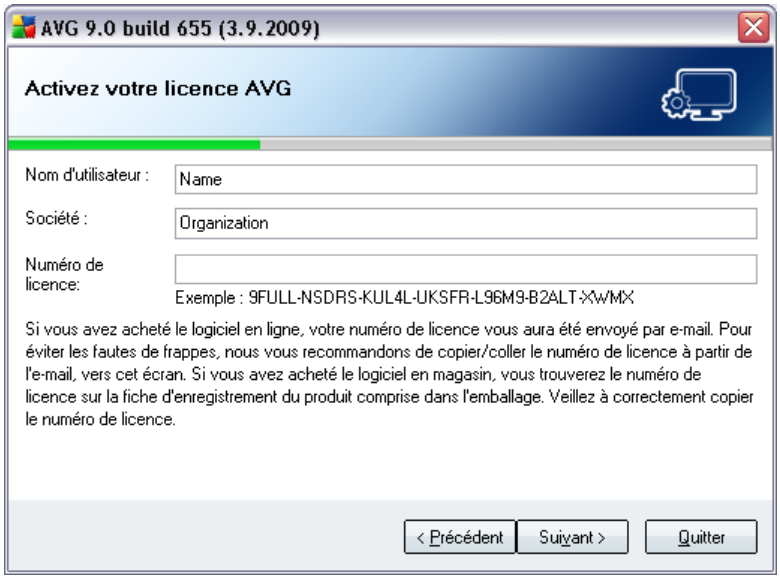
L'installation personnalisée est réservée aux utilisateurs expérimentés qui ont une raison valable d'installer AVG selon des paramètres non standard. Cela leur permet notamment d'adapter le programme à une configuration système spécifique.

5.5. Activer votre licence 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 d'achat se trouve sur la pochette du CD-ROM dans l'emballage du produit **AVG 9 Internet Security** . Le numéro de licence figure dans le mail de confirmation que vous avez reçu après avoir acheté le produit **AVG 9 Internet**

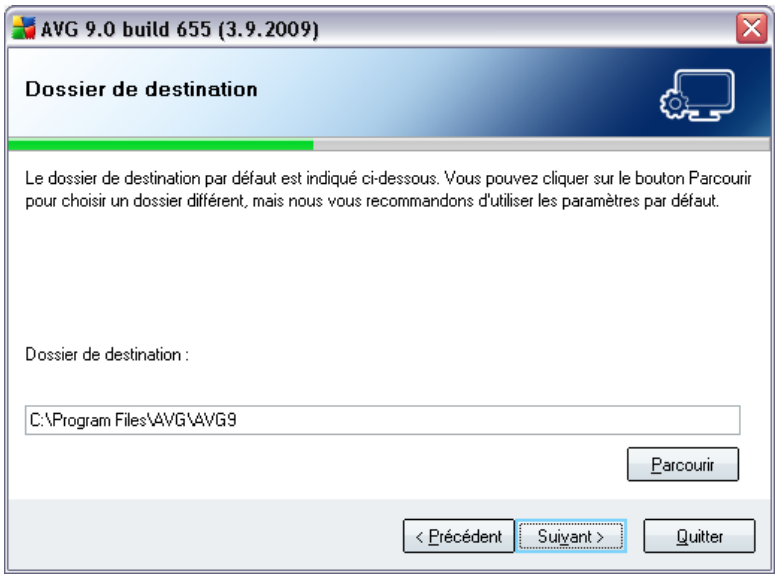
Security par Internet. Vous devez saisir le numéro tel qu'il apparaît. Si le numéro de licence est disponible au format électronique (*par exemple, dans un mail*), il est recommandé de l'insérer à l'aide de la méthode copier-coller.



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

Si, à l'étape précédente, vous avez opté pour l'installation standard, vous accédez directement à la boîte de dialogue de la ***Barre d'outils de sécurité AVG***. En revanche, si vous avez opté pour l'installation personnalisée, la boîte de dialogue ***Dossier de destination*** s'affiche.

5.6. Installation personnalisée - Dossier de destination

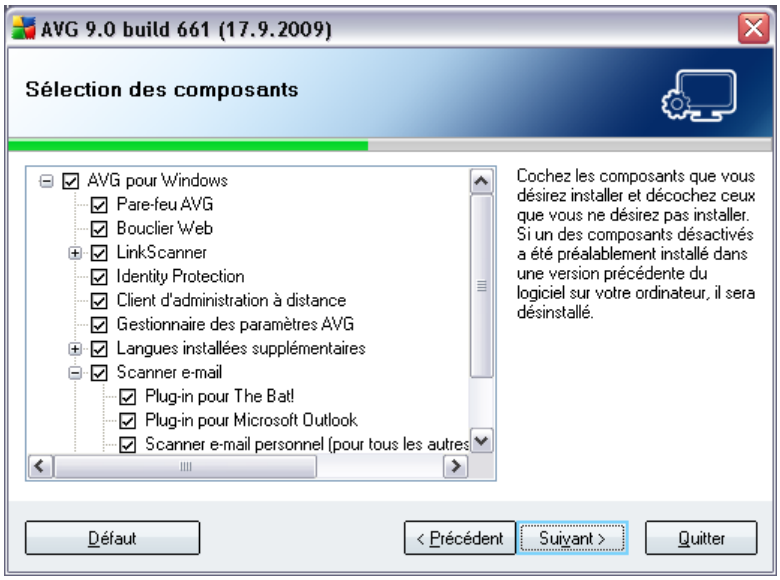


La boîte de dialogue ***Dossier de destination*** permet d'indiquer le dossier dans lequel les fichiers d'installation sont enregistrés. **AVG 9 Internet Security** Par défaut, AVG est installé dans le dossier contenant les fichiers de programme sur le lecteur C:. Si un tel dossier n'existe pas, vous serez invité à confirmer, dans une nouvelle boîte de dialogue, que vous acceptez qu'AVG le crée maintenant.

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.

5.7. Installation personnalisée - Sélection des composants



La boîte de dialogue ***Sélection des composants*** présente tous les composants qui peuvent être installés. **AVG 9 Internet Security** 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.

- ***Sélection de la langue***

  Dans la liste des composants à installer, vous pouvez définir la/les langue(s) dans la/lesquelles AVG doit être installé. Cochez la case ***Langues supplémentaires installées***, puis sélectionnez les langues désirées dans le menu correspondant.

- ***Plug-ins pour le scanner e-mail***

  Cliquez sur l'élément ***Scanner E-mail*** pour ouvrir et choisir le plug-in à installer afin d'assurer la sécurité de la messagerie. Par défaut, le ***Plug-in pour Microsoft Outlook*** sera installé. Si la licence que vous avez achetée inclut le composant ***Anti-Spam***, ce dernier sera aussi automatiquement installé. Une autre option spécifique est le ***Plug-in pour The Bat!*** Si vous utilisez un autre client de messagerie (*MS Exchange, Qualcomm Eudora, ...*), sélectionnez

l'option ***Scanner e-mail personnel*** afin de sécuriser votre communication automatiquement, quel que soit le programme que vous utilisez.

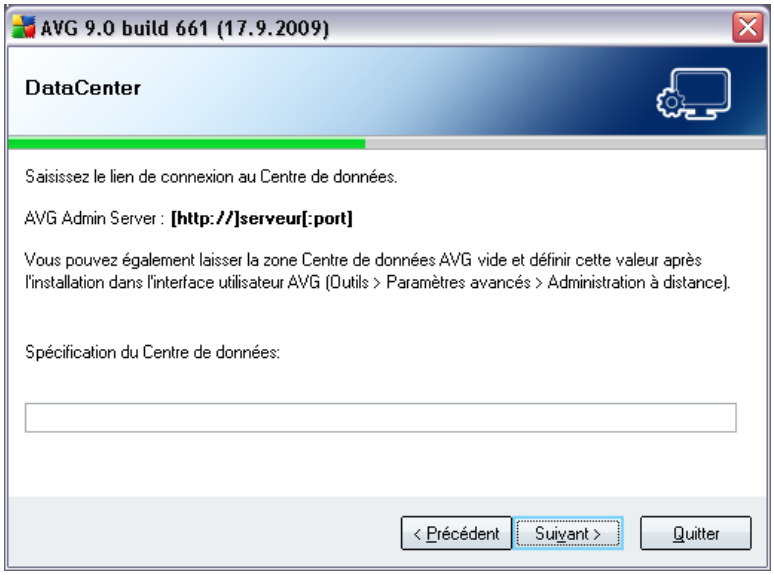
- ***Administration à distance***

  Si vous envisagez de connecter votre ordinateur au composant Administration à distance AVG plus tard, cochez également cet élément afin de l'installer.

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

5.8. AVG DataCenter

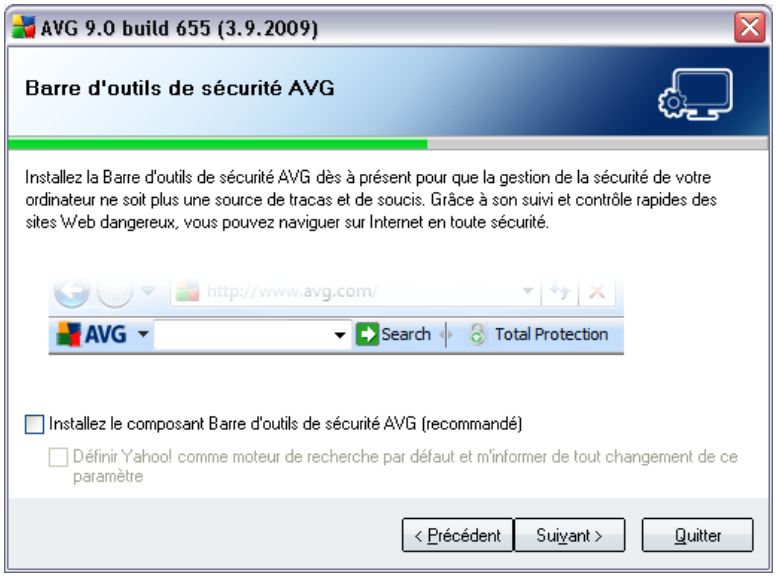
Si, dans la boîte de dialogue précédente, ***Installation personnalisée - Sélection du composant*** vous avez coché le composant ***Administration à distance*** à installer, - vous devez spécifier les paramètres ***AVG DataCenter***:



Dans le champ de texte ***Spécification AVG DataCenter*** entrez la chaîne de connexion ***AVG DataCenter***sous la forme d'un *serveur[:port]*. Si cette information n'est pas disponible pour l'instant, laissez ce champ vide et vous pouvez définir la configuration ultérieurement dans la boîte de dialogue***Paramètres avancés / Administration à distance***.

Pour plus d'informations sur Administration à distance AVG, reportez vous à la documentation AVG Edition Réseau (Guide de l'utilisateur); téléchargeable depuis le site Web AVGhttp://www.avg.com/).

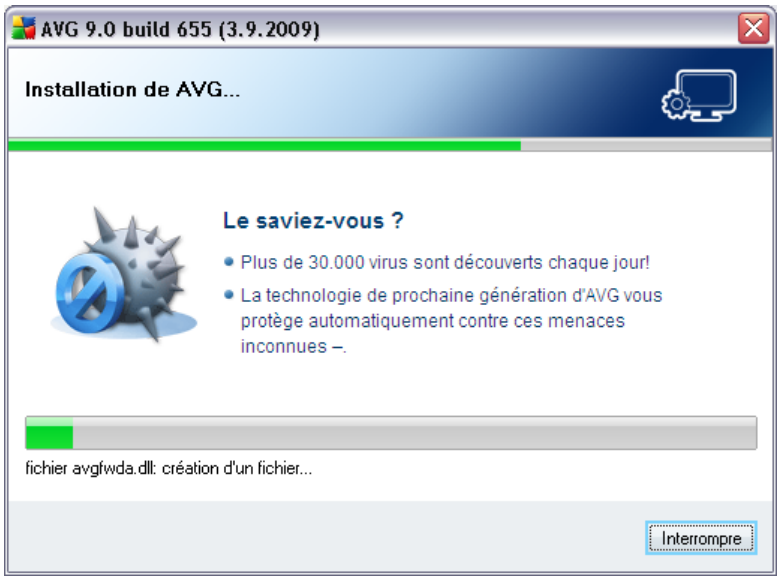
5.9. Barre d'outils de sécurité AVG



Dans la boîte de dialogue ***Barre d'outils de sécurité AVG***, vous pouvez décider si vous voulez installer la ***Barre d'outils de sécurité AVG*** (*vérification des résultats trouvés par les moteurs de recherche sur Internet*). Si vous ne modifiez pas les paramètres par défaut, ce composant sera installé automatiquement sur votre navigateur Internet afin de vous fournir la protection la plus complète pendant que vous surfez sur Internet.

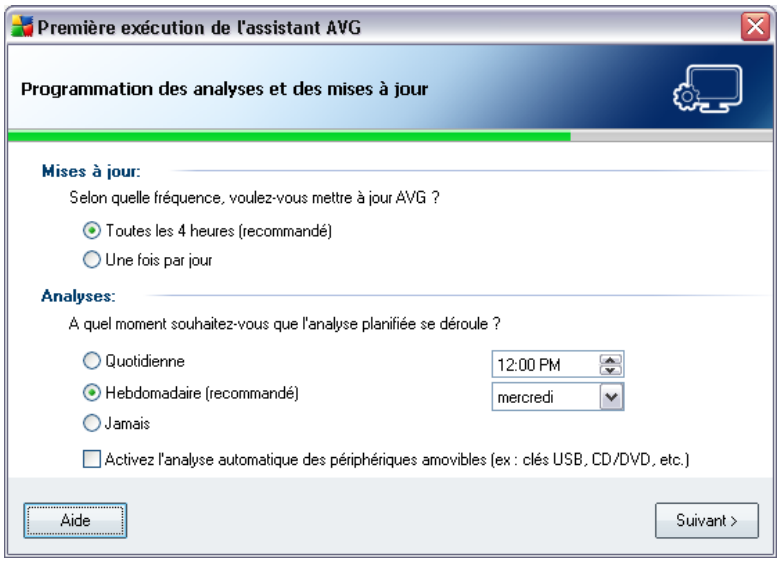
5.10. Installation d'AVG

La boîte de dialogue ***Installation d'AVG*** affiche la progression du processus d'installation et ne requiert aucune intervention de votre part :



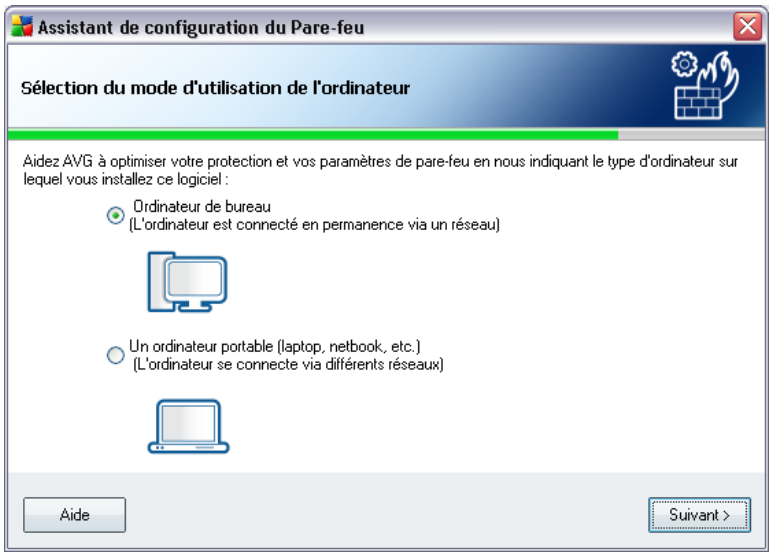
Une fois que l'installation est terminée, vous accédez automatiquement à la boîte de dialogue suivante.

5.11. Programmation des analyses et des mises à jour



Dans la boîte de dialogue de ***programmation des analyses et des mises à jour régulières***, définissez la fréquence de vérification des fichiers de mise à jour et précisez l'heure à laquelle l'analyse programmée doit avoir lieu. Il est recommandé de conserver les valeurs par défaut. Cliquez sur le bouton ***Suivant*** pour passer à l'écran suivant.

5.12. Sélection du mode d'utilisation de l'ordinateur



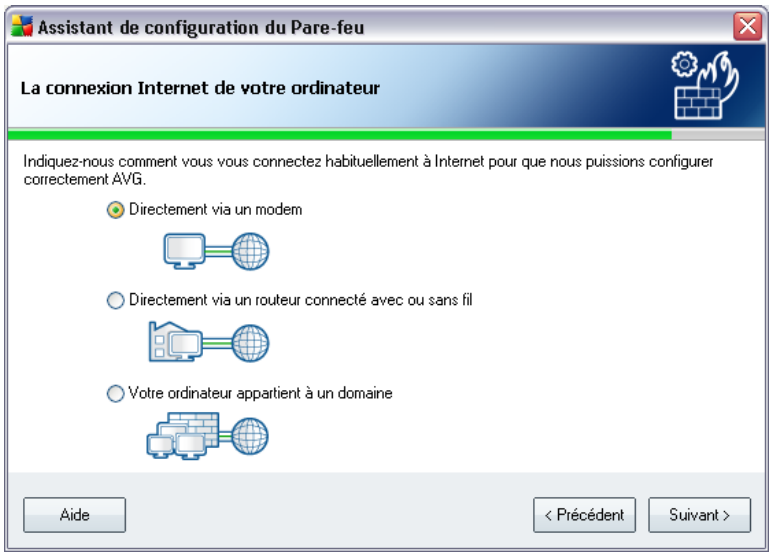
Dans cette boîte de dialogue, l'***assistant de configuration du Pare-feu*** vous demande d'indiquer le type d'ordinateur que vous utilisez. Il est évident, par exemple, que les règles de sécurité s'appliquant à un portable (*lorsque celui-ci est utilisé pour se connecter à Internet à partir d'un aéroport, d'une chambre d'hôtel, etc.*) doivent être plus strictes que celle d'un ordinateur appartenant à un domaine (*ordinateur relié au réseau de l'entreprise, etc.*). Sur la base du type d'usage de l'ordinateur sélectionné, les règles par défaut du ***Pare-feu*** seront définies en fonction d'un autre niveau de sécurité.

Vous avez le choix entre deux options :

- ***Ordinateur de bureau***
- ***Ordinateur portable***

Confirmez la sélection en cliquant sur le bouton ***Suivant*** et passez à la boîte de dialogue suivante.

5.13. Mode de connexion de votre réseau informatique



Dans cette boîte de dialogue, l'***assistant de configuration automatique*** du Pare-feu demande d'indiquer le mode de connexion de l'ordinateur à Internet. Basées sur le type de connexion sélectionné, les règles par défaut du ***Pare-feu*** seront définies en fonction de leur propre niveau de sécurité.

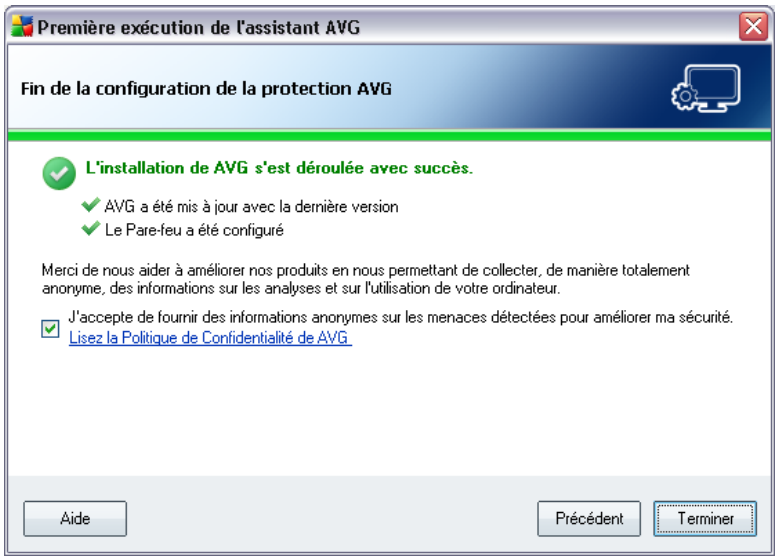
Vous avez le choix entre trois options :

- ***Directement à Internet***
- ***Petit réseau familial***
- ***Votre ordinateur fait partie d'un domaine***

Sélectionnez le type de connexion qui correspond le mieux à votre mode de connexion à Internet.

Confirmez la sélection en cliquant sur le bouton ***Suivant*** et passez à la boîte de dialogue suivante.

5.14. La configuration de la protection AVG est terminée



AVG 9 Internet Security est maintenant configuré.

Dans cette boîte de dialogue, vous pouvez activer l'option permettant de signaler de façon anonyme les exploits et les sites Web malveillants aux laboratoires d'AVG. Pour ce faire, cochez l'option ***J'accepte de fournir des informations ANONYMES sur les menaces détectées pour améliorer ma sécurité***.

Pour finir, cliquez sur le bouton ***Terminer***. Le redémarrage de votre ordinateur peut être nécessaire pour commencer à utiliser AVG.

6. Opérations à effectuer après l'installation

6.1. Enregistrement du produit

Après l'installation d'**AVG 9 Internet Security**, veuillez enregistrer votre produit en ligne sur le site Web d'AVG http://www.avg.com/, page ***Enregistrement*** (*suivez les instructions fournies à la page*). Après l'enregistrement, vous bénéficierez de tous les avantages associés à votre compte utilisateur AVG et aurez accès à la lettre d'informations d'AVG ainsi qu'aux autres services réservés exclusivement aux utilisateurs enregistrés.

6.2. Accès à l'interface utilisateur

L'***interface utilisateur d'AVG*** est accessible de plusieurs façons :

- double-cliquez sur l'icône AVG dans la barre d'état système
- double-cliquez sur l'icône AVG située sur le Bureau
- dans le menu ***Démarrer/ Programmes/AVG 9.0/Interface utilisateur AVG***

6.3. Analyse complète

Le risque de contamination de l'ordinateur par un virus avant l'installation d'**AVG 9 Internet Security** ne doit pas être écarté. C'est pour cette raison qu'il est recommandé de lancer une ***analyse complète*** afin de s'assurer qu'aucune infection ne s'est déclarée dans votre ordinateur.

Pour obtenir des instructions sur l'exécution d'une ***analyse complète***, reportez-vous au chapitre ***Analyse AVG***.

6.4. Test EICAR

Pour confirmer que l'installation d'**AVG 9 Internet Security** est correcte, effectuez un test EICAR.

Cette méthode standard et parfaitement sûre sert à tester le fonctionnement de l'anti-virus en introduisant un pseudo-virus ne contenant aucun fragment de code viral et ne présentant absolument aucun danger. La plupart des produits réagissent comme s'il s'agissait d'un véritable virus (*en lui donnant un nom significatif du type*

« *EICAR-AV-Test* »). Vous pouvez télécharger le test Eicar à partir du site Web Eicar à l'adresse www.eicar.com où vous trouverez toutes les informations nécessaires.

Essayez de télécharger le fichier ***eicar.com*** et enregistrez-le sur votre disque dur local. Immédiatement après avoir confirmé le téléchargement du fichier test, le ***Bouclier résident*** réagit en émettant un avertissement. Ce message du ***Bouclier résident*** indique qu'AVG est installé correctement sur votre ordinateur.

Si AVG ne considère par le fichier test Eicar comme un virus, il est recommandé de vérifier de nouveau la configuration du programme.

6.5. Configuration par défaut d'AVG

La configuration par défaut (*c'est-à-dire la manière dont l'application est paramétrée à l'issue de l'installation*) d'**AVG 9 Internet Security** est définie par le fournisseur du logiciel, qui ajuste les composants et les fonctions de manière à obtenir des performances optimales.

Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté.

Il est possible d'apporter certaines corrections mineures aux paramètres des composants AVG, directement dans l'interface utilisateur du composant concerné. Si vous voulez modifier la configuration AVG pour mieux l'adapter à vos besoins, accédez aux ***paramètres avancés d'AVG*** : cliquez sur le menu ***Outils/Paramètres avancés*** et modifiez la configuration AVG dans la boîte de dialogue ***Paramètres avancés d'AVG*** qui s'affiche.

7. Interface utilisateur AVG

AVG 9 Internet Security apparaît dans la fenêtre principale :

La fenêtre principale comprend plusieurs parties :

- ***Menu système*** *(barre de menus en haut de la fenêtre)* : ce système de navigation standard donne accès à l'ensemble des composants, des services et des fonctions AVG - détails >>
- ***Informations sur l'état de la sécurité*** *(partie supérieure de la fenêtre)* : donne des informations sur l'état actuel du programme AVG - détails >>
- ***Liens d'accès rapide*** *(partie gauche de la fenêtre)* : ces liens permettent d'accéder rapidement aux tâches AVG les plus importantes et les plus

courantes - détails >>

- ***Présentation des composants*** *(partie centrale de la fenêtre)* : présentation générale de tous les composants AVG installés - détails >>
- ***Statistiques*** *(partie gauche inférieure de la fenêtre)* : toutes les données statistiques sur le fonctionnement du programme - détails >>
- ***Icône d'état AVG*** *(coin inférieur droit de l'écran, sur la barre d'état système)* : elle indique l'état actuel du programme AVG - détails >>

7.1. Menu système

Le ***menu système*** est le système de navigation standard propre à toutes les applications Windows. Il se présente sous la forme d'une barre horizontale en haut de la fenêtre principale d'**AVG 9 Internet Security**. Servez-vous du menu système pour accéder aux composants, fonctions et services AVG de votre choix.

Le menu système inclut cinq sections principales :

7.1.1. Fichier

- ***Quitter*** - ferme l'interface utilisateur d'**AVG 9 Internet Security** . L'application AVG continue néanmoins de s'exécuter en arrière-plan de sorte que l'ordinateur reste protégé !

7.1.2. Composants

L'option ***Composants*** du menu système contient des liens qui renvoient vers tous les composants AVG installés et ouvrent la boîte de dialogue par défaut associée dans l'interface utilisateur :

- ***Présentation du système*** - bascule sur l'interface utilisateur par défaut et affiche une présentation générale de tous les composants installés, ainsi que leur état
- ***Anti-Virus*** - ouvre la page par défaut du composant ***Anti-Virus***
- ***Anti-Rootkit*** - ouvre la page par défaut du composant ***Anti-Rootkit***
- ***Anti-Spyware*** - ouvre la page par défaut du composant ***Anti-Spyware***
- ***Pare-feu*** - ouvre la page par défaut du composant ***Pare-feu***

- ***LinkScanner*** - ouvre la page par défaut du composant ***LinkScanner***
- ***System Tools*** - ouvre la page par défaut des ***System Tools***
- ***Anti-Spam*** - ouvre la page par défaut du composant ***Anti-Spam***
- ***Scanner e-mail*** - ouvre la page par défaut du composant ***Scanner e-mail***
- ***Identity Protection*** - ouvre la page par défaut du composant ***Identity Protection***
- ***Licence*** - ouvre la page par défaut du composant ***Licence***
- ***Bouclier Web*** - ouvre la page par défaut du composant ***Bouclier Web***
- ***Bouclier résident*** - ouvre la page par défaut du composant ***Bouclier résident***
- ***Mise à jour*** - ouvre la page par défaut du composant ***Mise à jour***

7.1.3. Historique

- ***Résultats des analyses*** - bascule sur l'interface d'analyse AVG et ouvre notamment la boîte de dialogue ***Résultats d'analyse***
- ***Détection du Bouclier résident*** - ouvre la boîte de dialogue contenant une vue générale des menaces détectées par le ***Bouclier résident***
- ***Détection du Scanner e-mail*** - ouvre la boîte de dialogue des pièces jointes détectées comme dangereuses par le composant ***Scanner e-mail***
- ***Objets trouvés par Bouclier Web*** - ouvre la boîte de dialogue contenant une vue générale des menaces détectées par le ***Bouclier Web***
- ***Quarantaine*** - ouvre l'interface de la zone de confinement (***Quarantaine***) dans laquelle AVG place les infections détectées qui n'ont pu, pour une raison quelconque, être réparées automatiquement A l'intérieur de cette quarantaine, les fichiers infectés sont isolés. L'intégrité de la sécurité de l'ordinateur est donc garantie et les fichiers infectés sont stockés en vue d'une éventuelle réparation future.
- ***Journal de l'historique des événements*** - ouvre l'interface de l'historique des événements présentant toutes les actions d'**AVG 9 Internet Security** qui ont été consignées.

- ***Pare-feu*** - ouvre l'interface de configuration du pare-feu à l'onglet ***Journaux*** qui présente une vue générale des actions du pare-feu

7.1.4. Outils

- ***Analyse Complète*** - ouvre l'interface d'analyse AVG et procède à l'analyse de l'intégralité des fichiers de l'ordinateur

- ***Analyser le dossier sélectionné*** - ouvre l'interface d'analyse AVG et permet de spécifier, au sein de l'arborescence de l'ordinateur, les fichiers et les dossiers à analyser

- ***Analyser le fichier*** - permet de lancer sur demande l'analyse d'un fichier sélectionné dans l'arborescence du disque

- ***Mise à jour depuis*** - lance automatiquement le processus de mise à jour d' **AVG 9 Internet Security**

- ***Mise à jour depuis le répertoire*** - procède à la mise à jour grâce aux fichiers de mise à jour situés dans le dossier spécifié de votre disque local. Notez que cette option n'est recommandée qu'en cas d'urgence, c'est-à-dire si vous ne disposez d'aucune connexion Internet (*si, par exemple, l'ordinateur est infecté et déconnecté d'Internet ou s'il est relié à un réseau sans accès à Internet, etc.*). Dans la nouvelle fenêtre qui apparaît, sélectionnez le dossier dans lequel vous avez placé le fichier de mise à jour et lancez la procédure de mise à jour.

- ***Paramètres avancés*** - ouvre la boîte de dialogue ***Paramètres avancés AVG*** dans laquelle vous modifiez au besoin la **AVG 9 Internet Security** configuration. En général, il est recommandé de conserver les paramètres par défaut de l'application tels qu'ils ont été définis par l'éditeur du logiciel.

- ***Paramètres du Pare-feu*** - ouvre une nouvelle boîte de dialogue permettant de définir la configuration avancée du composant ***Pare-feu***

7.1.5. Aide

- ***Sommaire*** - ouvre les fichiers d'aide du programme AVG

- ***Obtenir de l'aide en ligne*** - affiche le site Web d'AVG (http://www.avg.com/) à la page du centre de support clients

- ***Site Internet AVG*** - ouvre le site Web d'AVG (http://www.avg.com/)

- ***A propos des virus et des menaces*** - ouvre l'***Encyclopédie des virus en***

ligne, où vous pouvez consulter des informations détaillées sur le virus identifié

- ***Réactiver*** - ouvre la boîte de dialogue ***Activer AVG*** avec les données que vous avez saisies dans la boîte de dialogue ***Personnaliser AVG*** au cours du processus d'installation. Dans cette boîte de dialogue, vous indiquez votre numéro de licence en lieu et place de la référence d'achat (*le numéro indiqué lors de l'installation d'AVG*) ou de votre ancien numéro (*si vous installez une mise à niveau du produit AVG, par exemple*).

- ***Enregistrer maintenant*** - renvoie à la page d'enregistrement du site Web d'AVG (http://www.avg.com/). Veuillez compléter le formulaire d'enregistrement ; seuls les clients ayant dûment enregistré leur produit AVG peuvent bénéficier de l'assistance technique gratuite.

- ***A propos de AVG*** - ouvre la boîte de dialogue ***Informations*** comportant cinq onglets spécifiant le nom du programme, la version du programme et de la base de données virale, les informations système, le contrat de licence et les informations de contact d'***AVG Technologies CZ***.

7.2. Informations sur l'état de la sécurité

La section contenant les ***informations sur l'état de la sécurité*** figure dans la partie supérieure de la fenêtre principale AVG. Les informations sur l'état en cours de la sécurité du programme **AVG 9 Internet Security** sont toujours présentées à cet emplacement. Les icônes illustrées ont la signification suivante :

 L'icône verte indique qu'AVG est pleinement opérationnel. Votre système est totalement protégé et à jour ; tous les composants installés fonctionnent convenablement.

 L'icône orange signale qu'un ou plusieurs composants ne sont pas correctement configurés, il est conseillé d'examiner leurs propriétés ou paramètres. Aucun problème critique à signaler ; vous avez sans doute choisi de désactiver certains composants. Vous êtes protégé par AVG. Certains paramètres d'un composant réclament toutefois votre attention. Son nom est indiqué dans la section d'***informations sur l'état de la sécurité*** .

Cette icône s'affiche également si, pour une raison quelconque, vous décidez d' ignorer l'erreur d'un composant (*l'option Ignorer l'état du composant est*

disponible dans le menu contextuel apparaissant suite à un clic droit sur l'icône du composant en question, dans la vue des composants de la fenêtre principale AVG). Vous pouvez être amené à utiliser cette option dans certaines situations, mais il est vivement conseillé de désactiver l'option ***Ignorer l'état du composant*** dès que possible.

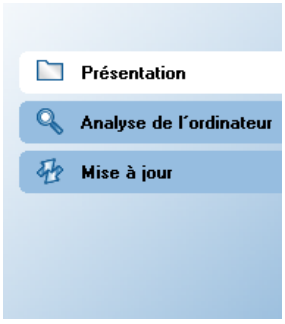
 L'icône de couleur rouge signale que le programme AVG est dans un état critique. Un ou plusieurs composants ne fonctionnent pas convenablement et AVG n'est plus en mesure d'assurer la protection de l'ordinateur. Veuillez immédiatement vous porter sur le problème signalé. Si vous ne pouvez pas le résoudre, contactez l'équipe du support technique AVG.

Il est vivement conseillé de ne pas ignorer les informations sur l'***état de la sécurité*** et, en cas de problème indiqué, de rechercher immédiatement une solution. A défaut, vous risquez de mettre en péril la sécurité de votre système.

Remarque : *vous pouvez à tout moment obtenir des informations l'état d'AVG en consultant l'icône de la barre d'état système.*

7.3. Liens d'accès rapide

Les liens d'accès rapide *(panneau gauche de l'interface utilisateur AVG)* permettent d'accéder immédiatement aux fonctions AVG les plus importantes et les plus utilisées :



- ***Présentation***- ce lien permet de passer de l'interface AVG affichée à l'interface par défaut, qui affiche tous les composants installés - voir le chapitre ***Présentation des composants >>***
- ***Analyse de l'ordinateur*** - ce lien affiche l'interface d'analyse d'AVG dans laquelle vous pouvez lancer directement des analyses, programmer des analyses ou modifier leurs paramètres - voir le chapitre ***Analyse AVG >>***

- ***Mise à jour*** - ce lien ouvre l'interface de mise à jour et lance immédiatement le processus de mise à jour du programme AVG - voir le chapitre ***Mises à jour AVG*** >>

Ces liens sont accessibles en permanence depuis l'interface utilisateur. Lorsque vous cliquez sur un lien d'accès rapide, l'interface utilisateur graphique ouvre une nouvelle boîte de dialogue, mais les liens d'accès rapides restent disponibles. Par ailleurs, le processus est représenté de manière visuelle - (*voir illustration 2)*.

7.4. Présentation des composants

La section ***Présentation des composants*** figure dans le panneau central de l' interface utilisateur AVG. La section comprend deux parties :

- Présentation de tous les composants installés représentés par une icône accompagnée d'un message signalant si le composant est actif ou non
- Description du composant sélectionné

Dans **AVG 9 Internet Security** , le panneau de ***présentation des composants*** contient des renseignements sur les composants suivants :

- ***Le composant Anti-Virus*** garantit que l'ordinateur est protégé contre les virus essayant de pénétrer dans le système- détails >>
- ***Le composant Anti-Spyware*** analyse vos applications en arrière-plan lorsqu'elles sont activées - détails >>
- ***Le composant Anti-Spam*** vérifie tous les mails entrants et marque les courriers indésirables comme SPAM - détails >>
- ***Le composant Pare-feu*** régit la manière dont votre ordinateur échange des données avec les autres ordinateurs par Internet ou par le réseau local - détails >>
- ***Le composant LinkScanner*** examine les résultats de recherche affichés dans votre navigateur Internet - détails >>
- ***Le composant Anti-Rootkit*** détecte les programmes et les technologies cherchant à dissimuler des codes malveillants - détails >>
- ***Le composant System Tools*** décrit de manière détaillée l'environnement d' - détails >>

- ***Le composant Scanner e-mail*** vérifie la présence éventuelle de virus dans les mails entrants et sortants - détails >>
- ***Identity Protection*** - ce composant est conçu pour empêcher les usurpateurs d'identité de dérober vos ressources numériques personnelles importantes - détails >>
- ***Le composant Licence*** affiche le texte complet de l'accord de licence AVG - détails >>
- ***Le composant Bouclier Web*** analyse toutes les données téléchargées par le navigateur Internet - détails >>
- ***Le composant Bouclier résident*** s'exécute en arrière-plan et analyse les fichiers lorsqu'il sont copiés, ouverts ou enregistrés - détails >>
- ***Le composant Mise à jour*** recherche la présence d'une mise à jour AVG - détails >>

Cliquer sur l'icône d'un composant permet de le mettre en surbrillance dans la vue générale des composants. Par ailleurs, la fonctionnalité de base du composant est décrite en bas de l'interface utilisateur. Cliquer deux fois sur l'icône d'un composant a pour effet d'ouvrir la propre interface du composant présentant une liste de données statistiques.

Cliquez avec le bouton droit de la souris sur l'icône d'un composant : après l'ouverture de l'interface graphique du composant en question, vous serez en mesure de sélectionner l'état ***Ignorer l'état du composant***. Sélectionnez cette option pour indiquer que vous avez noté l'état incorrect du composant, mais que vous souhaitez conserver la configuration AVG en l'état et ne plus être avisé de l'erreur par la couleur grisée de l'icône de la barre d'état système.

7.5. Statistiques

La section ***Statistiques*** figure en bas à gauche de l'interface utilisateur AVG. Elle présente une liste d'informations sur le fonctionnement du programme :

- ***Analyse*** - indique la date à laquelle la dernière analyse a eu lieu
- ***Mise à jour*** - indique la date à laquelle une mise à jour a été exécutée pour la dernière fois
- ***BD virale***- précise la version de la base de données virale actuellement installée

- ***Version d'AVG*** - indique la version du programme actuellement installée *(le numéro se présente sous la forme 8.0.xx. 8.0 désigne la version du produit et xx le numéro du build)*

- ***Expiration de la licence*** - précise la date à laquelle votre licence AVG cessera d'être valide

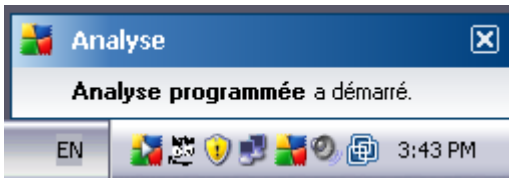
7.6. Icône de la barre d'état système

L'icône de la barre d'état système (*dans la barre des tâches Windows*) précise l'état en cours d'**AVG 9 Internet Security**. Elle est toujours visible dans la barre d'état, que la fenêtre principale AVG soit ouverte ou fermée.

Lorsqu'elle est simplement en couleur, l'icône de la ***barre d'état système*** indique que tous les composants AVG sont actifs et entièrement opérationnels. Par ailleurs, l'icône AVG dans la barre d'état s'affiche en couleurs. Si AVG signale une erreur mais que vous en avez été averti et avez choisi·d'***ignorer l'état du composant***.

Une icône grise avec un point d'exclamation signale un problème (*composant inactif, erreur, etc.*). Double-cliquez sur l'***icône de la barre d'état système*** pour ouvrir la fenêtre et modifier un composant.

L'icône de la barre d'état système fournit également des informations sur les activités actuelles du programme AVG et le changement éventuel de l'état du programme (*par exemple, le lancement automatique d'une analyse programmée ou d'une mise à jour, le changement de profil du pare-feu, une modification relative à l'état d'un composant, une erreur...*) par la fenêtre contextuelle qui s'affiche depuis l'icône de la barre d'état système d'AVG :



L'***icône de la barre d'état système*** peut aussi servir de lien d'accès rapide à la fenêtre principale AVG. Pour l'utiliser, il suffit de double-cliquer dessus. En cliquant avec le bouton droit de la souris sur l'***icône de la barre d'état système***, un menu contextuel contenant les options suivantes apparaît :

- ***Ouvrir l'Interface utilisateur AVG*** - cette commande permet d'afficher l' interface utilisateur AVG

- ***Mettre à jour*** - cette option permet de lancer une mise à jour immédiate

8. Composants AVG

8.1. Anti-Virus

8.1.1. Principes de l'Anti-Virus

Le moteur d'analyse du logiciel anti-virus examine les fichiers et l'activité des fichiers (ouverture/fermeture des fichiers, etc.) afin de déceler la présence de virus connus. Tout virus détecté sera bloqué, puis effacé ou placé en quarantaine. La plupart des anti-virus font également appel à la méthode heuristique en utilisant les caractéristiques des virus, appelées également signatures des virus, pour analyser les fichiers. En d'autres termes, l'analyse anti-virus est en mesure de filtrer un virus inconnu si ce nouveau virus porte certaines caractéristiques de virus existants.

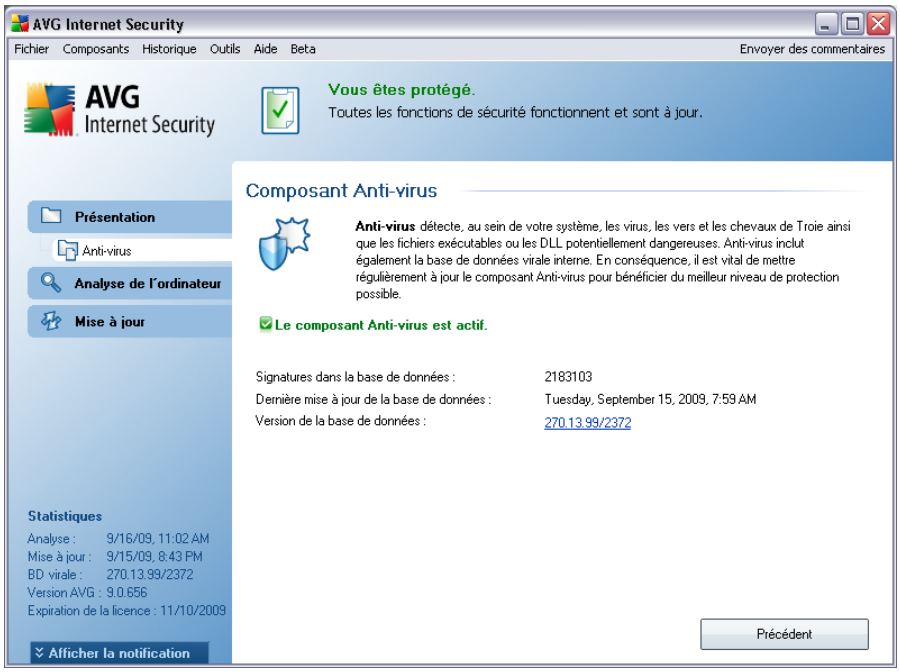
Rappelons que la fonction essentielle d'une protection anti-virus consiste à empêcher l'exécution de tout virus inconnu sur l'ordinateur.

Aucune technologie n'est infaillible, c'est pourquoi la fonction ***Anti-Virus*** combine plusieurs technologies pour repérer ou identifier un virus et garantir la protection de votre ordinateur :

- Analyse - recherche d'une chaîne de caractère typique d'un virus donné
- Analyse heuristique - émulation dynamique des instructions de l''objet analysé dans un environnement de machine virtuelle
- Détection générique - détection des instructions caractéristiques d'un virus ou d'un groupe de virus donné

AVG peut aussi analyser et détecter des exécutables ou bibliothèques DLL qui peuvent se révéler malveillants pour le système. De telles menaces portent le nom de programmes potentiellement dangereux (types variés de spywares, d'adwares, etc.). Enfin, AVG analyse la base de registre de votre système afin de rechercher toute entrée suspecte, les fichiers Internet temporaires ou les cookies. Il vous permet de traiter les éléments à risque de la même manière que les infections.

8.1.2. Interface de l'Anti-Virus



L'interface du composant ***Anti-Virus*** donne des informations de base sur la fonctionnalité du composant, sur son état actuel (Le composant *Anti-Virus est actif.*), ainsi que des statistiques sur la fonction ***anti-virus*** :

- ***Signatures dans la base de données***- indique le nombre de virus définis dans la version actualisée de la base de données virale
- ***Dernière mise à jour de la base de données***- précise la date et l'heure à laquelle la base de données a été mise à jour
- ***Version de la base de données virale*** - spécifie le numéro de la version la plus récente de la base de données ; ce nombre est incrémenté à chaque mise à jour de la base de données

L'interface du composant n'a qu'un seul bouton de commande (***Précédent***) - ce bouton permet de revenir à l'interface utilisateur AVG par défaut (présentation des composants).

Remarque : *l'éditeur du logiciel a configuré tous les composants AVG de manière à obtenir des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être*

*réalisé par un utilisateur expérimenté. Si vous devez modifier la configuration d'AVG, sélectionnez le menu **Outils / Paramètres avancés** et modifiez la configuration d'AVG dans la boîte de dialogue Paramètres avancés d'AVG qui apparaît.*

8.2. Anti-Spyware

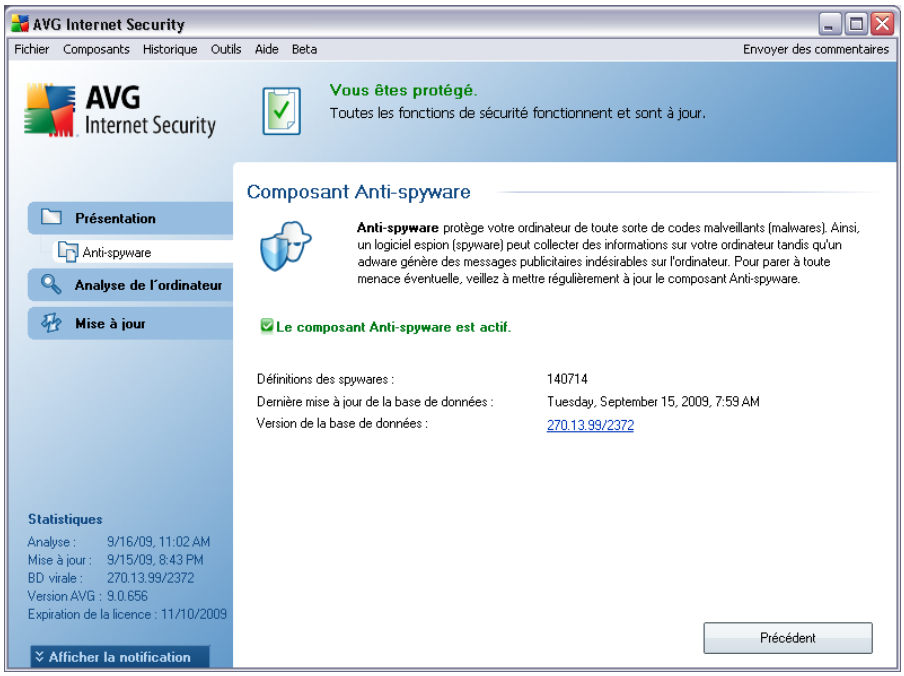
8.2.1. Principes de l'Anti-Spyware

Le terme spyware désigne généralement un code malicieux et plus précisément un logiciel qui collecte des informations depuis l'ordinateur d'un utilisateur, à l'insu de celui-ci. Certains spywares installés volontairement peuvent contenir des informations à caractère publicitaire, des pop-ups ou d'autres types de logiciels déplaisants.

Actuellement, les sites Web au contenu potentiellement dangereux sont les sources d'infection les plus courantes. D'autres vecteurs comme la diffusion par mail ou la transmission de vers et de virus prédominent également. La protection la plus importante consiste à définir un système d'analyse en arrière-plan, activé en permanence (tel que le composant ***Anti-Spyware***) agissant comme un bouclier résident afin d'analyser les applications exécutées en arrière-plan.

L'introduction de codes malicieux dans votre ordinateur, avant installation du programme AVG, ou en cas d'oubli de l'application des dernières mises à jour de la base de données **AVG 9 Internet Security** et du programme est un risque potentiel. Pour cette raison, AVG vous offre la possibilité d'analyser intégralement votre ordinateur à l'aide d'une fonction prévue à cet effet. Il se charge également de détecter les codes malicieux inactifs ou en sommeil (ceux qui ont été téléchargés, mais non activés).

8.2.2. Interface de l'Anti-Spyware



L'interface du composant ***Anti-Spyware*** donne un bref aperçu de la fonctionnalité du composant et fournit des informations sur son état actuel (Le composant *Anti-Spyware est actif*) et des statistiques sur le composant ***Anti-Spyware*** :

- ***Signatures de spywares :*** - indique le nombre d'exemples de spywares définis dans la dernière version de la base de données
- ***Dernière mise à jour de la base de données***- précise la date et l'heure à laquelle la base de données a été mise à jour
- ***Version de la base de données*** - spécifie le numéro de la version de la base de données la plus récente ; ce nombre est incrémenté à chaque mise à jour de la base de données

L'interface du composant n'affiche qu'un seul bouton de commande (***Précédent***) - ce bouton permet de revenir à l'interface utilisateur AVG par défaut (présentation des composants).

Remarque : *l'éditeur du logiciel a configuré tous les composants AVG de manière à obtenir des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être*

*réalisé par un utilisateur expérimenté. Si vous devez modifier la configuration d'AVG, sélectionnez le menu **Outils / Paramètres avancés** et modifiez la configuration d'AVG dans la boîte de dialogue Paramètres avancés d'AVG qui apparaît.*

8.3. Anti-Spam

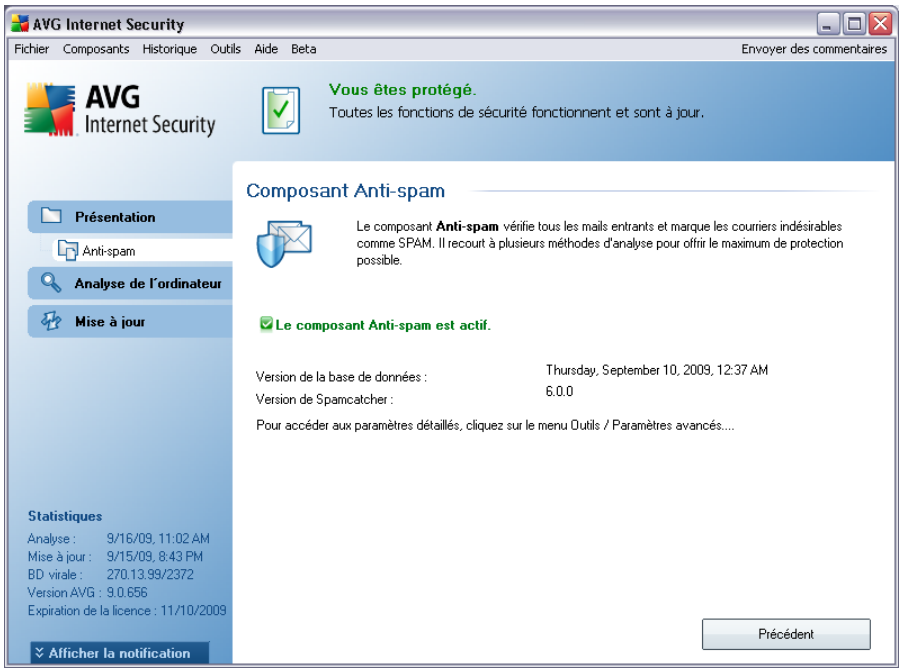
Le terme « spam » désigne un message indésirable ; il s'agit généralement d'un produit ou d'un service à caractère publicitaire envoyé en masse à de nombreuses adresses électroniques ayant pour conséquence d'encombrer les boîtes aux lettres des destinataires. Il faut distinguer le spam des autres messages 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.

8.3.1. Principes de l'Anti-Spam

Le composant AVG Anti-Spam vérifie tous les messages entrants et marque les courriers indésirables comme étant du SPAM. ***AVG Anti-Spam*** est capable de modifier l'objet du message (*identifié comme du spam*) en ajoutant une chaîne spéciale. Il est très facile ensuite de filtrer vos messages dans votre client de messagerie.

Le composant AVG Anti-Spam utilise plusieurs méthodes d'analyse pour traiter chaque message afin d'offrir un niveau de protection maximal contre les messages indésirables. Pour détecter les messages indésirables, le composant ***AVG Anti-Spam*** exploite une base de données régulièrement mise à jour. Vous pouvez également faire appel à des serveurs RBL (*(bases de données publiques répertoriant les adresses électroniques d'expéditeurs de spam connus*) et ajouter manuellement des adresses électroniques à votre liste blanche (*pour ne jamais les considérer comme du spam*) et à votreliste noire (*(pour systématiquement les considérer comme du spam*).

8.3.2. Interface de l'Anti-Spam



La boîte de dialogue du composant ***Anti-Spam*** décrit brièvement le fonctionnement du composant, indique son état actuel (Le composant *Anti-Spam est actif*) et fournit les données statistiques suivantes :

- ***Dernière mise à jour de la base de données***- précise la date et l'heure à laquelle la base de données a été mise à jour
- ***Version de Spamcatcher*** - définit le numéro de la dernière version du moteur anti-spam

L'interface du composant n'affiche qu'un seul bouton de commande (***Précédent***) - ce bouton permet de revenir à l'interface utilisateur AVG par défaut (*présentation des composants*).

Remarque : *l'éditeur du logiciel a configuré tous les composants AVG de manière à obtenir des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté. Si vous devez modifier la configuration d'AVG, sélectionnez le menu* ***Outils / Paramètres avancés*** *et modifiez la configuration d'AVG dans la boîte de dialogue Paramètres avancés d'AVG qui apparaît.*

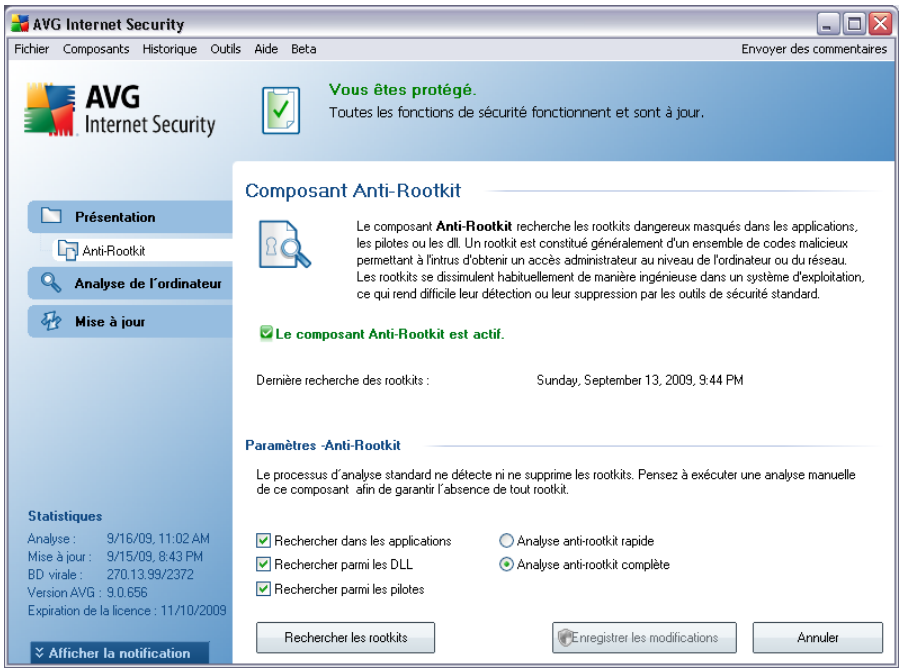
8.4. Anti-Rootkit

Un rootkit est un programme conçu pour prendre le contrôle du système, sans l'autorisation de son propriétaire et de son administrateur légitime. Un accès matériel est rarement nécessaire car un rootkit est prévu pour s'introduire dans le système d'exploitation exécuté sur le matériel. En règle générale, les rootkits dissimulent leur présence dans le système en contournant ou en ne se conformant pas aux mécanismes de sécurité standard du système d'exploitation. Souvent, ils prennent la forme de chevaux de Troie et font croire aux utilisateurs que leur exécution est sans danger pour leurs ordinateurs. Pour parvenir à ce résultat, différentes techniques sont employées : dissimulation de processus aux programmes de contrôle ou masquage de fichiers ou de données système, au système d'exploitation.

8.4.1. Principes de l'Anti-Rootkit

Le composant AVG Anti-Rootkit est un outil spécialisé dans la détection et la suppression des rootkits dangereux. Ces derniers sont des programmes et technologies de camouflage destinés à masquer la présence de logiciels malveillants sur l'ordinateur. ***AVG Anti-Rootkit*** peut détecter des rootkits selon un ensemble de règles prédéfinies. Notez que tous les rootkits sont détectés (*pas seulement ceux qui sont infectés*). Si ***AVG Anti-Rootkit*** détecte un rootkit, cela ne veut pas forcément dire que ce dernier est infecté. Certains rootkits peuvent être utilisés comme pilotes ou faire partie d'applications correctes.

8.4.2. Interface de l'Anti-Rootkit



L'interface utilisateur ***Anti-Rootkit*** décrit brièvement le fonctionnement du composant, indique son état actuel (Le composant*Anti-Rootkit est actif.*) et fournit des informations sur la dernière analyse ***Anti-Rootkit*** effectuée.

Dans la partie inférieure de la boîte de dialogue figure la section ***Paramètres - Anti-Rootkit*** , dans laquelle vous pouvez configurer les fonctions élémentaires de la détection de rootkits. Cochez tout d'abord les cases permettant d'indiquer les objets à analyser :

- ***Rechercher dans les applications***
- ***Rechercher parmi les DLL***
- ***Rechercher parmi les pilotes***

Vous pouvez ensuite choisir le mode d'analyse des rootkits :

- ***Analyse anti-rootkit rapide*** - analyse seulement le dossier système (*généralement, c:\Windows*)
- ***Analyse anti-rootkit complète*** - analyse tous les disques accessibles sauf

A: et B:

Les boutons de commande disponibles sont :

- ***Rechercher les rootkits*** - comme l'analyse anti-rootkit ne fait pas partie de l'***analyse complète de l'ordinateur***, vous devez l'exécuter directement depuis l'interface ***Anti-Rootkit*** à l'aide de ce bouton
- ***Enregistrer les modifications*** : cliquez sur ce bouton pour enregistrer toutes les modifications réalisées dans cette interface et pour revenir à l'***Interface utilisateur AVG*** par défaut (vue d'ensemble des composants)
- ***Annuler*** : cliquez sur ce bouton pour revenir à l'***Interface utilisateur AVG*** par défaut (vue d'ensemble des composants) sans enregistrer les modifications que vous avez effectuées

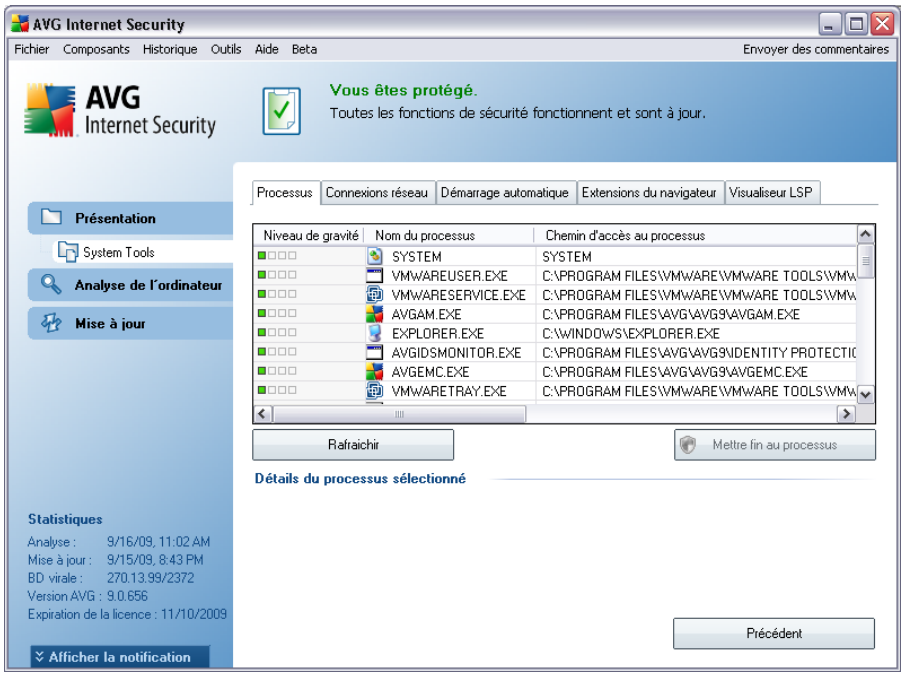
8.5. System Tools

System Tools désigne des outils décrivant de manière détaillée l'environnement d'**AVG 9 Internet Security** . Le composant présente :

- Processus - liste des processus (applications en cours d'exécution) actifs sur votre ordinateur
- Connexions réseau - liste des connexions actives
- Démarrage automatique - liste des applications qui s'exécutent au démarrage de Windows
- Extensions du navigateur - liste des plug-ins (applications) installés sur votre navigateur Internet
- Visualiseur LSP - liste des fournisseurs LSP (Layered Service Providers)

Certaines vues sont modifiables, mais notez que cette possibilité ne doit être réservée qu'aux utilisateurs très expérimentés !

8.5.1. Processus



La boîte de dialogue ***Processus*** indique les processus, (*c'est-à-dire les applications*) actuellement actives sur l'ordinateur. La liste est constituée de plusieurs colonnes :

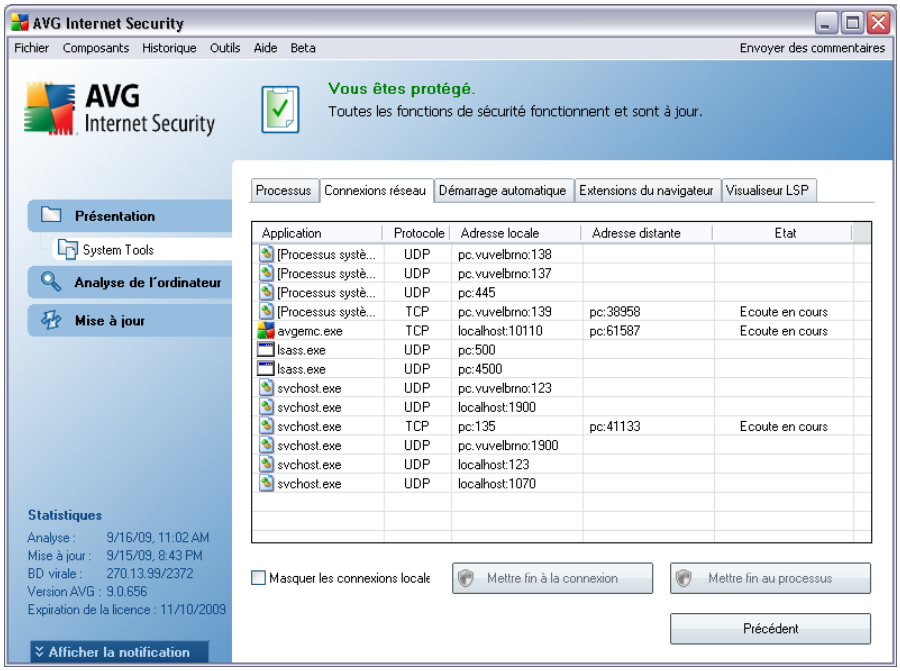
- ***Niveau de gravité*** - identification graphique de la gravité du processus en cours sur quatre niveaux allant du moins dangereux (■□□□) au plus grave (■■■■)
- ***Nom du processus*** - nom du processus en cours
- ***Chemin d'accès au processus*** - indique le chemin d'accès physique menant à un processus actif
- ***Fenêtre*** - indique, le cas échéant, le nom de la fenêtre de l'application
- ***Internet*** - indique si le processus actif se connecte à Internet (*Oui/Non*)
- ***Service*** - indique si le processus est un service (*Oui/Non*)
- ***PID*** - numéro d'identification du processus propre à Windows permettant d'identifier de manière unique un processus interne

Boutons de commande

Les boutons de commande disponibles dans l'interface ***Outils système*** sont :

- ***Actualiser*** - met à jour la liste des processus en fonction de l'état actuel
- ***Mettre fin au processus*** - Vous pouvez sélectionner une ou plusieurs applications et les arrêter en cliquant sur ce bouton. ***nous vous recommandons vivement de n'arrêter aucune application à moins d'être absolument certain qu'elle représente une menace véritable!***
- ***Retour*** - revenir à l'***Interface utilisateur AVG*** par défaut (vue d'ensemble des composants).

8.5.2. Connexions réseau



La boîte de dialogue ***Connexions réseau*** dresse la liste des connexions actives. Voici les différentes colonnes affichées :

- ***Application*** - nom de l'application en rapport avec la connexion. Cette information est seulement disponible sous Windows XP.

- ***Protocole*** - type de protocole de transmission utilisé par la connexion :
    - TCP - protocole utilisé avec Internet Protocol (IP) pour communiquer des informations par Internet.
    - UDP - protocole pouvant remplacer le protocole TCP
- ***Adresse locale*** - adresse IP de l'ordinateur local et numéro de port utilisé
- ***Adresse distante*** - adresse IP de l'ordinateur distant et numéro de port auquel il est relié. Si possible, il spécifie également le nom d'hôte de l'ordinateur distant.
- ***Etat*** - indique l'état actuel le plus probable*Connecté, Le serveur doit s'arrêter, Ecouter, Fermeture active terminée, Fermeture passive, Fermeture active*)

Pour répertorier seulement les connexions externes, cochez la case ***Masquer les connexions locales*** qui figure dans la partie inférieure de la boîte de dialogue, sous la liste.

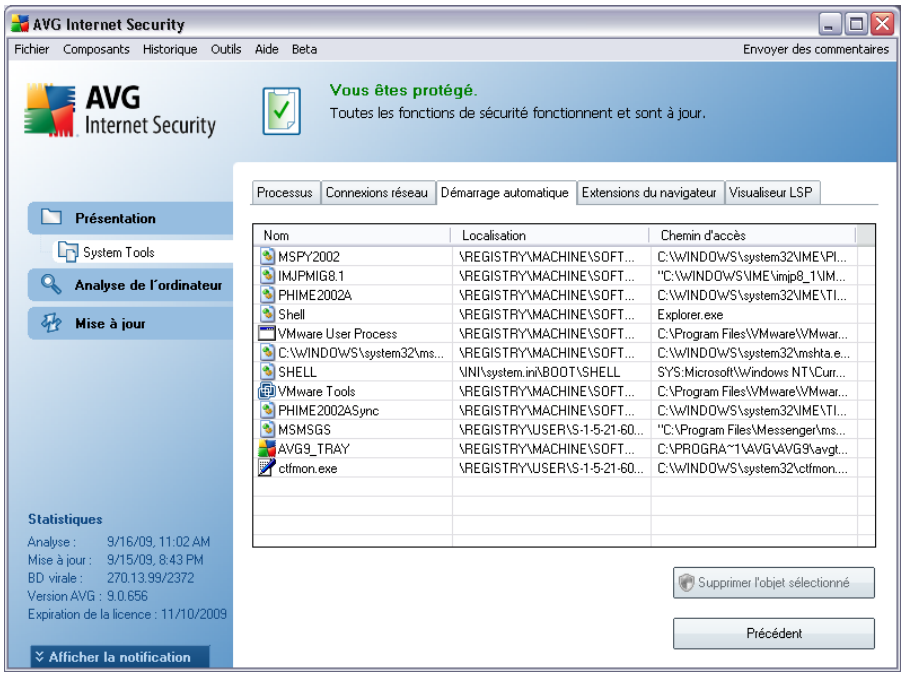
Boutons de commande

Les boutons de commande disponibles sont :

- ***Mettre fin à la connexion*** - ferme une ou plusieurs connexions sélectionnées dans la liste
- ***Mettre fin au processus*** - ferme une ou plusieurs applications liées aux connexions sélectionnées dans la liste (*Ce bouton est seulement disponible sur les systèmes d'exploitation Windows XP*)
- ***Retour*** : revenir à l'***Interface utilisateur AVG*** par défaut (vue d'ensemble des composants).

Parfois, il n'est possible d'arrêter que les applications actuellement connectées ! Nous vous recommandons vivement de n'arrêter aucune connexion à moins d'être absolument certain qu'elle représente une véritable menace.

8.5.3. Démarrage automatique

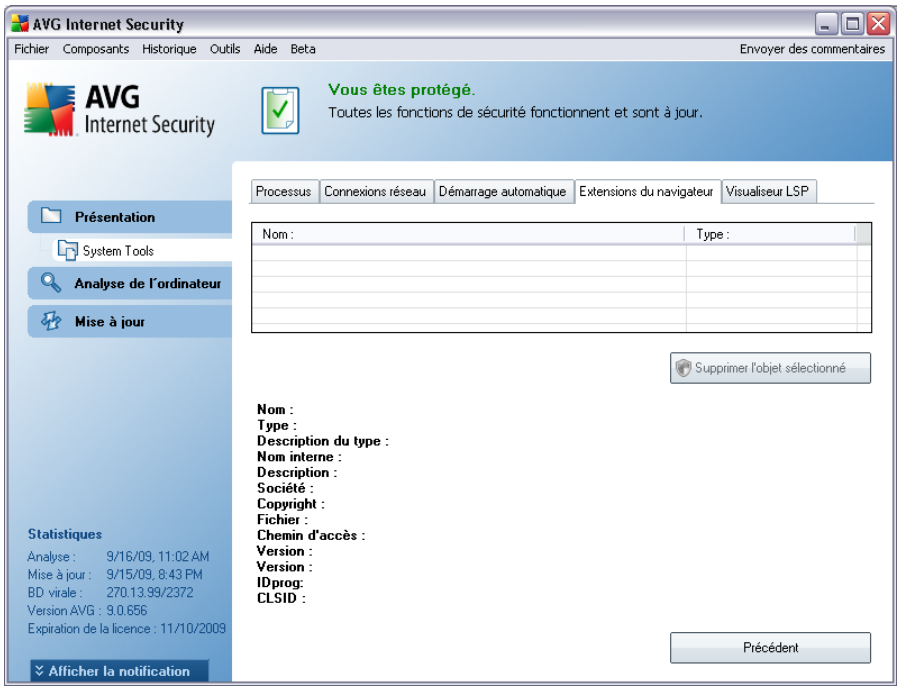


La boîte de dialogue de ***démarrage automatique*** indique toutes les applications qui sont exécutées lors du démarrage système de Windows. Très souvent, des applications malveillantes se greffent sur l'entrée de la base de registre de démarrage.

Vous pouvez supprimer une ou plusieurs entrées en les sélectionnant, puis en cliquant sur le bouton ***Supprimer la sélection.*** Le bouton ***Précédent*** vous permet de basculer vers l'***Interface utilisateur AVG*** par défaut (aperçu des composantes).

nous vous recommandons vivement de n'enlever aucune application de la liste à moins d'être absolument certain qu'elle représente une menace véritable!

8.5.4. Extensions du navigateur



La boîte de dialogue***Extensions du navigateur*** contient la liste des plugins (*ou applications*) qui sont installés dans votre navigateur Internet. Cette liste est constituée des plugins standards ainsi que des programmes potentiellement malveillants. Cliquez sur un objet figurant dans la liste pour obtenir plus d'informations sur le plug-in sélectionné s'affichant dans la section inférieure de la boîte de dialogue.

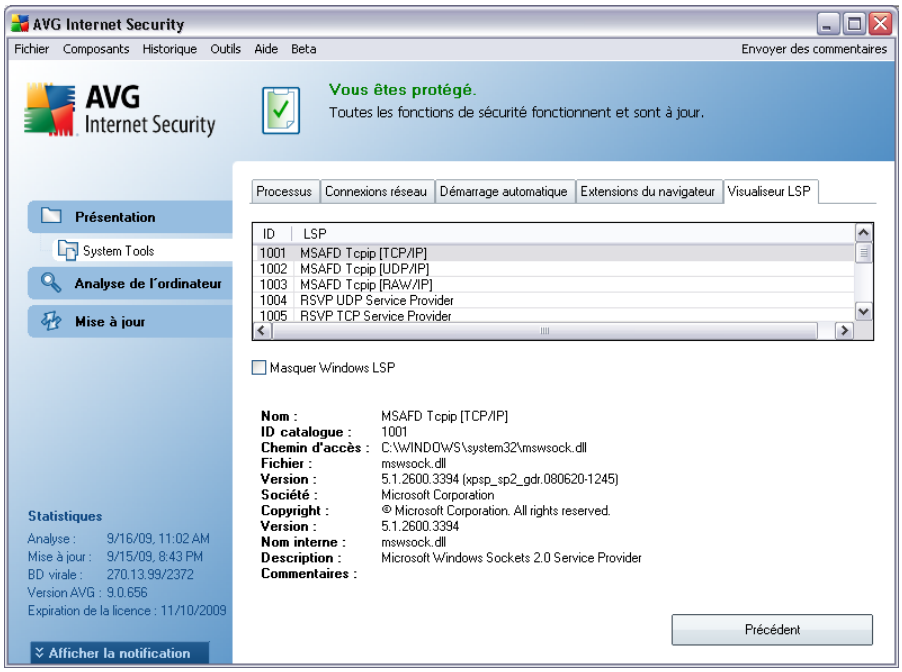
Boutons de commande

Les boutons de commande qui sont disponibles dans l'onglet ***Extension du navigateur*** sont :

- ***Supprimer l'objet sélectionné*** - supprime le plug-in mis en surbrillance dans la liste. ***Nous vous recommandons vivement de ne supprimer aucun plug-in dans la liste sauf si vous êtes absolument certain qu'il représente une menace véritable !***

- ***Retour*** - : revenir à l'***Interface utilisateur d'AVG*** par défaut (vue d'ensemble des composants)

8.5.5. Visualiseur LSP



La boîte de dialogue ***Visualiseur LSP*** dresse la liste des fournisseurs de service de connexion (ou fournisseurs LSP).

Un ***fournisseur de service de connexion*** est un pilote système lié aux services réseau du système d'exploitation Windows. Il a accès à toutes les données qui parviennent et sortent de l'ordinateur et peut éventuellement les modifier. En l'absence de certains fournisseurs LSP, Windows ne sera pas en mesure d'établir la connexion avec d'autres ordinateurs ou avec Internet. Cependant, notez que des applications de type malwares peuvent s'installer sous forme de LSP et ainsi avoir accès à toutes les données transmises par l'ordinateur. En conséquence, le passage en revue de la liste permet de repérer les menaces LSP potentielles.

Dans certaines conditions, il est également possible de réparer certains LSP dont le lien est interrompu (*notamment si un fichier est supprimé alors que les entrées correspondantes dans la base de registre sont conservées en l'état*). Un nouveau bouton permettant de résoudre ce genre de problème s'affiche dès lors qu'un LSP réparable est détecté.

Pour ajouter le LSP Windows à la liste, désactivez la case ***Masquer Windows LSP*** Le bouton ***Précédent*** vous permet de basculer vers l'***Interface utilisateur d'AVG*** par défaut (*aperçu des composantes*).

8.6. Pare-Feu

Un pare-feu est un système prévu pour appliquer des règles de contrôle d'accès entre plusieurs réseaux en bloquant/autorisant le trafic. Le composant Pare-feu dispose d'un jeu de règles destiné à protéger le réseau interne contre les attaques venant de l'extérieur (généralement d'Internet) et contrôle l'ensemble du trafic au niveau de chaque port réseau. Les communications sont évaluées en fonction de règles définies et sont ensuite autorisées ou interdites. Si le pare-feu détecte une tentative d'intrusion, il « bloque » l'opération de manière à empêcher l'intrus d'accéder à votre ordinateur.

Le pare-feu est configuré pour autoriser ou bloquer la communication interne ou externe (dans les deux sens, entrante ou sortante) passant par les ports définis et pour les applications définies. Par exemple, le pare-feu peut être configuré pour autoriser uniquement la transmission de données entrantes et sortantes transitant par Microsoft Internet Explorer. Toute tentative pour transmettre des données par un autre navigateur sera bloquée.

Le pare-feu empêche que des informations qui permettraient de vous identifier personnellement soient envoyées sans votre accord. Il régit la manière dont votre ordinateur échange des données avec les autres ordinateurs, que ce soit sur Internet ou dans un réseau local. Au sein d'une entreprise, le pare-feu permet de contrecarrer les attaques initiées par des utilisateurs internes, travaillant sur d'autres ordinateurs reliés au réseau.

Recommandation : *En règle générale, il est déconseillé d'utiliser plusieurs pare-feu sur un même ordinateur. La sécurité de l'ordinateur n'est pas améliorée par l'installation de plusieurs pare-feux. Il est plus probable que des conflits se produisent entre deux applications. Nous vous conseillons donc de n'utiliser qu'un seul pare-feu sur votre ordinateur et de désactiver tous les autres pare-feu afin d'éviter des conflits entre AVG et ces programmes, ainsi que d'autres problèmes.*

8.6.1. Principes de fonctionnement du pare-feu

Dans AVG, le composant ***Pare-feu*** contrôle l'ensemble du trafic transitant sur chaque port de votre ordinateur. En fonction des règles définies, le ***Pare-feu*** évalue les applications en cours d'exécution sur votre ordinateur (et qui cherchent à se connecter à Internet/au réseau local) ou les applications qui essaient de se connecter à votre ordinateur depuis l'extérieur. Pour chacune de ces applications, le ***Pare-feu*** autorise ou interdit les communications transitant sur les ports réseau. Par défaut, si l'application est inconnue (c'est-à-dire, aucune règle de ***pare-feu*** n'est définie), il vous sera demandé d'autoriser ou de bloquer la tentative de communication.

Remarque : Le *Pare-feu AVG n'est pas conçu pour les plateformes serveur !*

Actions possibles du Pare-feu AVG :

- Autorise ou bloque automatiquement les tentatives de communication des applications connus ou demande votre confirmation
- Utilise des profils complets avec des règles prédéfinies en fonction de vos besoins
- Conserve une archive de tous les profils et paramètres définis
- Change automatiquement de profil lors de la connexion à divers réseaux ou de l'utilisation de divers adaptateurs réseau

8.6.2. Profils de pare-feu

Le ***pare-feu*** vous permet de définir des règles de sécurité spécifiques suivant si l'ordinateur est situé dans un domaine, s'il est autonome ou s'il s'agit d'un ordinateur portable. Chacune de ces options appelle un niveau de protection différent, géré par un profil particulier. En d'autres termes, un ***profil de pare-feu*** est une configuration spécifique du composant ***Pare-feu***. Vous pouvez utiliser plusieurs configurations prédéfinies de ce type.

Profils disponibles

- ***Autoriser tout*** - un profil système de ***Pare-feu*** prédéfini par l'éditeur, qui est toujours présent. Lorsque ce profil est activé, toute les communications réseau sont autorisées et aucune règle de procédure de sécurité n'est appliquée, de la même manière que si la protection du ***Pare-feu*** était désactivée *(par exemple, toutes les applications sont autorisées, mais les paquets sont toujours vérifiés - pour désactiver complètement tout filtrage, vous devez désactiver le Pare-feu)*. Ce profil système ne peut pas être dupliqué ni supprimé et ses paramètres ne peuvent pas être modifiés.
- ***Bloquer tout*** - un profil système de ***Pare-feu*** prédéfini par le fabricant, qui est toujours présent. Lorsque ce profil est activé, toutes les communications réseau sont bloquées et l'ordinateur ne peut ni accéder à d'autres réseaux, ni recevoir des communications provenant de l'extérieur. Ce profil système ne peut pas être dupliqué, ni supprimé et ses paramètres ne peuvent pas être modifiés.
- ***Profils personnalisés***:

- ***Ordinateur nomade***– recommandé pour les PC domestiques directement connectés à Internet ou les ordinateurs portables se connectant à Internet en dehors du réseau sécurisé de l'entreprise. Sélectionnez cette option en cas de connexion à domicile ou via un petit réseau d'entreprise sans contrôle centralisé. De même, cette option est recommandée lorsque vous vous déplacez et connectez votre portable en différents endroits inconnus et potentiellement dangereux (*cybercafé, chambre d'hôtel, etc.*). Des règles plus strictes seront alors créées dans la mesure où aucune protection supplémentaire n'est généralement prévue pour ce type d'utilisation.

- ***Ordinateur inclus dans un réseau*** – recommandé pour les ordinateurs en réseau local, par exemple dans les écoles ou les réseaux d'entreprise. Etant donné que les ordinateurs en réseau sont généralement protégés par d'autres éléments de sécurité, le niveau de protection est moins élevé que dans d'autres profils.

- ***Réseau domestique*** – recommandé pour les ordinateurs reliés en réseau, comme les très petits réseaux d'entreprise connectés en poste à poste, sans serveur central, par exemple.

Changement de profil

L'utilitaire Changement de profil permet au ***Pare-feu*** de changer automatiquement de profil lorsqu'il détecte une activité sur un adaptateur réseau ou lorsque vous êtes connecté sur un certain type de réseau. Si aucun profil n'a été assigné à un zone de réseau, à la prochaine connexion à cette zone, une boîte de dialogue du ***Pare-feu*** vous invitera à lui attribuer un profil.

Vous pouvez assigner des profils à toutes les interfaces réseau ou à toutes les zones de réseau et définir des paramètres complémentaires dans la boîte de dialogue ***Profils adaptateurs et réseaux***, où vous pouvez aussi désactiver cette fonctionnalité si vous ne désirez pas l'utiliser. *Dans ce cas, quel que soit le type de la connexion, le profil par défaut sera utilisé*).

Les utilisateurs d'un ordinateur portable, par exemple, trouveront très pratique cette fonctionnalité, car ils utilisent plusieurs interfaces réseau pour se connecter (WiFi, Ethernet, etc.). Si vous possédez un ordinateur de bureau et n'utilisez qu'un seul type de connexion *(par exemple, une connexion câblée à Internet), vous n'avez pas besoin de vous soucier du basculement de profil, car vous ne l'utiliserez probablement jamais* .

8.6.3. Interface du Pare-feu

L'interface du composant ***Pare-feu*** donne des informations de base sur la fonctionnalité du composant, ainsi que des données statistiques sur le ***Pare-feu*** :

- ***Le pare-feu est activé depuis*** - temps écoulé depuis le dernier démarrage du Pare-feu
- ***Paquets bloqués*** - nombre de paquets bloqués par rapport au nombre total de paquets vérifiés
- ***Total des paquets*** - nombre total de paquets vérifiés au cours de l'exécution du Pare-feu

Configuration standard du composant

- ***Sélectionner le profil du pare-feu*** - dans la liste déroulante, sélectionnez un des profils définis - deux profils sont disponibles en permanence (les *profils par défaut nommés* ***Autoriser tout*** *et* ***Bloquer tout***), alors que les autres profils sont insérés manuellement en modifiant un profil dans la boîte de dialogue ***Profils*** des ***paramètres du Pare-feu***.

- ***Activer le mode jeu*** - Cochez cette case pour vous assurer que pendant l'exécution d'applications en plein écran (jeux, présentations PowerPoint, etc.), le ***pare-feu*** n'affichera pas de questions sur le blocage des communications ou des applications inconnues. Si une application inconnue tente de communiquer par le réseau pendant ce temps, le ***pare-feu*** autorise ou bloque automatiquement la tentative selon les paramètres définis dans le profil actif.

- ***Etat du Pare-feu*** :

  - ***Pare-feu activé*** - sélectionnez cette option pour autoriser la communication avec les applications dont le jeu de règles est "Autorisé" dans le profil de ***Pare-feu*** sélectionné

  - ***Pare-feu désactivé*** - cette option désactive intégralement le ***Pare-feu*** : l'ensemble du trafic réseau est autorisé sans aucune vérification.

  - ***Mode Urgence (bloque tout le trafic Internet)*** - cette option bloque l'ensemble du trafic sur chaque port réseau ; le ***Pare-feu*** fonctionne, mais le trafic réseau est intégralement arrêté

Remarque : *l'éditeur du logiciel a configuré tous les composants AVG de manière à obtenir des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté. Si vous êtes amené à modifier la configuration du Pare-feu, cliquez sur le menu* ***Outils / Paramètres du Pare-feu*** *et modifiez la configuration du Pare-feu dans la boîte de dialogue* ***Paramètres avancés d'AVG*** *qui s'affiche alors.*

Boutons de commande

- ***Assistant de configuration*** - cliquez sur le bouton pour lancer la boîte de dialogue correspondante (*utilisée dans le processus d'installation*) appelée ***Sélection du mode d'utilisation de l'ordinateur***où vous pouvez spécifier la configuration du composant***Pare-feu***

- ***Enregistrer*** - cliquez sur ce bouton pour enregistrer et appliquer les modifications entrées dans la boîte de dialogue

- ***Annuler*** - cliquez sur ce bouton pour revenir à l'interface utilisateur AVG *par défaut (présentation des composants*)

8.7. Scanner e-mail

Le courrier électronique figure parmi les sources les plus courantes d'infection par virus ou Cheval de Troie. Les techniques d'hameçonnage (ou phishing) et d'envoi de messages non sollicités en masse (spam) rendent la messagerie encore plus vulnérable. Les comptes gratuits de messagerie présentent un risque plus élevé de recevoir des messages malveillants (*d'autant qu'ils utilisent rarement une technologie anti-spam*) et qu'ils sont très prisés des particuliers. Par ailleurs, en consultant des sites inconnus depuis leur domicile et en fournissant des données personnelles (*adresse e-mail, par exemple*) dans des formulaires en ligne, ces usagers contribuent à augmenter le risque d'attaque par e-mail. Les sociétés utilisent généralement des comptes de messagerie à usage professionnel et appliquent des filtres anti-spam et autres moyens pour réduire ce risque.

8.7.1. Principes du Scanner e-mail

Le composant ***Scanner e-mail*** analyse automatiquement les messages entrants et sortants. Vous pouvez l'utiliser avec les clients de messagerie qui ne disposent pas de leur propre plug-in dans AVG (*par exemple : Outlook Express, Mozilla, Incredimail, etc.*).

Lors de l'installation d'AVG, des serveurs sont automatiquement créés pour assurer la vérification des messages, l'un pour les messages entrants, et l'autre pour les messages sortants. Grâce à ces deux serveurs, les messages sont vérifiés automatiquement sur les ports 110 et 25 (*ports standard affectés à l'envoi/la réception de messages*).

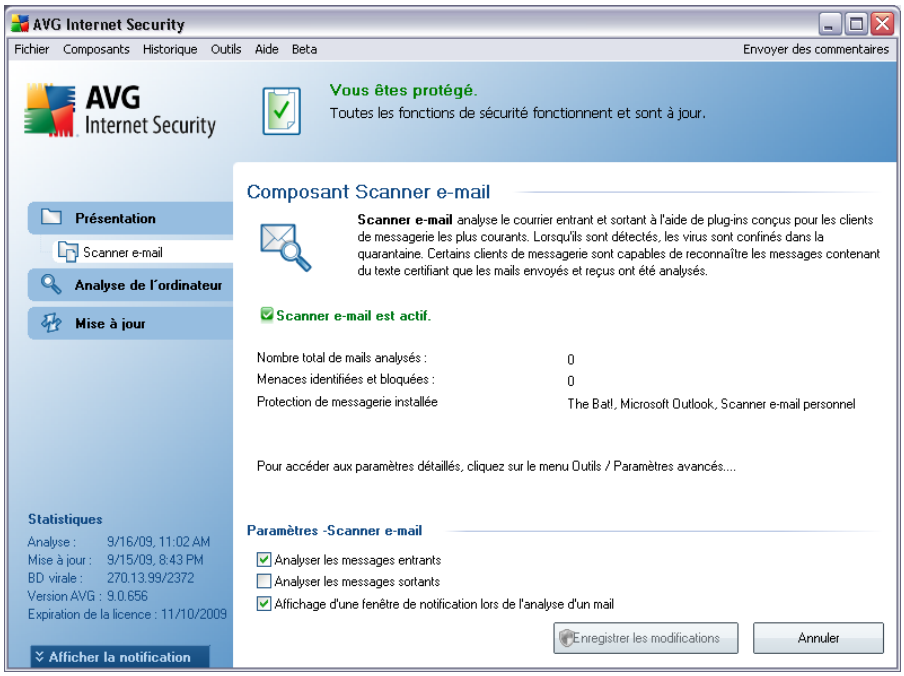
Le scanner e-mail personnel fonctionne comme une interface entre le client de messagerie et les serveurs de messagerie sur Internet.

- ***Message entrant :*** Lorsque vous recevez un message du serveur, le composant ***Scanner e-mail***vérifie s'il ne contient pas de virus, supprime les pièces jointes infectées (le cas échéant) et ajoute la certification. Lorsque des virus sont détectés, ils sont immédiatement placés en ***Quarantaine***. Le message est ensuite transmis au client de messagerie.

- ***Message sortant :*** Un message est envoyé du client de messagerie au scanner e-mail. Ce dernier vérifie que le message et ses pièces jointes ne contiennent pas de virus. Ensuite, il l'envoie au serveur SMTP (*l'analyse des messages sortants est désactivée par défaut et peut-être configurée de façon manuelle*).

Remarque : *AVG E-mail Scanner n'est pas conçu pour les plateformes serveur !*

8.7.2. Interface du Scanner e-mail



La boîte de dialogue du composant ***Scanner e-mail*** décrit de façon concise la fonctionnalité du composant et signale son état actuel (Le composant *Scanner e-mail est actif.*). Elle donne également les informations statistiques suivantes :

- ***Nombre total de mails analysés*** - nombre des messages vérifiés depuis le dernier lancement du ***Scanner e-mail*** (*si nécessaire, cette valeur peut être rétablie ; par exemple pour des besoins de statistique : Rétablir la valeur*)
- ***Menaces identifiées et bloquées*** - indique le nombre d'infections détectées dans les messages depuis le dernier lancement de ***Scanner e-mail***
- ***Protection de messagerie installée*** : informations sur le plug-in de protection de messagerie adapté à votre client de messagerie installé par défaut

Configuration standard du composant

Dans la partie inférieure de la boîte de dialogue, une section intitulée ***Paramètres du Scanner e-mail*** permet de modifier certaines fonctions élémentaires de la fonctionnalité du composant :

- ***Analyser les messages entrants*** - cochez cette case pour instaurer l'analyse de tous les courriers adressés à votre compte. -Par défaut, la case est activée et il est recommandé de ne pas modifier ce paramètre!

- ***Analyser les messages sortants*** - cochez cette case pour confirmer que tous les messages envoyés à partir de votre compte doivent être analysés. par défaut, cette option est désactivée.

- *Afficher l'icône de notification durant l'analyse des messages* - pendant l'analyse, le composant ***Scanner e-mail*** affiche une boîte de dialogue indiquant l'opération en cours (*connexion au serveur, téléchargement d'un message, analyse du message, ...*). Cette option est activée et ne peut pas être modifiée.

La configuration avancée du composant ***Scanner e-mail*** est accessible par le biais de l'option de menu ***Outils/Paramètres avancés***. Notez toutefois que cette tâche devrait être réservée aux seuls utilisateurs expérimentés.

Remarque : *l'éditeur du logiciel a configuré tous les composants AVG de manière à obtenir des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté. Si vous devez modifier la configuration d'AVG, sélectionnez le menu* ***Outils / Paramètres avancés*** *et modifiez la configuration d'AVG dans la boîte de dialogue Paramètres avancés d'AVG qui apparaît.*

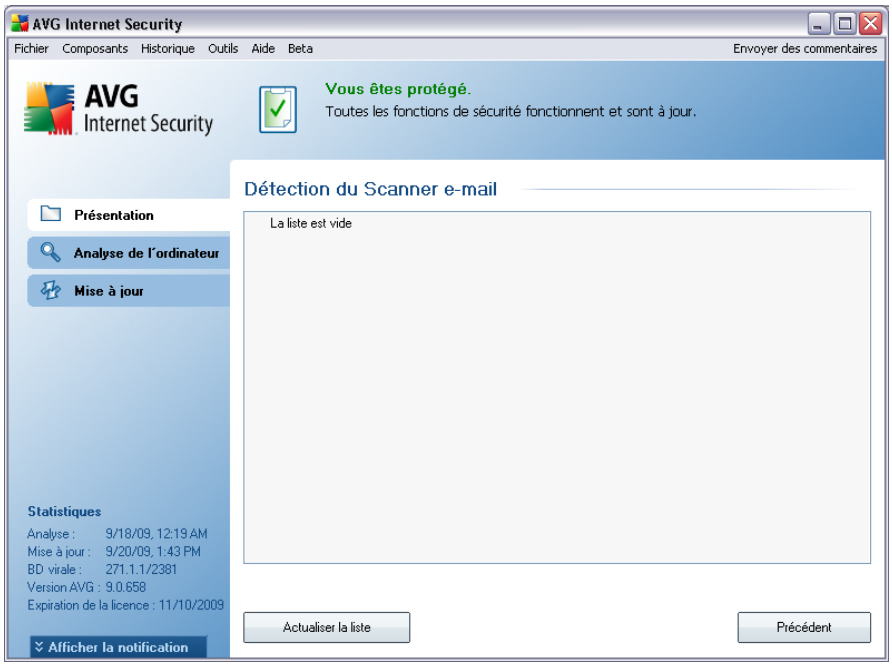
Boutons de commande

Les boutons de commande disponibles dans l'interface du ***Scanner e-mail*** sont les suivants :

- ***Enregistrer les modifications*** - cliquez sur ce bouton pour enregistrer et appliquer les modifications apportées dans cette boîte de dialogue

- ***Annuler*** - cliquez sur ce bouton pour revenir à l'interface utilisateur AVG par défaut (présentation des composants)

8.7.3. Détection du Scanner e-mail



Dans la boîte de dialogue ***Détection du Scanner e-mail*** (*accessible via l'option de menu Historique / Détection du Scanner e-mail*) , vous verrez la liste de tous les éléments détectés par le composant ***Scanner e-mail*** . Les informations suivantes accompagnent chaque objet détecté :

- ***Infection***- description (et éventuellement le nom) de l'objet détecté
- ***Objet*** - emplacement de l'objet
- ***Résultat*** - action effectuée sur l'objet détecté
- ***Date de la détection*** - date et heure auxquelles l'objet suspect a été détecté
- ***Type d'objet*** - type de l'objet détecté

Dans la partie inférieure de la boîte de dialogue, sous la liste, vous trouverez des informations sur le nombre total d'objets détectés répertoriés ci-dessus. Par ailleurs, vous êtes libre d'exporter la liste complète des objets détectés dans un fichier (***Exporter la liste dans le fichier***) et de supprimer toutes les entrées des objets détectés (***Vider la liste***).

Boutons de commande

Les boutons de commande disponibles dans l'interface de ***Détection du Scanner e-mail*** sont :

- ***Actualiser la liste*** - met à jour la liste des menaces détectées
- ***Retour*** : revenir à l'***Interface utilisateur AVG*** par défaut (vue d'ensemble des composants)

8.8. Identity Protection

AVG Identity Protection est un produit anti-code malicieux conçu pour empêcher les usurpateurs d'identité de dérober vos mots de passe, données de compte bancaire, numéros de carte de crédit et autres ressources numériques personnelles importantes au moyen de tout type de logiciel malicieux (*code malicieux*) ciblant votre PC. Ce programme s'assure que tous les programmes s'exécutant sur votre ordinateur fonctionnent correctement. ***AVG Identity Protection*** détecte et bloque de façon permanente les comportements suspects et protège votre ordinateur contre tous les nouveaux contenus malveillants.

8.8.1. Principes d'Identity Protection

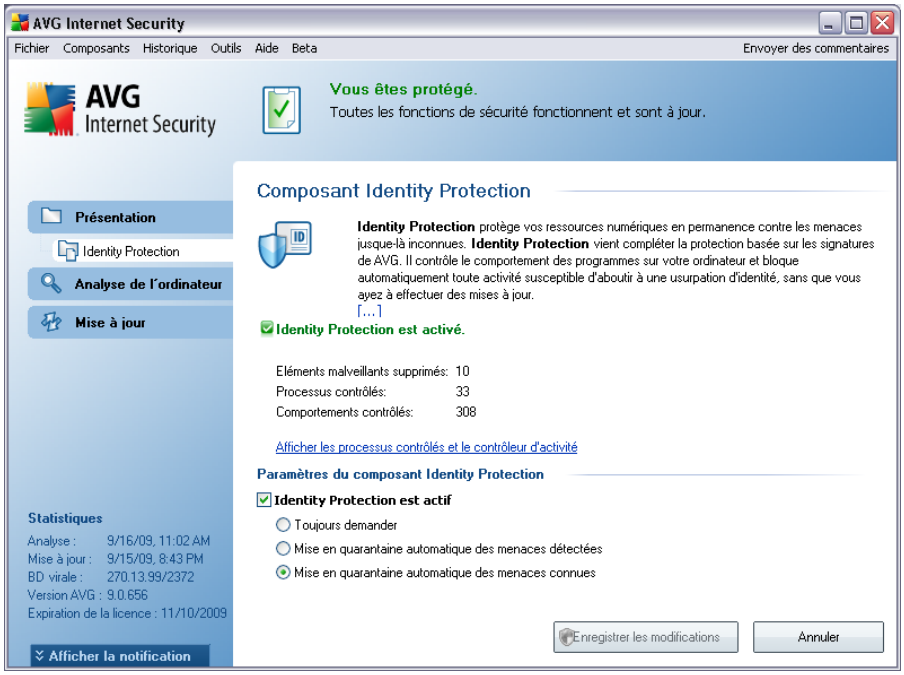
AVG Identity Protection est un composant Anti-malware qui vous protège contre tout type de programme malveillant (*spywares, bots, usurpation d'identité, etc.*) à l'aide de technologies d'analyse du comportement. Ce programme vous assure une protection de type zero-day, contre les nouveaux virus. Les codes malicieux deviennent de plus en plus sophistiqués et prennent la forme d'applications courantes à même d'ouvrir votre ordinateur à un pirate, afin de lui permettre d'usurper votre identité, à distance. ***AVG Identity Protection*** vous protège de tous ces nouveaux codes malicieux basés sur l'exécution. C'est une solution de protection complémentaire au programme ***AVG Anti-Virus*** qui vous protège des virus connus et dissimulés dans des fichiers à l'aide des mécanismes de signature et d'analyse.

Nous vous recommandons vivement d'installer à la fois les composants AVG Anti-Virus et AVG Identity Protection afin que votre ordinateur soit complètement protégé.

8.8.2. Interface d'Identity Protection

L'interface du composant ***Identity Protection*** décrit brièvement le fonctionnement de base du produit, indique son état (*AVG Identity Protection est actif et fonctionne normalement.*) et fournit quelques statistiques :

- ***Programmes malveillants supprimés*** - indique le nombre d'applications détectées comme programmes malveillants et supprimées
- ***Processus contrôlés*** - nombre d'applications actives contrôlées par IDP
- ***Comportements contrôlés*** - nombre d'actions spécifiques en cours au sein des applications contrôlées



Configuration standard du composant

Au bas de la boîte de dialogue se trouve la section des ***paramètres d'Identity Protection*** qui permet de modifier certaines options élémentaires du fonctionnement du composant :

- ***Identity Protection est actif*** - (*option activée par défaut*) : cochez cette option pour activer le composant IDP et accéder à d'autres options de modification.

Dans certains cas, ***Identity Protection*** peut signaler qu'un fichier inoffensif est suspect ou dangereux. Comme ***Identity Protection*** détecte les menaces sur la base de leur comportement, ce type de problème survient généralement lorsqu'un programme tente d'enregistrer les pressions de touches du clavier ou d'installer d'autres programmes, ou encore lorsqu'un nouveau pilote est installé

sur l'ordinateur.

En conséquence, vous devez sélectionner une des options suivantes pour spécifier le comportement du composant ***Identity Protection*** en cas de détection d'une activité suspecte :

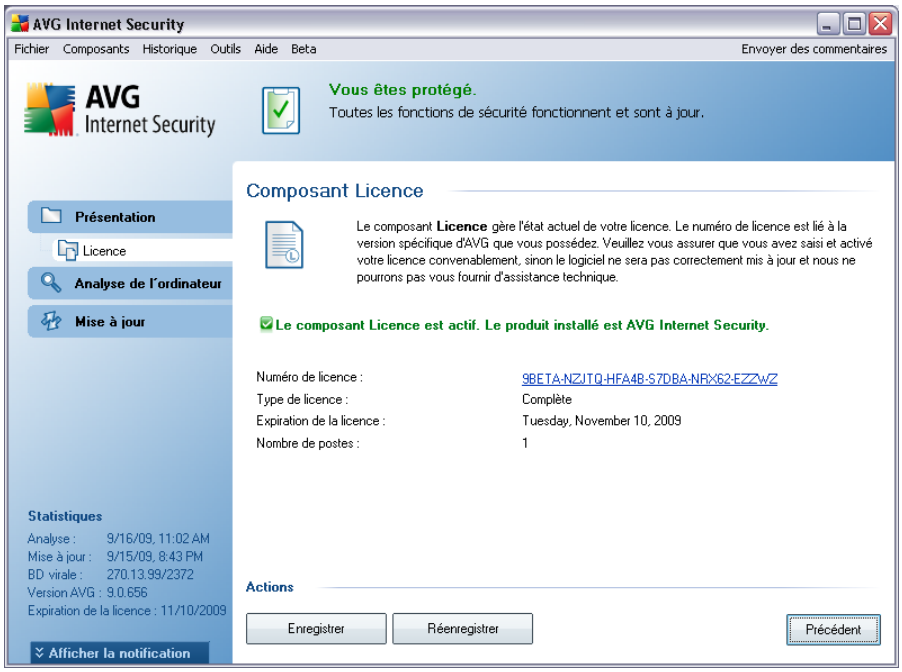
- ***Toujours demander*** - si IDP détecte une application comme programme malveillant, vous devez confirmer s'il doit la bloquer
- ***Mettre automatiquement en quarantaine les menaces détectées*** - toutes les applications détectées comme des programmes malveillants sont automatiquement bloquées
- ***Mettre automatiquement en quarantaine les menaces connues*** - seuls les programmes malveillants identifiés avec une certitude absolue sont bloqués (*cette option est activée par défaut et il est recommandé de ne pas la modifier, sauf si vous avez une bonne raison de le faire*)

Boutons de commande

Les boutons de commande disponibles dans l'interface du ***Scanner e-mail*** sont les suivants :

- ***Enregistrer les modifications*** - cliquez sur ce bouton pour enregistrer et appliquer les modifications apportées dans cette boîte de dialogue
- ***Annuler*** - cliquez sur ce bouton pour revenir à l'interface utilisateur AVG par défaut (présentation des composants)

8.9. Licence



L'interface du composant ***Licence*** fournit une description sommaire du fonctionnement du composant et des informations sur son état actuel (le composant *Licence est actif.*) et les renseignements suivants :

- ***Numéro de licence*** - précise le numéro de licence complet. Lorsque vous saisissez un numéro de licence, vous devez le saisir exactement tel qu'il est affiché. Par conséquent, nous vous recommandons vivement de toujours recourir à la méthode "copier & coller" pour toute utilisation du numéro de licence.

- ***Type de licence*** - indique le type de produit installé.

- ***Expiration de la licence*** - cette date détermine la durée de validité de la licence. Pour continuer d'utiliser **AVG 9 Internet Security** après cette date, il est nécessaire de renouveler votre licence. Le renouvellement peut être réalisé en ligne sur le site Web d'AVG (http://www.avg.com/).

- ***Nombre de postes*** - nombre de postes de travail sur lequel vous êtes autorisé à installer le produit **AVG 9 Internet Security**.

Boutons de commande

- ***Enregistrer*** - renvoie à la page d'enregistrement du site Web d'AVG (http://www.avg.com/). Merci de compléter le formulaire d'enregistrement ; seuls les clients ayant dûment enregistré leur produit AVG peuvent bénéficier de l'assistance technique gratuite.

- ***Réactiver*** - affiche la boîte de dialogue ***Activer AVG*** avec les données saisies dans la boîte de dialogue ***Personnaliser AVG*** au cours du processus d'installation. Dans cette boîte de dialogue, vous indiquez votre numéro de licence en lieu et place de la référence d'achat (*le numéro indiqué lors de l'installation d'AVG*) ou de votre ancien numéro (*si vous installez une mise à niveau du produit AVG, par exemple*).

- ***Précédent*** - cliquez sur ce bouton pour revenir à l'interface utilisateur AVG par défaut (présentation des composants).

8.10. LinkScanner

8.10.1. Principes de LinkScanner

Le composant ***LinkScanner*** vous protège contre les sites Web conçus pour installer des programmes malveillants sur votre ordinateur via le navigateur Internet ou ses plugins. La technologie ***LinkScanner*** comporte deux fonctionnalités, à savoir ***AVG Search-Shield*** et ***AVG Active Surf-Shield*** :

- ***AVG Search Shield*** contient une liste de sites Web (*adresses URL*) reconnus comme dangereux. Lors de vos recherches sur Google, Yahoo!, MSN ou Baidu, tous les résultats sont analysés en fonction de cette liste et une icône faisant foi de diagnostic s'affiche (*pour les résultats de recherche Yahoo! seuls les icônes indiquant que le "site Web est piraté" s'affichent*). De même, si vous saisissez directement une adresse dans votre navigateur ou cliquez sur un lien quelconque (figurant par exemple dans un e-mail), il est automatiquement analysé et bloqué si nécessaire.

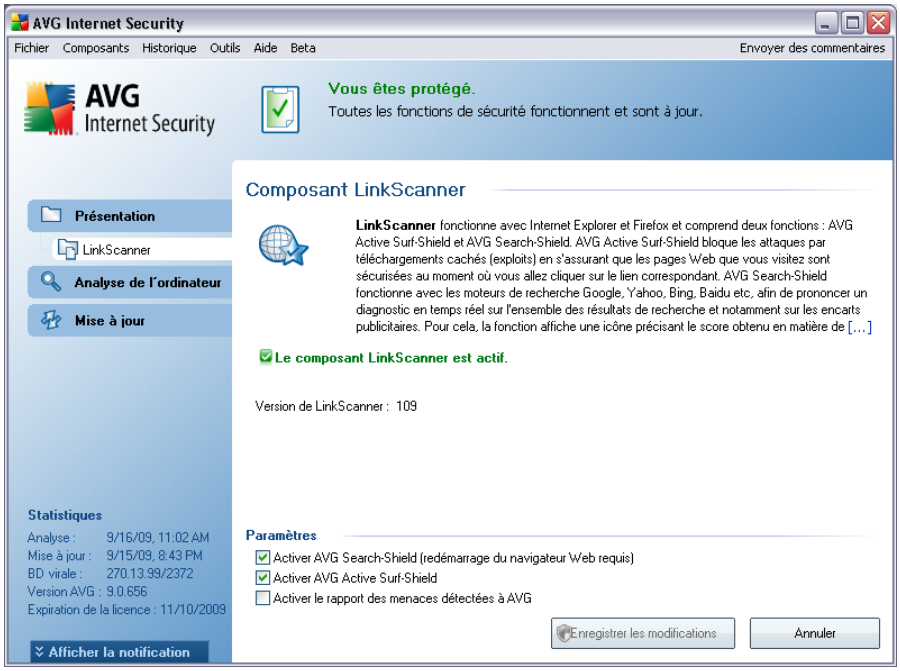
- ***AVG Active Surf-Shield*** analyse le contenu des sites Web que vous visitez, quelles que soient leurs adresses. Même si ***AVG Search Shield*** ne détecte pas un site Web donné (*par exemple, lorsqu'un nouveau site malveillant est créé ou lorsqu'un site fiable est contaminé par un programme malveillant*), ***AVG Active Surf-Shield*** le détecte et le bloque si vous essayez d'y accéder.

Remarque : *AVG LinkScanner n'est pas conçu pour les plateformes serveur !*

8.10.2. Interface de LinkScanner

Le composant ***LinkScanner*** comprend deux éléments que vous pouvez activer/ désactiver dans l'interface du ***composant LinkScanner***:

L'interface du composant ***LinkScanner*** décrit brièvement le fonctionnement du composant, indique son état actuel (*le composant LinkScanner est actif.*). En outre, vous trouverez des informations sur le numéro de version de la base de données la plus récente du composant ***LinkScanner*** (*Version du composant*|*LinkScanner*).



Dans la partie inférieure de la boîte de dialogue, vous pouvez modifier plusieurs options :

- ***Activer*** ***Activer SearchShield*** - (*paramètre activé par défaut*) : icônes de notification portant sur les recherches effectuées dans Google, Yahoo ou MSN ; le contenu des sites renvoyés par ces moteurs de recherche a été préalablement vérifié.

- ***Activer*** ***AVG Active Surf-Shield*** : *(paramètre activé par défaut*) : protection active (*en temps réel*) contre les sites utilisant des exploits lors de la demande d'accès. Les connexions à des sites malveillants et leur contenu piégé sont

bloqués au moment où l'utilisateur demande à y accéder via un navigateur Web (*ou toute autre application qui utilise le protocole HTTP*).

- ***Activer le signalement à AVG des menaces détectées*** - cochez cette case pour permettre le retour d'informations sur les exploits et les sites frauduleux détectés par les utilisateurs via les fonctions ***Safe Surf*** ou ***Safe Search*** et pour enrichir la base de données sur les activités malveillantes qui existent dans le Web.

8.10.3. AVG Search-Shield

Lorsque vous naviguez sur Internet en ayant pris soin d'activer ***AVG Search-Shield***, une vérification s'effectue sur tous les résultats de recherche retournés par la plupart des moteurs de recherche comme Yahoo!, Google, MSN, etc. sont analysés. Grâce à cette vérification de liens et au signalement des mauvais liens, les liens dangereux ou suspects sont systématiquement signalés dans la ***barre d'outils de sécurité d'AVG*** avant que vous ne les ouvriez. Vous naviguez ainsi en toute sécurité uniquement dans des sites Web sécurisés.

Lorsqu'un lien proposé dans une page de résultats de recherche fait l'objet d'une évaluation, une icône particulière apparaît pour indiquer qu'une vérification du lien est en cours. Une fois l'évaluation terminée, l'icône d'information appropriée s'affiche :

 La page associée est sécurisée (*avec le moteur de recherche Yahoo! intégré à la barre d'outils de sécurité d'AVG cette icône ne sera pas affichée*).

 La page associée ne contient pas de menaces, mais paraît néanmoins suspecte (*son origine comme son objet n'est pas explicite. Il est par conséquent préférable de ne pas l'utiliser pour les achats électroniques, etc.*).

 La page associée au lien semble fiable, mais contient des liens vers des pages dont le contenu est dangereux ou dont le code est suspect même s'il ne présente pas de menaces directes pour le moment.

 La page associée contient des menaces actives ! Pour votre propre sécurité, vous n'êtes pas autorisé à visiter la page.

 La page associée n'étant pas accessible, elle ne peut pas faire l'objet d'une analyse.

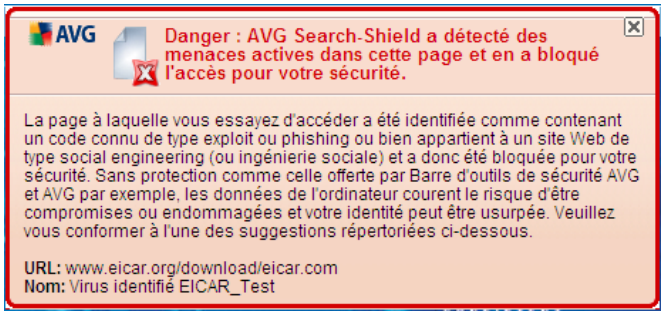
Le fait de placer le pointeur sur une icône d'évaluation permet d'obtenir des informations sur le lien en question. Ces informations fournissent des renseignements

supplémentaires sur la menace éventuelle, l'adresse IP du lien et la date de l'analyse effectuée par AVG:

8.10.4. AVG Active Surf-Shield

Cette protection puissante bloque le contenu malveillant de toute page Web que vous êtes sur le point d'afficher et empêche son téléchargement sur l'ordinateur. Lorsque cette fonction est activée, cliquer sur un lien ou saisir une adresse URL menant à un site dangereux bloque automatiquement l'ouverture de la page Web correspondante prévenant toute infection. Il est important de garder en mémoire que les pages Web contenant des exploits peuvent infecter votre ordinateur au détour d'une simple visite du site incriminé. Pour cette raison, quand vous demandez à consulter une page Web dangereuse contenant des exploits et d'autres menaces sérieuses, la ***barre d'outils de sécurité AVG*** n'autorisera pas votre navigateur à l'afficher.

Si vous rencontrez un site Web malveillant, la ***barre d'outils de sécurité AVG*** vous le signalera depuis votre navigateur en affichant un écran comparable à celui-ci :



L'accès à un tel site Web est très risqué et ne peut être recommandé !

8.11. Bouclier Web

8.11.1. Principes du Bouclier Web

Le Bouclier Web est une protection résidente en temps réel ; il analyse le contenu des pages Web visitées (et les fichiers qu'elles contiennent) avant qu'elles ne soient affichées dans le navigateur ou téléchargées sur l'ordinateur.

Lorsque le Bouclier Web détecte la présence de scripts Java dangereux dans la page demandée, il bloque son affichage. Il peut aussi reconnaître les codes malveillants contenus dans une page et arrêter immédiatement le téléchargement afin que ces codes ne s'infiltrent pas dans l'ordinateur.

Remarque : le *Bouclier Web AVG n'est pas conçu pour les plateformes serveur !*

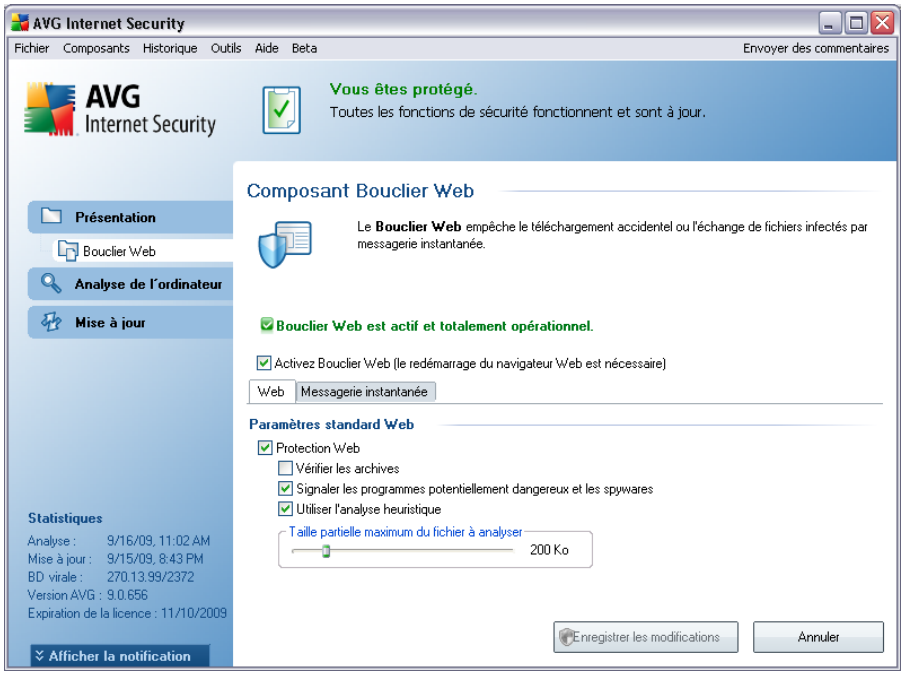
8.11.2. Interface du Bouclier Web

L'interface du composant ***Bouclier Web*** décrit le comportement de ce type de protection. Vous trouverez par la suite plus d'informations sur l'état actuel du composant (Le *bouclier Web est actif et totalement opérationnel.*). Dans la partie inférieure de la boîte de dialogue, vous trouverez des options d'édition élémentaires pour ce composant.

Configuration standard du composant

En premier lieu, vous avez le choix d'activer ou de désactiver le ***Bouclier Web*** en cochant la case ***Activer le Bouclier Web***. Cette option est sélectionnée par défaut : le composant ***Bouclier Web***est donc actif. Si toutefois, pour une raison valable, vous deviez modifier ces paramètres, nous vous recommandons de laisser ce composant actif. Lorsque la case est cochée et que le ***Bouclier Web*** est en cours d'exécution, des options de configuration supplémentaires sont proposées, que vous pouvez modifier sous deux onglets :

- ***Web*** - permet de modifier la configuration du composant chargé d'analyser le contenu des sites Web. L'interface d'édition propose plusieurs options de configuration élémentaires, décrites ci-après :

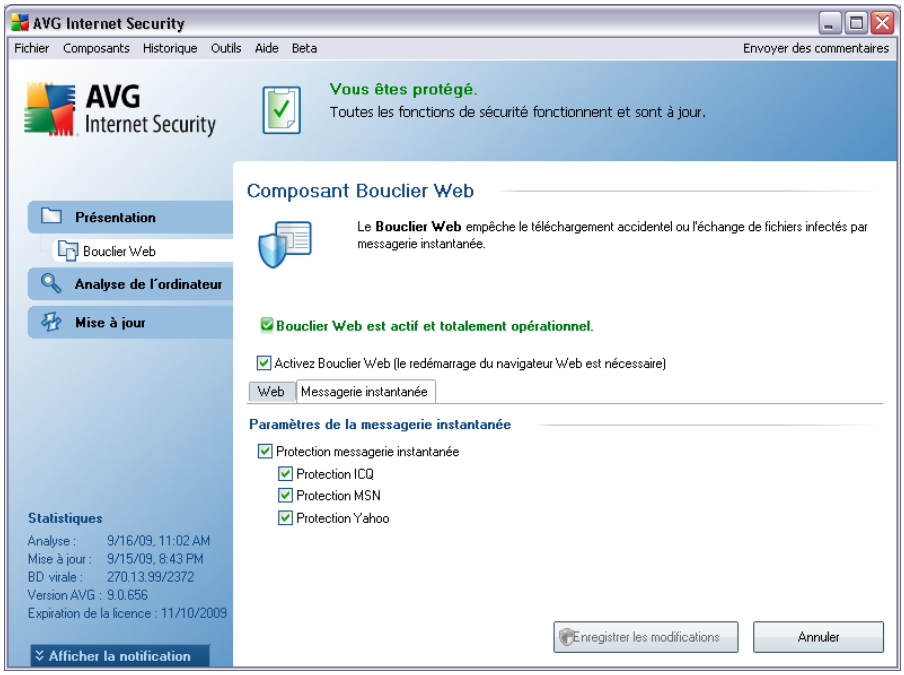


o ***Protection Web*** - cette option confirme que le ***Bouclier Web*** doit analyser le contenu des pages Web. Si elle est activée (*par défaut*), vous pouvez activer/désactiver les options suivantes :

- ***Vérifier les archives*** - analyse le contenu des archives éventuelles contenues dans la page Web à afficher
- ***Signaler les programmes potentiellement dangereux*** - recherche la présence éventuelle de programmes potentiellement dangereux (*exécutables fonctionnant comme des adwares ou des spywares*) inclus dans la page Web à afficher
- ***Utiliser l'analyse heuristique*** - analyse le contenu de la page à afficher en appliquant la méthode heuristique *(émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel - voir le paragraphe Principes de l'Anti-Virus*)
- ***Taille maximale de fichier à analyser*** - si des fichiers inclus figurent dans la page affichée, vous pouvez aussi analyser leur contenu avant de les télécharger sur l'ordinateur. Notez cependant que l'analyse de fichiers volumineux peut prendre du temps et ralentir considérablement le téléchargement de la page Web. Utilisez le curseur pour fixer la taille de fichier maximale que le ***Bouclier***

Web peut prendre en charge. Même si le fichier téléchargé est plus volumineux que le maximum spécifié et ne peut donc pas être analysé par le ***Bouclier Web***, vous restez protégé : si le fichier est infecté, le ***Bouclier résident*** le détecte immédiatement.

- ***Messagerie instantanée*** : permet de modifier les paramètres du composant portant sur l'analyse de la messagerie instantanée (*par exemple, ICQ, MSN Messenger, Yahoo...*).



o Protection de la messagerie instantanée - cochez cette case si vous voulez que le Bouclier Web vérifie que les communications en ligne sont exemptes de virus. Si l'option est activée, vous pouvez préciser l'application de messagerie instantanée à contrôler (actuellement, **AVG 9 Internet Security** prend en charge les applications ICQ, MSN et Yahoo).

Remarque : *l'éditeur du logiciel a configuré tous les composants AVG de manière à obtenir des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté. Si vous devez modifier la configuration d'AVG, sélectionnez le menu* ***Outils / Paramètres avancés*** *et modifiez la configuration d'AVG dans la boîte de dialogue Paramètres avancés d'AVG qui apparaît.*

Boutons de commande

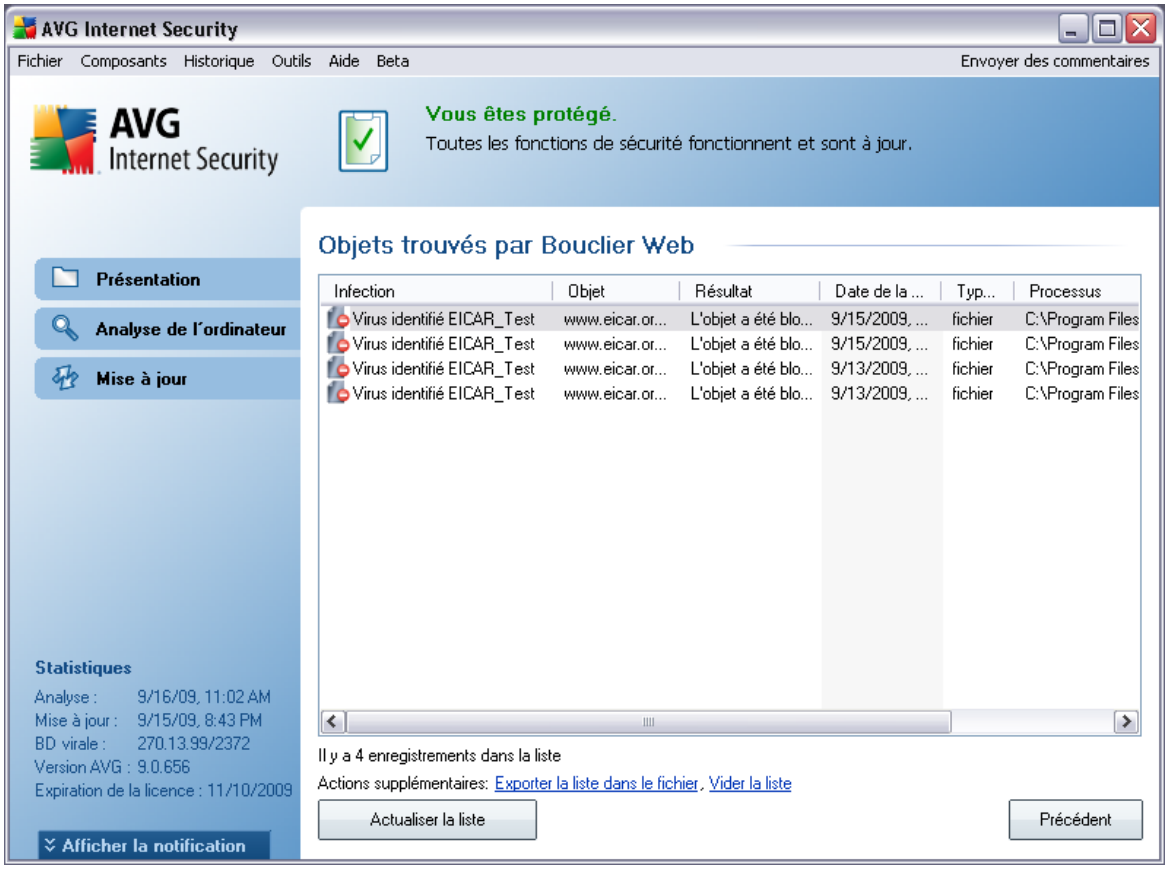
Les boutons de commande disponibles dans l'interface du ***Bouclier Web*** sont :

- ***Enregistrer*** - cliquez sur ce bouton pour enregistrer et appliquer les modifications entrées dans la boîte de dialogue
- ***Annuler*** - cliquez sur ce bouton pour revenir à l'interface utilisateur AVG par défaut (*avec la présentation générale des composants*)

8.11.3. Détection Bouclier Web

Bouclier Web - Il analyse le contenu des pages Web visitées (et les fichiers qu'elles contiennent) avant qu'elles ne soient affichées dans le navigateur ou téléchargées sur l'ordinateur. Vous serez immédiatement informé grâce à la boîte de dialogue suivante si une menace est détectée :

La page Web suspecte ne sera pas ouverte et la détection de la menace sera consignée dans la liste des ***Objets trouvés par Bouclier Web*** (cette vue générale des menaces détectées est accessible via le menu système ***Historique / Objets trouvés par Bouclier Web***.



Les informations suivantes accompagnent chaque objet détecté :

- ***Infection***- description (*et éventuellement le nom*) de l'objet détecté.
- ***Objet*** - source de l'objet (*page Web*)
- ***Résultat*** - action effectuée sur l'objet détecté
- ***Date de la détection*** - date et heure auxquelles la menace a été détectée et bloquée
- ***Type d'objet*** - type de l'objet détecté
- ***Processus*** - action réalisée pour solliciter l'objet potentiellement dangereux en vue de sa détection

Dans la partie inférieure de la boîte de dialogue, sous la liste, vous trouverez des

informations sur le nombre total d'objets détectés répertoriés ci-dessus. Par ailleurs, vous êtes libre d'exporter la liste complète des objets détectés dans un fichier (***Exporter la liste dans le fichier***) et de supprimer toutes les entrées des objets détectés (***Vider la liste***). Le bouton ***Actualiser la liste*** permet de mettre à jour la liste des menaces détectées par le ***Bouclier Web***. Le bouton ***Précédent*** vous permet de basculer vers l'***Interface utilisateur AVG*** par défaut (aperçu des composants).

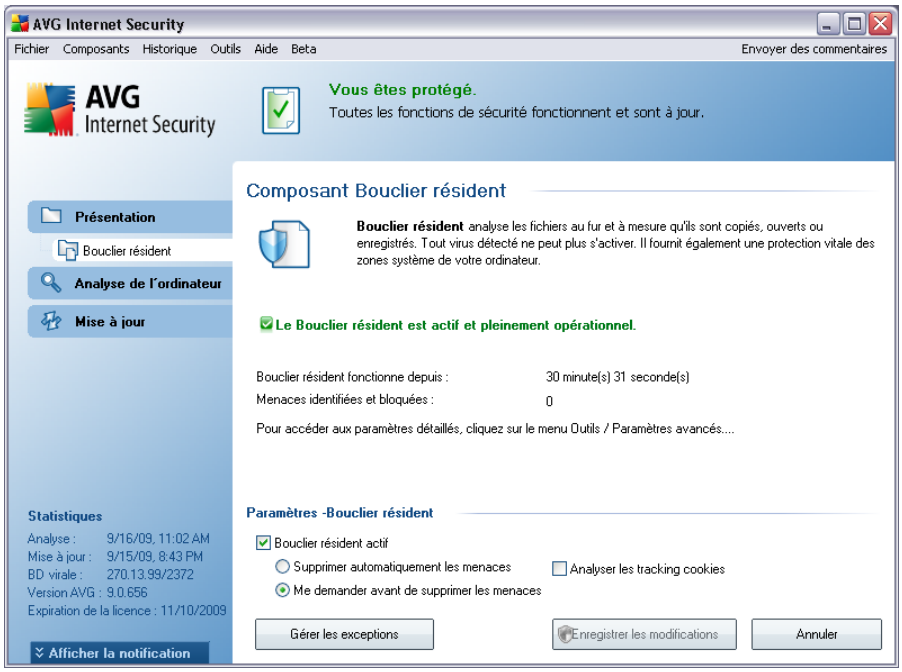
8.12. Bouclier résident

8.12.1. Principes du Bouclier résident

Le composant ***Bouclier résident*** assure une protection en temps réel de votre ordinateur. Il analyse chaque fichier ouvert, enregistré ou copié et surveille les zones système de l'ordinateur. Si le composant***Bouclier résident***détecte un virus dans un fichier, il interrompt l'opération en cours et ne donne donc pas la possibilité au virus de s'activer. Généralement, vous ne remarquez pas ce processus, car il fonctionne ''en arrière-plan''. Vous êtes seulement averti en cas de détection de menaces, tandis que le ***Bouclier résident*** bloque l'activation de la menace et l'éradique. Le ***Bouclier résident*** est chargé dans la mémoire de votre ordinateur au démarrage du système.

Attention: le Bouclier résident est chargé dans la mémoire de votre ordinateur au cours du démarrage ; il est vital qu'il reste toujours activé!

8.12.2. Interface du Bouclier résident



Outre une présentation des données statistiques les plus importantes et de l'état actuel du composant (Le *Bouclier résident est actif et entièrement opérationnel*), l'interface du ***Bouclier résident*** fournit également les valeurs des paramètres fondamentaux du composant. Les données statistiques fournies sont les suivantes :

- ***Le Bouclier résident est actif depuis***- indique le temps écoulé depuis le lancement du composant
- ***Menaces identifiées et bloquées*** - nombre d'infections détectées dont l'ouverture ou l'exécution a été bloquée (*si nécessaire, cette valeur peut être rétablie ; par exemple pour des besoins de statistique : Rétablir la valeur*)

Configuration standard du composant

Dans la partie inférieure de la boîte de dialogue figure la section ***Paramètres du Bouclier résident***, où vous pouvez éditer les paramètres de base du composant (*comme pour tous les autres composants, la configuration détaillée est accessible via la commande Paramètres avancée du menu système Fichier*).

L'option ***Le Bouclier résident est actif*** permet d'activer ou désactiver la protection

résidente. Par défaut, cette fonction est activée. Si la protection résidente est activée, vous pouvez définir plus précisément la manière dont les infections détectées sont traitées (c'est-à-dire supprimées) :

- automatiquement (***Supprimer automatiquement toutes les menaces***)
- ou seulement après accord de l'utilisateur (***Me demander avant de supprimer les menaces***)

Cette option n'a pas d'impact sur le niveau de la sécurité, mais reflète uniquement les préférences utilisateur.

Dans les deux cas, vous conservez la possibilité de ***supprimer automatiquement les cookies.*** Dans certaines circonstances, vous pouvez activer cette option pour appliquer le niveau de sécurité le plus élevé. Notez que cette option est désactivée par défaut. (*cookies : des portions de texte envoyées par un serveur à un navigateur Web et renvoyées en l'état par le navigateur chaque fois que ce dernier accède au serveur. Les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs telles que leurs préférences en matière de site ou le contenu de leurs paniers d'achat électroniques*).

Remarque : *l'éditeur du logiciel a configuré tous les composants AVG de manière à obtenir des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté. Si vous devez modifier la configuration d'AVG, sélectionnez le menu* ***Outils / Paramètres avancés*** *et modifiez la configuration d'AVG dans la boîte de dialogue Paramètres avancés d'AVG qui apparaît.*

Boutons de commande

Les boutons de commande disponibles dans l'interface du ***Bouclier résident*** sont :

- ***Gérer les exceptions*** - ouvre la boîte de dialogue ***Répertoires exclus du Bouclier résident*** où vous pouvez définir les dossiers à ne pas inclure dans la recherche du ***Bouclier résident***
- ***Enregistrer les modifications*** - cliquez sur ce bouton pour enregistrer et appliquer les modifications apportées dans cette boîte de dialogue
- ***Annuler*** - cliquez sur ce bouton pour revenir à l'***interface utilisateur AVG*** par défaut (présentation des composants)

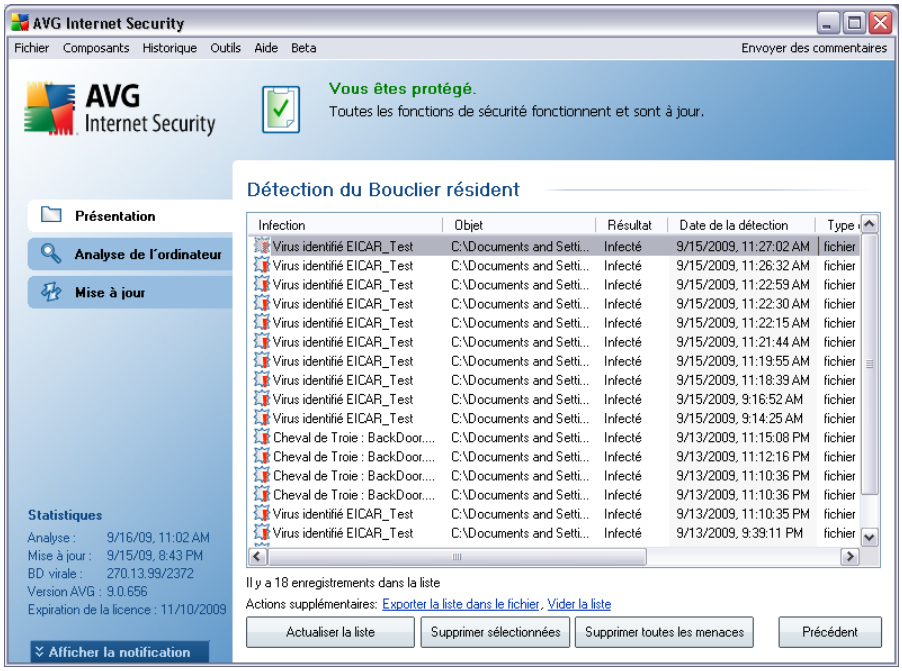
8.12.3. Détection du Bouclier résident

Le composant Bouclier résident analyse les fichiers lorsqu'ils sont copiés, ouverts ou enregistrés. Lorsqu'un virus ou tout autre type de menace est détecté, vous êtes averti immédiatement via la boîte de dialogue suivante :

Cette boîte de dialogue fournit des informations sur la menace détectée et vous invite à décider d'une action à prendre :

- ***Réparer*** : si la réparation est possible, AVG va nettoyer automatiquement le fichier infecté ; cette option est l'action recommandée
- ***Placer en quarantaine*** : le virus sera placé dans la ***Quarantaine d'AVG***
- ***Accéder au fichier*** - cette option vous redirige vers l'emplacement d'origine de l'objet suspect (*ouvre une nouvelle fenêtre de Windows Explorer*)
- ***Ignorer*** : nous vous recommandons fortement de ne PAS utiliser cette option sauf si vous avez une très bonne raison de le faire !

Vous trouverez des informations sur la présentation des menaces détectées par le ***Bouclier résident*** dans la boîte de dialogue ***Détection Bouclier résident*** accessible via l'option menu système ***Historique / Détection du Bouclier résident***:



La ***détection du Bouclier résident*** répertorie les objets détectés par le ***Bouclier résident*** comme étant dangereux, puis réparés ou déplacés en ***quarantaine***. Les informations suivantes accompagnent chaque objet détecté :

- ***Infection***- description (et éventuellement le nom) de l'objet détecté
- ***Objet*** - emplacement de l'objet
- ***Résultat*** - action effectuée sur l'objet détecté
- ***Moment de la détection*** - date et heure auxquelles l'objet a été détecté
- ***Type d'objet*** - type de l'objet détecté
- ***Processus*** - action réalisée pour solliciter l'objet potentiellement dangereux en vue de sa détection

Dans la partie inférieure de la boîte de dialogue, sous la liste, vous trouverez des informations sur le nombre total d'objets détectés répertoriés ci-dessus. Par ailleurs, vous êtes libre d'exporter la liste complète des objets détectés dans un fichier (***Exporter la liste dans le fichier***) et de supprimer toutes les entrées des objets détectés (***Vider la liste***). Le bouton ***Actualiser la liste*** permet de rafraîchir la liste des menaces détectées par le ***Bouclier résident***. Le bouton ***Précédent*** vous permet

de basculer vers l'***Interface utilisateur AVG*** par défaut (aperçu des composantes).

8.13. Mise à jour

Aucun logiciel de sécurité ne peut garantir une protection fiable contre la diversité des menaces à moins d'une mise à jour régulière. Les auteurs de virus sont toujours à l'affût de nouvelles failles des logiciels ou des systèmes d'exploitation. Chaque jour apparaissent de nouveaux virus, malwares et attaques de pirates. C'est pour cette raison que les éditeurs de logiciels ne cessent de diffuser des mises à jour et des correctifs de sécurité visant à combler les vulnérabilités identifiées.

C'est pourquoi il est essentiel de mettre régulièrement à jour votre produit AVG !

L'objet du composant ***Mise à jour*** est de vous aider à gérer la régularité des mises à jour. Dans ce composant, vous pouvez planifier le téléchargement automatique des fichiers de mise à jour par Internet ou depuis le réseau local. Les mises à jours de définitions de virus fondamentales doivent être exécutées quotidiennement si possible. Les mises à jour du programme, moins urgentes, peuvent se faire sur une base hebdomadaire.

Remarque : *veuillez lire attentivement le chapitre Mises à jour AVG pour plus d'informations sur les différents types et niveaux de mises à jour.*

Le Gestionnaire de téléchargement AVG est un outil simple qui facilite la gestion des téléchargements de produits AVG à usage personnel. Il configure le produit, le type de licence et la langue en fonction de vos choix. L'avantage majeur de cet utilitaire est qu'il vous permet de gérer le téléchargement de produits AVG selon vos besoins. En outre, le fichier d'installation le plus récent est toujours téléchargé, de sorte que tout le programme AVG est mis à jour après l'installation.

Gestionnaire de téléchargement AVG

- Il télécharge toujours le dernier fichier d'installation ;
- Il réduit la taille du fichier téléchargé ;
- Il prend en charge la reprise du téléchargement au cas où ce dernier échoue pour une raison quelconque ;
- Il est compatible avec toutes les éditions du programme AVG réservées à un usage personnel

Remarque :*Retenez que le Gestionnaire de téléchargement AVG ne supporte pas le*

téléchargement des Editions Réseau et SBS. Il fonctionne uniquement sous Windows 2000 (SP4 + Pack correctif cumulatif), Windows XP (SP2 et version supérieure) et Windows Vista (toutes les éditions).

8.13.1. Principes du composant Mise à jour

Le Gestionnaire de téléchargement AVG fonctionne comme suit :

- D'abord, il est nécessaire de télécharger l'application ***Gestionnaire de téléchargement AVG*** elle-même. Après l'exécution du ***Gestionnaire de téléchargement AVG***, vous êtes invité à choisir la langue de la procédure d'installation.

- Ensuite, le ***Gestionnaire de téléchargement AVG*** tente d'établir une connexion Internet en vue d'effectuer le test de connectivité. Une fois le test réussi, vous serez en mesure de choisir la version du programme AVG que vous souhaitez installer (*version complète, version d'évaluation, version gratuite*).

- Après le choix de la version du programme AVG, vous êtes invité à sélectionner le produit que vous voulez installer.

- Enfin, tous les fichiers d'installation requis vont être téléchargés. ***Le Gestionnaire de téléchargement AVG*** se referme et ***l'installation AVG*** débute***.***

8.13.2. Interface du composant Mise à jour

L'interface de ***Mise à jour*** affiche des informations sur la fonctionnalité du composant et son état actuel (Le composant *Mise à jour est actif*), ainsi que des données statistiques :

- ***Dernière mise à jour*** - précise la date et l'heure à laquelle la base de données a été mise à jour
- ***Version de la base de données virale*** - spécifie le numéro de la version la plus récente de la base de données ; ce nombre est incrémenté à chaque mise à jour de la base de données
- ***Prochaine mise à jour prévue*** - indique l'heure exacte à laquelle la prochaine mise à jour de la base de données est programmée

Configuration standard du composant

Dans la partie inférieure de la boîte de dialogue, section ***Paramètres - Mise à jour***, vous pouvez modifier les règles appliquées au lancement des mises à jour. Vous pouvez choisir de télécharger automatiquement les fichiers de mise à jour (***Exécuter les mises à jour automatiques***) ou simplement à la demande. Par défaut, l'option

Exécuter les mises à jour automatiques est activée (option recommandée). Le téléchargement régulier des fichiers de mise à jour les plus récents est un facteur vital pour les performances de tout logiciel de sécurité.

Il est possible de préciser le moment auquel exécuter la mise à jour :

- ***Régulièrement*** - définissez la périodicité
- ***A intervalle spécifique*** - définissez le jour et la date

Par défaut, la mise à jour a lieu toutes les 4 heures. Il est généralement recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité.

Remarque : *l'éditeur du logiciel a configuré tous les composants AVG de manière à obtenir des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté. Si vous devez modifier la configuration d'AVG, sélectionnez le menu* ***Outils / Paramètres avancés*** *et modifiez la configuration d'AVG dans la boîte de dialogue Paramètres avancés d'AVG qui apparaît.*

Boutons de commande

Les boutons de commande disponibles dans l'interface du ***Mise à jour*** sont :

- ***Mise à jour*** - exécute une mise à jour immédiate
- ***Enregistrer les modifications*** - cliquez sur ce bouton pour enregistrer et appliquer les modifications apportées dans cette boîte de dialogue
- ***Annuler*** - cliquez sur ce bouton pour revenir à l'***interface utilisateur AVG*** par défaut (présentation des composants)

8.14. Barre d'outils de sécurité AVG

La barre d'outils de sécurité AVG est un nouvel outil qui fonctionne en association avec le composant ***Link Scanner***. Elle vérifie les résultats trouvés par les moteurs de recherche sur Internet (*Yahoo!, Google, MSN, Baidu*).

Si vous choisissez d'installer la barre d'outils lors de l'installation**AVG 9 Internet Security** , elle sera ajoutée automatiquement au navigateur Web.

Vous pouvez utiliser la barre d'outils de sécurité pour commander les fonctions

LinkScanner et régler son fonctionnement, mais aussi pour mettre à jour **AVG 9 Internet Security** lorsque de nouvelles versions sont disponibles.

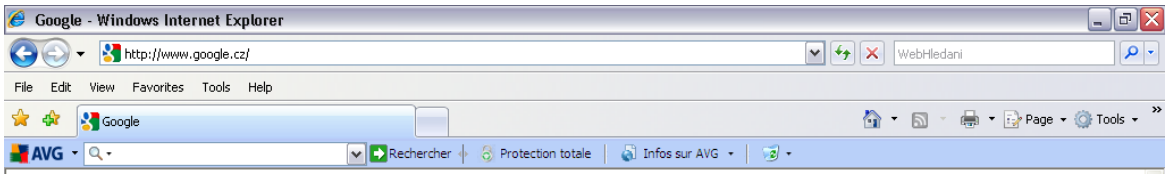
Note:*Si vous utilisez un navigateur autre qu'Internet Explorer (par exemple, Avant Browser), elle peut fonctionner de manière inattendue.*

8.14.1. Barre d'outils de sécurité AVG Interface

La ***barre d'outils de sécurité AVG*** est conçue pour fonctionner avec ***MS Internet Explorer*** (*version 6.0 ou supérieure*) et avec ***Mozilla Firefox*** (*version 1.5 ou supérieure*).

Remarque : la *Barre de sécurité AVG n'est pas conçue pour les plateformes serveur !*

Une fois que vous avez décidé d'installer la ***barre de sécurité AVG*** *durant le processus d'installation AVG on vous invitera à déterminer si vous allez installer le composant ou non*, le composant apparaîtra sous la barre d'adresse de votre navigateur:



La ***barre d'outils de sécurité AVG*** comprend les éléments suivants :

- ***Icône du logo AVG*** - donne accès aux éléments généraux de la barre d'outils. Cliquez sur le logo afin d'être redirigé vers le site Web d'AVG http://www.avg.com/. Un clic sur le pointeur situé au regard de l'icône AVG donne accès aux éléments suivants :
    - ***Informations sur la barre d'outils*** - un lien vers la page d'accueil de la ***barre d'outils de sécurité AVG*** qui contient des informations détaillées sur la protection de la barre d'outils
    - ***Lancement d'AVG 9.0*** - ouvre l'interface utilisateur AVG
    - ***Options*** - ouvre une boîte de dialogue de configuration vous permettant d'adapter les paramètres de la ***barre d'outils de sécurité AVG*** à vos besoins - voir le chapitre suivant ***Options barre d'outils de sécurité AVG***
    - ***Supprimer l'historique*** - vous permet de *Supprimer tout l'historique*de

la barre d'outils de sécurité AVG,d'*Effacer l'historique des recherches, l'historique de naviguation, l'historique des téléchargements,{*et *l'historique des cookies*.

- **Mise à jour** - recherche les nouvelles mises à jour pour la **barre d'outils de sécurité AVG**

- **Aide** - regroupe les fonctions permettant d'ouvrir le fichier d'aide, de contacter le **support technique d'AVG** ou de consulter les informations sur la version en cours de la barre d'outils

- **Recherche zone de recherche** - un moyen facile et sécurisé pour parcourir le Web à l'aide de Yahoo!. rechercher Saisissez un mot ou une expression dans la zone de recherche, puis cliquez sur **Rechercher** pour lancer la recherche directement sur le serveur Yahoo!, , quelle que soit la page affichée. La zone de recherche récapitule l'historique des recherches. Les recherches effectuées via la zone de recherche sont analysées par la protection AVG Search-Shield.

- **Bouton AVG Active Surf-Shield** - ce bouton (actif/inactif) contrôle l'état de la protection **AVG Active Surf-Shield**

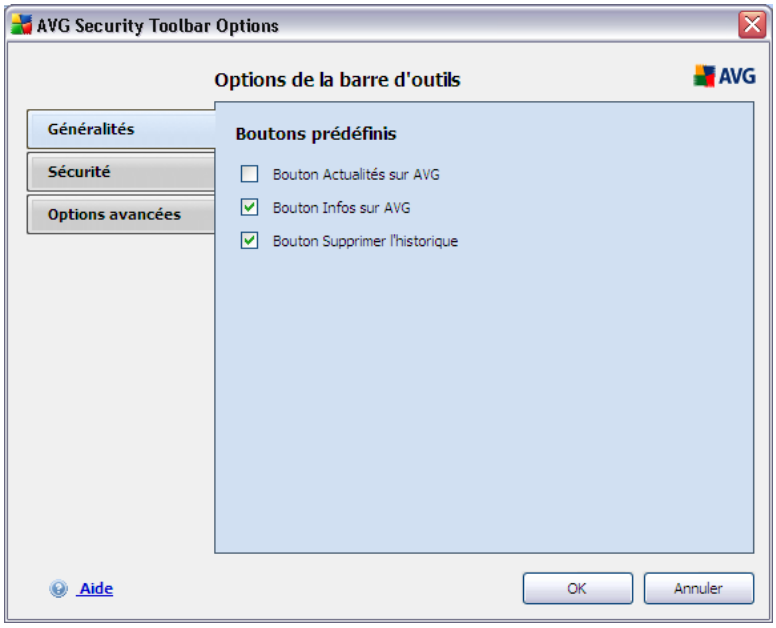
- **Bouton AVG Search-Shield** - ce bouton actif/inactif contrôle l'état de la protection **AVG Search-Shield**

- **Bouton Infos sur AVG** - fournit des liens vers des informations de sécurité importantes sur le site Web d'AVG (http://www.avg.com/).

8.14.2. Options de la Barre d'outils de sécurité AVG

Toutes les options de configuration des paramètres de la **barre d'outils de sécurité AVG** sont directement accessibles depuis le panneau de la **barre d'outils de sécurité AVG**. L'interface d'édition est accessible depuis le menu de la barre d'outils *AVG / Options* dans une nouvelle boîte de dialogue appelée **Options de la barre d'outils**, qui est divisée en trois sections :

- **Généralités**



Dans cet onglet vous pouvez spécifier le bouton qui doit être affiché / masqué dans le panneau de la ***barre d'outils de sécurité:***

- ***Bouton Actualités AVG*** - cette option affiche le bouton ***Actualités AVG***. Vous pouvez ouvrir un menu déroulant contenant des liens vers des communiqués de presses sur les nouveautés AVG en cliquant sur le bouton du panneau de la ***barre de sécurité AVG***.

- ***Bouton Infos AVG*** - le bouton ***Infos AVG***donne accès à un menu contenant les options suivantes:

  - *Infos sur la barre d'outils* - donne accès à la page du produit ***Barre d'outils de sécurité AVG*** qui fournit des informations détaillées sur le composant

  - *À propos des menaces* - donne accès à la page Web du laboratoire d'analyse virale AVG en fournissant des informations sur les menaces actuelles, les recommandations concernant la suppression de virus, la foire aux questions etc.

  - *Actualités AVG*- donne accès à la page Web qui fournit les derniers communiqués de presse sur AVG.

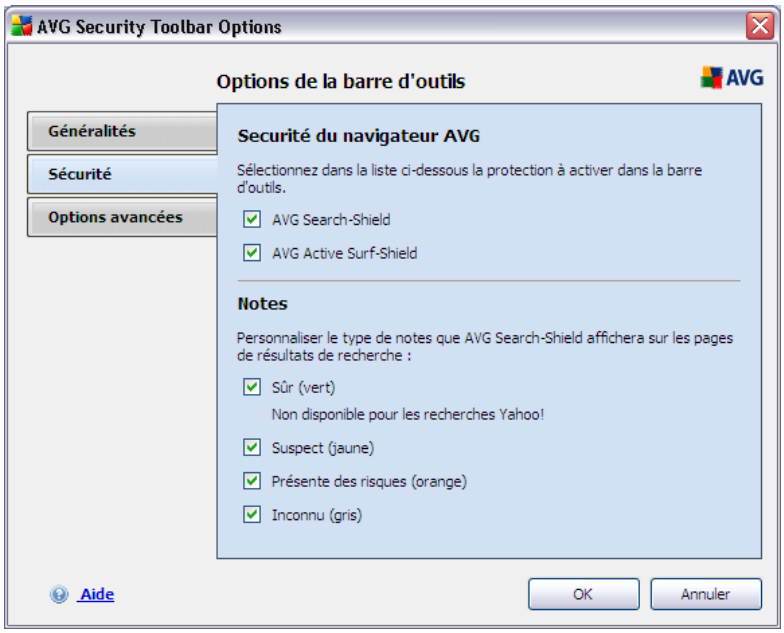
  - *Niveau de menace actuel* - donne accès à la page Web qui fournit

une représentation graphique du niveau de menace actuel sur le Web

- *Encyclopédie de virus* -donne accès à la page Encyclopédie de virus où vous pouvez rechercher les virus particuliers par nom et obtenir des informations détaillées sur chacun d'entre eux.

o ***Bouton Effacer l'historique*** - ce bouton vous permet d'*Effacer tout l'historique,* ou d'*Effacer l'historique des recherches, l'historique de navigation, l'historique des téléchargements,* ou d'*Effacer les cookies* à partir du panneau de la ***Barre d'outils de sécurité AVG.***

- ***Sécurité***



L'onglet de ***Sécurité*** est divisé en deux sections, ***Sécurité du navigateur AVG*** et ***Notes***, où vous pouvez cocher des cases afin de définir les fonctionnalités de la ***barre d'outils de sécurité AVG*** que vous voulez utiliser:

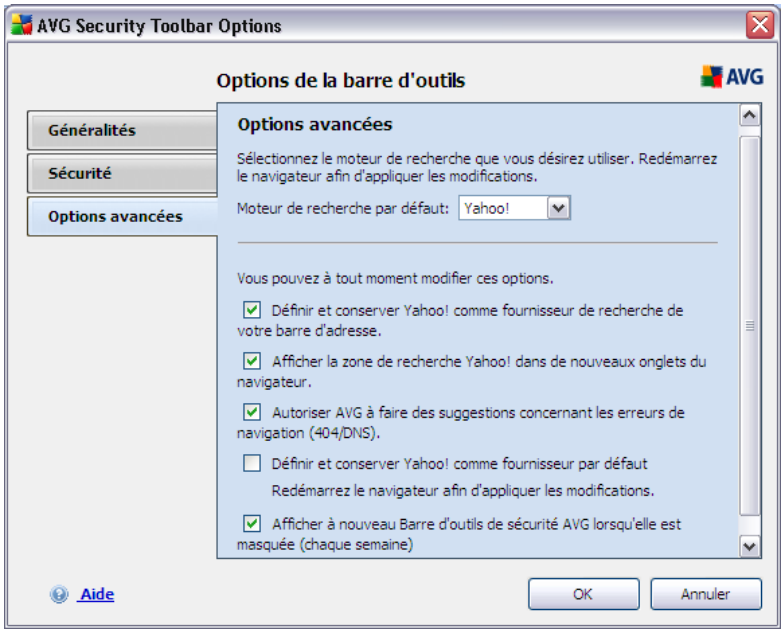
o ***Sécurité du navigateur AVG*** - cochez cet élément pour activer ou désactiver le service ***AVG Search-Shield*** et/ou ***AVG Active Surf-Shield***

o ***Notes*** - permet de sélectionner les symboles graphiques utilisés pour les notes de résultat de recherche par le composant ***AVG Search-Shield*** que vous voulez utiliser :

- la page est exempte de virus
- la page est suspecte
- la page contient des liens vers des pages dont le contenu est dangereux
- la page contient des menaces actives
- la page n'étant accessible, elle ne peut pas faire l'objet d'une analyse.

Cocher l'option correspondante pour confirmer que vous voulez être informé sur ce niveau de menace particulier. Cependant, l'affichage d'un point rouge attribué aux pages contenant des menaces actives et dangereuses ne peut pas être désactivé. ***Il est recommandé de garder la configuration par défaut et de ne la changer qu'en cas d'absolue nécessité.***

- ***Options avancées***



Dans l'onglet ***Options avancées*** vous pouvez activer ou désactiver d'autres paramètres spécifiques de la ***Barre d'outils de sécurité AVG*** :

- ***Définir et conserver Yahoo! comme moteur de recherche dans la barre d'adresse*** *activé par défaut*) - si vous la cochez, cette option vous permet de saisir un mot clé de recherche directement dans la barre d'adresse de votre navigateur Internet et le service Yahoo! sera automatiquement utilisé pour rechercher les sites correspondants.

- ***Afficher la zone de recherche zone de recherche dans les nouveaux onglets du navigateur*** (*activé par défaut*) - si vous la cochez, cette option affiche la zone de recherche Yahoo! dans chaque nouvel onglet du navigateur Internet.

- ***Autoriser AVG à rediriger les erreurs de navigation*** (*activé par défaut*) - si lors de votre recherche sur le net vous tombez sur une page inexistante ou qui ne peut pas s'afficher (*erreur 404*), ***la barre d'outils de sécurité AVG*** proposera automatiquement une liste de pages alternatives sur le même sujet.

- ***Définir et conserver Yahoo! comme moteur de recherche de votre navigateur*** (*désactivé par défaut*) - Yahoo! est le moteur de recherche par défaut pour la recherche Web dans la ***barre d'outils de sécurité AVG***, et en activant cette option il peut aussi devenir le moteur de recherche par défaut de votre navigateur.

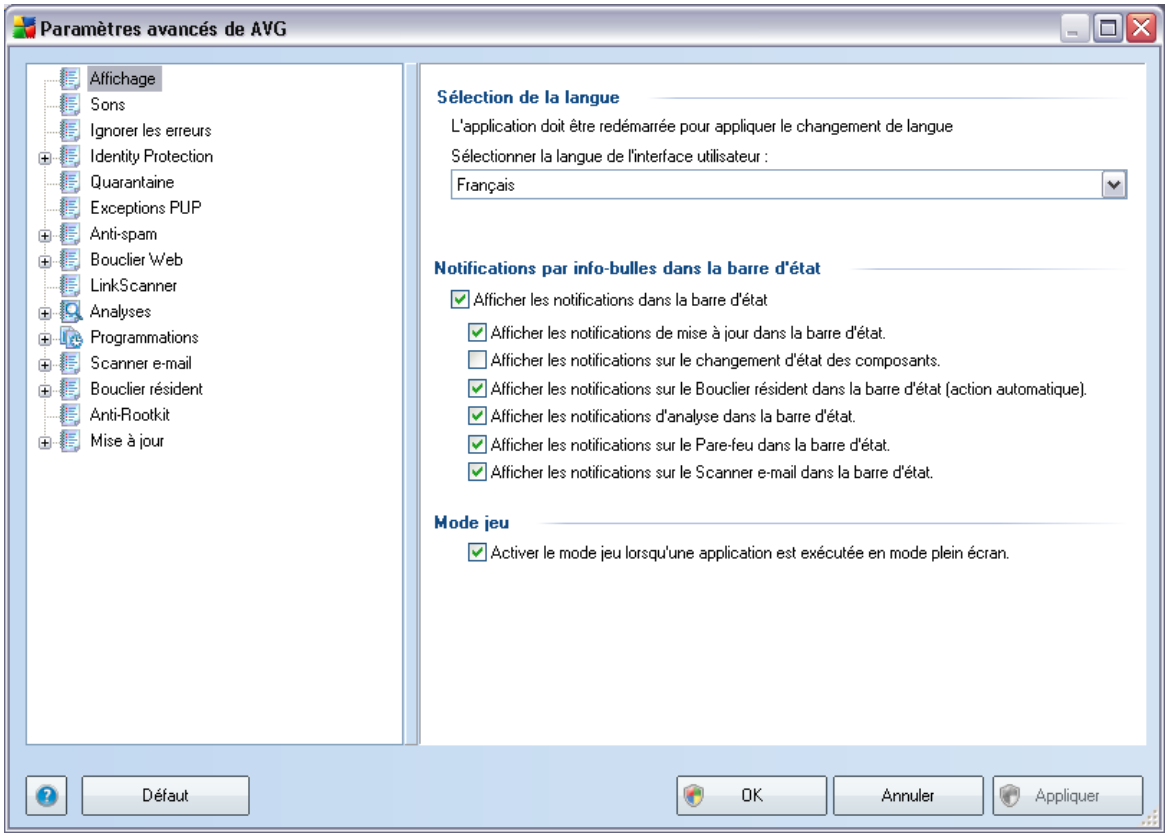
- ***Afficher à nouveau la barre d'outil de sécurité AVG lorsqu'elle est masquée (chaque semaine)*** - (*activée par défaut*) - cette option est activée par défaut et lorsque votre ***barre d'outils de sécurité AVG*** est masquée par erreur, elle sera affichée de nouveau dans une semaine.

9. Paramètres avancés d'AVG

La boîte de dialogue de configuration avancée d'**AVG 9 Internet Security** a pour effet d'ouvrir une nouvelle fenêtre intitulée ***Paramètres avancés d'AVG***. Cette fenêtre se compose de deux parties : la partie gauche présente une arborescence qui permet d'accéder aux options de configuration du programme. Sélectionnez le composant dont vous voulez corriger la configuration *(ou celle d'une partie spécifique)* pour ouvrir la boîte de dialogue correspondante dans la partie droite de la fenêtre.

9.1. Affichage

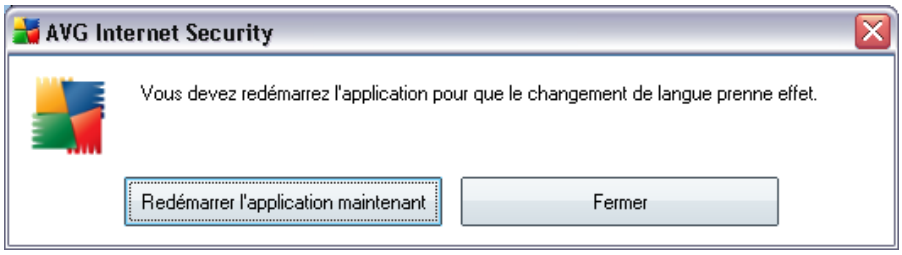
Le premier élément de l'arborescence de navigation, ***Affichage***, porte sur les paramètres généraux de l'interface utilisateur AVG et sur des options élémentaires du comportement de l'application :



Sélection de la langue

La section ***Sélection de la langue*** permet de choisir dans le menu déroulant la langue qui sera utilisée dans l'ensemble de l'interface utilisateur AVG. La liste déroulante ne propose que les langues que vous avez préalablement choisies au cours du processus d'installation (voir le chapitre Installation personnalisée - Sélection des composants). Pour que le changement de langue prenne effet, vous devez redémarrer l'interface utilisateur comme suit :

- Sélectionnez une langue, puis confirmez votre choix en cliquant sur le bouton ***Appliquer*** (angle inférieur droit)
- Appuyez sur le bouton***OK*** pour confirmer
- Une nouvelle boîte de dialogue s'affiche indiquant que l'application doit être redémarrée pour que le changement de langue de l'interface utilisateur AVG soit effectif.



Notifications par info-bulles dans la barre d'état

Dans cette section, vous pouvez désactiver l'affichage des info-bulles concernant l'état de l'application. Par défaut, les notifications s'affichent et il est recommandé de conserver cette configuration. Les info-bulles signalent généralement des changements d'état de composants AVG à prendre en considération.

Si toutefois, pour une raison particulière, vous souhaitez ne pas afficher ces notifications ou en afficher seulement quelques-unes (les notifications liées à un composant déterminé d'AVG, par exemple), vous pouvez indiquer vos préférences en cochant/désélectionnant les options suivantes :

- ***Afficher les notifications dans la barre d'état système*** - par défaut, activée *(cochée)* ; les notifications s'affichent. Désélectionnez cette option pour désactiver l'affichage de toutes les notifications par info-bulles.

Lorsqu'elle est active, vous pouvez sélectionner les notifications qui doivent s'afficher :

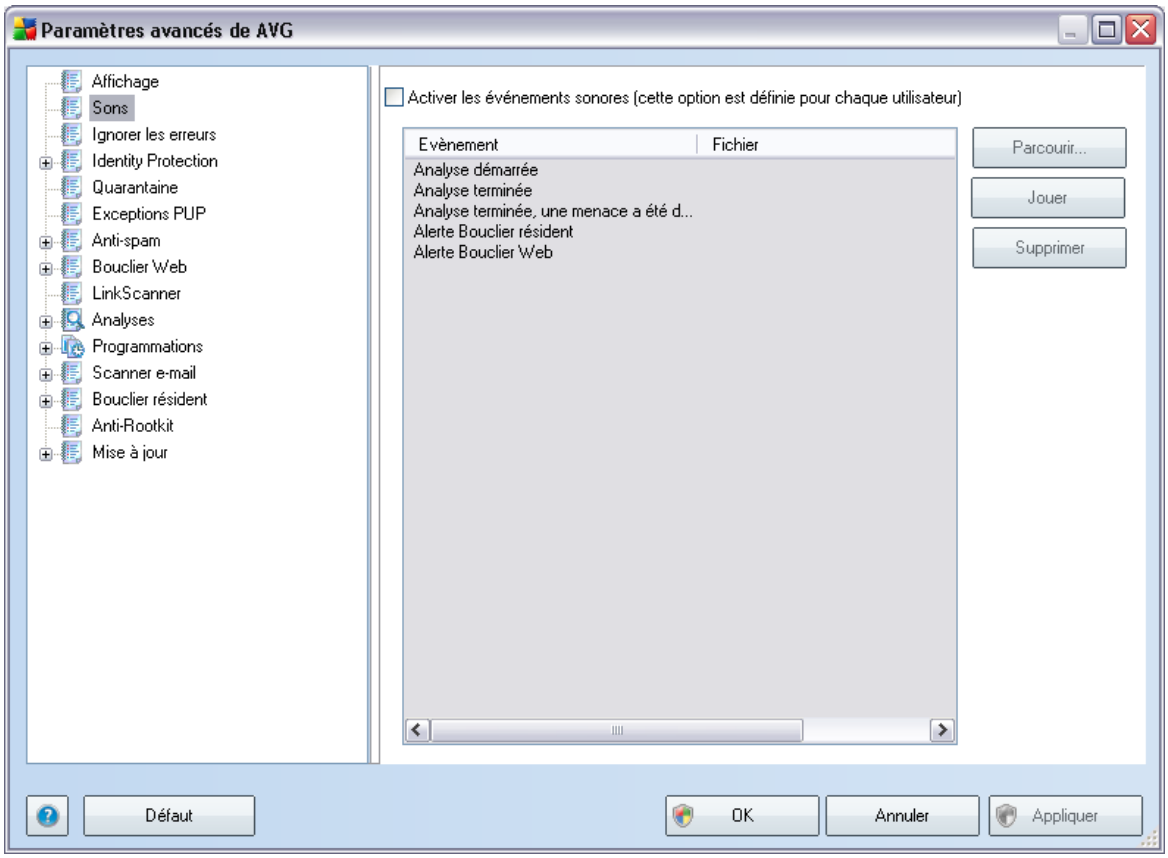
- ***Afficher des notifications dans la barre d'état système concernant la mise à jour*** - indiquez s'il faut afficher les informations sur le lancement de la mise à jour AVG, la progression et la fin du processus ;
- ***Afficher les notifications concernant le changement d'état des composants*** - indiquez s'il faut afficher des informations sur l'activité/ arrêt d'activité des composants ou les problèmes éventuels. Lorsque cette option signale un état d'anomalie dans un composant, elle a la même fonction d'information que l'icône dans la barre d'état système (changement de couleur) signalant un problème lié à un composant AVG;
- ***Afficher des notifications dans la barre d'état système concernant le Bouclier résident*** - indiquez s'il faut afficher ou supprimer les informations sur les processus d'enregistrement, de copie et d'ouverture de fichier ;
- ***Afficher des notifications dans la barre d'état système concernant l'analyse*** - indiquez s'il faut afficher les informations sur le lancement automatique de l'analyse programmée, sa progression et ses résultats ;
- ***Afficher des notifications dans la barre d'état système concernant le Pare-feu*** - décidez s'il faut afficher les informations concernant les processus et le statut du Pare-feu (par exemple, les avertissements sur l'activation/la désactivation d'un composant, les éventuels goulets d'étranglement, etc.).
- ***Afficher des notifications dans la barre d'état système concernant le Scanner e-mail*** - indiquez s'il faut afficher les informations sur l'analyse de tous les messages entrants et sortants.

Mode jeu

Cette fonction AVG a été conçue pour les applications s'exécutant en plein écran et qui nécessitent une communication avec Internet. Dans ce cas, la boîte de dialogue AVG pourrait perturber (*(réduction de la fenêtre ou distorsion du graphisme)*). Pour éviter ce type de problème, il est recommandé de cocher la case ***Activer le mode jeu lorsqu'une application est exécutée en mode plein écran*** (*(paramètre par défaut)*).

9.2. Sons

Dans la boîte de dialogue ***Sons*** vous pouvez spécifier si vous désirez être informé des actions spécifiques d'AVG, par des sons. Si c'est le cas, cochez l'option***Activer les évènements sonores*** (*désactivée par défaut*) pour activer la liste des actions AVG.

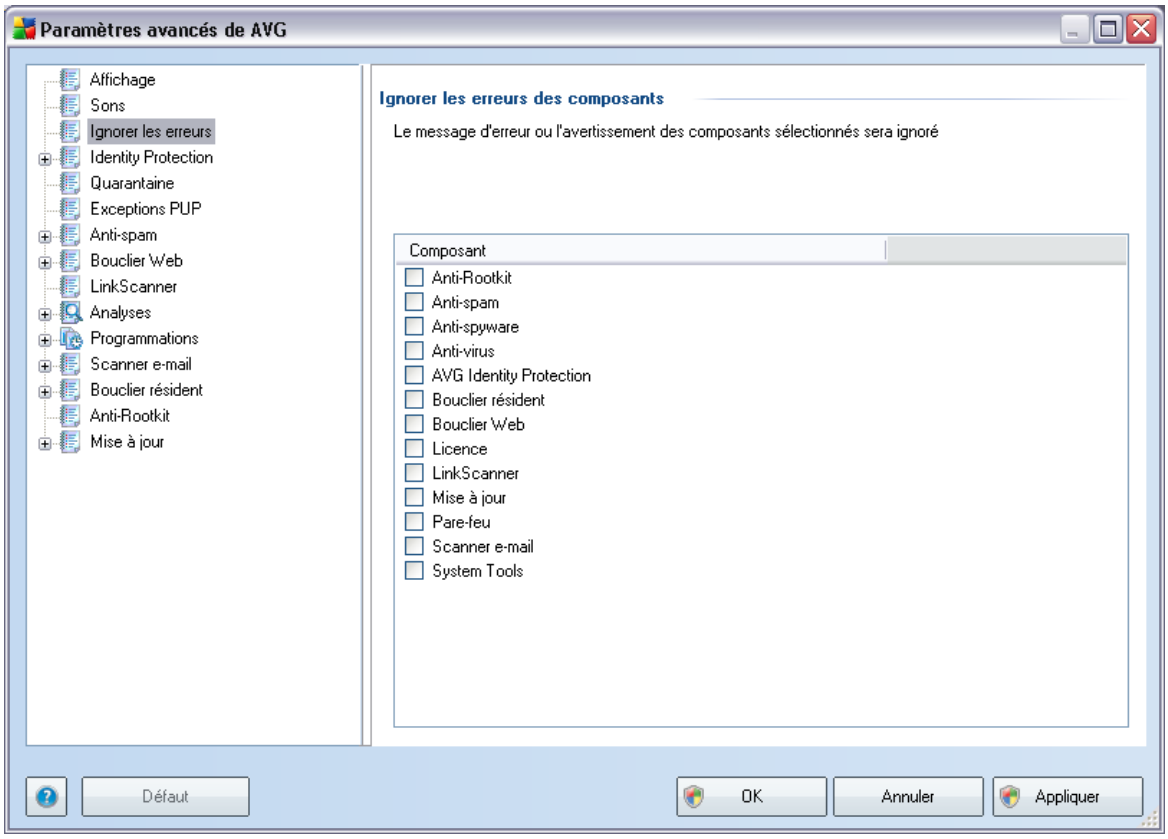


Ainsi, sélectionnez l'évènement correspondant à partir de la liste et recherchez (***Parcourir***) un son approprié que vous souhaitez affecter à cet événement. Pour écouter le son sélectionné, mettez en surbrillance l'évènement dans la liste et appuyez sur le bouton ***Jouer***. Utilisez le bouton ***Supprimer*** pour supprimer le son affecté à cet événement spécifique.

Remarque : *Seuls les sons *.wav sont pris en charge!*

9.3. Ignorer les erreurs

Dans la boîte de dialogue ***Ignorer les erreurs des composants***, vous pouvez cocher les composants dont vous ne souhaitez pas connaître l'état :



Par défaut, aucun composant n'est sélectionné dans cette liste. Dans ce cas, si l'état d'un des composants est incorrect, vous en serez immédiatement informé par le biais des éléments suivants :

- ***icône de la barre d'état système*** - si tous les composants d'AVG fonctionnent correctement, l'icône apparaît en quatre couleurs ; cependant, si une erreur se produit l'icône apparaît avec un point d'exclamation de couleur jaune,
- description du problème existant dans la section relative à l'***état de sécurité*** de la fenêtre principale d'AVG

Il peut arriver que pour une raison particulière, vous soyez amené·à désactiver

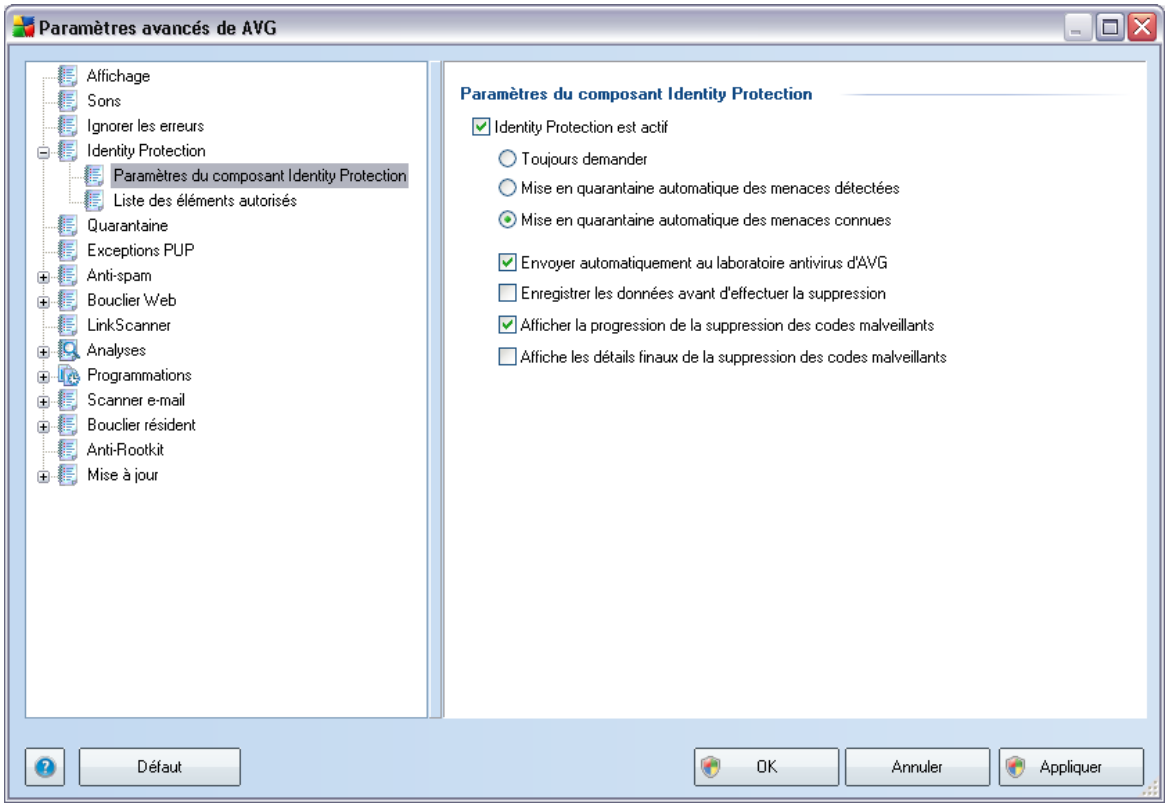
provisoirement un composant (*cela n'est pas recommandé ; vous devez toujours veiller à maintenir les composants activés et appliquer la configuration par défaut*). Dans ce cas, l'icône dans la barre d'état système signale automatiquement une erreur au niveau du composant. Toutefois, il est impropre de parler d'erreur alors que vous avez délibérément provoqué la situation à l'origine du problème et que vous êtes conscient du risque potentiel. Parallèlement, dès qu'elle apparaît en couleurs pastels, l'icône ne peut plus signaler toute autre erreur susceptible d'apparaître par la suite.

Aussi, dans la boîte de dialogue ci-dessus, sélectionnez les composants qui risquent de présenter une erreur (*composants désactivés*) dont vous voulez ignorer l'état. Une option similaire, ***Ignorer l'état du composant***, est également disponible pour certains composants depuis la vue générale des composants figurant dans la fenêtre principale d'AVG.

9.4. Identity Protection

9.4.1. Paramètres d'Identity Protection

La boîte de dialogue des ***Paramètres du composant Identity Protection*** permet d'activer ou de désactiver les fonctions essentielles du composant ***Identity Protection*** :



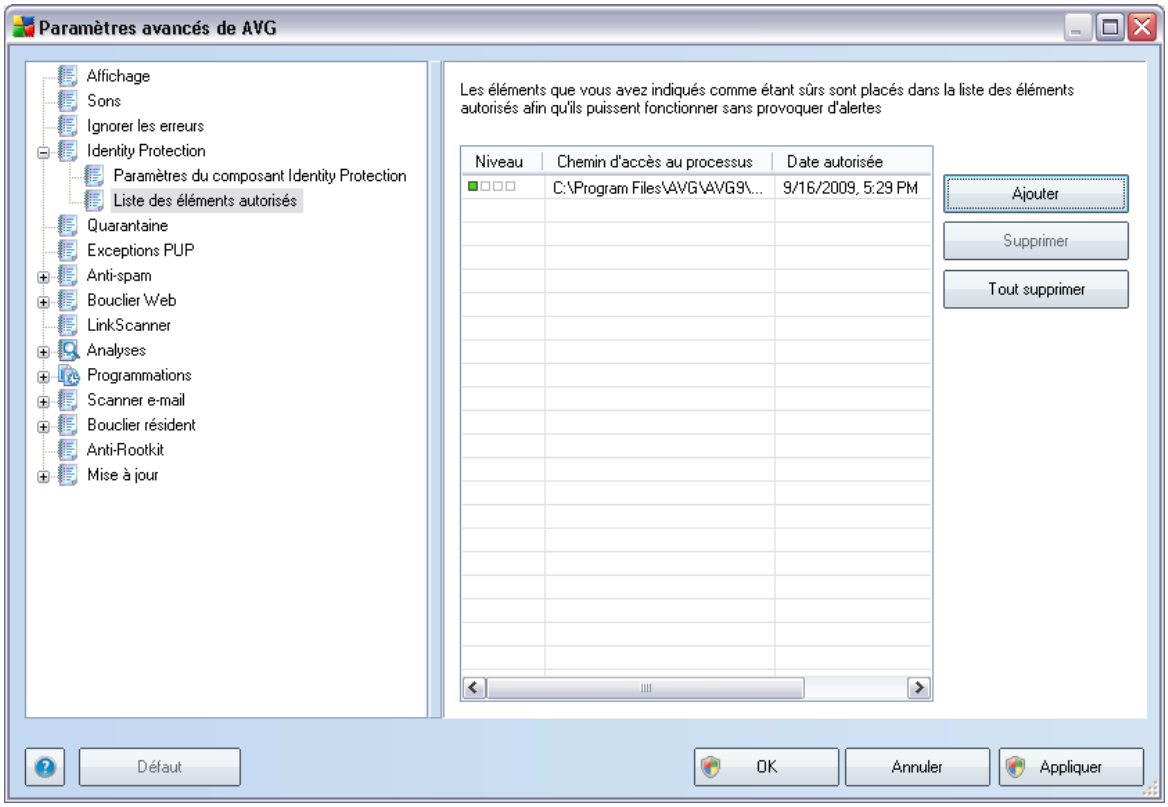
- ***Mise en quarantaine automatique des menaces détectées*** - (*désactivé par défaut*): cochez cette case pour indiquer que vous voulez déplacer automatiquement en quarantaine toutes les menaces détectées dans le composant Quarantaine AVG. Vous avez la possibilité de conserver les paramètres par défaut. Dans ce cas, lorsqu'une menace est détectée, vous êtes invité à confirmer si elle doit être mise en quarantaine pour s'assurer que les applications à exécuter ne sont pas supprimées.

- ***Envoyer automatiquement aux laboratoires d'AVG*** - (*option activée par défaut*) - laissez cette case cochée afin d'alimenter la base de données d'informations sur les activités malveillantes présentes sur Internet et de nous aider à identifier de nouvelles menaces.

9.4.2. Liste des éléments autorisés

Si, dans la boîte de dialogue ***Paramètres d'Identity Protection*** , vous avez choisi de ne pas activer l'élément ***Mettre automatiquement en quarantaine les fichiers détectés***, à chaque fois qu'un programme malveillant potentiellement dangereux est détecté, vous êtes invité à confirmer s'il doit être supprimé. Si vous décidez de définir

l'application suspecte comme étant sécurisée (*en vous basant sur son comportement*) et confirmez qu'elle doit être maintenue sur votre ordinateur, celle-ci est ajoutée à la ***liste Autorisés*** et n'est plus signalée comme élément potentiellement dangereux :



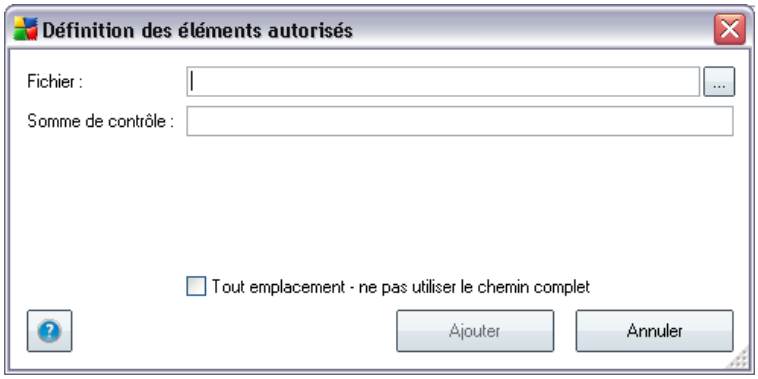
La***liste autorisée*** fournit les informations suivantes sur chaque processus:

- ***Niveau*** identification graphique de la gravité du processus en cours sur quatre niveaux allant du moins dangereux (■□□□) au plus grave (■■■■)
- ***Chemin d'accès au processus*** - chemin d'accès à l'emplacement du fichier exécutable du (*processus*) d'application
- ***Date d'autorisation*** -date à laquelle l'application a été définie comme étant sécurisée

Boutons de commande

Les boutons de commande disponibles dans l'interface du ***Bouclier résident*** sont :

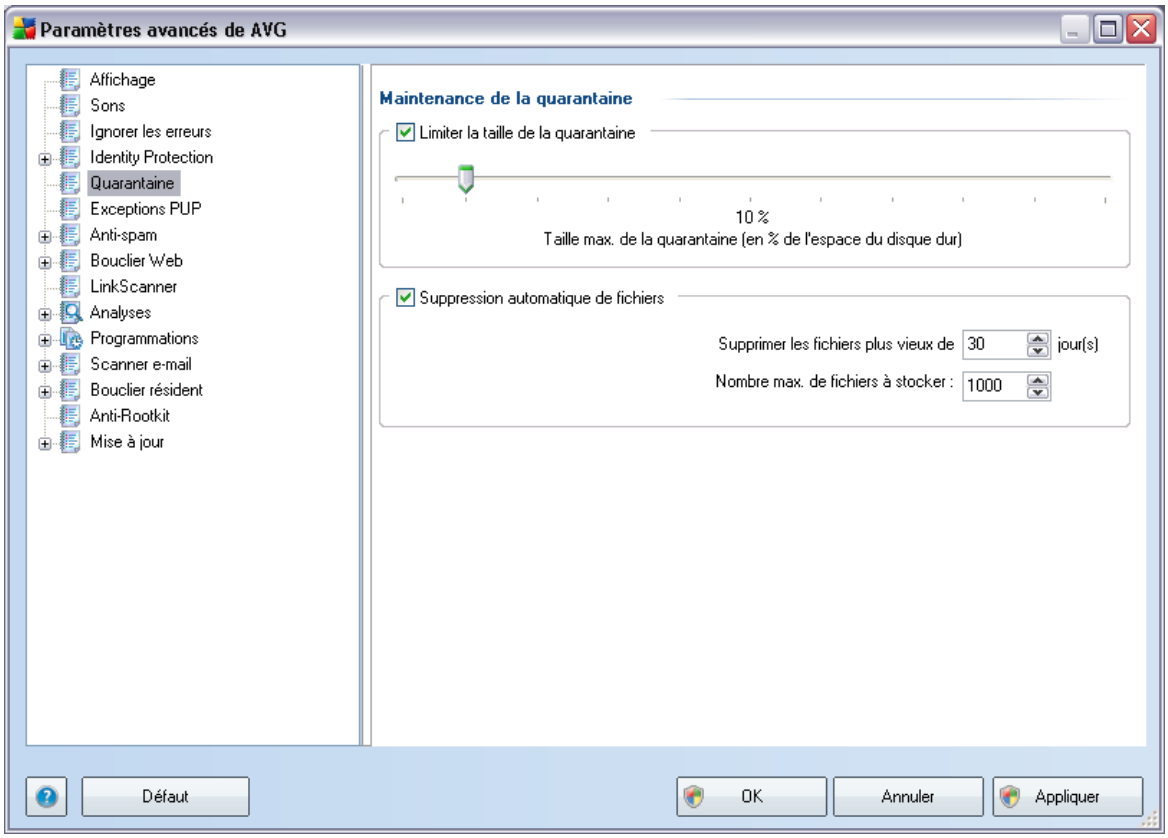
- ***Ajoutez*** - cliquez sur ce bouton pour ajouter un élément à la liste. La boîte de dialogue suivante s'affiche:



  - ***Fichier*** - spécifiez le chemin d'accès complet du fichier (*de l'application*) à considérer comme étant une exception
  - ***Somme de contrôle*** - affiche la "signature" unique du fichier choisi. Il s'agit d'une chaîne de caractères générée automatiquement, qui permet à AVG de distinguer sans risque d'erreur ce fichier parmi tous les autres. La somme de contrôle est générée et affichée une fois le fichier ajouté.
  - ***Tout emplacement*** - ne pas utiliser le chemin complet - si vous souhaitez définir ce fichier comme une exception uniquement à un emplacement spécifique, veillez à ne pas cocher cette case.

- ***Supprimer*** - cliquez sur ce bouton pour supprimer l'application de la liste
- ***Supprimer tout*** - cliquez sur ce bouton pour supprimer toutes les applications répertoriées

9.5. Quarantaine

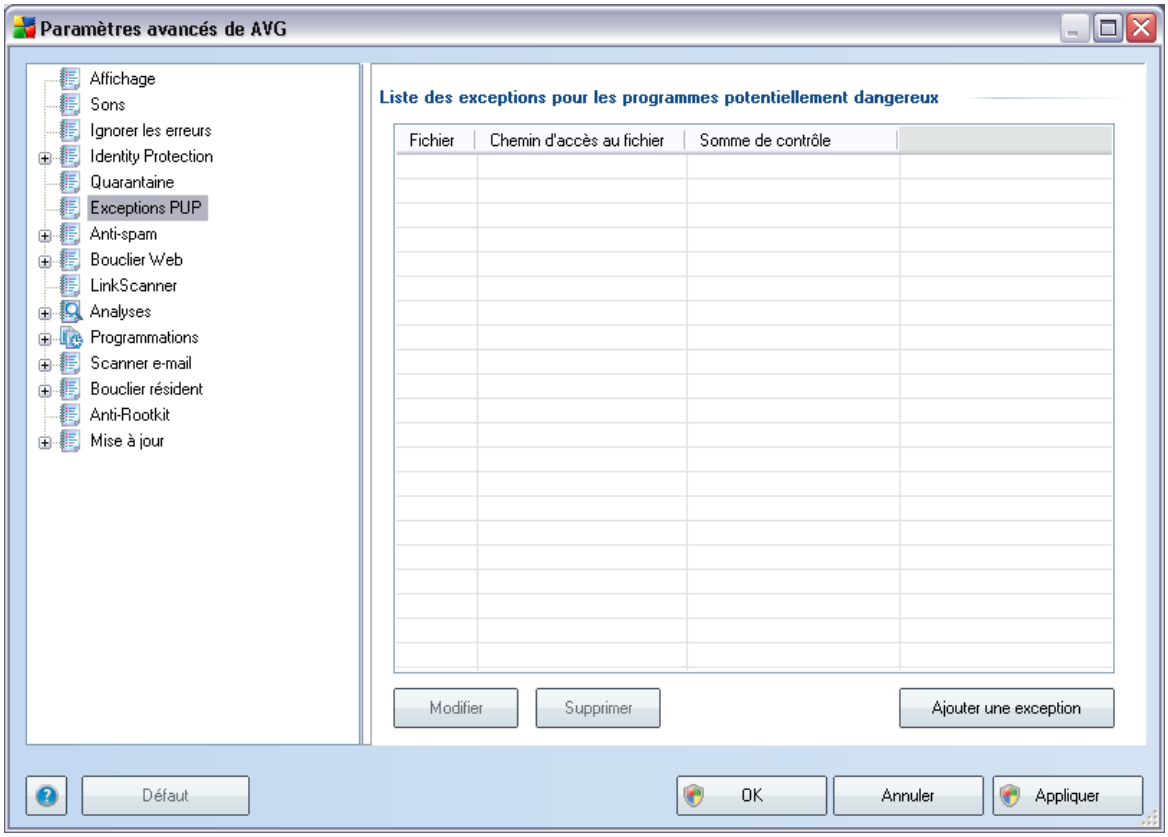


La boîte de dialogue ***Maintenance de la quarantaine*** permet de définir plusieurs paramètres liés à l'administration des objets stockés dans la ***Quarantaine*** :

- ***Limiter la taille de la quarantaine*** - utilisez le curseur pour ajuster la taille de la ***quarantaine***. La taille est indiquée par rapport à la taille de votre disque local.
- ***Suppression automatique de fichiers*** - dans cette section, définissez la durée maximale de conservation des objets en ***quarantaine*** (***Supprimer les fichiers plus vieux de ... jours***) ainsi que le nombre maximal de fichiers à conserver en ***quarantaine*** (***Nombre max. de fichiers à stocker***)

9.6. Exceptions PUP

AVG 9 Internet Security est en mesure d'analyser et de détecter des exécutables ou bibliothèques DLL qui peuvent s'avérer malveillants envers le système. Dans certains cas, il est possible que l'utilisateur souhaite conserver certains programmes considérés comme potentiellement dangereux sur son ordinateur *(ceux installés volontairement, par exemple*). Certains programmes, et notamment ceux fournis gratuitement, font partie de la famille des adwares. Or, ce type de programme peut être signalé par AVG comme un ***programme potentiellement dangereux***. Si vous souhaitez malgré tout le conserver sur votre ordinateur, il suffit de le définir comme une exception de programme potentiellement dangereux :

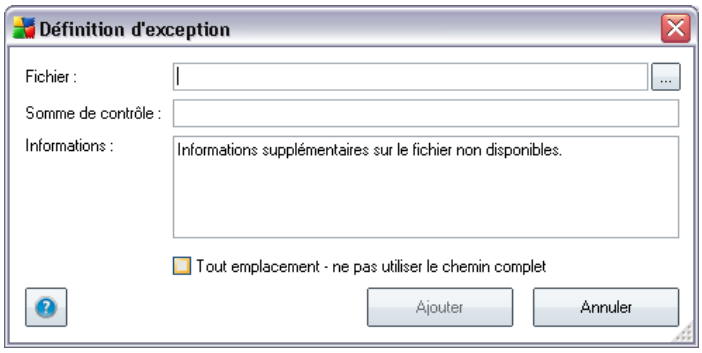


La boîte de dialogue ***Liste des exceptions pour les programmes potentiellement dangereux*** dresse la liste des exceptions déjà définies et actuellement valides par rapport aux programmes indésirables. Vous pouvez modifier la liste, supprimer des éléments existants ou ajouter une nouvelle exception. Vous trouverez les informations suivantes dans la liste de chaque exception :

- ***Fichier*** - indique le nom de l'application correspondante
- ***Chemin d'accès au fichier*** - indique le chemin d'accès à l'emplacement de l'application
- ***Somme de contrôle*** - affiche la "signature" unique du fichier choisi. Il s'agit d'une chaîne de caractères générée automatiquement, qui permet à AVG de distinguer sans risque d'erreur ce fichier parmi tous les autres. La somme de contrôle est générée et affichée une fois le fichier ajouté.

Boutons de commande

- ***Modifier*** - ouvre une boîte de dialogue d'édition (*identique à la boîte de dialogue permettant de définir une nouvelle exception, voir ci-dessus*) d'une exception déjà définie dans laquelle vous modifiez les paramètres de l'exception
- ***Supprimer*** - supprime l'élément sélectionné de la liste des exceptions
- ***Ajouter une exception*** - ouvre une boîte de dialogue dans laquelle vous définissez les paramètres de l'exception à créer :



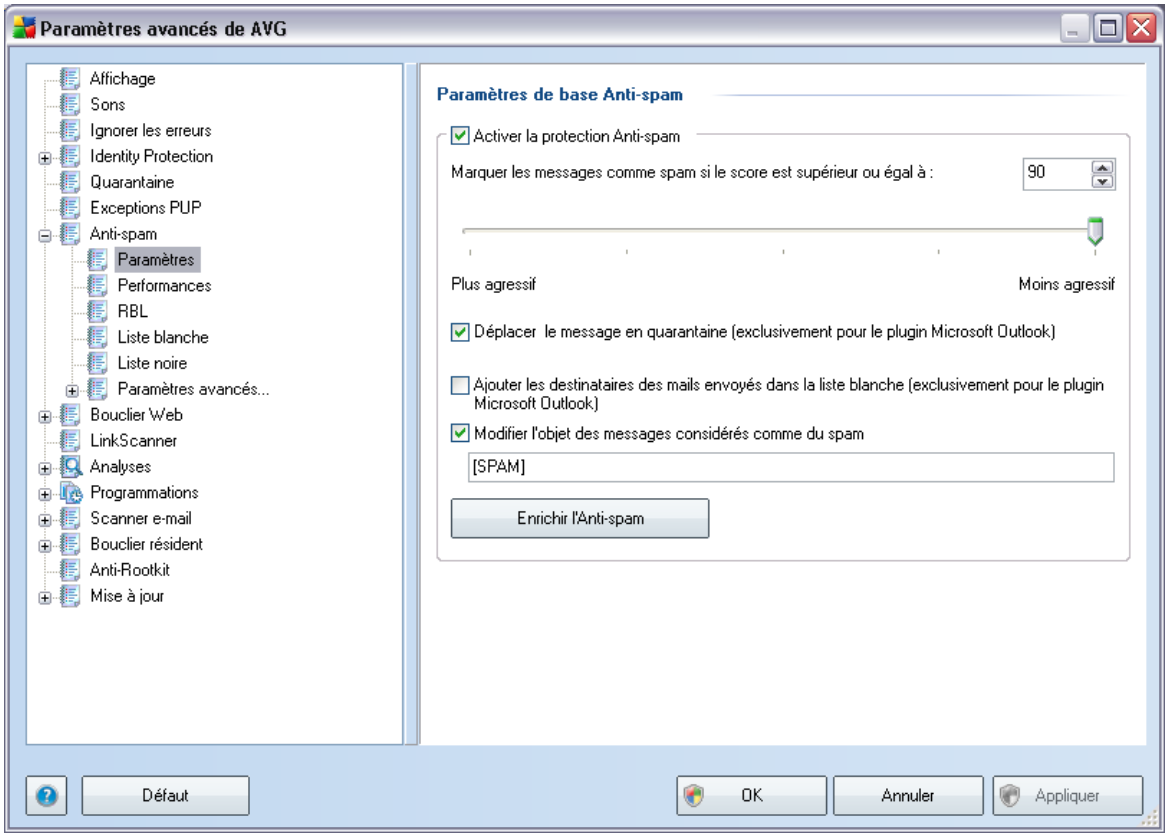
  - ***Fichier*** - spécifiez le chemin d'accès complet du fichier à identifier comme étant une exception
  - ***Somme de contrôle*** - affiche la "signature" unique du fichier choisi. Il s'agit d'une chaîne de caractères générée automatiquement, qui permet à AVG de distinguer sans risque d'erreur ce fichier parmi tous les autres. La somme de contrôle est générée et affichée une fois le fichier ajouté.
  - ***Informations*** - affiche des informations supplémentaires sur le fichier

(*licence, version, etc.*)

- ***Tout emplacement - ne pas utiliser le chemin complet*** - si vous souhaitez définir le fichier comme étant une exception unique à un emplacement spécifique, ne cochez pas cette case.

9.7. Anti-Spam

9.7.1. Paramètres



Dans la boîte de dialogue ***Paramètres de base anti-spam***, décochez la case ***Activer la protection anti-spam*** pour autoriser/interdire l'analyse anti-spam dans les communications par e-mail. Cette option est activée par défaut et comme toujours, il est recommandé de garder la configuration par défaut et de ne la changer qu'en cas d'absolue nécessité

Vous pouvez ensuite sélectionner également des mesures de contrôle plus ou moins strictes en matière de 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 ajuster le paramètre ***Marquer les messages comme spam si le score est supérieur à***, entrez le score qui convient (*entre 0 et 100*) ou faites glisser le curseur vers la gauche ou vers la droite (*dans ce cas la plage de valeurs va 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.***

Dans la boîte de dialogue ***Paramètres standard anti-spam***, vous pouvez aussi définir la façon dont les messages indésirables doivent être traités :

- ***Déplacer le message en quarantaine*** - cochez cette case pour que tous les messages détectés comme du courrier indésirables soient automatiquement transférés dans le dossier des messages indésirables de votre client de messagerie ;
- ***Ajouter les destinataires des messages envoyés à la liste blanche*** - cocher cette case pour confirmer que tous les destinataires des messages envoyés sont fiables et que tous les messages provenant de ces comptes e-

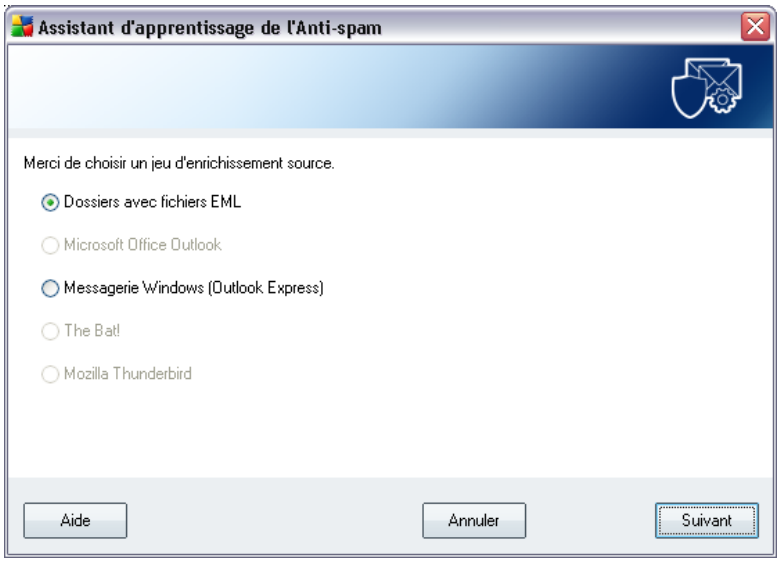
mail peuvent être transmis ;

- ***Modifier l'objet des messages considérés comme du courrier indésirable*** - cochez cette case pour signaler tous les messages détectés comme du courrier indésirable 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.

Boutons de commande

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

Le premier écran de l'***Assistant d'apprentissage 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

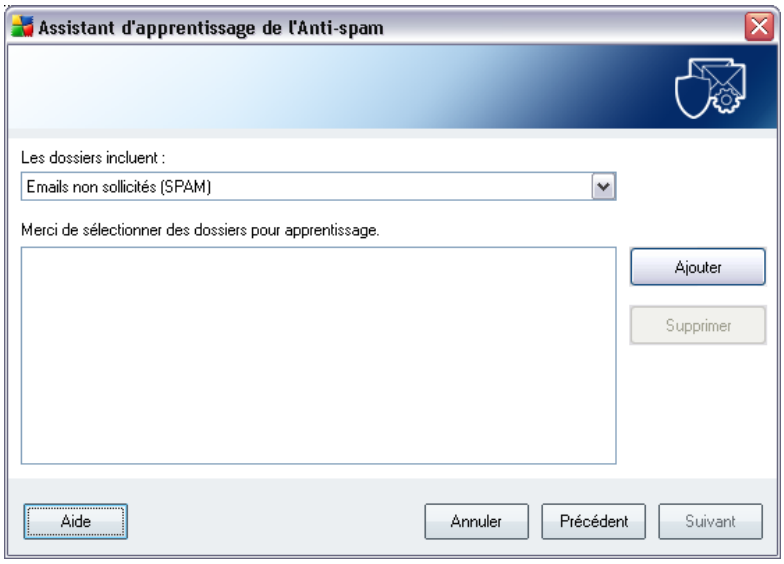
- ***Dossiers avec fichiers EML*** - si vous utilisez un autre programme de messagerie, commencez par enregistrer les messages dans un dossier spécifique (*au format .eml*) ou assurez-vous que vous connaissez l'emplacement des dossiers dans lesquels sont stockés les messages du client de messagerie. 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.

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

Dossiers avec fichiers EML



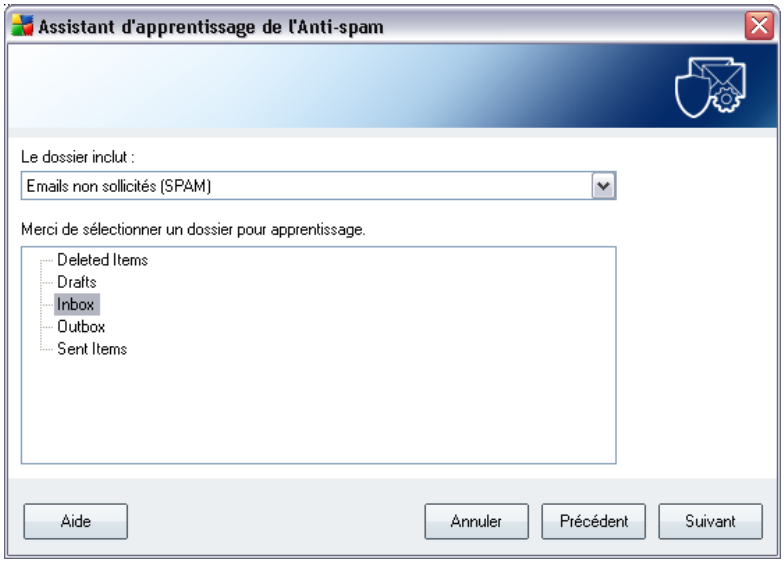
Dans cette boîte de dialogue, sélectionnez le dossier contenant les messages à utiliser pour la procédure d'enrichissement. Cliquez sur le bouton ***Ajouter*** pour localiser le dossier contenant les fichiers .eml (*messages e-mail enregistrés*). Le dossier sélectionné apparaît dans la boîte de dialogue.

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

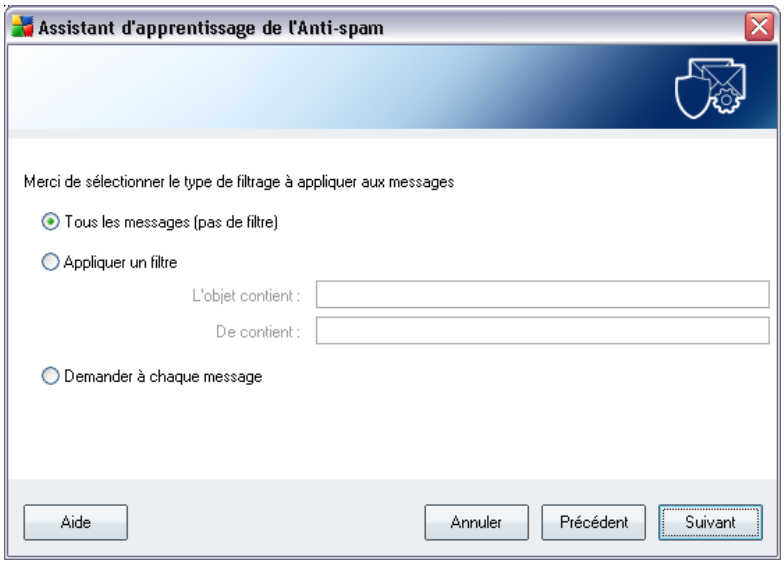
Lorsque vous avez choisi une option, une nouvelle boîte de dialogue apparaît.



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***.



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 le contenu du 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***.

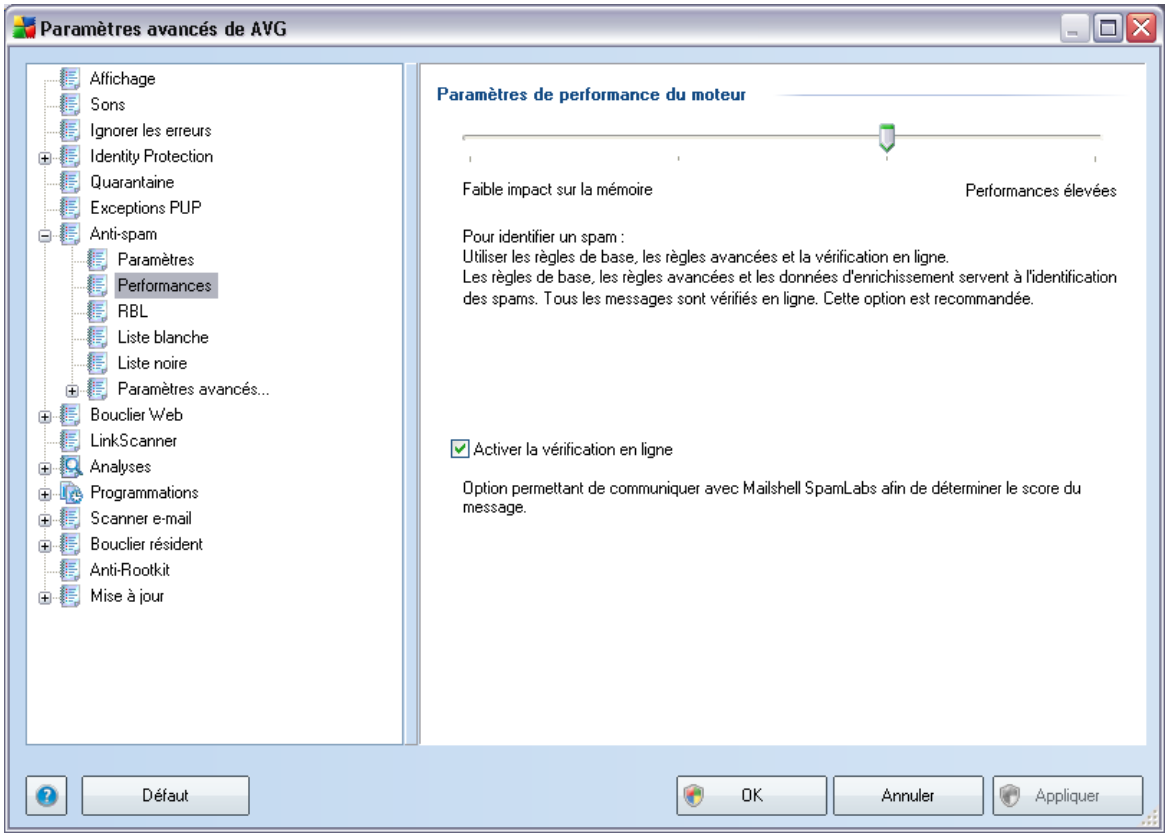
Pour accéder aux options avancées du filtrage, activez l'option ***Utiliser le filtre***. Vous pouvez spécifier un mot (*nom*), une partie d'un mot ou une phrase à rechercher dans l'objet des messages et/ou dans le champ de l'expéditeur. Tous les messages correspondant exactement aux critères définis 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.

9.7.2. 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

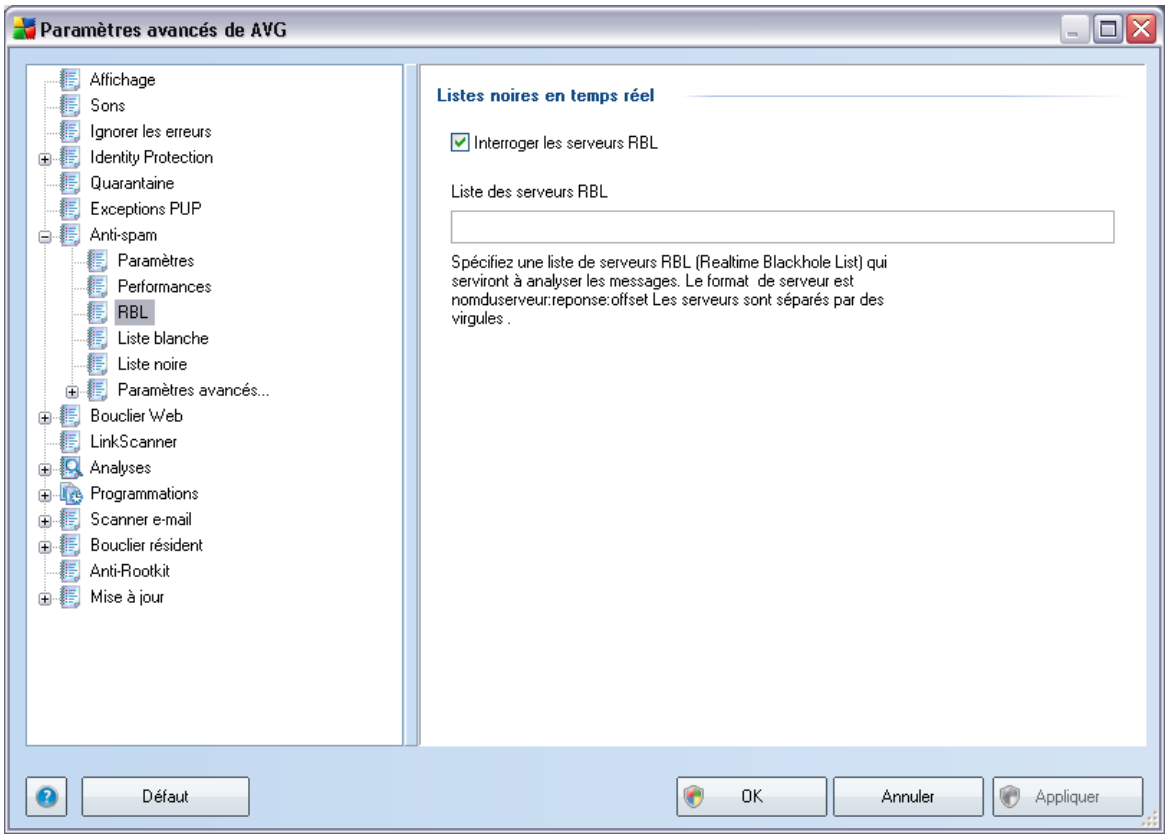
importante. Pendant l'analyse destinée à identifier le spam, les fonctions suivantes seront utilisées : règles et cache de base de données de spam, règles standard et avancées, adresses IP et bases de données de l'expéditeur de spam.

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.

9.7.3. 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.

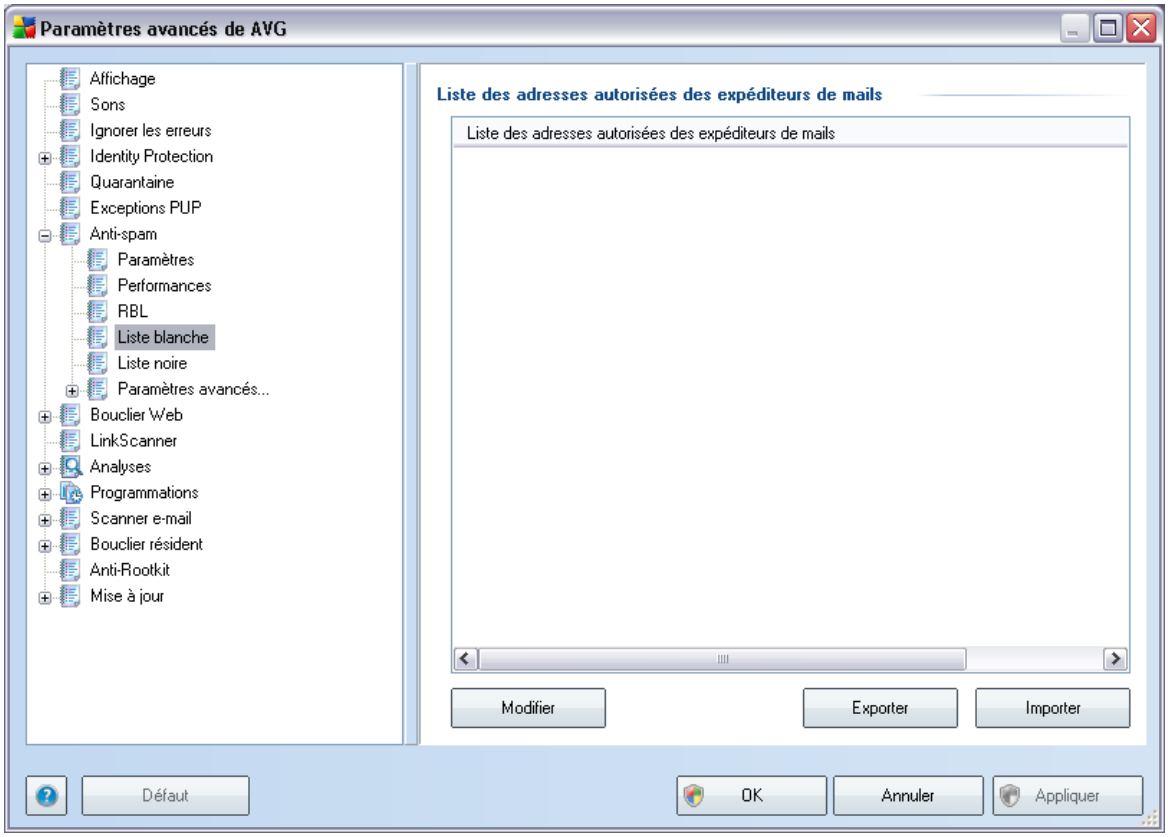
La ***liste des serveurs RBL*** permet de définir les emplacements des serveurs RBL.

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.

9.7.4. Liste blanche

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



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 :

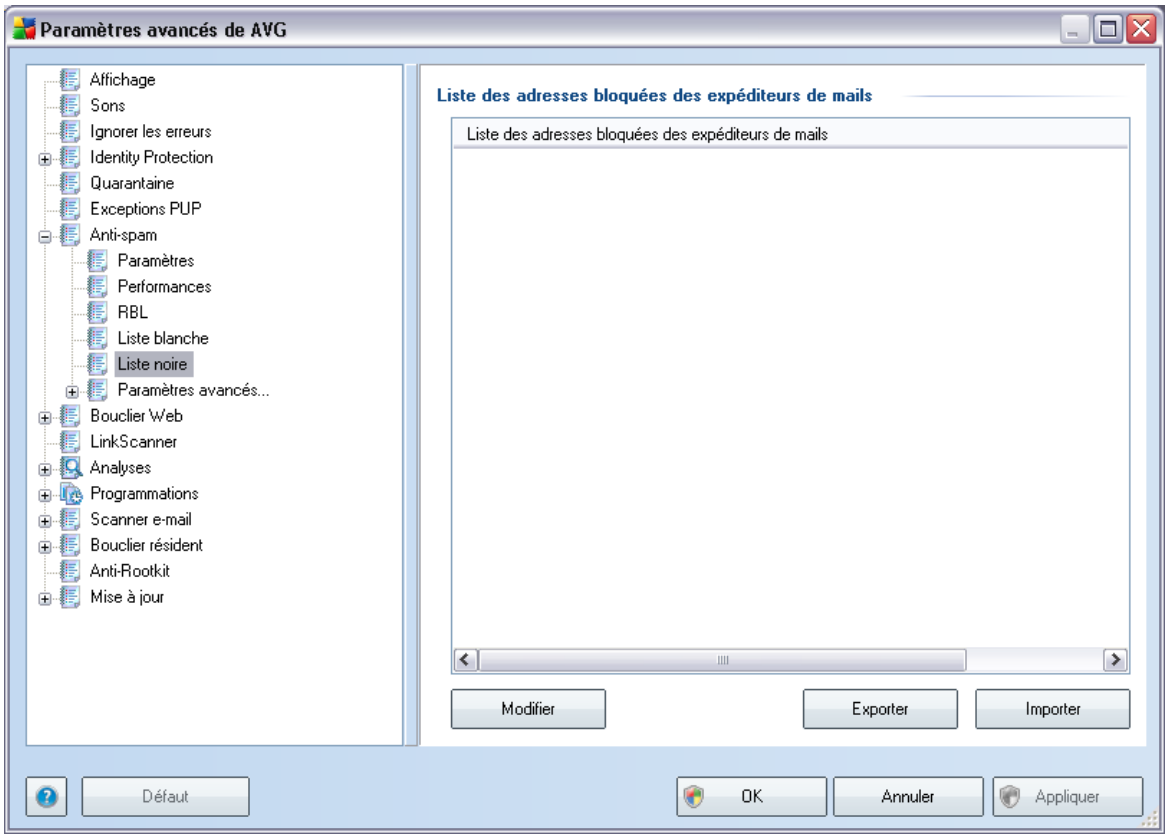
- ***Modifier*** - cliquez sur ce bouton pour ouvrir une boîte de dialogue permettant de définir manuellement une liste d'adresses (*la méthode copier-coller convient également*). Insérez une entrée (*expéditeur, nom de domaine*) par ligne.

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

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

9.7.5. 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 même, vous pouvez dresser une liste de noms de domaines complets (*sociétédespam.com*, par exemple) dont vous avez reçu ou pensez recevoir du courrier indésirable. 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 une entrée (*expéditeur, 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.
- ***Importer*** - si vous avez déjà préparé un fichier texte d'adresses électroniques/de noms de domaines, cliquez simplement sur ce bouton pour l'importer. Ce fichier doit être au format texte brut et contenir une seule entrée (*adresse, nom de domaine*) par ligne.

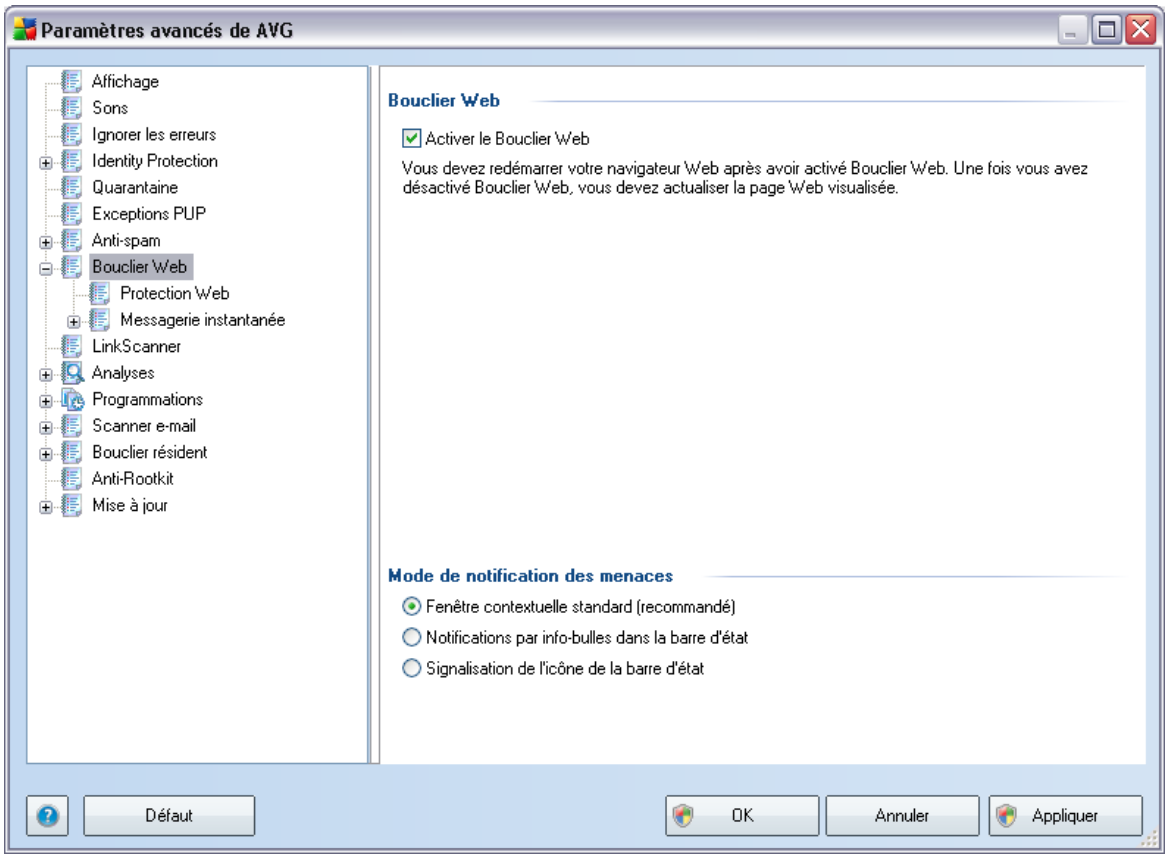
9.7.6. Paramètres avancés

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

9.8. Bouclier Web



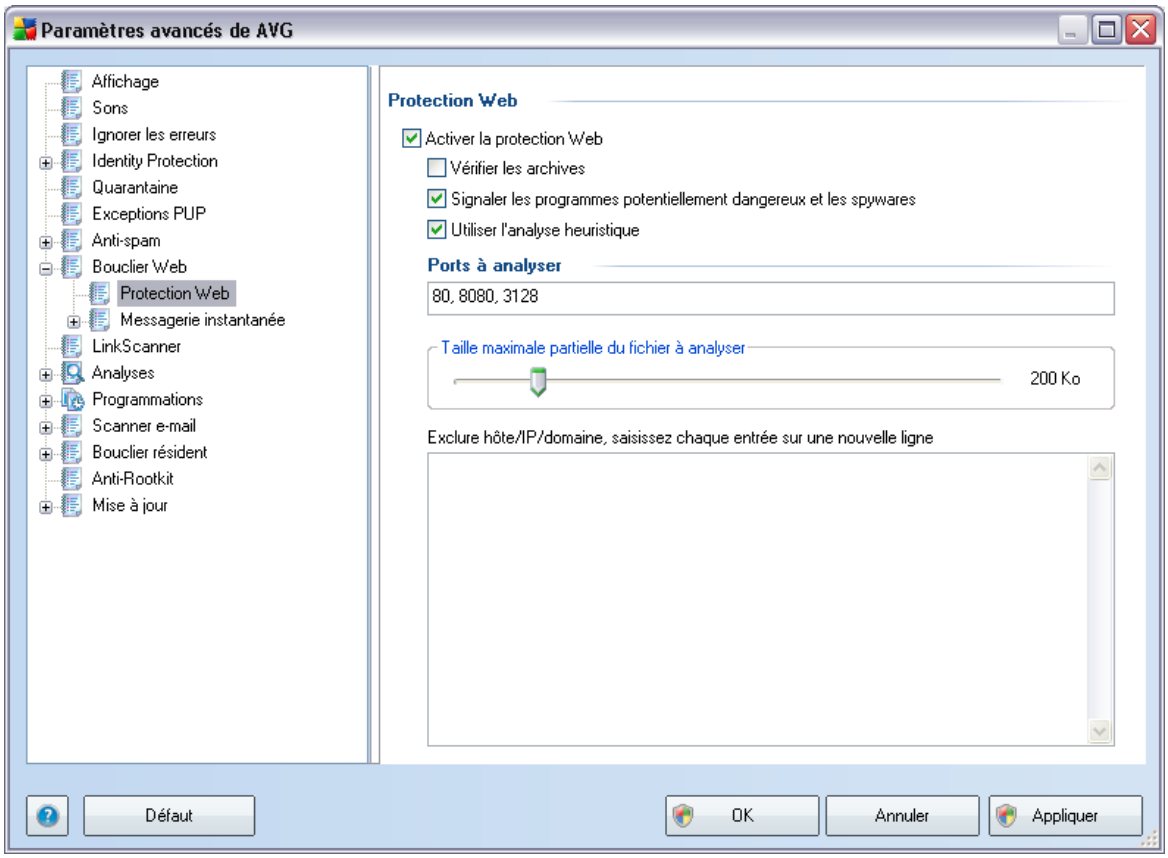
La boîte de dialogue ***Protection Web*** permet d'activer ou de désactiver totalement le composant ***Bouclier Web*** via l'option ***Activer le Bouclier Web*** (*activée par défaut*). Pour accéder aux paramètres avancés de ce composant, utilisez les boîtes de dialogue suivantes, comme indiqué dans l'arborescence de navigation :

- ***Protection Web***
- ***Messagerie instantanée***

Mode de notification des menaces

Au bas de la boîte de dialogue, sélectionnez le mode de notification des menaces détectées : boîte de dialogue contextuelle standard, info-bulle dans la barre d'état ou infos contenues dans l'icône de la barre d'état.

9.8.1. Protection Web



La boîte de dialogue ***Protection Web*** vous permet de modifier à votre convenance la configuration du composant chargé de l'analyse du contenu des sites Web. L'interface d'édition propose plusieurs options de configuration élémentaires, décrites ci-après :

- ***Activer le composant Protection Web*** - cette option confirme que le ***Bouclier Web*** doit analyser le contenu des pages Web. Si elle est activée (*par défaut*), vous pouvez activer/désactiver les options suivantes :
    - ***Vérifier les archives*** - analyse le contenu des archives éventuelles contenues dans la page Web à afficher .
    - ***Signaler les programmes potentiellement dangereux et les spywares*** - recherche les programmes potentiellement dangereux (*des exécutables fonctionnant comme des codes espions ou des spywares*) contenus dans la page Web à afficher et les infections par spywares.

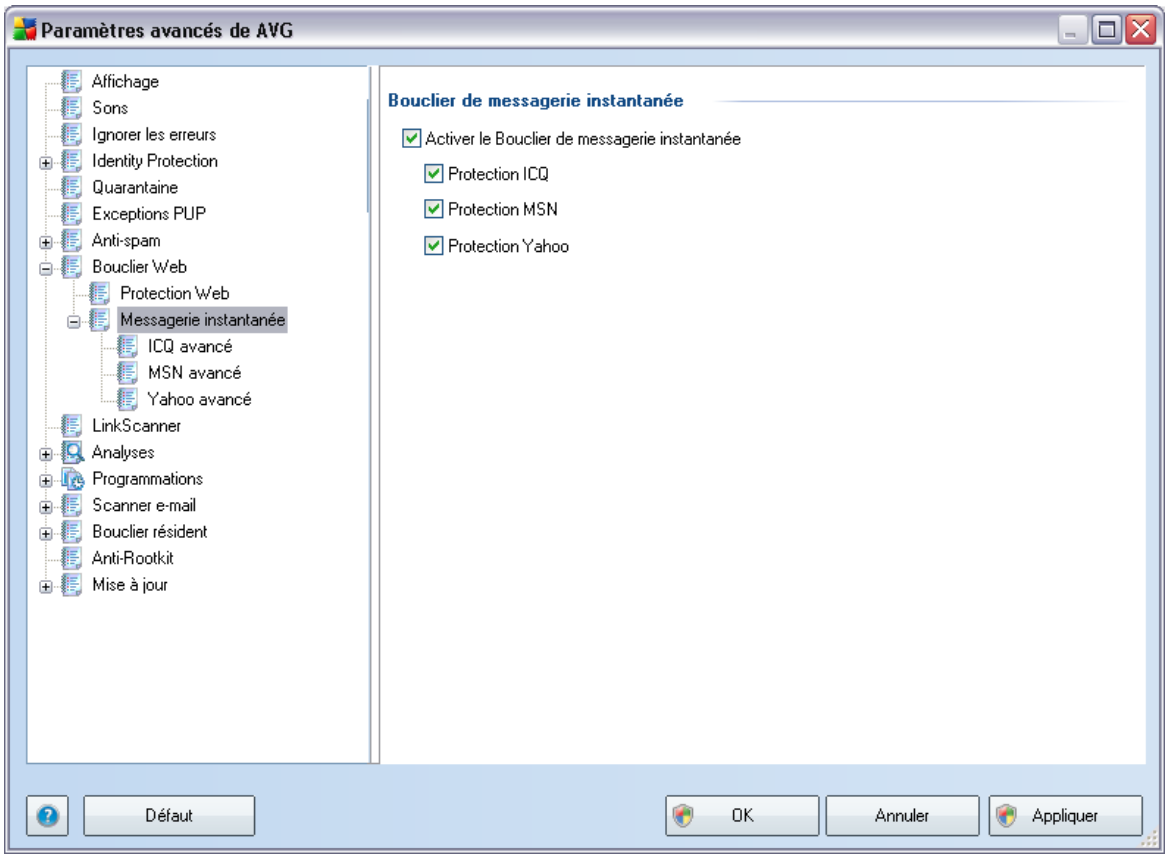
- ***Utiliser l'analyse heuristique*** - analyse le contenu de la page à afficher en appliquant la méthode heuristique (*l'émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*).

- ***Ports à analyser***- ce champ dresse la liste des numéros de port de communication HTTP standard. Si la configuration de votre ordinateur est différente, vous pouvez modifier les numéros de port en conséquence.

- ***Taille maximale des fichiers à analyser*** - si les fichiers inclus figurent dans la page affichée, vous pouvez également analyser leur contenu avant même qu'ils ne soient téléchargés sur votre ordinateur. Notez cependant que l'analyse de fichiers volumineux peut prendre du temps et ralentir considérablement le téléchargement des pages Web. Utilisez le curseur pour fixer la taille de fichier maximale à faire analyser par le ***Bouclier Web***. Même si le fichier téléchargé est plus volumineux que la maximum spécifié et ne peut donc pas être analysé, vous restez protégé : si le fichier est infecté, le ***Bouclier résident*** le détecte immédiatement.

- ***Exclure hôte/IP/domaine*** - dans la zone de texte, saisissez le nom exact d'un serveur (*hôte, adresse IP, adresse IP avec masque ou URL*) ou un domaine qui ne doit pas faire l'objet d'une analyse par le ***Bouclier Web***. En conséquence, n'excluez que les hôtes dont vous pouvez affirmer qu'ils ne fourniront jamais un contenu Web dangereux.

9.8.2. Messagerie instantanée

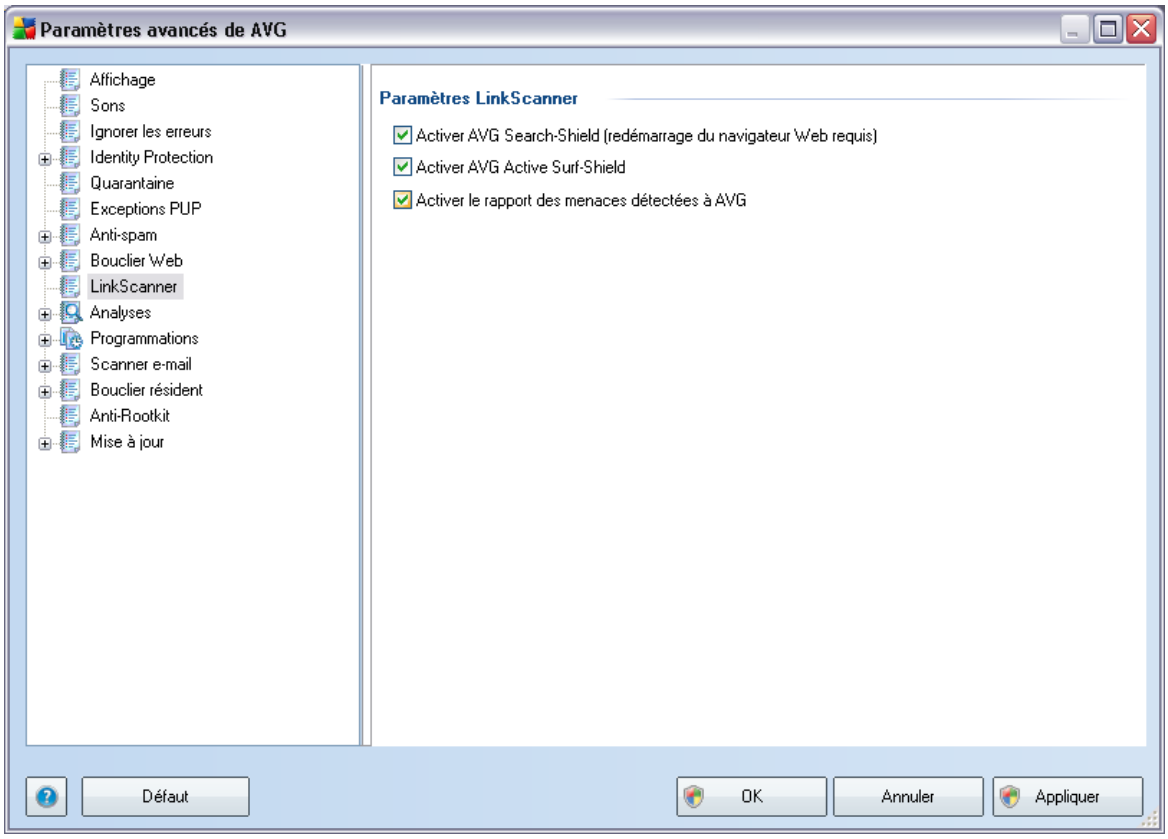


La boîte de dialogue ***Bouclier de messagerie instantanée*** permet de modifier les paramètres du composant ***Bouclier Web*** concernant l'analyse de la messagerie instantanée. Actuellement, seuls trois programmes de messagerie instantanée sont pris en charge : ***ICQ***, ***MSN*** et ***Yahoo*** - cochez les cases correspondant aux communications pour lesquelles le ***Bouclier Web*** doit attester l'absence de virus.

Pour déterminer de manière plus précise les utilisateurs à autoriser et à bloquer, accédez à la boîte de dialogue qui convient (***ICQ avancé***, ***MSN avancé, Yahoo avancé***) et établissez la ***liste blanche*** (*liste des utilisateurs autorisés à communiquer avec vous*) et la ***liste noire*** (*liste des utilisateurs à bloquer*).

9.9. LinkScanner

La boîte de dialogue des ***Paramètres LinkScanner*** permet d'activer ou de désactiver les fonctions essentielles du composant ***LinkScanner*** :



- ***Activer AVG SearchShield*** - (*paramètre activé par défaut*): icônes de notification portant sur les recherches effectuées dans Google, Yahoo, MSN ou Baidu après vérification du contenu des sites renvoyés par ces moteurs de recherche.

- ***Activer AVG Active Surf-Shield*** : *(paramètre activé par défaut)* : protection active (*en temps réel*) contre les sites utilisant des exploits lors de la demande d'accès. Les connexions à des sites malveillants et leur contenu piégé sont bloqués au moment où l'utilisateur demande à y accéder via un navigateur Web (*ou toute autre application qui utilise le protocole HTTP*).

- ***Activer le signalement à AVG des menaces détectées*** - *(paramètre activé par défaut)* : cochez cette case pour permettre le retour d'informations sur les

exploits et les sites frauduleux détectés par les utilisateurs par le biais des fonctions ***Active Surf-Shield*** ou ***AVG Search-Shield***pour enrichir la base de données sur les activités malveillantes qu'on trouve dans le Web.

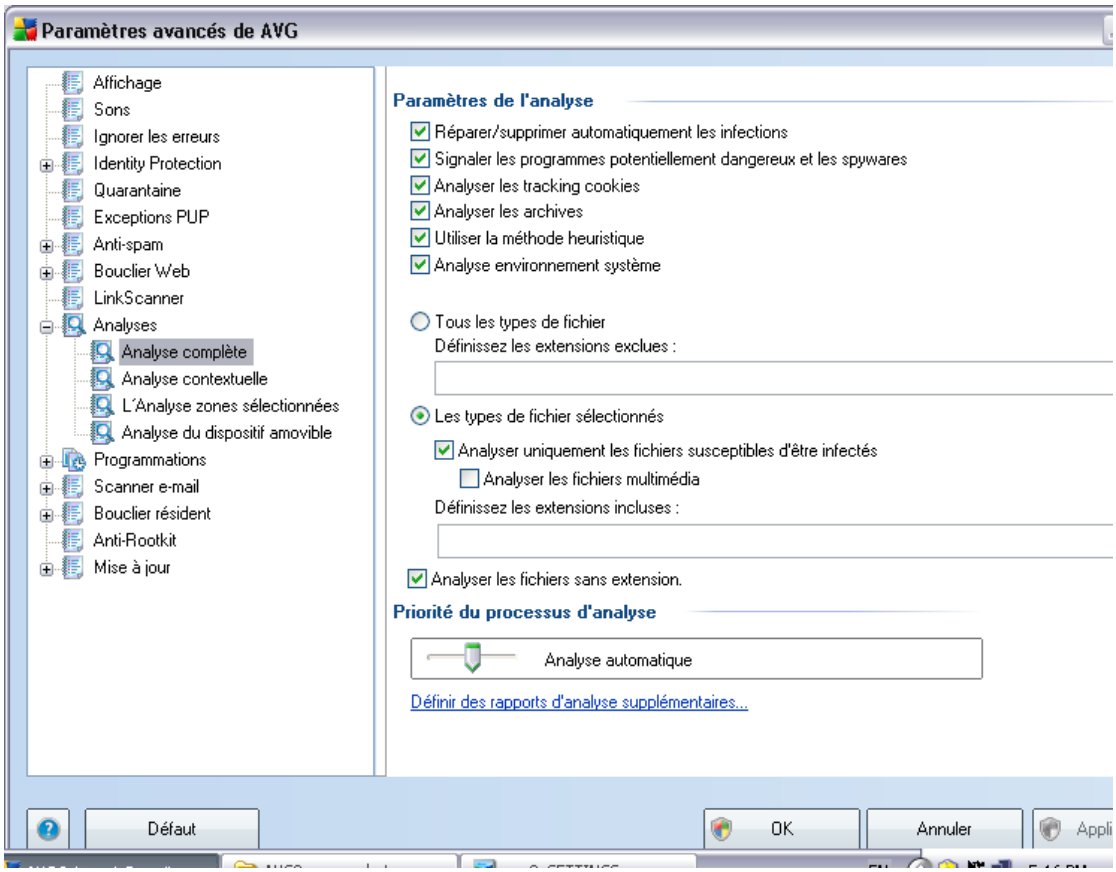
9.10. Analyses

Les paramètres d'analyse avancés sont répartis en trois catégories selon le type d'analyse spécifique tel qu'il a été défini par le fournisseur du logiciel :

- ***Analyse complète*** - analyse standard prédéfinie appliquée à l'ensemble des fichiers contenus dans l'ordinateur
- ***Analyse contextuelle*** : analyse spécifique d'un objet directement sélectionné dans l'environnement de l'Explorateur Windows
- ***Analyse zones sélectionnées*** - analyse standard prédéfinie appliquée aux zones spécifiées de l'ordinateur
- ***Analyse des périphériques amovibles*** : analyse spécifique des périphériques amovibles connectés à votre ordinateur

9.10.1. Analyse complète

L'option ***Analyse complète*** permet de modifier les paramètres d'une analyse prédéfinie par l'éditeur du logiciel, ***Analyse de la totalité de l'ordinateur*** :



Paramètres de l'analyse

La section ***Paramètres de l'analyse*** présente la liste de paramètres d'analyse susceptibles d'être activés ou désactivés :

- ***Réparer/supprimer automatiquement les infections*** –(lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement, si cela est possible. Si la désinfection automatique du fichier n'est pas possible (ou si cette option est désactivée), un message de détection de virus s'affiche. Il vous appartient alors de déterminer le traitement à appliquer à l'infection. La procédure recommandée consiste à confiner le fichier infecté en quarantaine.

- ***Signaler les programmes potentiellement dangereux et les spywares*** - ce paramètre contrôle la fonctionnalité ***Anti-Virus*** qui détecte les programmes potentiellement dangereux (*fichiers exécutables fonctionnant comme des spywares ou des adwares*) et les bloque ou les supprime.

- ***Rechercher les cookies*** – ce paramètre du composant Anti-Spyware indique que les cookies doivent être détectés ; (*les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs telles que leurs sites favoris ou le contenu de leur panier d'achat électronique*).

- ***Analyser les archives*** – ce paramètre indique que l'analyse doit examiner tous les fichiers même ceux stockés dans des archives ZIP, RAR, etc.

- ***Utiliser la méthode heuristique*** - l'analyse heuristique (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*) est l'une des méthodes employées pour détecter des virus pendant l'analyse.

- ***Analyser l'environnement système*** - l'analyse vérifie aussi les fichiers système de l'ordinateur.

Ensuite, vous pouvez choisir d'analyser

- ***Tous les types de fichier*** avec la possibilité de définir les éléments à exclure de l'analyse en dressant une liste d'extensions de fichiers séparées par des virgules et correspondant aux fichiers à exclure de l'analyse ; ou

- ***Types de fichier sélectionnés*** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers média (*vidéo, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.

- Vous pouvez également choisir l'option ***Analyser les fichiers sans extension*** - celle-ci est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.

Priorité du processus d'analyse

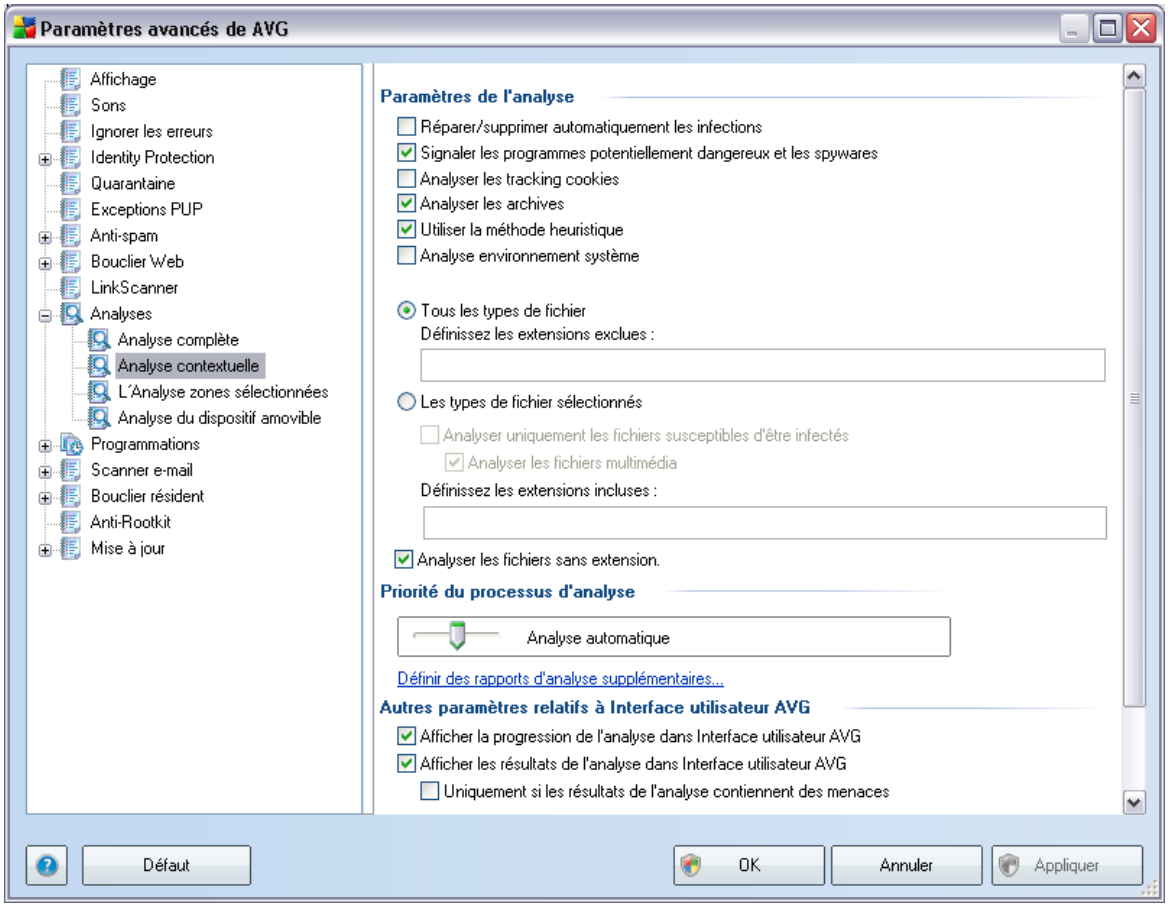
Dans la section ***Priorité du processus d'analyse***, il est possible de régir la durée de l'analyse en fonction des ressources système. Par défaut, cette option est réglée sur le niveau intermédiaire d'utilisation des ressources. Cette configuration permet d'accélérer l'analyse : elle réduit la durée de l'analyse, mais sollicite fortement les ressources système et ralentit considérablement les autres activités de l'ordinateur (*cette option convient lorsque l'ordinateur est allumé, mais que personne n'y travaille*). Inversement, vous pouvez réduire l'utilisation des ressources système en augmentant la durée de l'analyse.

Définir des rapports d'analyse supplémentaires ...

Cliquez sur le lien ***Définir des rapports d'analyse supplémentaires ...*** pour ouvrir la boîte de dialogue ***Rapports d'analyse*** où vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :

9.10.2. Analyse contextuelle

Similaire à l'entrée précédente ***Analyse complète*** , l'entrée ***Analyse contextuelle*** propose plusieurs options permettant d'adapter les analyses prédéfinies par le fournisseur du logiciel. La configuration actuelle s'applique à l'analyse d'objets spécifiques exécutée directement dans l'Explorateur Windows (*extension des menus*), voir le chapitre ***Analyse dans l'Explorateur Windows*** :

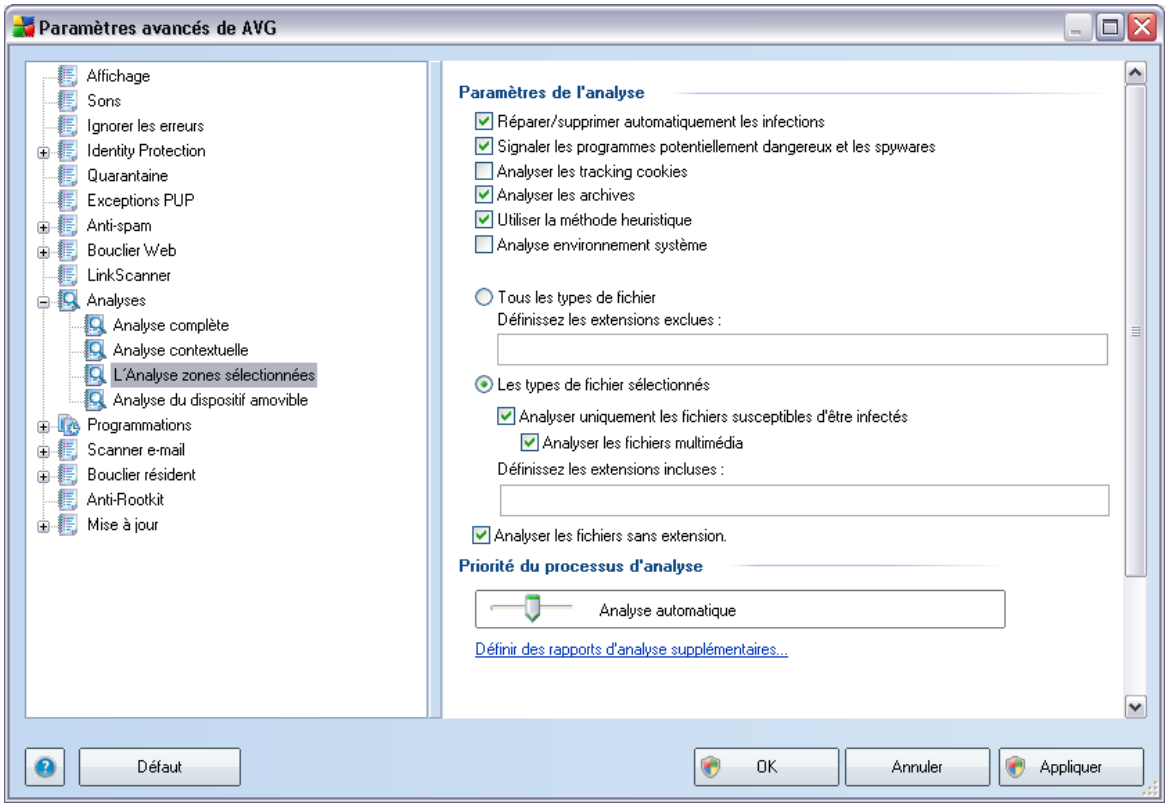


La liste des paramètres correspond à celle proposée pour l'***Analyse complète***. Cependant, la configuration par défaut est différente : dans l'***Analyse complète***, les principaux paramètres sont sélectionnés tandis que pour l'***analyse contextuelle***(***analyse dans l'Explorateur Windows***) seuls les paramètres pertinents sont activés.

Remarque : *Pour obtenir une description des paramètres spécifiques, consultez le chapitre* ***Paramètres avancés d'AVG / Analyses / Analyser tout l'ordinateur****.*

9.10.3. Analyse zones sélectionnées

L'interface d'édition de l'***Analyse zones sélectionnées*** est identique à celle de l' ***Analyse complète***. Les options de configuration sont les mêmes, à ceci près que les paramètres par défaut sont plus stricts pour l'***Analyse complète***.

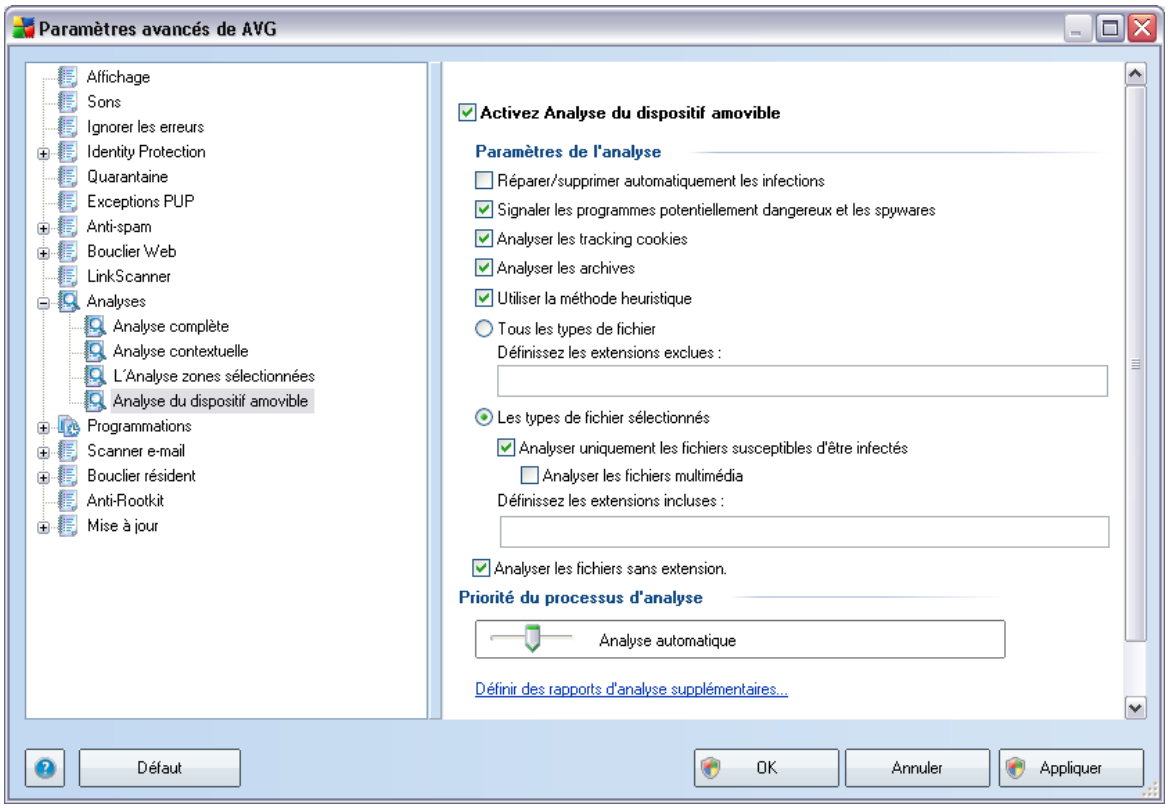


Tous les paramètres définis dans cette boîte de dialogue de configuration s'appliquent uniquement aux zones sélectionnées pour analyse dans l'option ***Analyse zones sélectionnées***! Si vous cochez l'option ***Analyser les rootkits*** dans cette boîte de dialogue de configuration, une recherche rapide de rootkit uniquement sera effectuée (c'est-à-dire la recherche de rootkits dans les zones sélectionnées uniquement).

Remarque : *pour obtenir une description de paramètres spécifiques, reportez-vous au chapitre* ***Paramètres avancés AVG / Analyses / Analyse complète****.*

9.10.4. Analyse du dispositif amovible

En outre, l'interface de configuration de l'***Analyse des périphériques amovibles*** ressemble beaucoup à celle intitulée ***Analyser tout l'ordinateur*** :



L'***Analyse des périphériques amovibles*** est lancée automatiquement chaque fois que vous connectez un périphérique amovible à l'ordinateur. Par défaut, cette fonctionnalité est désactivée. Cependant, il est primordial d'analyser les périphériques amovibles, car ils constituent l'une des sources d'infection majeurs. Pour que cette analyse soit activée et s'effectue automatiquement en cas de besoin, cochez la case ***Activer l'analyse des périphériques amovibles*** .

Remarque : *Pour obtenir une description des paramètres spécifiques, consultez le chapitre* ***Paramètres avancés d'AVG / Analyses / Analyser tout l'ordinateur****.*

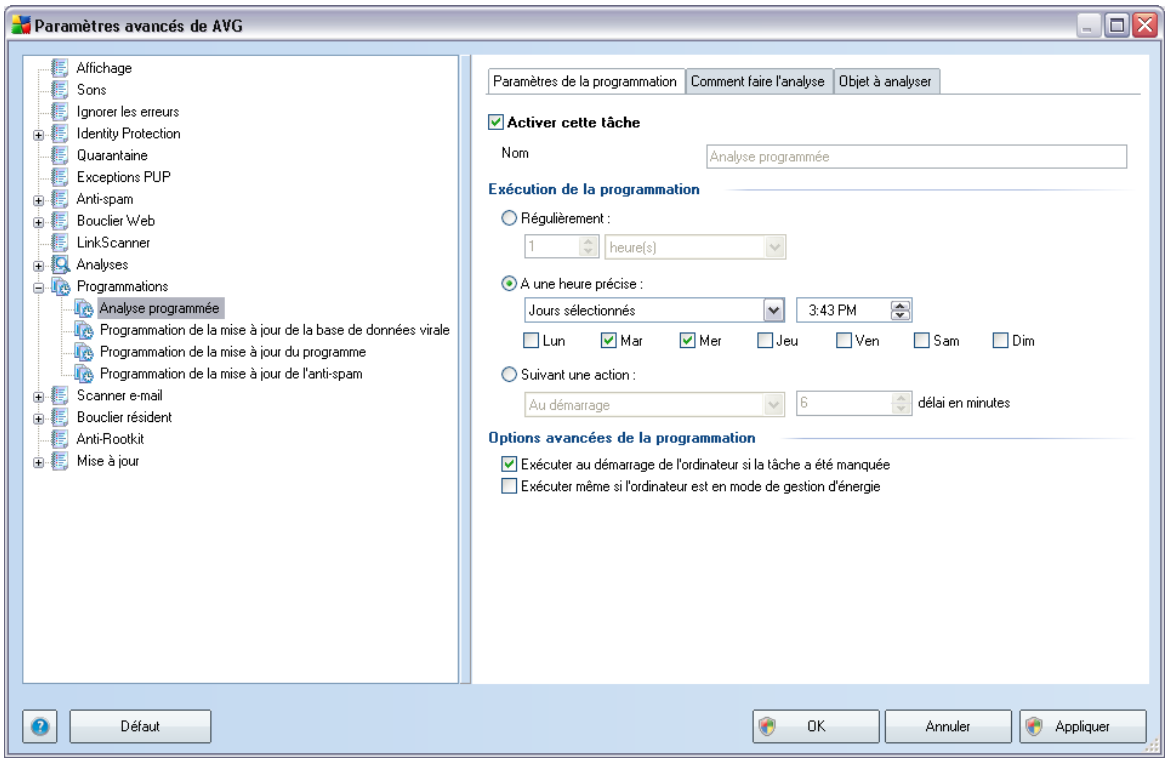
9.11. Programmations

Dans l'entrée ***Programmations***, vous êtes libre de modifier les paramètres par défaut des éléments suivants :

- Programmation de l'analyse complète de l'ordinateur
- Programmation de la mise à jour de la base de données virale
- Programmation de la mise à jour du programme
- Programmation des mises à jour de l'Anti-Spam

9.11.1. Analyse programmée

Les paramètres de l'analyse programmée peuvent être modifiés (*ou une nouvelle analyse peut être programmée*) depuis les trois onglets :



Dans l'onglet ***Paramètres de la programmation***, vous pouvez cocher/décocher la case ***Activer cette tâche*** pour désactiver temporairement l'analyse programmée et le réactiver au moment opportun.

Dans la zone de texte ***Nom*** (*option désactivée pour toutes les programmations par défaut*), le nom est attribué à cette programmation par le fournisseur du programme. Pour les programmations nouvellement ajoutées (*vous pouvez ajouter une nouvelle programmation en cliquant avec le bouton droit de la souris sur l'élément* ***Programmation de l'analyse*** *situé à gauche de l'arborescence de navigation*), vous pouvez spécifier votre propre nom. Dans ce cas, la zone de texte est ouverte et vous pouvez y apporter des modifications. Veillez à utiliser toujours des noms courts, descriptifs et appropriés pour distinguer facilement les différentes analyses par la suite.

Exemple : *il n'est pas judicieux d'appeler l'analyse "Nouvelle analyse" ou "Mon analyse", car ces noms ne font pas référence au champ réel de l'analyse. A l'inverse, "Analyse des zones système" est un nom descriptif précis. Il est également nécessaire de spécifier dans le nom de l'analyse si l'analyse concerne l'ensemble de l'ordinateur ou une sélection de fichiers ou de dossiers. Notez que les analyses personnalisées sont toujours basées sur l'Analyse zones sélectionnés.*

Dans cette boîte de dialogue, vous définissez plus précisément les paramètres de l'analyse :

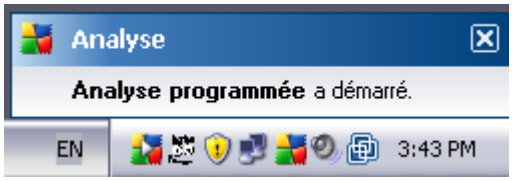
Exécution de la programmation

Ici, spécifiez l'intervalle entre chaque exécution de la nouvelle analyse. La périodicité peut être définie à l'aide d'une répétition lancée à l'issue d'un délai déterminé (***Régulièrement***), à une date et à une heure précises (***Exécuter à un moment précis***) ou encore suivant un événement auquel sera associé le lancement de l'analyse (***Suivant une action***).

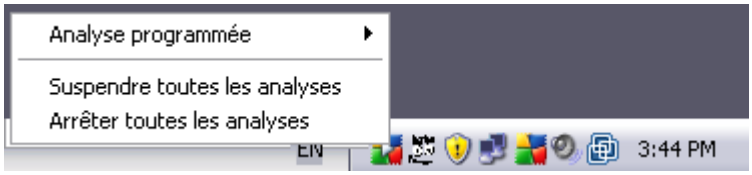
Options avancées de la programmation

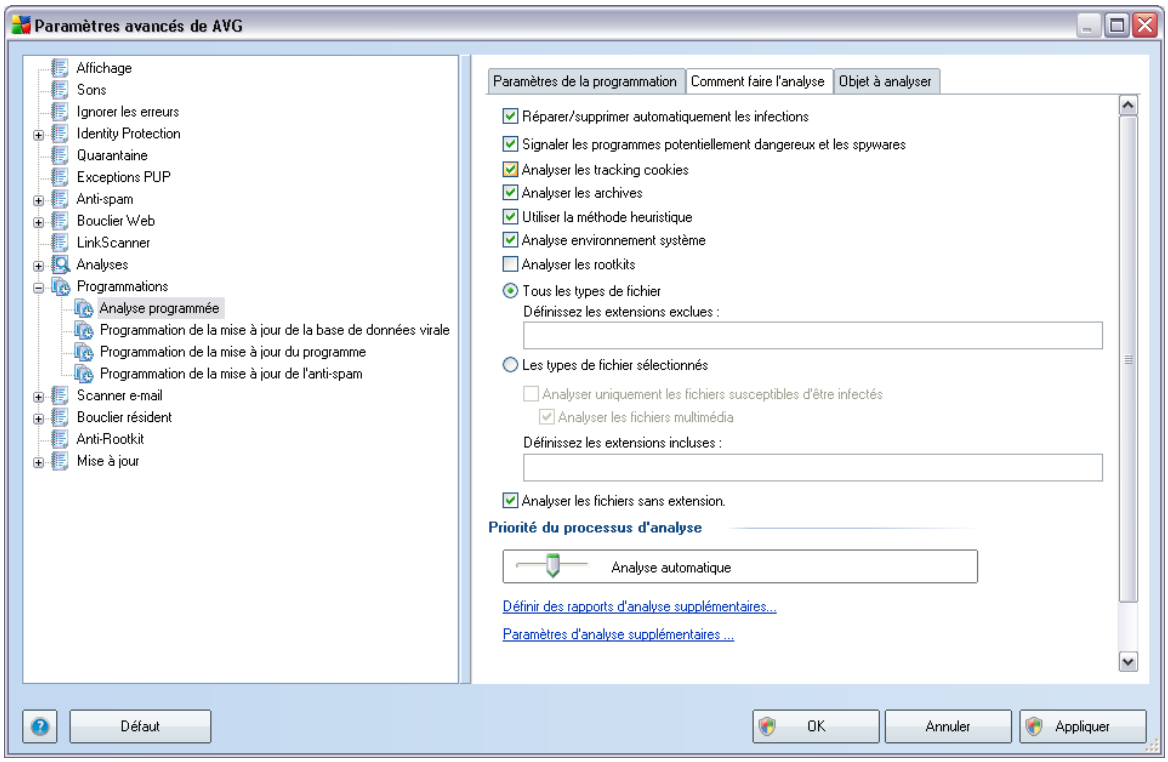
Cette section permet de définir dans quelles conditions l'analyse doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

Lorsque l'analyse programmée est lancée à l'heure spécifiée, une fenêtre vous en informe par le biais d'une fenêtre contextuelle de l'icône dans la barre d'état système AVG :



Une nouvelle icône de la barre d'état système AVG s'affiche alors·(*en couleurs avec une flèche blanche - voir illustration ci-dessus*) et signale qu'une analyse programmée est en cours. Cliquer avec le bouton droit sur l'icône signalant une analyse AVG en cours ouvre un menu contextuel dans lequel vous êtes libre d'interrompre ou même de stopper l'analyse :





Dans l'onglet ***Comment faire l'analyse***, vous trouverez une liste de paramètres d'analyse qui peuvent être activés ou désactivés. Par défaut, la plupart des paramètres sont activés et appliqués lors de l'analyse. Il est vivement conseillé de ne pas modifier la configuration prédéfinie sans motif valable :

- ***Réparer/supprimer automatiquement les infections*** –(*option activée par défaut*) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement si une solution le permet. Si la désinfection automatique du fichier n'est pas possible (ou si cette option est désactivée), un message de détection de virus s'affiche. Il vous appartient alors de déterminer le traitement à appliquer à l'infection. L'action recommandée consiste à confiner le fichier infecté en quarantaine.

- ***Signaler les programmes potentiellement dangereux et les spywares*** - (*option activée par défaut*) : ce paramètre contrôle la fonctionnalité Anti-Virus qui détecte les programmes potentiellement dangereux (*fichiers exécutables fonctionnant comme des spywares ou des adwares*) afin de les bloquer ou de les supprimer.

- ***Analyser les tracking cookies*** - (*option activée par défaut*) : ce paramètre du composant Anti-Spyware indique que les cookies doivent être détectés au cours de l'analyse ; *les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations spécifiques concernant les utilisateurs comme leurs sites préférés ou le contenu de leur panier d'achat électronique*)

- ***Analyser les archives*** – (*option activée par défaut*) : ce paramètre indique que l'analyse doit examiner tous les fichiers même ceux stockés dans des archives (archives ZIP, RAR, par exemple).

- ***Utiliser la méthode heuristique*** – (*option activée par défaut*) : l'analyse heuristique (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*) est l'une des méthodes employées pour détecter des virus pendant l'analyse.

- ***Analyser environnement système*** - (*option activée par défaut*) : l'analyse vérifie les fichiers système de l'ordinateur.

- ***Analyser les rootkits*** – cochez cette option si vous souhaitez inclure la détection de rootkits dans l'analyse complète de l'ordinateur. La détection seule de rootkits est aussi proposée dans le composant ***Anti-Rootkit;***

Ensuite, vous pouvez choisir d'analyser

- ***Tous les types de fichier*** avec la possibilité de définir les éléments à ne pas inclure dans l'analyse en dressant une liste d'extensions de fichiers séparées

par des virgules et exclues de l'analyse ; ou les

- ***Les types de fichier sélectionnés*** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'infection ne sont pas analysés ; il s'agit par exemple de fichiers de texte brut ou de certains types de fichier non exécutables*), y compris les fichiers média (*video, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par des virus.*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.

- Vous pouvez également choisir l'option ***Analyser les fichiers sans extension*** - celle-ci est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.

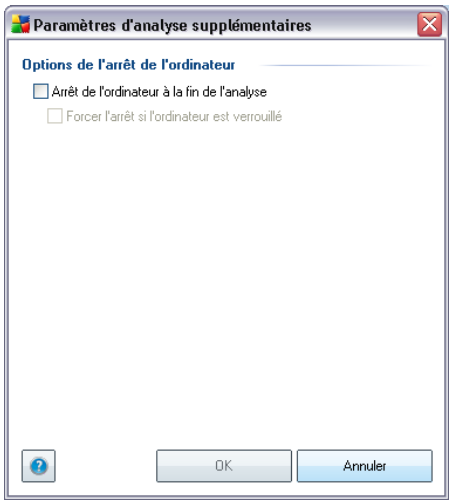
Priorité du processus d'analyse

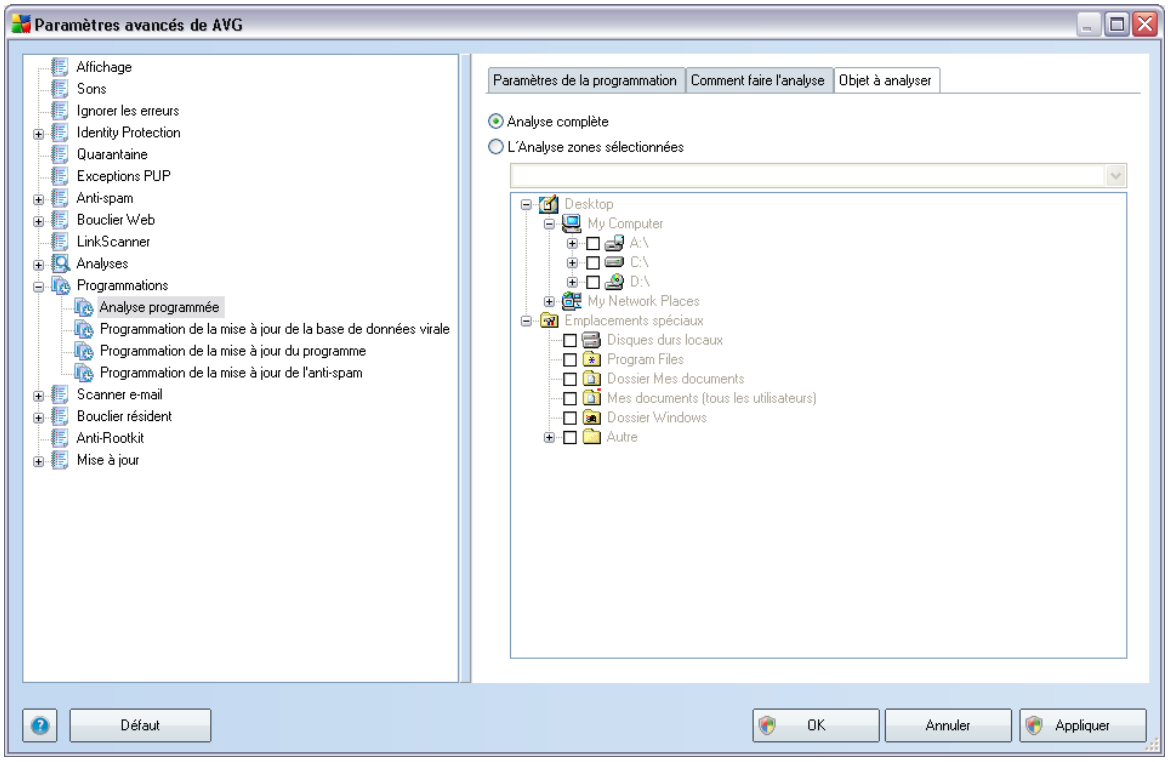
Dans la section ***Priorité du processus d'analyse***, il est possible de régir la durée de l'analyse en fonction des ressources système. Par défaut, cette option est réglée sur le niveau intermédiaire d'utilisation des ressources. Cette configuration permet d'accélérer l'analyse : elle réduit la durée de l'analyse, mais sollicite fortement les ressources système et ralentit considérablement les autres activités de l'ordinateur (*cette option convient lorsque l'ordinateur est allumé, mais que personne n'y travaille*). Inversement, vous pouvez réduire l'utilisation des ressources système en augmentant la durée de l'analyse.

Cliquez sur le lien ***Définir des rapports d'analyse supplémentaires ...*** pour ouvrir la boîte de dialogue ***Rapports d'analyse*** où vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :

Cliquez sur ***Définir des rapports d'analyse supplémentaires...*** pour ouvrir la

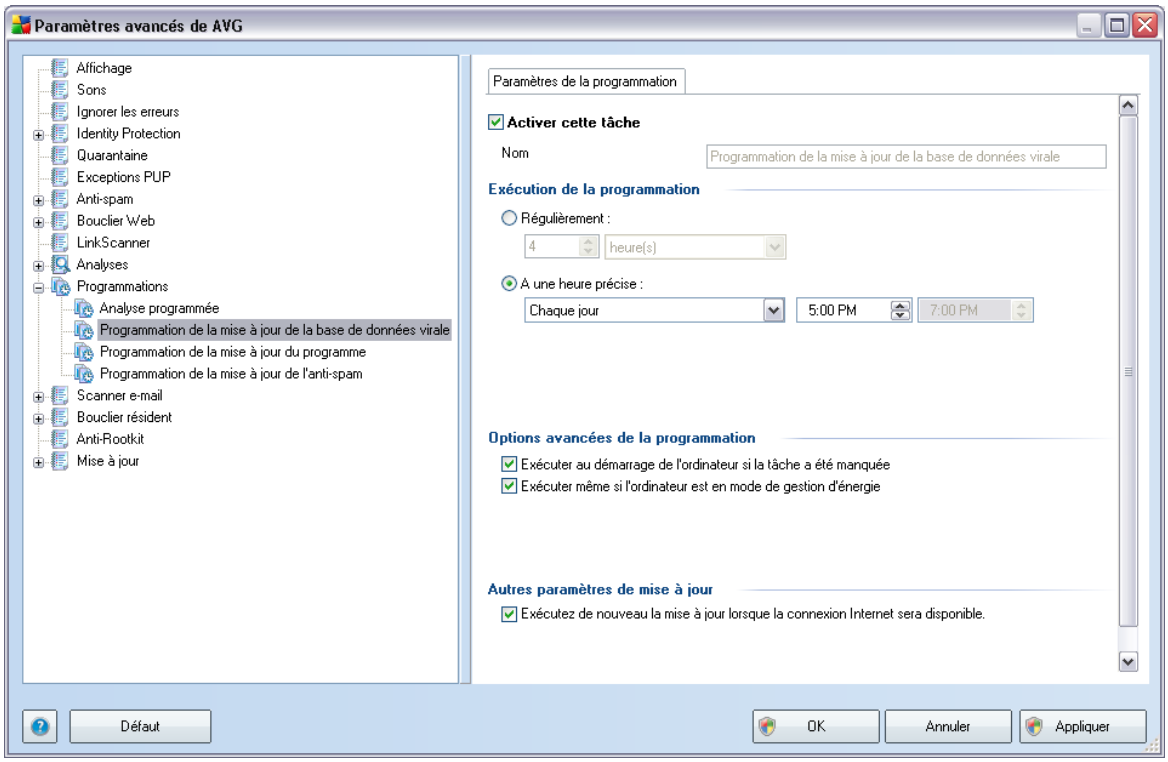
boîte de dialogue ***Options de l'arrêt de l'ordinateur***, où vous indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Une fois l'option ***Arrêt de l'ordinateur à la fin de l'analyse*** confirmée, l'option ***Forcer l'arrêt si l'ordinateur est verrouillé*** s'active et vous permet d'arrêter l'ordinateur même s'il est verrouillé.





Sous l'onglet ***Objet à analyser***, indiquez si vous voulez programmer l'analyse complète ou l'analyse des zones sélectionnées. Si vous optez pour la deuxième solution, la structure de l'arborescence affichée dans la partie inférieure de la boîte de dialogue devient active et permet de définir les dossiers qui vous intéressent.

9.11.2. Programmation de la mise à jour de la base de données virale



Dans l'onglet ***Paramètres de la programmation***, vous pouvez cocher/décocher la case ***Activer cette tâche*** pour désactiver temporairement la mise à jour programmée de la base virale et la réactiver au moment opportun.

La programmation de la mise à jour de la base de données virale est assurée par le composant ***Mise à jour***. La boîte de dialogue correspondante vous permet de définir des paramètres détaillés de la programmation de la mise à jour :

Dans la zone de texte ***Nom*** (*désactivée pour toutes les programmations par défaut*), le nom est attribué à cette même programmation par le fournisseur du programme. Pour les programmations nouvellement ajoutées (*vous pouvez ajouter une nouvelle programmation en cliquant avec le bouton droit de la souris sur l'élément* ***Programmation de la mise à jour de la base de données virale*** *situé à gauche de l'arborescence de navigation*), vous pouvez spécifier votre propre nom. Dans ce cas, la zone de texte est ouverte et vous pouvez y apporter des modifications. Veillez à toujours utiliser des noms courts, descriptifs et appropriés pour distinguer facilement les différentes programmations par la suite.

Exécution de la programmation

Dans cette section, spécifiez la fréquence à laquelle la nouvelle mise à jour programmée de la base de données virale sera lancée. Il est possible de répéter l'exécution de la mise à jour à l'issue d'un délai déterminé (***Régulièrement***), d'une date et d'une heure précises (***A une heure précise***) ou encore d'un évènement auquel sera associé l'exécution de la mise à jour (***Suivant une action***).

Options avancées de la programmation

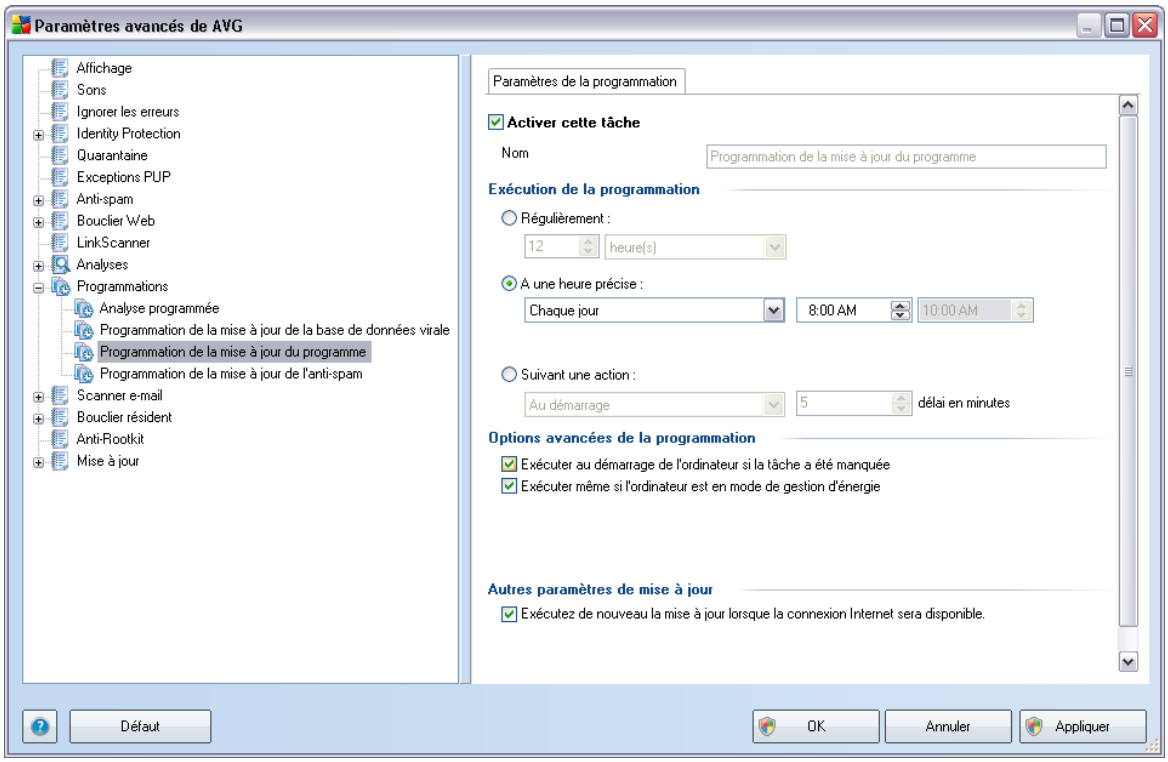
Cette section permet de définir dans quelles conditions la mise à jour de la base de données virale doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

Autres paramètres de mise à jour

Enfin, cochez l'option ***Exécuter de nouveau la mise à jour lorsque la connexion Internet sera disponible*** pour vous assurer qu'en cas d'interruption de la connexion Internet et d'échec de la mise à jour, le processus est relancé dès le rétablissement de la connexion Internet.

Lorsque la mise à jour programmée est lancée à l'heure spécifiée, une fenêtre vous en informe par le biais d'une icône dans la barre d'état système AVG (*à condition que vous ayez conservé la configuration par défaut de la boîte de dialogue* ***Paramètres avancés/Affichage***).

9.11.3. Programmation de la mise à jour du programme



Dans l'onglet ***Paramètres de la programmation***, vous pouvez décocher la case ***Activer cette tâche*** pour désactiver temporairement la mise à jour de l'application programmée et la réactiver au moment opportun.

Dans la zone de texte ***Nom*** (*désactivée pour toutes les programmations par défaut*), le nom est attribué à cette même programmation par le fournisseur du programme. Pour les programmations nouvellement ajoutées (*vous pouvez ajouter une nouvelle programmation en cliquant avec le bouton droit de la souris sur l'élément* ***Programmation de la mise à jour de l'application*** *situé à gauche de l'arborescence de navigation*), vous pouvez spécifier votre propre nom. Dans ce cas, la zone de texte est ouverte et vous pouvez y apporter des modifications. Veillez à toujours utiliser des noms courts, descriptifs et appropriés pour distinguer facilement les différentes programmations par la suite.

Exécution de la programmation

Ici, spécifiez l'intervalle entre chaque exécution de la mise à jour de l'application

programmée. La périodicité peut être définie à l'aide d'une répétition lancée à l'issue d'un délai déterminé (***Régulièrement***), à une date et à une heure précises (***A une heure précise***) ou encore suivant un événement auquel sera associé le lancement de la mise à jour (***Suivant une action***).

Options avancées de la programmation

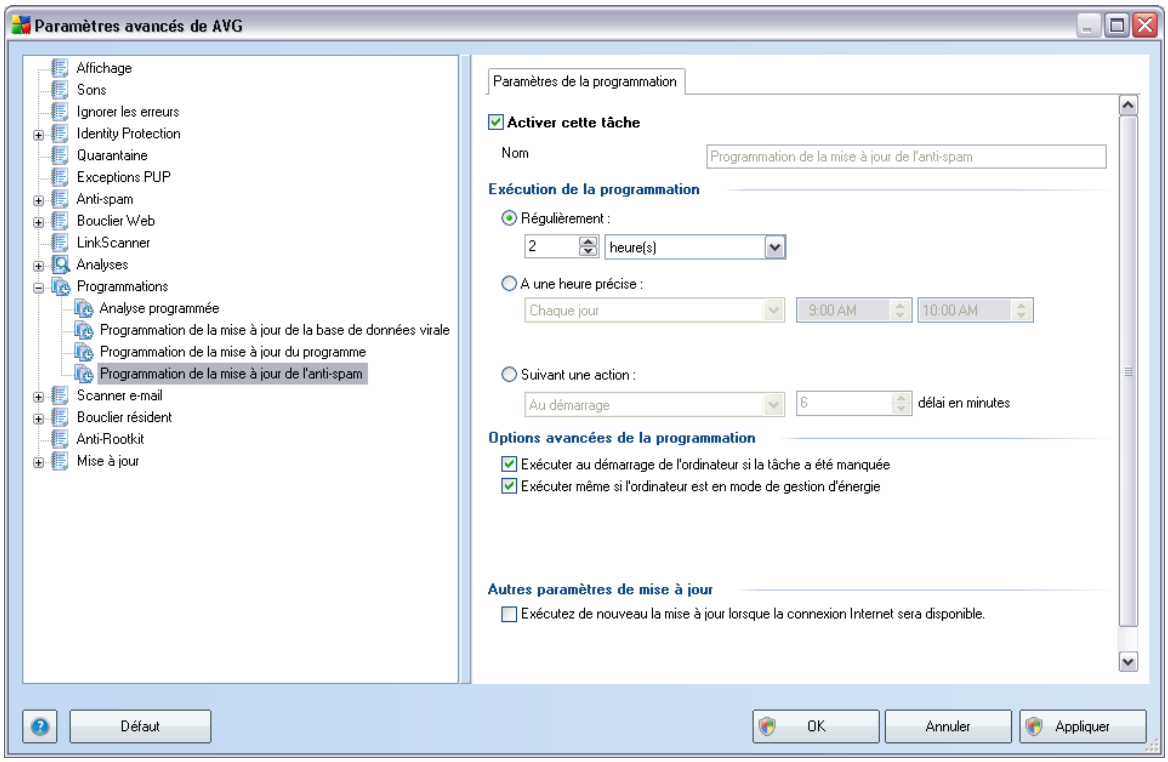
Cette section permet de définir dans quelles conditions la mise à jour de l'application doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

Autres paramètres de mise à jour

Cochez l'option ***Exécuter de nouveau la mise à jour lorsque la connexion Internet sera disponible*** pour vous assurer qu'en cas d'interruption de la connexion Internet et d'échec de la mise à jour, le processus est relancé dès le rétablissement de la connexion Internet.

Lorsque la mise à jour programmée est lancée à l'heure spécifiée, une fenêtre vous en informe par le biais d'une icône dans la barre d'état système AVG (*à condition que vous ayez conservé la configuration par défaut de la boîte de dialogue* ***Paramètres avancés/Affichage***).

9.11.4. Programmation de la mise à jour de l'anti-spam



Dans l'onglet ***Paramètres de la programmation***, vous pouvez cocher/décocher la case ***Activer cette tâche*** pour désactiver temporairement la ***mise à jour programmée de l'***Anti-Spam et la réactiver au moment opportun.

La programmation de la mise à jour de l'***Anti-Spam*** est prise en charge par le composant ***Mise à jour***. Dans la boîte de dialogue correspondante, vous spécifiez en détail le programme de mise à jour :

Dans la zone de texte ***Nom*** (*désactivée pour toutes les programmations par défaut*), le nom est attribué à cette programmation par le fournisseur du programme. Pour les programmations nouvellement ajoutées (*vous pouvez ajouter une nouvelle programmation en cliquant avec le bouton droit de la souris sur l'élément* ***Programmation de la mise à jour de l'Anti-Spam*** *situé à gauche de l'arborescence de navigation*), vous pouvez spécifier votre propre nom. Dans ce cas, la zone de texte est ouverte et vous pouvez y apporter des modifications. Veillez à toujours utiliser des noms courts, descriptifs et appropriés pour distinguer facilement les différentes programmations par la suite.

Exécution de la programmation

Ici, spécifiez la fréquence de mise à jour du composant ***Anti-Spam*** . La périodicité peut être définie à l'aide d'une répétition selon un délai déterminé (***Régulièrement*****),** ***à une date et à une heure précises (***A une heure précise***) ou encore suivant un événement auquel sera associé le lancement de la mise à jour (***Suivant une action).

Options avancées de la programmation

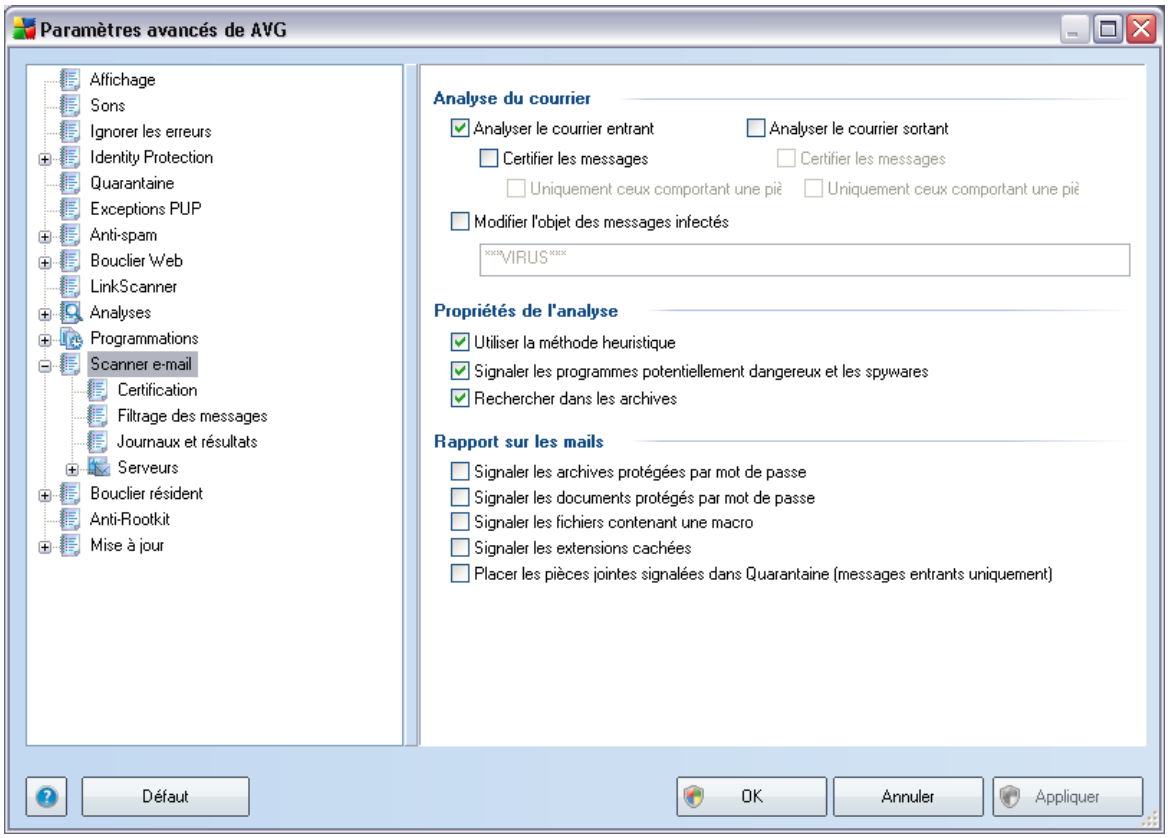
Cette section permet de définir dans quelles conditions la mise à jour ***anti-spam*** doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

Autres paramètres de mise à jour

Cochez l'option ***Exécuter de nouveau la mise à jour lorsque la connexion Internet sera disponible*** pour vous assurer qu'en cas d'interruption de la connexion Internet et d'échec de la mise à jour d'***Anti-Spam*** , le processus est relancé dès le rétablissement de la connexion Internet.

Lorsque l'analyse programmée est exécutée à l'heure spécifiée, une fenêtre vous en informe par le biais d'une icône dans la barre d'état système AVG (*à condition que vous ayez conservé la configuration par défaut de la boîte de dialogue* ***Paramètres avancés/Affichage***).

9.12. Scanner e-mail



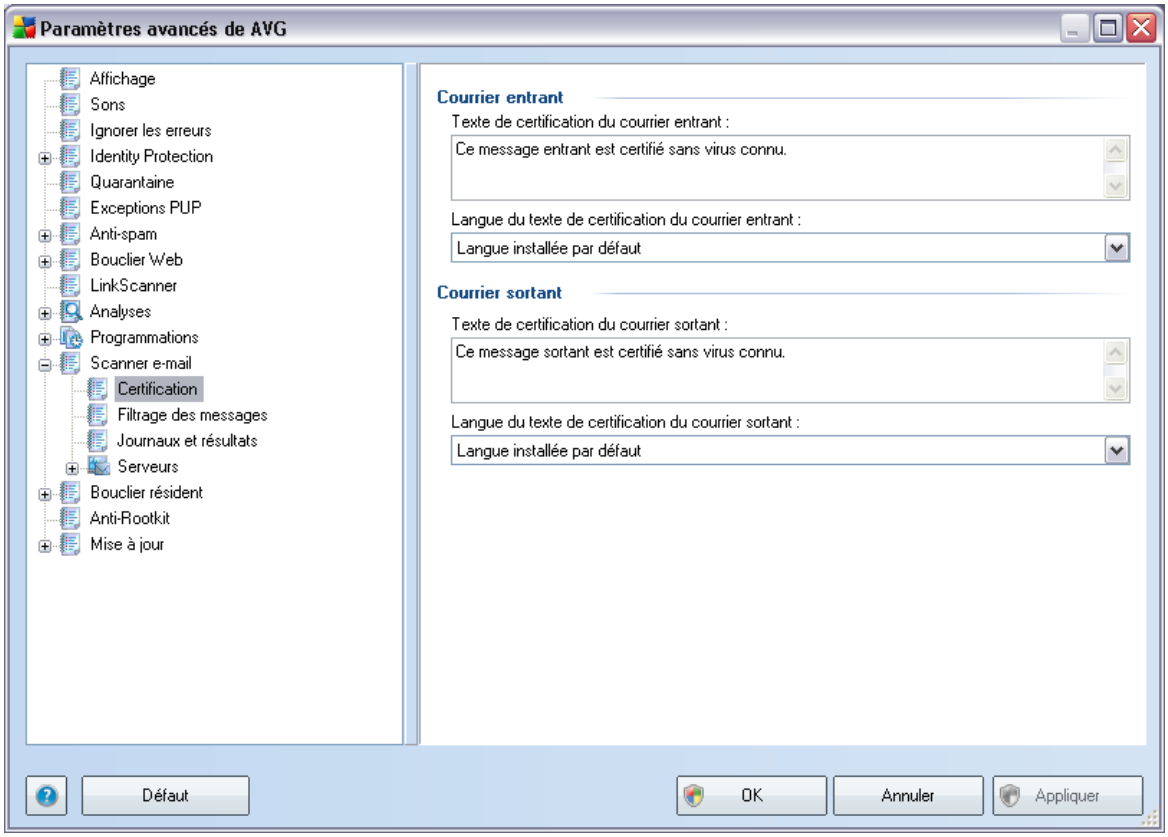
La boîte de dialogue ***Scanner e-mail*** est divisée en trois parties :

- ***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***).

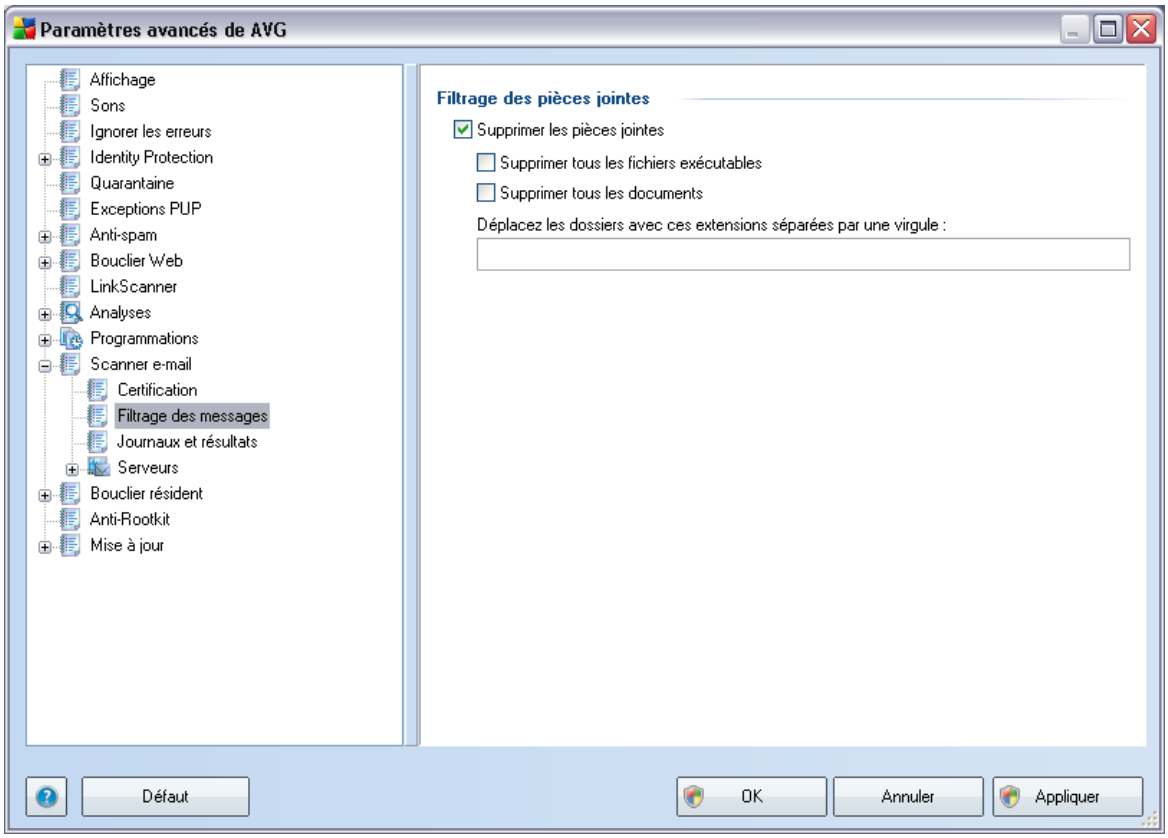
- ***Rapport sur les pièces jointes***- indiquez si vous voulez être averti par e-mail lorsque l'analyse d'un e-mail révèle la présence d'une archive protégée par mot de passe,d'un document protégé par mot de passe, d'une macro contenant un fichier et/ou d'un fichier dont l'extension est masquée. En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

9.12.1. 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***.

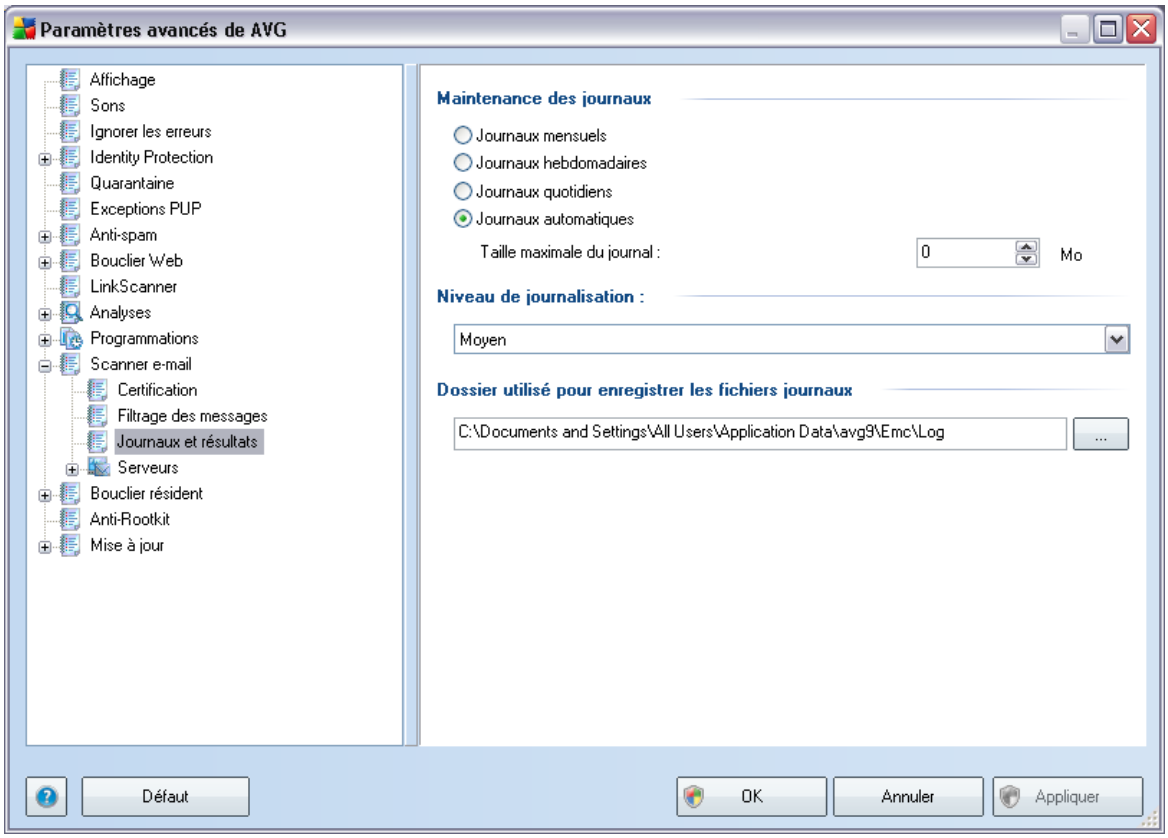
9.12.2. Filtrage des messages



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

9.12.3. Journaux et résultats

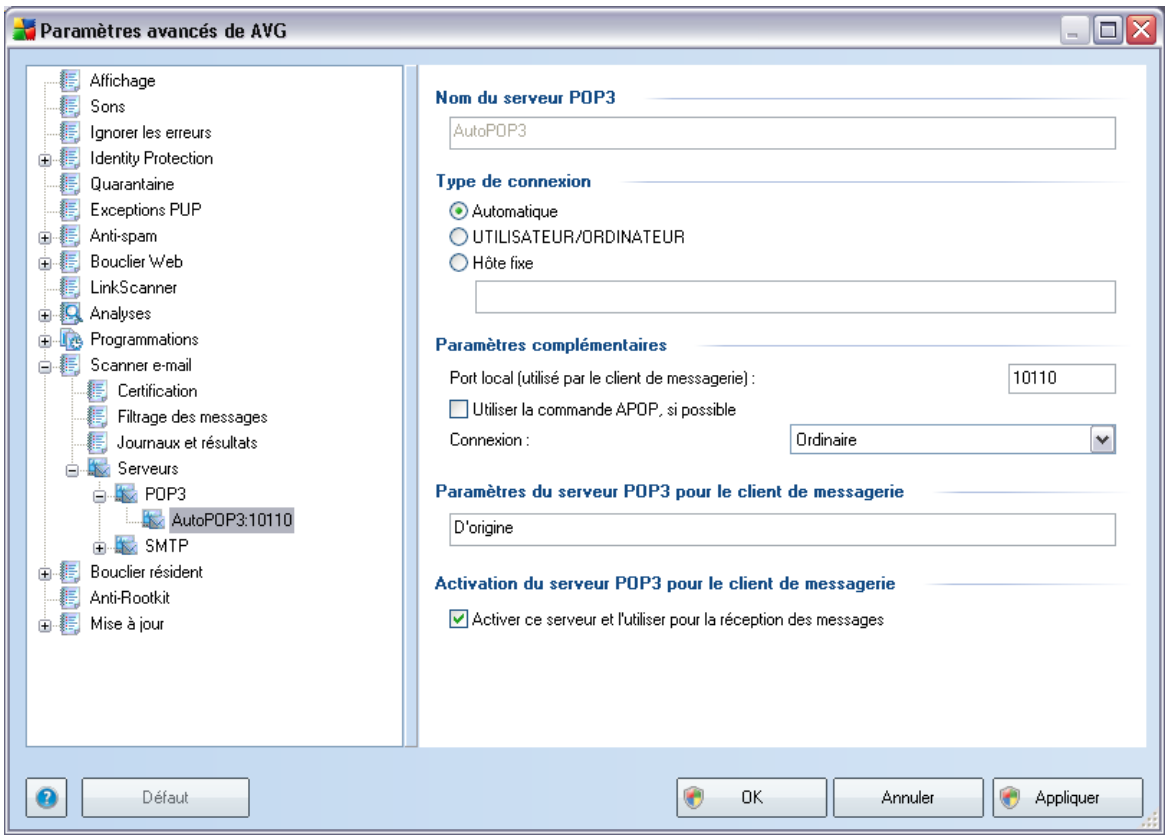


La boîte de dialogue ouverte à l'aide de l'élément de navigation ***Journaux et résultats*** permet de spécifier les paramètres de la maintenance des résultats de l'analyse. La boîte de dialogue comprend plusieurs sections :

- ***Maintenance des journaux*** - vous permet de définir si les informations sur l'analyse des messages doivent être consignées quotidiennement, hebdomadairement, mensuellement ou autrement, et de fixer la taille maximale du fichier journal (*en Mo*)
- ***Niveau de journalisation*** - par défaut, le niveau moyen - vous pouvez sélectionner un niveau inférieur (*enregistrement des informations de base sur la connexion*) ou supérieur (*enregistrement de l'ensemble du trafic*)
- ***Dossier utilisé pour enregistrer les fichiers journaux*** - définit l'emplacement des fichiers journaux

9.12.4. Serveurs

Dans la section ***Serveurs*** , vous pouvez éditer les paramètres de serveur pour le composant ***E-mail Scanner***, ou configurer un nouveau serveur à l'aide du bouton ***Ajouter un nouveau serveur***.



Dans cette boîte de dialogue (accessible depuis la commande ***Serveurs / POP3***), vous configurez un nouveau serveur ***Scanner e-mail*** à l'aide du protocole POP3 pour les messages entrants :

- ***Nom du serveur POP3*** - saisissez le nom du serveur ou conservez le nom par défaut, AutoPOP3
- ***Type de connexion*** - définissez la méthode de sélection du serveur de messagerie pour les mails entrants.

- ***Automatique*** - la connexion est établie automatiquement selon les paramètres du client de messagerie.

- ***UTILISATEUR/ORDINATEUR*** - la méthode proxy est la méthode la plus simple et la plus couramment utilisée pour déterminer le serveur de messagerie de destination. Pour appliquer cette méthode, spécifiez le nom ou l'adresse (et le port, éventuellement) en tant que nom de connexion au serveur considéré, en séparant ces éléments par une barre oblique (/). Par exemple, pour le compte utilisateur1 sur le serveur pop. acme.com et le port 8200, le nom de connexion serait utilisateur1/pop. acme.com:8200.

- ***Hôte fixe*** - Dans ce cas, le programme utilise toujours le serveur spécifié dans ce champ. Veuillez indiquer l'adresse ou le nom de votre serveur de messagerie. Le nom de connexion reste inchangé. Pour le nom, vous pouvez utiliser un nom de domaine (pop.acme.com, par exemple) ainsi qu'une adresse IP (123.45.67.89, par exemple). Si le serveur de messagerie fait appel à un port non standard, il est possible de spécifier ce port à la suite du nom du serveur en séparant ces éléments par le signe deux-points (pop.acme.com:8200, par exemple). Le port standard des communications POP3 est le port 110.

- ***Paramètres complémentaires*** - se rapporte à des paramètres plus détaillés :

  - ***Port local*** - indique le port sur lequel transitent les communications provenant de l'application de messagerie. Dans votre programme de messagerie, vous devez alors indiquer que ce port fait office de port de communication POP3.

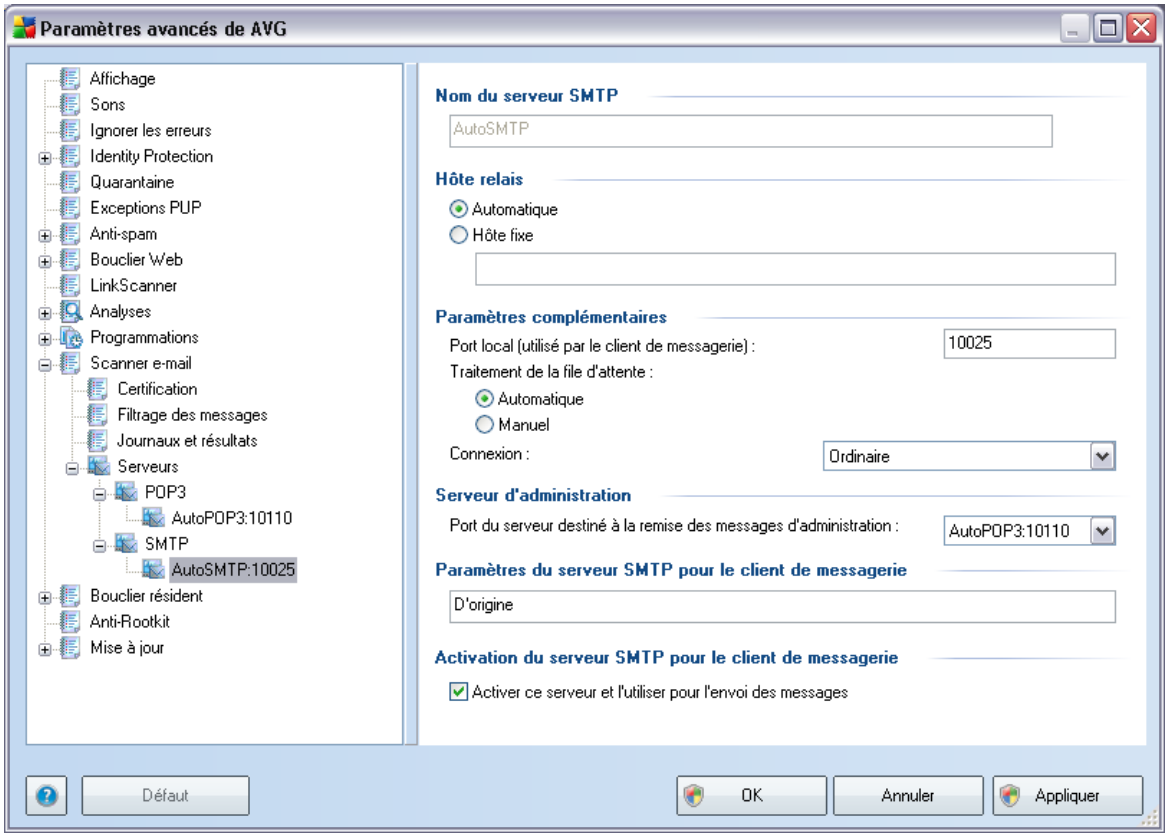
  - ***Utiliser la commande APOP, si possible*** - cette option fournit une connexion serveur plus sécurisée. Cette indication garantit que le ***Scanner e-mail*** utilisera une autre méthode pour transférer le mot de passe du compte utilisateur de connexion. Le mot de passe sera transmis au serveur, mais dans un format non ouvert et crypté à l'aide d'une chaîne de variables envoyée par le serveur lui-même. Cette fonction n'est évidemment disponible que si elle est prise en charge par le serveur de messagerie de destination.

  - ***Connexion*** - dans la liste déroulante, vous pouvez spécifier le type de connexion à utiliser (Ordinaire/SSL/SSL par défaut). Si vous optez pour une connexion SSL, les données sont envoyées sous forme cryptée, sans risquer d'être analysées ou contrôlées par une tierce partie. Cette fonction également n'est disponible que si elle est prise en charge par le

serveur de messagerie de destination.

- ***Activation du serveur POP3 pour le client de messagerie*** - fournit des précisions sur les paramètres nécessaires à la bonne configuration de votre client de messagerie (notamment pour permettre au ***Scanner e-mail*** de vérifier les mails entrants). Ce résumé est établi en fonction des paramètres spécifiés dans cette boîte de dialogue et les boîtes de dialogue connexes.

- ***Activation du serveur POP3 pour le client de messagerie*** - cochez/décochez cette case pour activer ou désactiver le serveur POP3 spécifié



Dans cette boîte de dialogue (accessible depuis la commande ***Serveurs / SMTP***), vous configurez un nouveau serveur ***Scanner e-mail*** à l'aide du protocole SMTP pour les messages sortants :

- ***Nom du serveur SMTP*** - saisissez le nom du serveur ou conservez le nom

par défaut AutoSMTP

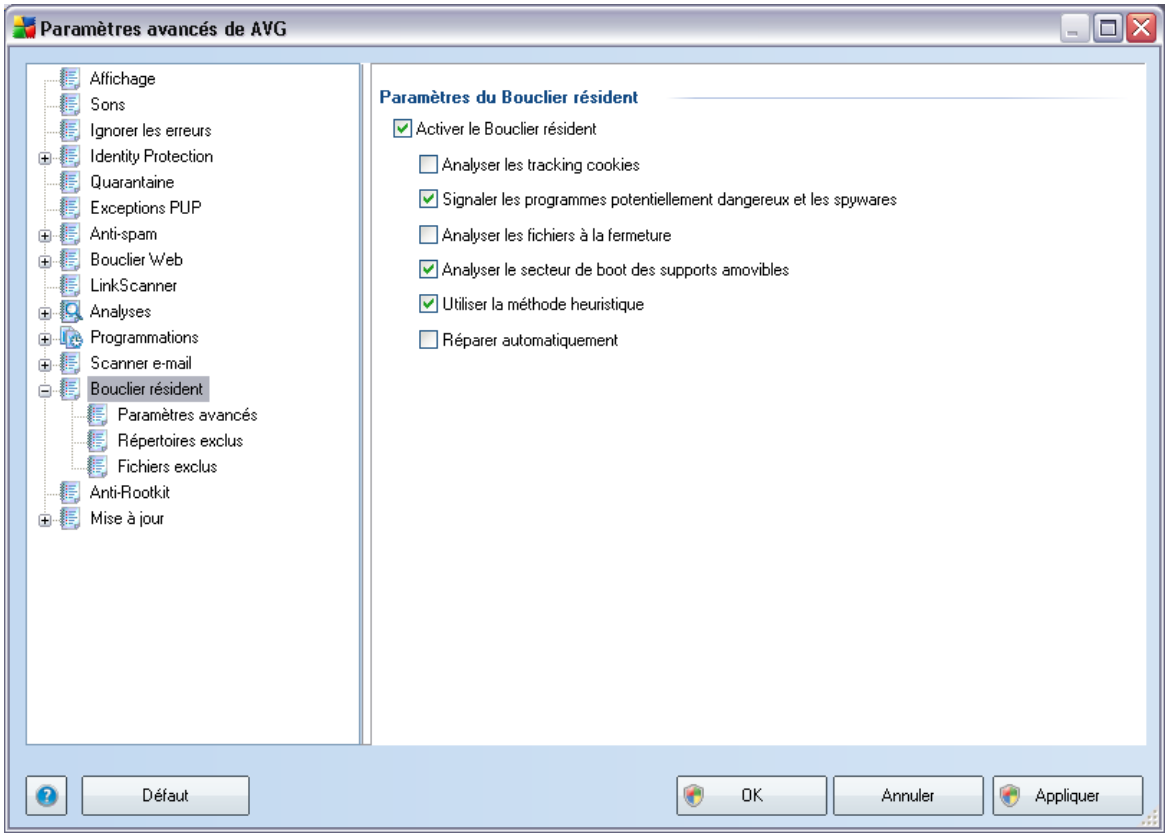
- ***Hôte relais*** - définit la méthode de sélection du serveur de messagerie délivrant le courrier sortant :
    - ***Automatique*** - la connexion est établie automatiquement selon les paramètres du client de messagerie
    - ***Hôte fixe*** - dans ce cas, le programme utilise toujours le serveur spécifié dans ce champ. Veuillez indiquer l'adresse ou le nom du serveur de messagerie. En guise de nom, vous pouvez utiliser un nom de domaine (smtp.acme.com, par exemple) ainsi qu'une adresse IP (123.45.67.89, par exemple). Si le serveur de messagerie fait appel à un port non standard, il est possible de saisir ce port à la suite du nom du serveur en séparant ces éléments par le signe deux-points (smtp.acme.com:8200, par exemple). Le port standard des communications SMTP est le port 25.
- ***Paramètres complémentaires*** - spécifie des paramètres plus détaillés :
    - ***Port local*** - indique le port sur lequel transitent les communications provenant de l'application de messagerie. Dans votre programme de messagerie, vous devez alors indiquer que ce port fait office de port de communication SMTP.
    - ***Traitement de la file d'attente*** - détermine le comportement du ***Scanner e-mail*** lorsqu'il gère les instructions d'envoi de messages.
        - Automatique - le message sortant est livré (envoyé) immédiatement au serveur de messagerie cible
        - Manuel - le message est inséré dans la file d'attente de messages sortants et envoyé ultérieurement
    - ***Connexion*** - dans la liste déroulante, vous pouvez spécifier le type de connexion à utiliser (Ordinaire/SSL/SSL par défaut). Si vous optez pour une connexion SSL, les données sont envoyées sous forme cryptée, sans risque d'être contrôlées ou surveillées par une tierce partie. Cette fonction n'est disponible que si elle est prise en charge par le serveur de messagerie de destination.
- ***Serveur d'administration*** - désigne le numéro du port du serveur utilisé pour la remise (par retour) de rapports d'administration. Ce type de rapport est généré, par exemple, si le serveur de messagerie cible n'est pas disponible

ou s'il rejette le message sortant.

- ***Paramètres du serveur SMTP*** - fournit des informations sur la façon de configurer le client de messagerie afin que les mails sortants soient vérifiés en fonction des paramètres de vérification modifiés du serveur. Ce résumé est établi en fonction des paramètres spécifiés dans cette boîte de dialogue et les boîtes de dialogue connexes.

9.13. Bouclier résident

Le composant ***Bouclier résident*** protège directement les fichiers et les dossiers contre les virus, les spywares et autres codes malicieux.



La boîte de dialogue ***Paramètres du Bouclier résident*** permet d'activer ou de désactiver la protection offerte par le ***Bouclier résident*** en sélectionnant ou en désélectionnant la case ***Activer le Bouclier résident*** (*option activée par défaut*). Vous pouvez aussi préciser les fonctions du ***Bouclier résident*** à appliquer :

- ***Analyser les cookies*** - ce paramètre définit les cookies à détecter au cours de l'analyse. (Les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs telles que leurs préférences en matière de site ou le contenu de leurs paniers d'achat électroniques)

- ***Signaler les programmes potentiellement dangereux et les spywares*** - (*paramètre activé par défaut*) analyse des programmes potentiellement dangereux (*applications exécutables se comportant comme des spywares ou des adwares*)

- ***Analyser les fichiers à la fermeture*** - ce type d'analyse garantit qu'AVG vérifie les objets actifs (par exemple, les applications, les documents…) à leur ouverture et à leur fermeture. Cette fonction contribue à protéger l'ordinateur contre certains types de virus sophistiqués

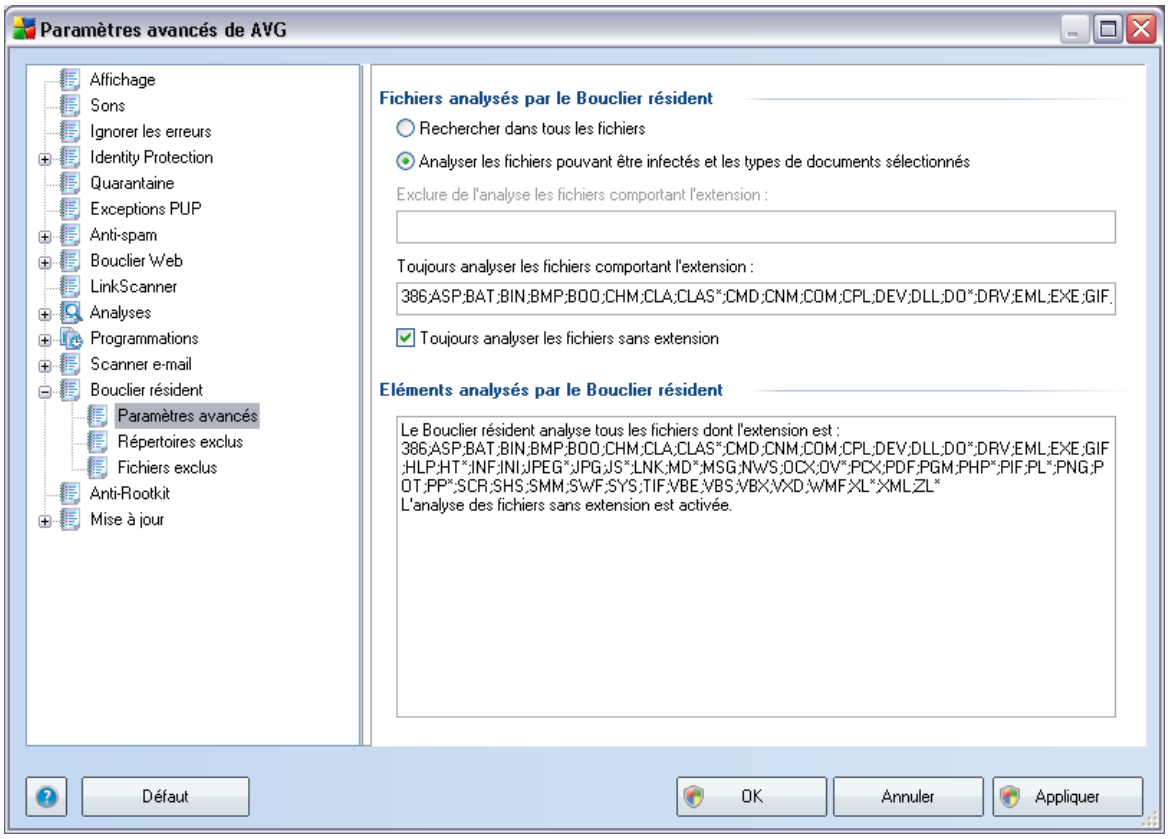
- ***Analyser le secteur d'initialisation (boot) des supports amovibles*** - (*option activée par défaut*)

- ***Utiliser la méthode heuristique***- (*option activée par défaut*) l'analyse heuristique est un moyen de détection (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*)

- ***Réparer automatiquement*** - toute infection détectée sera automatiquement réparée si un traitement est disponible

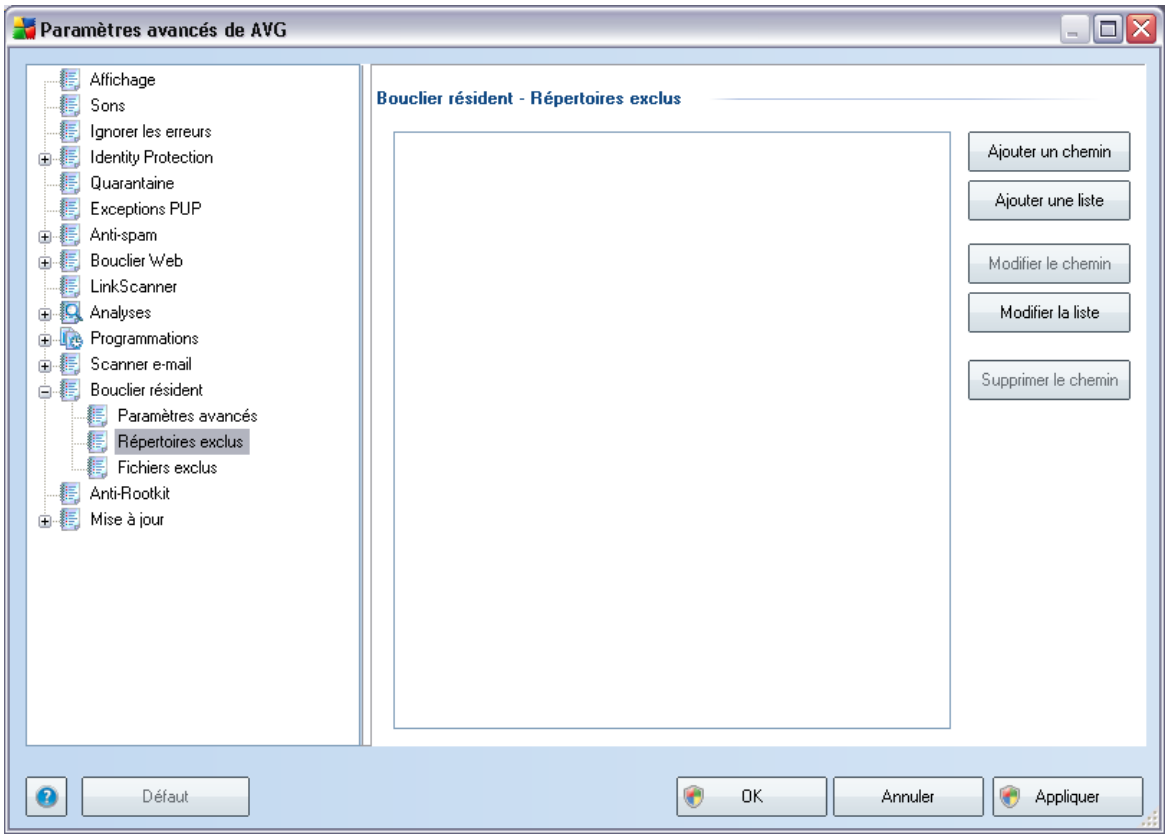
9.13.1. Paramètres avancés

Dans la boîte de dialogue ***Fichiers analysés par le Bouclier résident***, il est possible de spécifier les fichiers à analyser (*en fonction de leurs extensions*) :



Décidez si tous les fichiers ou seulement ceux qui sont susceptibles d'être infectés doivent être analysés. En l'occurrence, vous pouvez dresser la liste des extensions correspondant aux fichiers à exclure de l'analyse et la liste des extensions correspondant aux fichiers à analyser systématiquement.

9.13.2. Répertoires exclus



La boîte de dialogue ***Bouclier résident - Répertoires exclus*** offre la possibilité de définir les dossiers à exclure de l'analyse effectuée par le ***Bouclier résident.***

Il est vivement recommandé de n'exclure aucun répertoire, sauf en cas d'absolue nécessité.

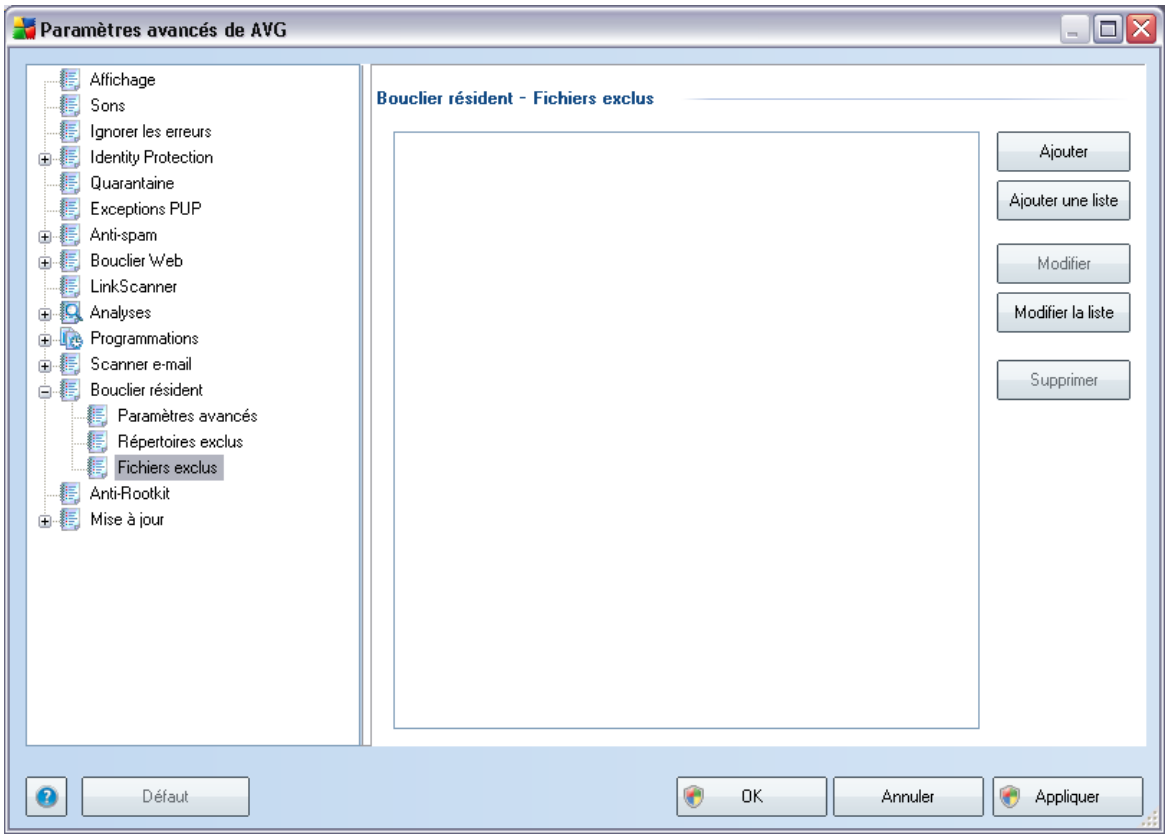
Cette boîte de dialogue présente les boutons de fonction suivantes :

- ***Ajouter un chemin*** – ce bouton permet de spécifier les répertoires que vous souhaitez exclure lors de l'analyse en les sélectionnant un à un dans l'arborescence de navigation du disque local
- ***Ajouter une liste*** – ce bouton permet de spécifier une liste complète de répertoires à exclure de l'analyse du ***Bouclier résident***
- ***Modifier le chemin*** - ce bouton permet de modifier le chemin d'accès à un

dossier sélectionné

- ***Modifier la liste*** – ce bouton permet de redéfinir la liste des dossiers
- ***Supprimer le chemin*** – ce bouton permet de supprimer le chemin d'accès à un dossier sélectionné dans la liste

9.13.3. Fichiers exclus



La boîte de dialogue ***Bouclier résident - Fichiers exclus*** se comporte comme celle précédemment décrite, à savoir ***Bouclier résident - Répertoires exclus*** mais à la place des dossiers, vous avez maintenant la possibilité de définir des fichiers spécifiques à exclure de l'analyse effectuée par le ***Bouclier résident***.

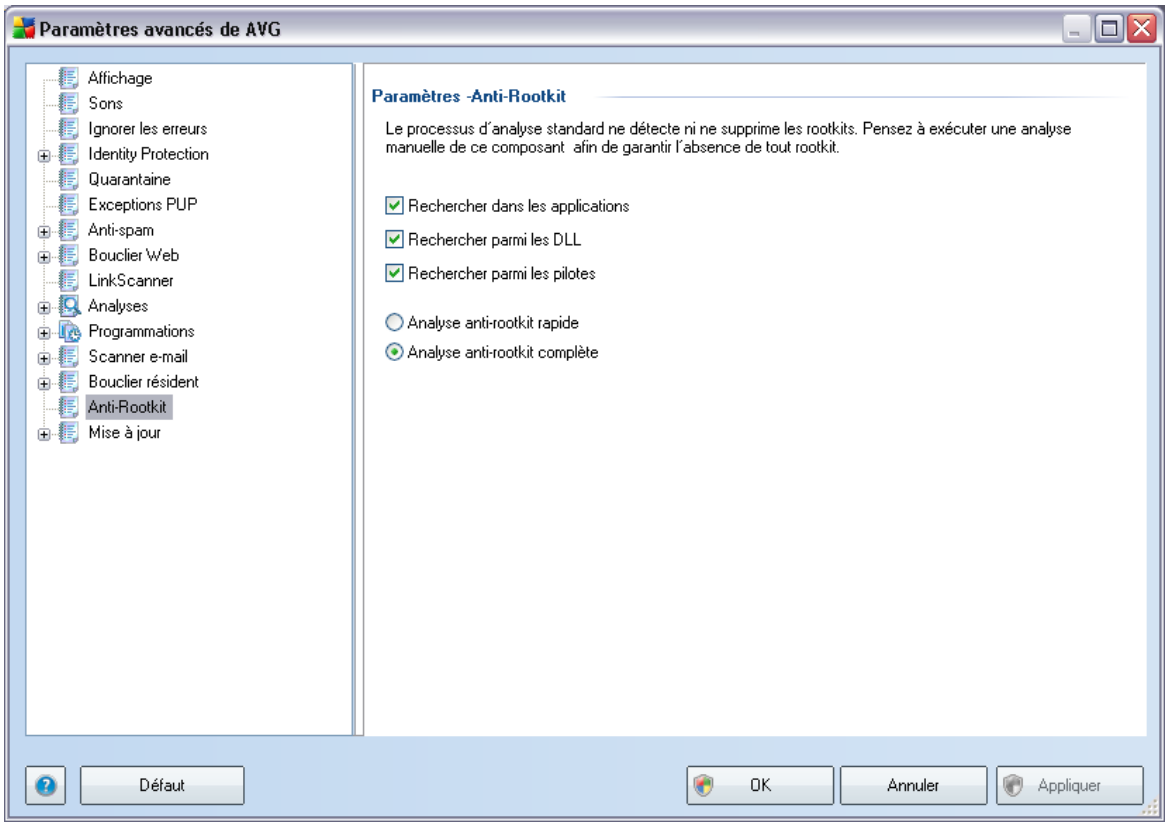
Il est vivement recommandé de n'exclure aucun fichier, sauf en cas d'absolue nécessité !

Cette boîte de dialogue présente les boutons de fonction suivantes :

- ***Ajouter*** – ce bouton permet de spécifier les répertoires que vous souhaitez exclure lors de l'analyse en les sélectionnant un à un dans l'arborescence de navigation du disque local
- ***Ajouter une liste*** – ce bouton permet de spécifier une liste complète de répertoires à exclure de l'analyse du ***Bouclier résident***
- ***Modifier*** - ce bouton permet de modifier le chemin d'accès à un dossier sélectionné
- ***Modifier la liste*** – ce bouton permet de redéfinir la liste des dossiers
- ***Supprimer*** – ce bouton permet de supprimer le chemin d'accès à un dossier sélectionné dans la liste

9.14. Anti-rootkit

Dans cette boîte de dialogue, vous pouvez modifier la configuration du composant ***Anti-Rootkit*** :



Modifier l'ensemble des du composant ***Anti-Rootkit*** comme indiqué dans cette boîte de dialogue est également possible depuis l'***interface du composant Anti-Rootkit***.

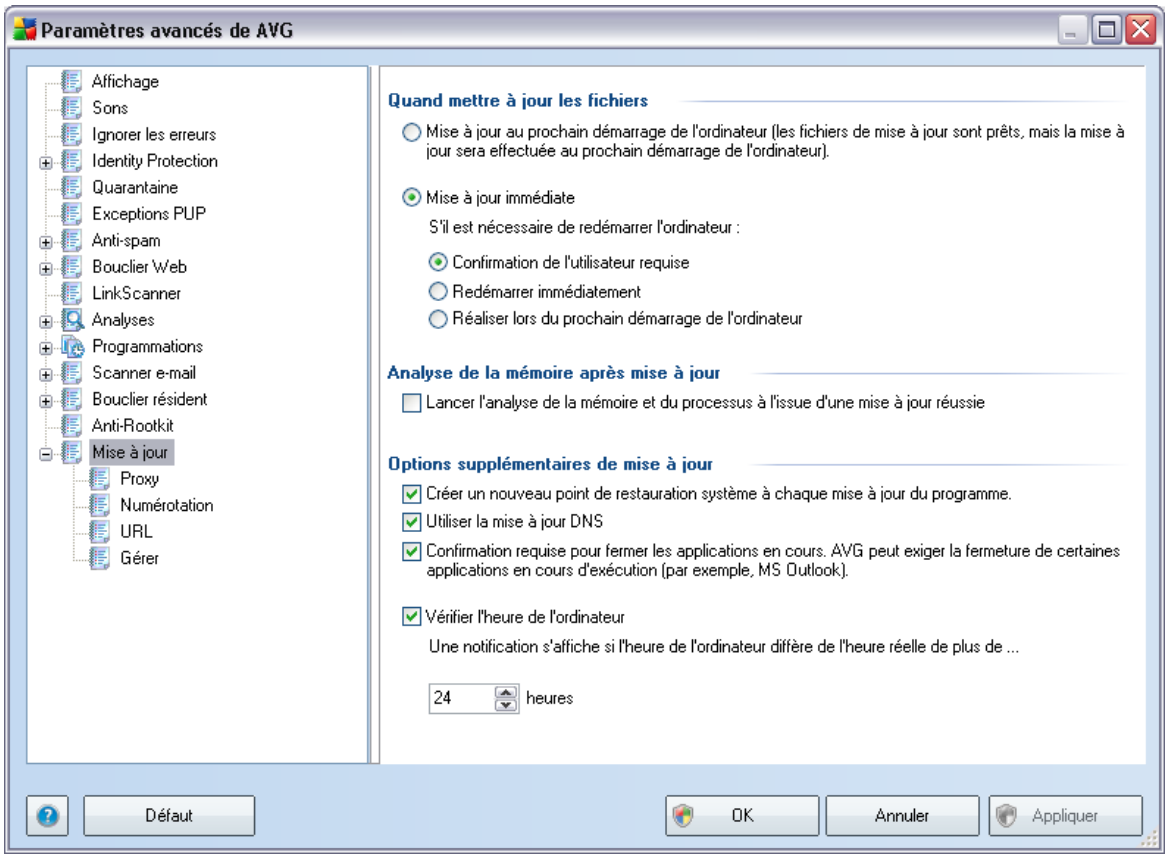
Cochez tout les cases permettant d'indiquer les objets à analyser :

- ***Rechercher dans les applications***
- ***Rechercher parmi les DLL***
- ***Rechercher parmi les pilotes***

Vous pouvez ensuite choisir le mode d'analyse des rootkits :

- ***Analyse anti-rootkit rapide*** - analyse seulement le dossier système (*généralement, c:\Windows*)
- ***Analyse anti-rootkit complète*** - analyse tous les disques accessibles sauf A: et B:

9.15. Mise à jour



L'élément de navigation ***Mise à jour*** ouvre une nouvelle boîte de dialogue dans laquelle vous spécifiez les paramètres généraux de la mise à jour du programme AVG :

Quand mettre à jour les fichiers

Dans cette section, vous avez le choix entre deux options : la mise à jour peut être

programmée pour être lancée au redémarrage de l'ordinateur ou être exécutée immédiatement. Par défaut, l'option de mise à jour immédiate est sélectionnée, car de cette façon AVG offre le niveau de sécurité optimal. Programmer une mise à jour au redémarrage suivant est seulement recommandé si l'ordinateur est régulièrement réamorcé (au moins une fois par jour).

Si vous décidez d'appliquer la configuration par défaut et lancer l'opération immédiatement, vous pouvez préciser les conditions dans lesquelles un redémarrage obligatoire doit être réalisé :

- ***Confirmation de l'utilisateur requise*** - un message vous invite à approuver le redémarrage nécessaire pour finaliser le processus de mise à jour
- ***Redémarrer immédiatement*** - l'ordinateur est redémarré automatiquement à l'issue de la mise à jour, votre accord n'est pas recherché
- ***Réaliser lors du prochain démarrage de l'ordinateur***- la finalisation du processus de mise à jour est différée jusqu'au redémarrage de l'ordinateur - rappelez-vous que cette option est à proscrire si l'ordinateur n'est pas fréquemment redémarré (moins d'une fois par jour).

Analyse de la mémoire après mise à jour

Cochez cette case pour indiquer que vous voulez lancer une nouvelle analyse de la mémoire après chaque mise à jour achevée avec succès. La dernière mise à jour téléchargée peut contenir de nouvelles définitions de virus et celles-ci peuvent être analysées automatiquement.

Options supplémentaires de mise à jour

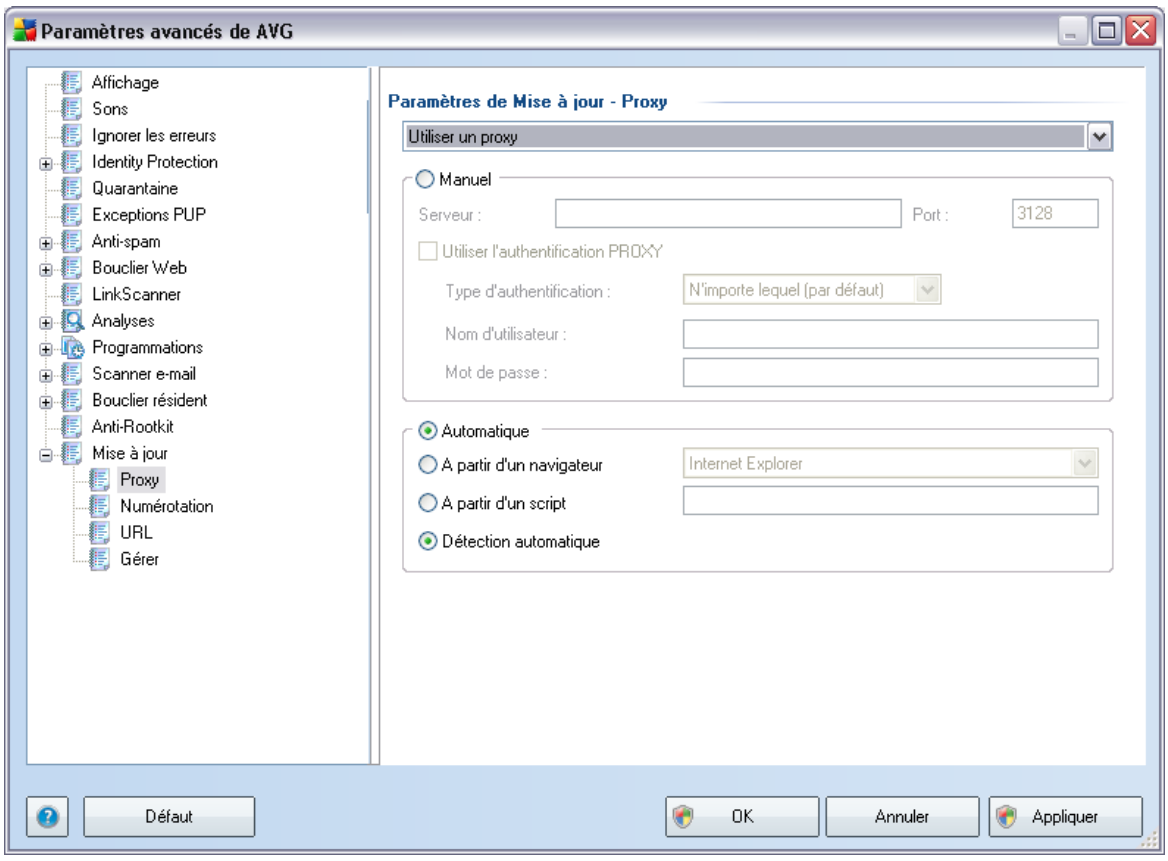
- ***Créer un nouveau point de restauration après chaque nouvelle mise à jour du programme*** : un point de restauration est créé avant le lancement d'une mise à jour du programme AVG. En cas d'échec de la mise à jour et de blocage de votre système d'exploitation, vous avez alors la possibilité de restaurer le système d'exploitation tel qu'il était configuré à partir de ce point. Cette option est accessible via Démarrer / Tous les programmes / Accessoires / Outils système / Restauration du système, mais seuls les utilisateurs expérimentés devraient effectuer des changements à ce niveau! Laissez cette case cochée si vous voulez utiliser cette fonctionnalité.
- ***Utiliser la mise à jour DNS*** : cochez cette case si vous voulez confirmer que vous voulez utiliser la méthode de détection des fichiers de mise à jour qui

élimine la quantité de données transférée entre le serveur de mise à jour et le client AVG ;

- ***Confirmation requise pour fermer les applications en cours*** (*option activée par défaut*) : cette option permet de vous assurer qu'aucune application actuellement en cours d'exécution ne sera fermée sans votre autorisation, si cette opération est requise pour la finalisation du processus de mise à jour ;

- ***Vérifier l'heure de l'ordinateur*** : cochez cette case si vous voulez être informé lorsque l'heure du système et l'heure correcte diffèrent de plus du nombre d'heures spécifié.

9.15.1. Proxy



Un serveur proxy est un serveur ou un service autonome s'exécutant sur un PC dans le but de garantir une connexion sécurisée à Internet. En fonction des règles de

réseau spécifiées, vous pouvez accéder à Internet directement, via le serveur proxy ou en combinant les deux possibilités. Dans la première zone (liste déroulante) de la boîte de dialogue ***Paramètres de mise à jour - Proxy***, vous êtes amené à faire un choix parmi les options suivantes :

- ***Utiliser un serveur proxy***
- ***Ne pas utiliser de serveur proxy***
- ***Utiliser un serveur proxy. En cas d'échec, se connecter en direct*** - paramètre défini par défaut

Si vous sélectionnez une option faisant appel au serveur proxy, vous devez spécifier des données supplémentaires. Les paramètres du serveur peuvent être configurés manuellement ou automatiquement.

Configuration manuelle

Si vous choisissez la configuration manuelle (cochez la case *Manuel pour activer la section correspondante dans la boîte de dialogue*), spécifiez les éléments suivants :

- ***Serveur*** – indiquez l'adresse IP ou le nom du serveur
- ***Port*** – spécifiez le numéro du port donnant accès à Internet (*par défaut, le port 3128) – en cas de doute, prenez contact avec l'administrateur du réseau*)

Il est aussi possible de définir des règles spécifiques à chaque utilisateur pour le serveur proxy. Si votre serveur proxy est configuré de cette manière, cochez l'option ***Utiliser l'authentification PROXY*** pour vous assurer que votre nom d'utilisateur et votre mot de passe sont valides pour établir une connexion à Internet via le serveur proxy.

Configuration automatique

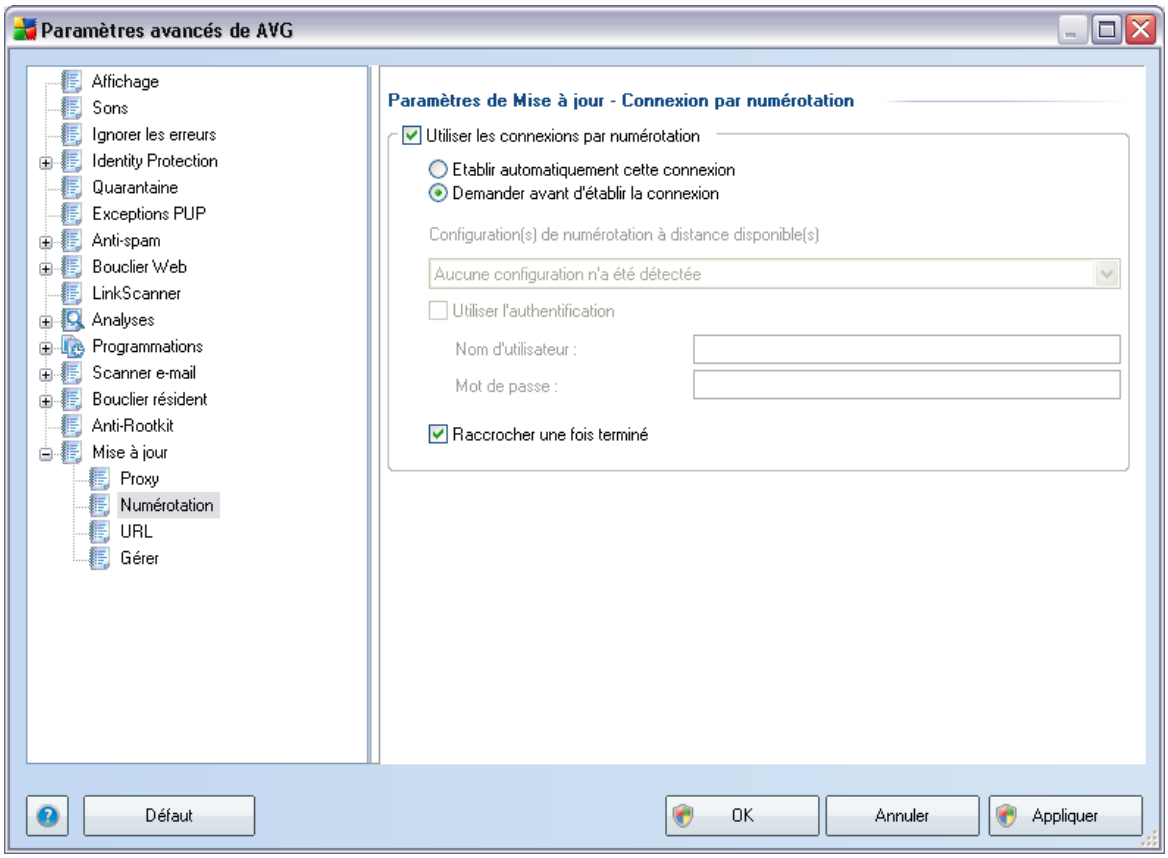
Si vous optez pour la configuration automatique (*cochez la case* ***Automatique****pour activer la section correspondante dans la boîte de dialogue*), puis spécifiez le type de configuration proxy désiré :

- ***A partir d'un navigateur*** - la configuration sera lue depuis votre navigateur Internet par défaut
- ***A partir d'un script*** - la configuration sera lue à partir d'un script téléchargé

avec la fonction renvoyant l'adresse proxy

- ***Détection automatique*** - la configuration sera détectée automatiquement à partir du serveur proxy

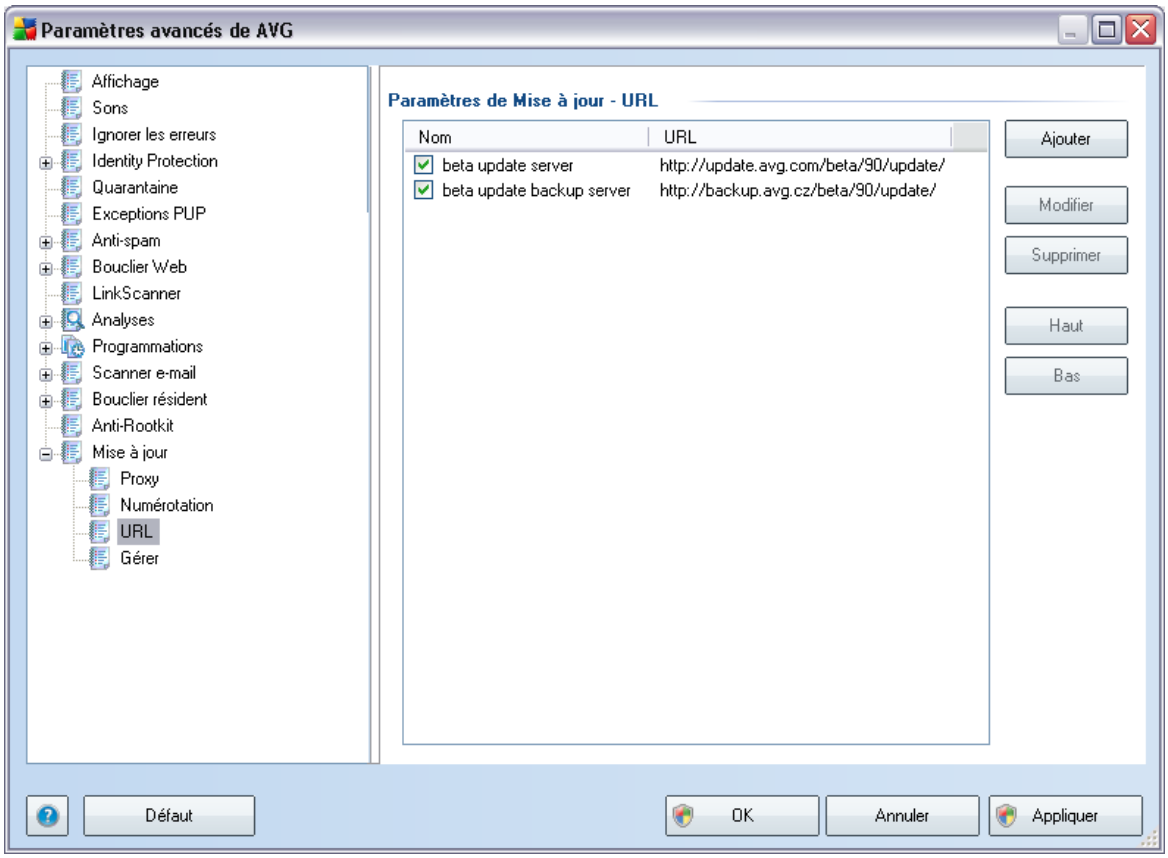
9.15.2. Numérotation



Tous les paramètres facultatifs de la boîte de dialogue ***Paramètres de mise à jour - Connexion par numérotation*** se rapportent à la connexion par numérotation à Internet. Les champs de cette boîte de dialogue sont activés à condition de cocher l'option ***Utiliser les connexions par numérotation***.

Précisez si vous souhaitez vous connecter automatiquement à Internet (***Etablir cette connexion automatiquement***) ou confirmer manuellement la connexion (***Demander avant d'établir la connexion***). En cas de connexion automatique, vous devez indiquer si la connexion doit prendre fin après la mise à jour (***Raccrocher une fois terminé***).

9.15.3. URL

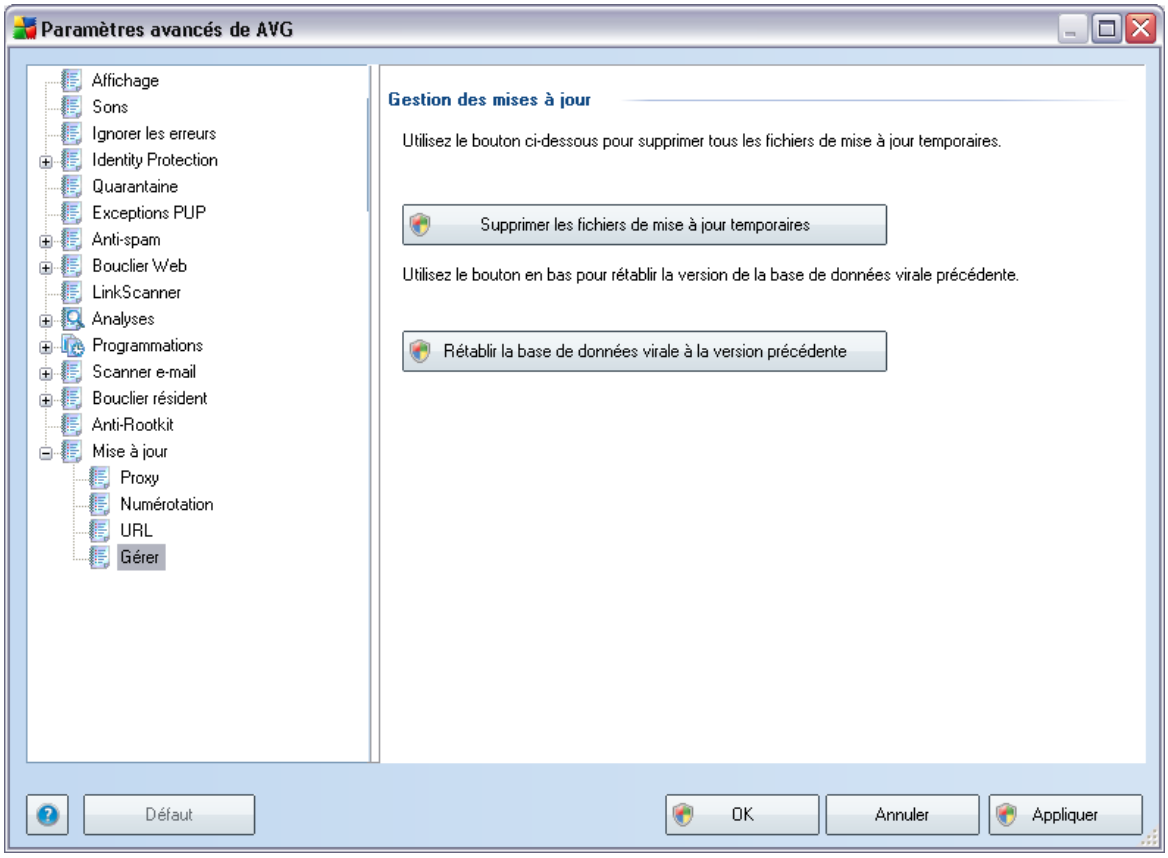


La boîte de dialogue ***URL*** contient une liste d'adresses Internet à partir desquelles il est possible de télécharger les fichiers de mise à jour. Vous pouvez redéfinir le contenu de cette liste à l'aide des boutons de fonction suivants :

- ***Ajouter*** – ouvre une boîte de dialogue permettant de spécifier une nouvelle adresse URL
- ***Modifier*** - ouvre une boîte de dialogue permettant de modifier les paramètres de l'URL sélectionnée
- ***Supprimer*** - retire l'URL sélectionnée de la liste
- ***Haut*** – déplace l'URL sélectionnée d'un rang vers le haut dans la liste
- ***Bas*** – déplace l'URL sélectionnée d'un rang vers le bas dans la liste

9.15.4. Gérer

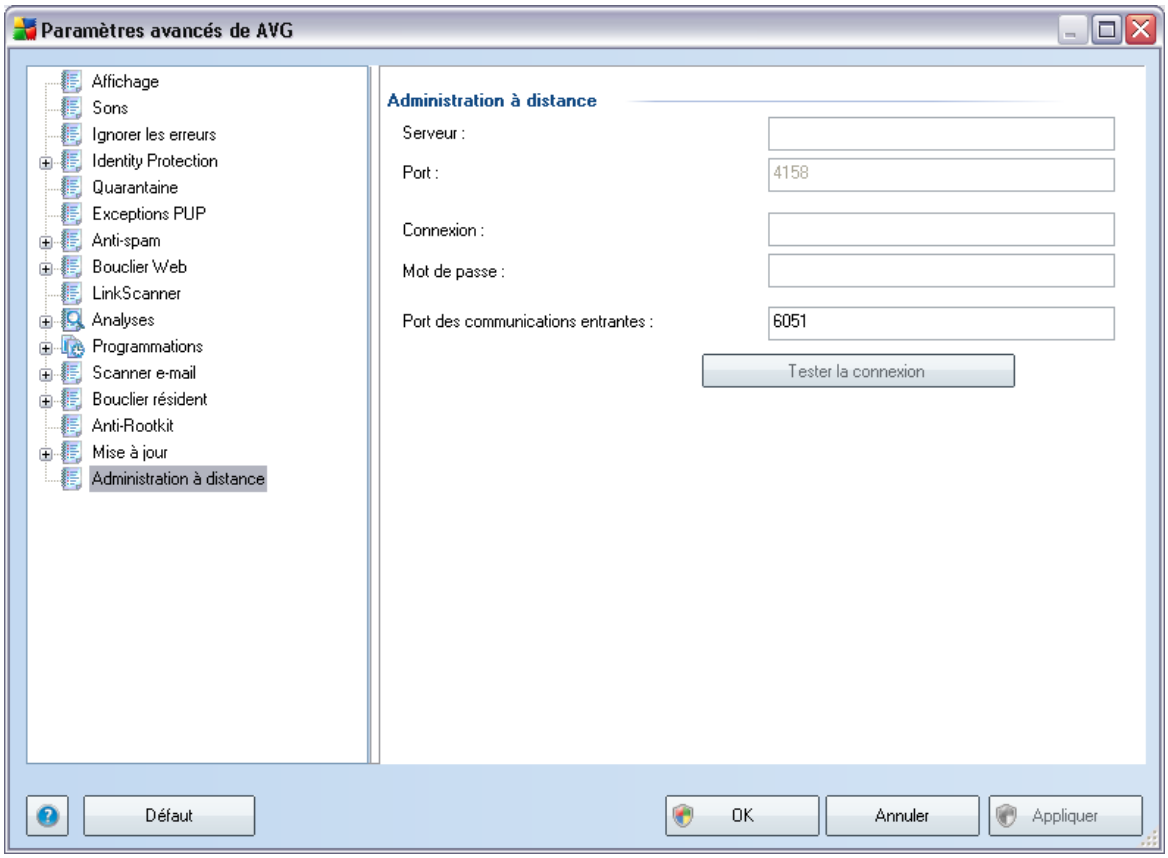
La boîte de dialogue ***Gérer*** propose deux options accessibles via deux boutons :



- ***Supprimer les fichiers de mise à jour temporaires*** - cliquez sur ce bouton pour supprimer tous les fichiers redondants de votre disque dur (*par défaut, ces fichiers sont conservés pendant 30 jours*)

- ***Revenir à la version précédente de la base virale*** – cliquez sur ce bouton pour supprimer la dernière version de la base virale de votre disque dur et revenir à la version précédente enregistrée (*la nouvelle version de la base de données sera incluse dans la mise à jour suivante*)

9.16. Administration à distance



Les paramètres de l'***administration à distance*** concernent la connexion du poste du client AVG au système d'administration à distance. Si vous envisagez de connecter la station au serveur d'administration à distance, veuillez spécifier les paramètres suivants :

- ***Serveur*** - nom du serveur (ou adresse IP) sur lequel AVG Admin Server est installé
- ***Port*** - indiquez le numéro du port sur lequel le client AVG communique avec AVG Admin Server (*le numéro de port 4158 est utilisé par défaut - si vous voulez l'utiliser, il est inutile de le spécifier de manière explicite*)
- ***Connexion*** - si les communications entre le client AVG et AVG Admin Server sont sécurisées, indiquez votre nom d'utilisateur ...

- ***Mot de passe*** - ... et votre mot de passe
- ***Port des communications entrantes*** - numéro de port par lequel le client AVG accepte les messages entrants en provenance du serveur AVG Admin Server

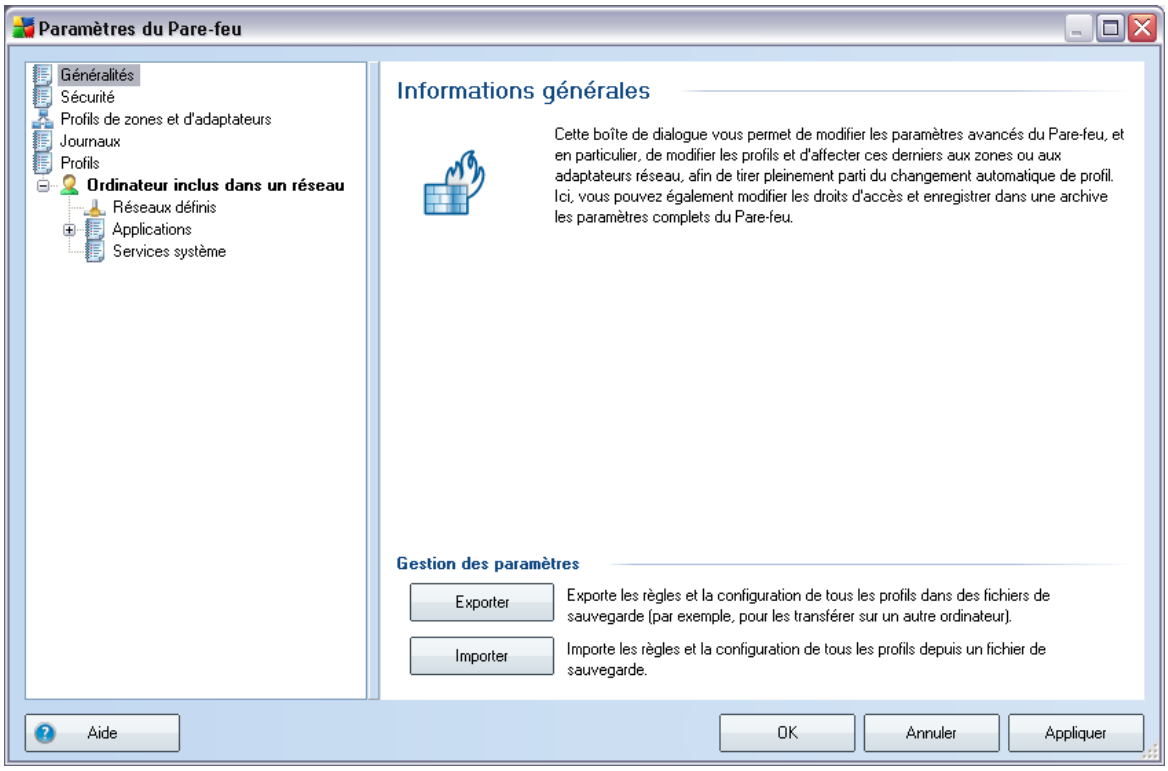
Le bouton ***Tester la connexion*** permet de vérifier que toutes les données spécifiées ci-dessus sont valables et peuvent être utilisées pour se connecter au Centre de données.

Remarque : *pour obtenir des informations détaillées sur l'administration à distance, merci de consulter la documentation relative à l'édition réseau d'AVG.*

10. Paramètres du Pare-feu

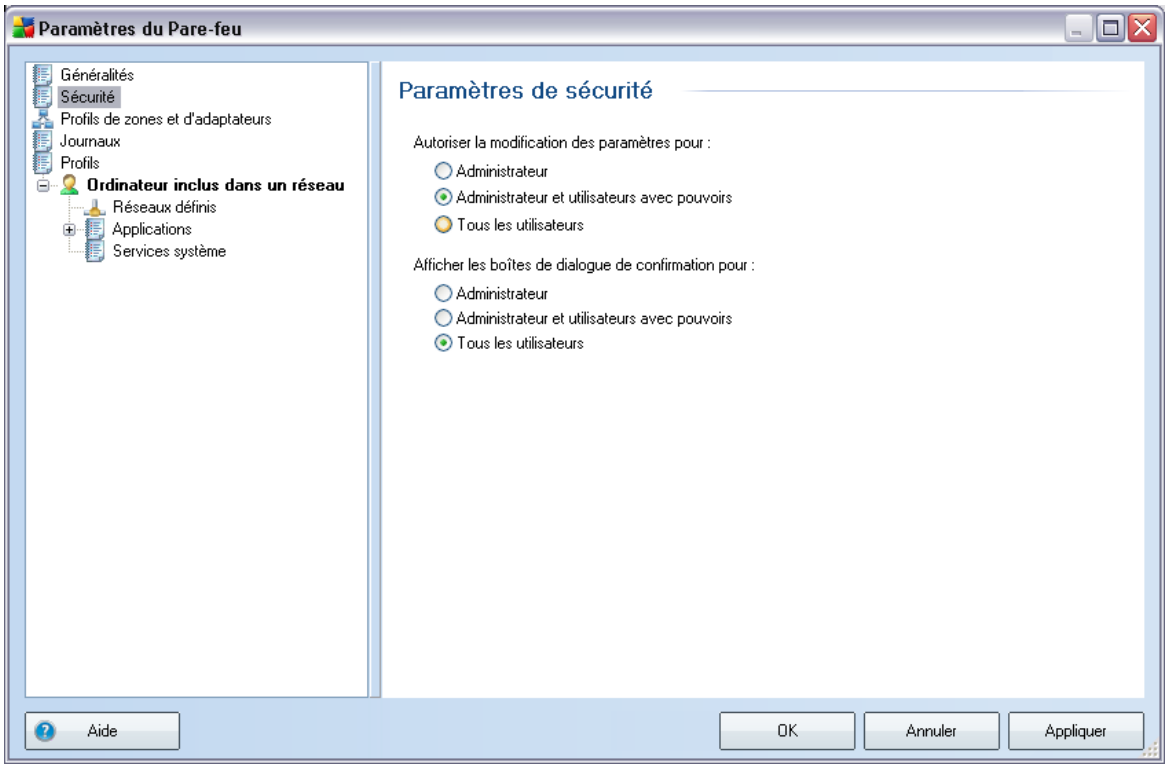
La configuration du ***Pare-feu*** s'affiche au sein d'une nouvelle fenêtre à partir de laquelle vous accédez à plusieurs boîtes de dialogue et configurez les paramètres avancés du composant. ***Cependant, la modification de la configuration avancée est exclusivement destinée aux spécialistes et aux utilisateurs expérimentés.***

10.1. Généralités



Dans la section ***Informations générales*** vous avez la possibilité d'***exporter*** et d'***importer*** ***la configuration du*** Pare-feu, à savoir d'exporter les règles et paramètres définis pour le ***Pare-feu*** dans les fichiers de sauvegarde, ou à l'inverse, en importer le contenu entier depuis un fichier de sauvegarde.

10.2. Sécurité



Dans la boîte de dialogue ***Paramètres de sécurité***, vous pouvez définir les règles générales du comportement du ***Pare-feu***et ce, indépendamment du profil sélectionné :

- ***Autoriser la modification des paramètres pour*** - spécifiez les personnes habilitées à adapter la configuration du ***Pare-feu***
- ***Afficher les boîtes de dialogue de confirmation pour*** - spécifiez les personnes auxquelles présenter les demandes de confirmation (*boîtes de dialogue sollicitant la décision de l'utilisateur dans les situations où aucune règle définie du* ***Pare-feu*** n'est applicable)

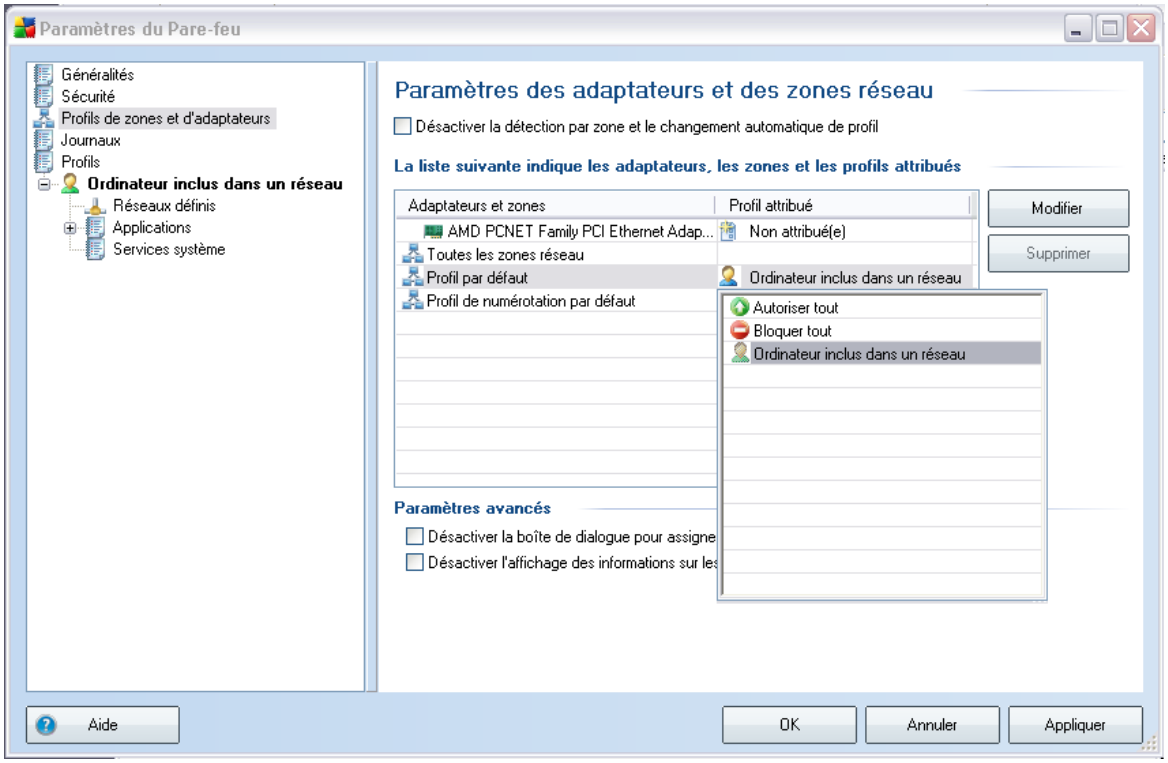
Pour ces deux options, il est possible d'attribuer l'autorisation spécifique à l'un des groupes utilisateurs suivants :

  - ***Administrateur*** – l'administrateur bénéficie d'un contrôle total sur le PC et a le droit d'affecter chaque utilisateur à des groupes dotés de droits spécifiquement définis.

- ***Administrateurs et utilisateurs avec pouvoirs*** – l'administrateur a le droit d'affecter chaque utilisateur à un groupe spécifique (*utilisateur avec pouvoir*) et de définir les droits des membres du groupe.

- ***Tous les utilisateurs*** – ensemble des autres utilisateurs n'appartenant à aucun groupe particulier.

10.3. Profils de zones et d'adaptateurs



La boîte de dialogue ***Paramètres des adaptateurs et des zones réseau*** permet de modifier les paramètres liés à l'attribution de profils définis à des adaptateurs déterminés, ainsi que la référence des réseaux correspondants :

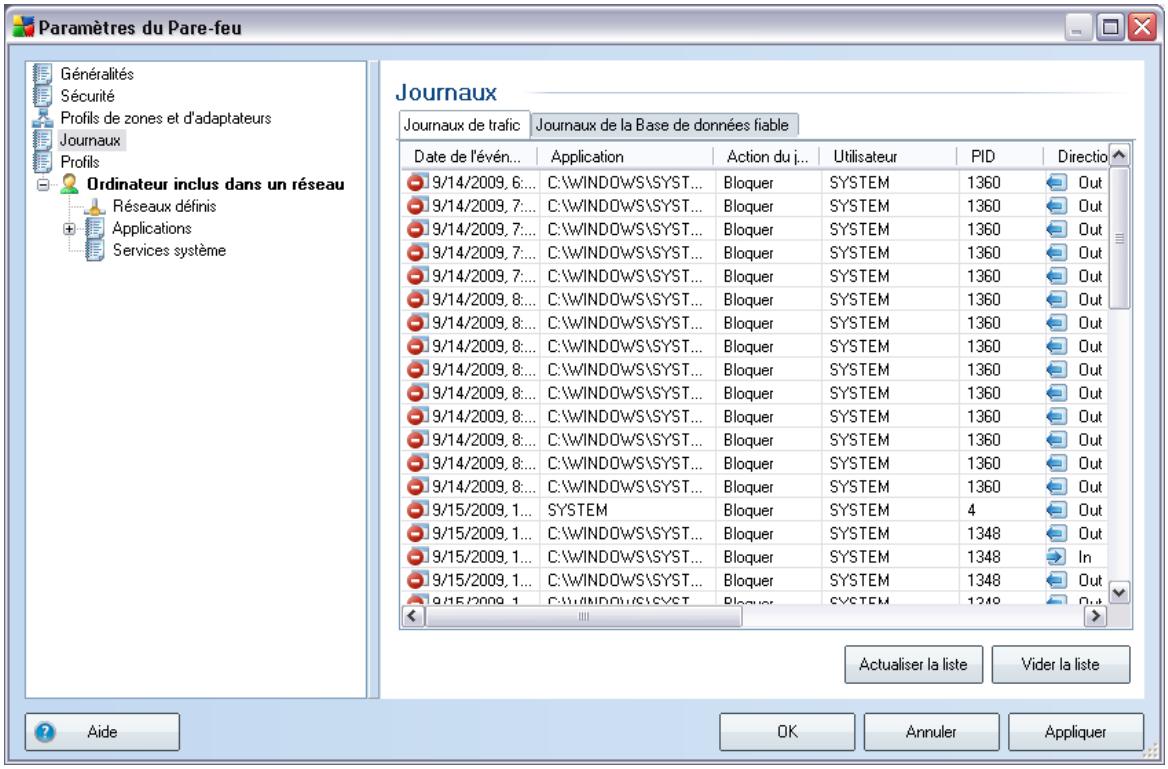
- ***Désactiver la détection par zone et le changement automatique de profil***- un profil défini peut être affecté à chaque type d'interface réseau, c'est-à-dire à chaque zone. Si vous ne souhaitez pas définir des profils spécifiques, le système utilisera un profil commun défini sur la base du type d' utilisation de l'ordinateur et de la conception du réseau informatique sélectionnés au cours du ***processus d'installation***. Si vous décidez de différencier des profils et de les attribuer à des adaptateurs et à des zones

spécifiques puis, pour une raison quelconque, souhaitez désactiver temporairement ce dispositif, il suffit de cocher l'option ***Désactiver la détection par zone et le changement automatique de profil***.

- ***La liste suivante indique les adaptateurs, les zones et les profils attribués*** - cette liste présente les adaptateurs et les zones détectés. Un profil spécifique peut être attribué à chacun d'eux à partir du menu des profils définis. Pour ouvrir cette liste déroulante, faites votre choix dans la liste des adaptateurs, puis sélectionnez un profil.

- ***Paramètres avancés*** - chaque option que vous sélectionnez désactive l'affichage d'un message d'information.

10.4. Journaux



La boîte de dialogue ***Journaux*** permet de passer en revue l'ensemble des actions et des évènements du ***Pare-feu*** qui ont été enregistrés ainsi que la description détaillée des paramètres associés (*date de l'évènement, nom de l'application, action du journal correspondante, nom d'utilisateur, PID, direction du trafic, type de protocole, numéros des ports locaux et distants, etc.*) sous deux onglets :

- ***Journaux de trafic*** - cet onglet fournit des informations sur l'activité de toutes les applications qui ont essayé de se connecter au réseau.

- ***Journaux de la base de données fiable*** - la *Base de données fiable* désigne les informations entrées dans la base de données interne d'AVG relatives aux applications certifiées et fiables pouvant toujours être autorisées à communiquer en ligne. Lorsqu'une nouvelle application tente pour la première fois de se connecter au réseau (*c'est-à-dire, lorsqu'aucune règle de pare-feu n'a encore été spécifiée pour cette application*), vous devez déterminer si la communication réseau doit être autorisée pour l'application correspondante. AVG recherche d'abord la *Base de données fiable*. Si l'application est répertoriée, elle sera automatiquement autorisée à accéder au réseau. Uniquement après cette opération, s'il n'existe aucune information relative à l'application disponible dans la base de données, vous serez invité à indiquer, dans une nouvelle fenêtre, si l'application doit être autorisée à accéder au réseau.

Boutons de commande

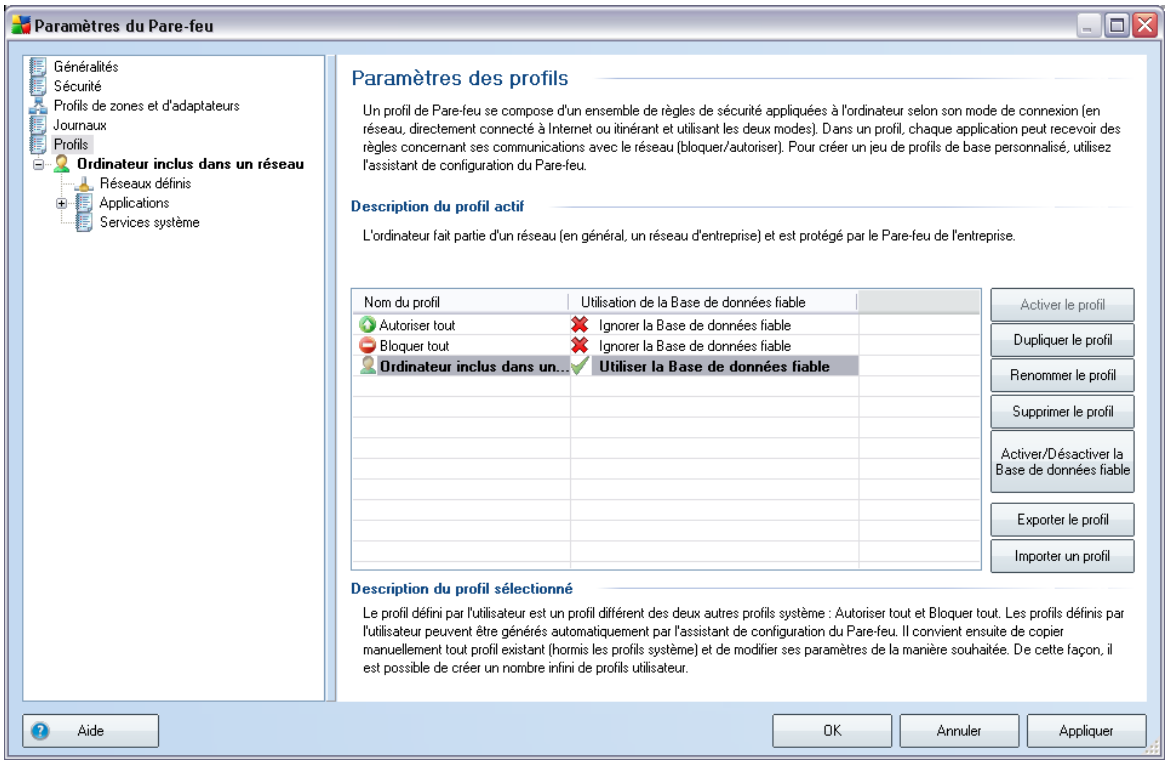
- ***Aide*** - ouvre la boîte de dialogue associée aux fichiers d'aide.

- ***Actualiser la liste*** - Il est possible de réorganiser les paramètres enregistrés dans le journal en fonction de l'attribut que vous sélectionnez : chronologiquement (*dates*) ou alphabétiquement (*autres colonnes*). Pour cela, cliquez simplement sur l'en-tête de colonne qui convient. Cliquez sur le bouton ***Actualiser la liste*** pour mettre à jour les informations affichées.

- ***Vider la liste*** - Permet de retirer toutes les entrées du tableau.

10.5. Profils

La boîte de dialogue ***Paramètres des profils*** inclut la liste de tous les profils disponibles.



Tous les autres profils autres que les profils système peuvent être édités directement depuis cette boîte de dialogue à l'aide des boutons de commande suivants :

- ***Activer le profil*** - ce bouton définit le profil sélectionné comme étant actif. La configuration de ce profil sera alors utilisée par le ***Pare-feu*** pour contrôler le trafic réseau
- ***Dupliquer le profil***- génère une copie conforme du profil sélectionné ; vous pouvez ensuite modifier la copie et la renommer pour obtenir un nouveau profil
- ***Renommer le profil*** - permet d'attribuer un nouveau nom au profil sélectionné
- ***Supprimer le profil*** - retire le profil sélectionné de la liste

- ***Activer/Désactiver la Base de données fiable*** - pour le profil sélectionné, vous pouvez décider d'utiliser les informations de la *Base de données fiable* (la *Base de données fiable désigne les données contenues dans la base de données interne d'AVG relatives aux applications fiables et certifiées pouvant toujours être autorisées à communiquer en ligne.*)

- ***Exporter le profil*** - enregistre la configuration du profil sélectionné dans un fichier en vue d'une utilisation ultérieure

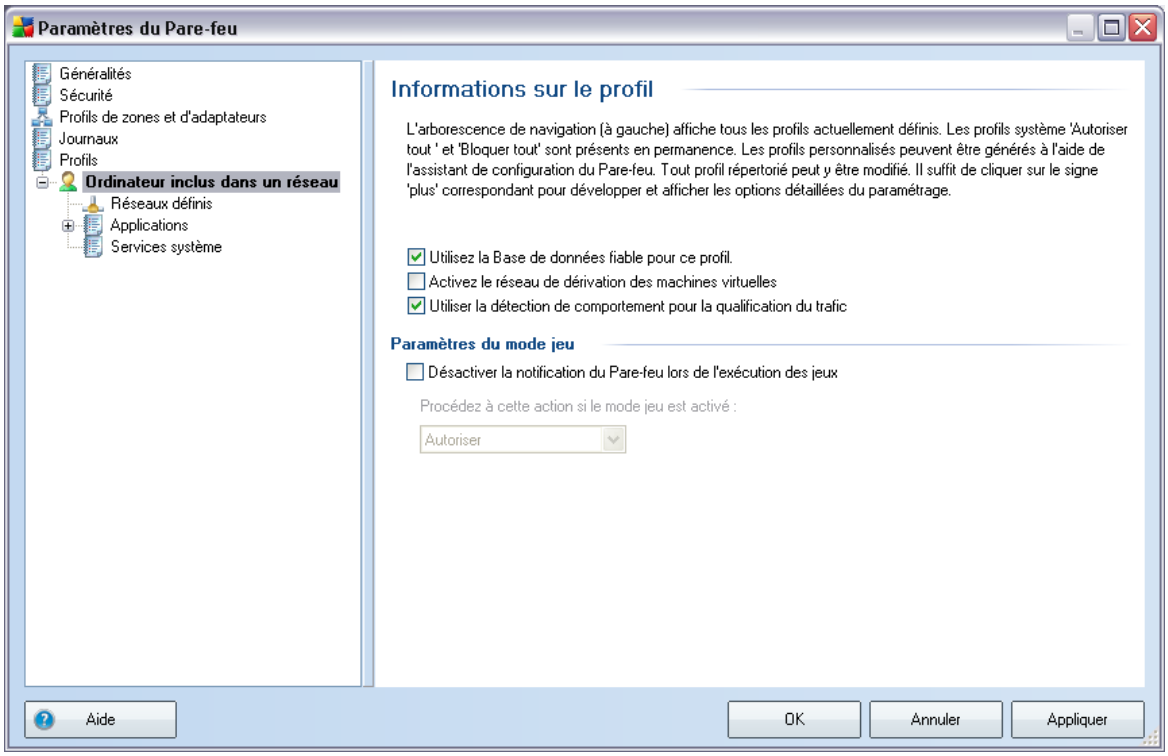
- ***Importer le profil*** - configure les paramètres du profil sélectionné en fonction des données exportées depuis le fichier de configuration de sauvegarde

- ***Aide*** - ouvre le fichier d'aide associé à la boîte de dialogue

Dans la partie inférieure de la boîte de dialogue, vous trouverez la description du profil actuellement sélectionné dans la liste.

L'arborescence de navigation située à gauche diffère selon le nombre de profils définis qui figurent dans la liste au sein de la boîte de dialogue ***Profil***. Chaque profil défini correspond à une branche spécifique placée sous l'entrée ***Profil***. Il est possible de modifier les profils dans les boîtes de dialogue suivantes (*identiques pour tous les profils*) :

10.5.1. Informations sur le profil



La boîte de dialogue ***Informations sur le profil*** est la première d'une série de boîtes de dialogue permettant de modifier les paramètres de configuration des profils. A chaque boîte de dialogue correspond un profil.

- ***Utiliser la base de données fiable*** - (*paramètre activé par défaut*) cochez cette option pour activer la *Base de données fiable* (*, c'est-à-dire les informations entrées dans la base de données interne d'AVG relatives à une application fiable et certifiée qui communique en ligne. Aucune règle n'a encore été spécifiée pour l'application correspondante. Vous devez déterminer s'il faut autoriser cette application à accéder au réseau. AVG a d'abord effectué une recherche dans la Base de données fiable. Si l'application est répertoriée, elle sera considérée comme sécurisée et sera autorisée à communiquer sur le réseau. Sinon, vous serez invité à indiquer si l'application doit être autorisée à communiquer sur le réseau* pour le profil approprié

- ***Activer le réseau de dérivation pour les machines virtuelles*** - (*paramètre désactivé par défaut*) cochez cette case pour permettre aux machines virtuelles WMware de se connecter directement à ce réseau

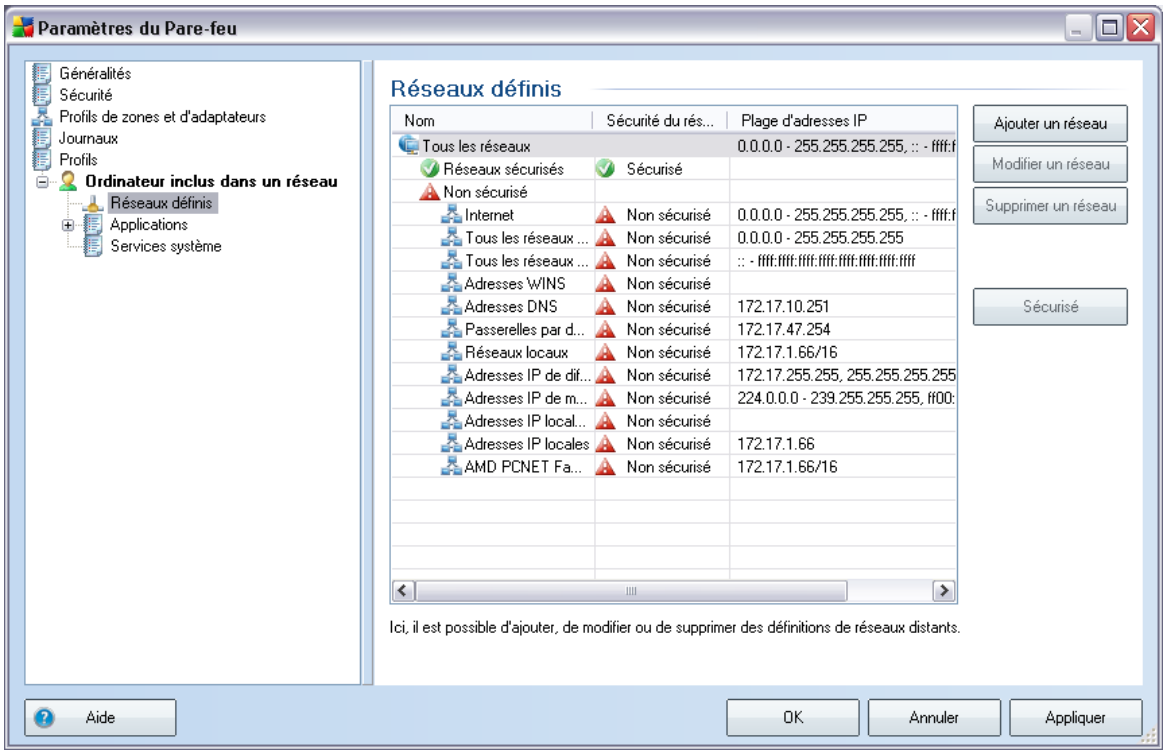
- ***Utiliser la détection de comportement pour la qualification du trafic*** - (*paramètre activé par défaut*) cochez cette case pour permettre au ***Pare-feu*** d'utiliser la fonctionnalité ***LinkScanner*** lors de l'évaluation d'une application - ***LinkScanner*** peut savoir si l'application affiche un comportement suspect ou si elle est fiable et peut être autorisée à communiquer en ligne.

Paramètres du mode jeu

Dans la section ***Paramètres du mode jeu***, vous indiquez et confirmez (en cochant la case associée) votre choix de laisser les messages d'information du ***Pare-feu*** s'afficher pendant le déroulement des applications en plein écran (*généralement des jeux, mais aussi toute autre application exécutée en plein écran comme les présentations PowerPoint*). Etant donné que ces messages peuvent être gênants.

Si vous cochez la case ***Désactiver les notifications du Pare-feu lors de l'exécution de jeux***, sélectionnez dans la liste déroulante l'action souhaitée lorsqu'une nouvelle application sans règle définie tente de communiquer sur le réseau (*ces applications vous invitent habituellement à répondre à une question dans une boîte de dialogue*). Toutes ces applications peuvent être autorisées ou bloquées.

10.5.2. Réseaux définis

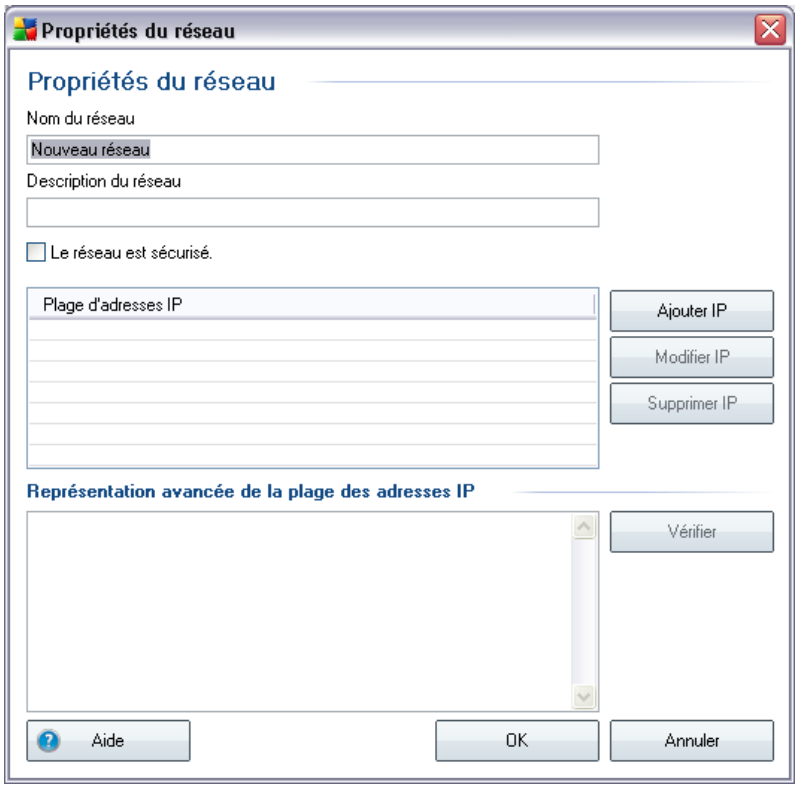


La boîte de dialogue ***Réseaux définis*** dresse la liste de tous les réseaux auxquels est relié l'ordinateur. Les informations suivantes sont fournies pour chaque réseau détecté :

- ***Réseaux*** - noms des réseaux auxquels l'ordinateur est relié
- ***Sécurité du réseau*** - par défaut, tous les réseaux sont considérés comme non sécurisés. Déclarez un réseau comme sécurisé seulement si vous êtes certain qu'il est fiable. (*Pour cela, cochez la case correspondante dans la liste et choisissez la commande Sécurisé dans le menu contextuel*). Tous les réseaux associés seront inclus dans le groupe des réseaux utilisés par l'application pour communiquer en appliquant le jeu de règles défini pour la valeur ***Autoriser la connexion sécurisée***
- ***Plage d'adresses IP*** - chaque réseau est automatiquement détecté et spécifié sous la forme d'une plage d'adresses IP

Boutons de commande

- ***Ajouter un réseau*** - ouvre la boîte de dialogue ***Propriétés du réseau***dans laquelle vous ajustez les paramètres du réseau nouvellement défini :



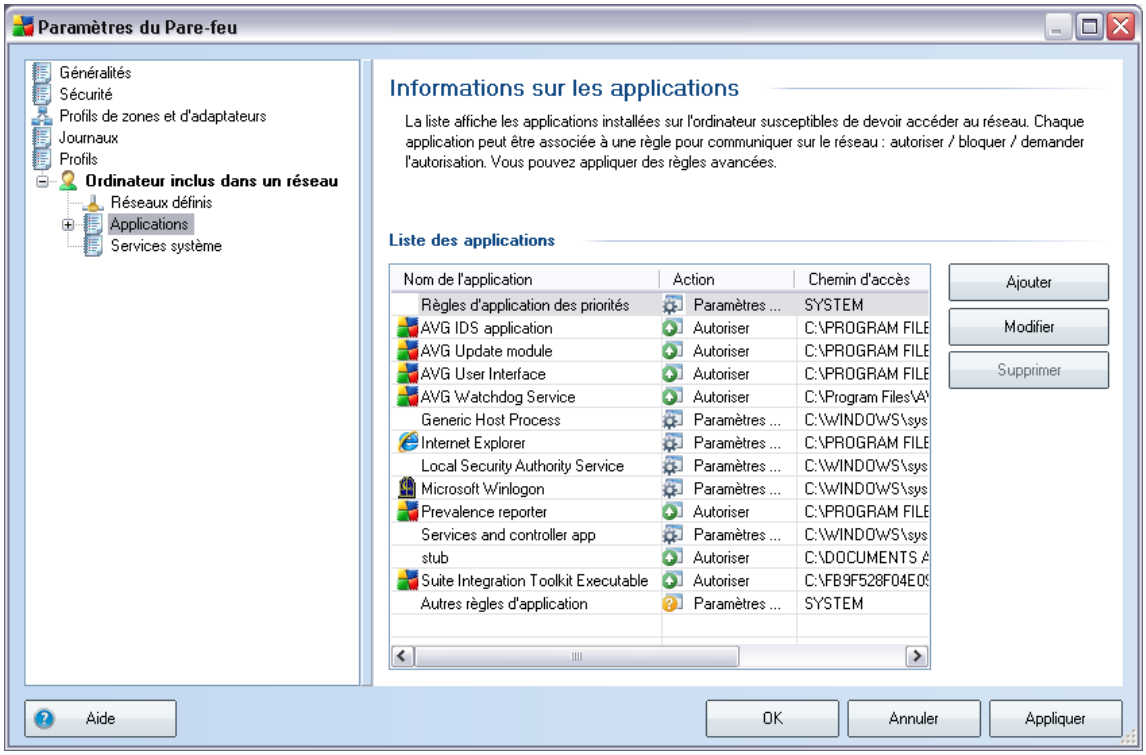
Dans cette boîte de dialogue, précisez le nom du réseau (champ ***Nom du réseau***), décrivez-le dans le champ ***Description du réseau***, puis indiquez s'il s'agit d'un réseau sécurisé. Le nouveau réseau peut être défini manuellement dans une boîte de dialogue distincte après avoir cliqué sur le bouton ***Ajouter IP*** (ou ***Modifier IP*** / ***Supprimer IP***). Dans cette boîte de dialogue, vous spécifiez le réseau en indiquant une plage d'adresses IP ou un masque réseau.

Pour un réseau étendu à intégrer au réseau actuel que vous venez de définir, vous pouvez utiliser l'option ***Représentation avancée de la plage des adresses IP*** : saisissez la liste intégrale des réseaux dans le champ de texte prévu à cet effet (*tous les formats standards sont pris en charge*), puis cliquez sur le bouton ***Vérifier*** pour vous assurer que le

format est effectivement reconnu. Cliquez ensuite sur ***OK*** pour valider et enregistrer les données.

- ***Modifier un réseau*** - ouvre la boîte de dialogue ***Propriétés du réseau*** (*voir ci-dessus*) dans laquelle vous pouvez modifier les paramètres d'un réseau déjà défini (*la boîte de dialogue est identique à la boîte de dialogue d'insertion d'un nouveau réseau, décrite au paragraphe précédent*)
- ***Supprimer un réseau*** - ce bouton retire la référence du réseau sélectionné de la liste des réseaux
- ***Marqué comme sécurisé*** - par défaut, tous les réseaux sont considérés comme non sécurisés. Déclarez un réseau comme sécurisé à l'aide de cette option uniquement si vous êtes absolument certain qu'il est fiable.
- ***Aide*** - ouvre le fichier d'aide associé à la boîte de dialogue

10.5.3. Applications

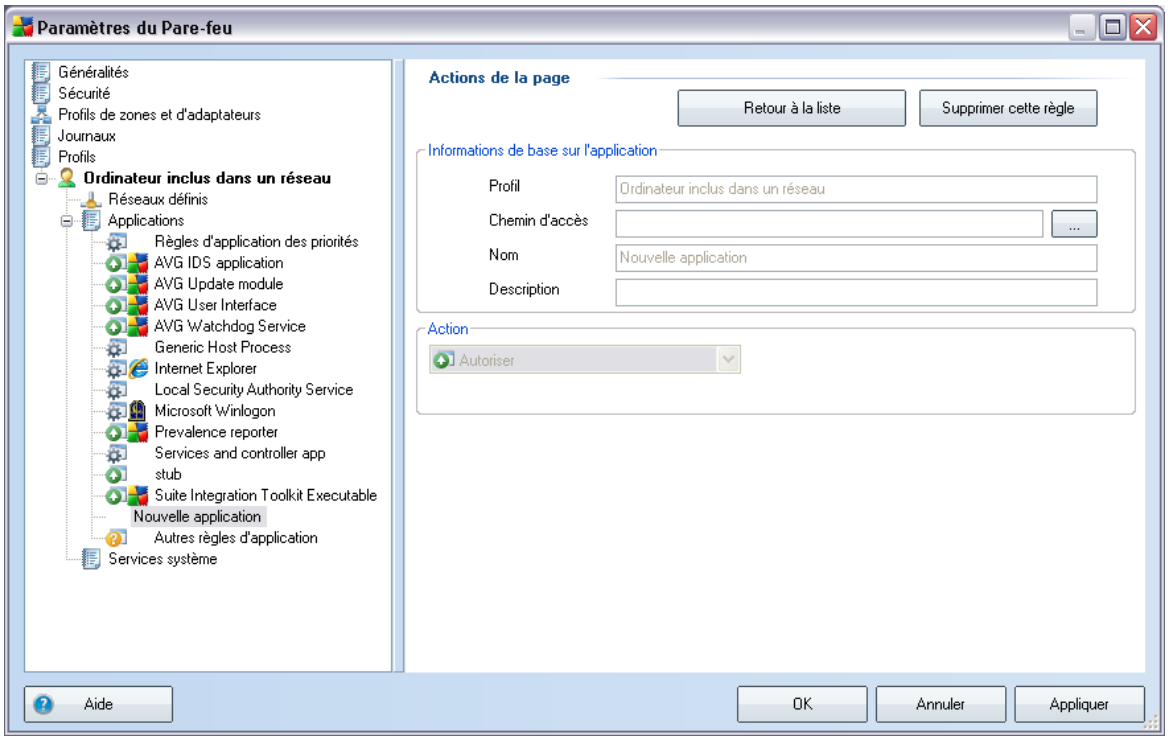


Dans la boîte de dialogue ***Informations sur les applications***, vous obtenez une vue d'ensemble de toutes les applications communiquant sur le réseau. La liste peut être

modifiée à l'aide des boutons suivants :

- ***Ajouter*** - ouvre la boîte de dialogue de définition du jeu de règles d'une nouvelle application
- ***Modifier***- ouvre la boîte de dialogue de modification du jeu de règles d'une application existante
- ***Supprimer*** - retire l'application sélectionnée de la liste
- ***Aide*** - ouvre le fichier d'aide associé à la boîte de dialogue

La boîte de dialogue permettant de définir le jeu de règles d'une nouvelle application s'affiche lorsque vous cliquez sur le bouton ***Ajouter*** de la boîte de dialogue ***Applications***, ***Paramètres du Pare-feu*** :



Dans cette boîte de dialogue, vous pouvez définir les données suivantes :

- ***Informations de base sur l'application*** - nom de l'application, brève

description et chemin d'accès à son emplacement sur le disque

- ***Action*** - dans la liste déroulante, sélectionnez une règle à appliquer au comportement de l'application :

  - ***Paramètres avancés -*** cette option permet de modifier la définition du jeu de règles présenté dans la partie inférieure de la boîte de dialogue *pour obtenir une description de la section, voir le paragraphe sur la* ***modification de l'application***

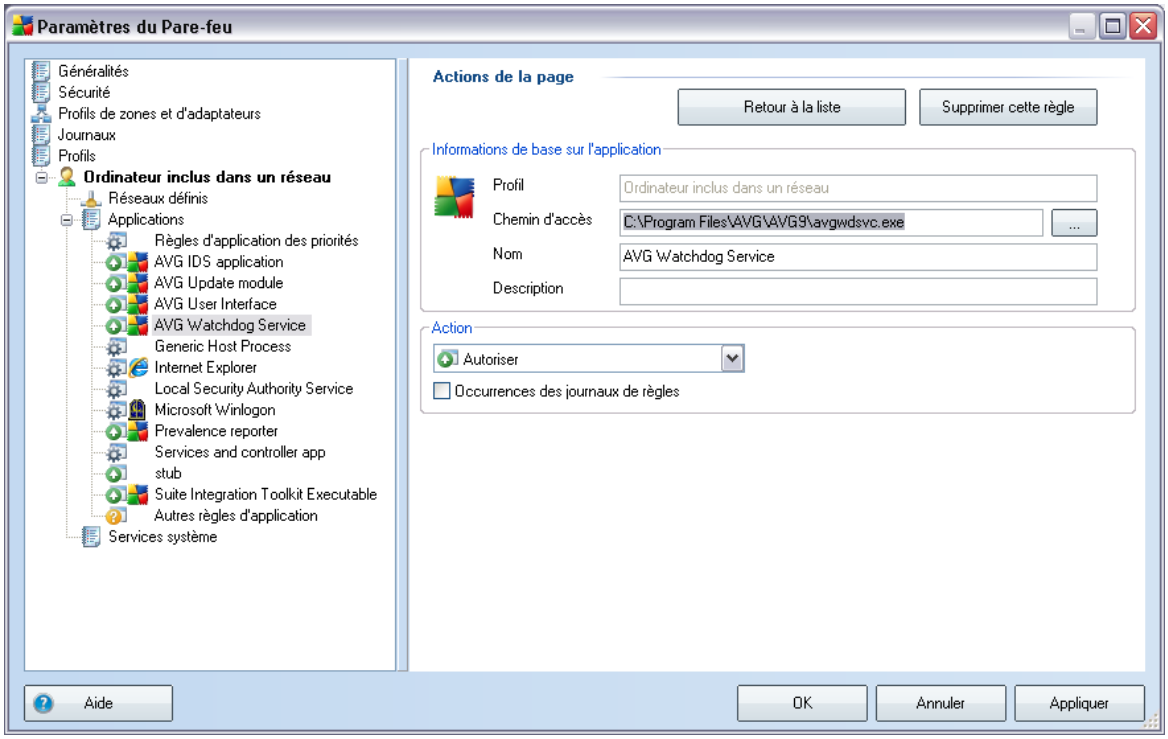
  - ***Autoriser tout -*** toute tentative de communication de l'application sera autorisée.

  - ***Autoriser la connexion sécurisée -*** l'application ne sera autorisée à communiquer que sur les réseaux sécurisés (*par exemple, la communication avec le réseau protégé de la société est autorisée, tandis que les communications via Internet sont bloquées*). Pour une présentation générale et une description des réseaux sécurisés, voir la boîte de dialogue ***Réseaux***

  - ***Demander -*** chaque fois que l'application tente de communiquer sur le réseau, vous serez invité à indiquer si cette communication doit être autorisée ou bloquée

  - ***Bloquer -*** toutes les tentatives de communication de l'application sont bloquées

Pour ouvrir la boîte de dialogue permettant de modifier le jeu de règles d'une application existante, utilisez le bouton ***Modifier*** de la boîte de dialogue ***Applications*** , ***Paramètres du Pare-feu*** :



Dans cette boîte de dialogue, vous pouvez modifier les paramètres de toutes les applications :

- ***Informations de base sur l'application*** - nom de l'application, brève description et chemin d'accès à son emplacement sur le disque
- ***Action*** - dans la liste déroulante, sélectionnez une règle à appliquer au comportement de l'application :
  - ***Paramètres avancés -*** cette option permet de modifier la définition du jeu de règles présenté dans la partie inférieure de la boîte de dialogue
  - ***Autoriser tout -*** toutes les tentatives de communication de l'application sont autorisées.
  - ***Autoriser la connexion sécurisée -*** l'application ne sera autorisée à communiquer que sur les réseaux sécurisés (*par exemple, la communication avec le réseau protégé de la société est autorisée, tandis que les communications via Internet sont bloquées*). Pour une présentation générale et une description des réseaux sécurisés, voir la boîte de dialogue ***Réseaux***

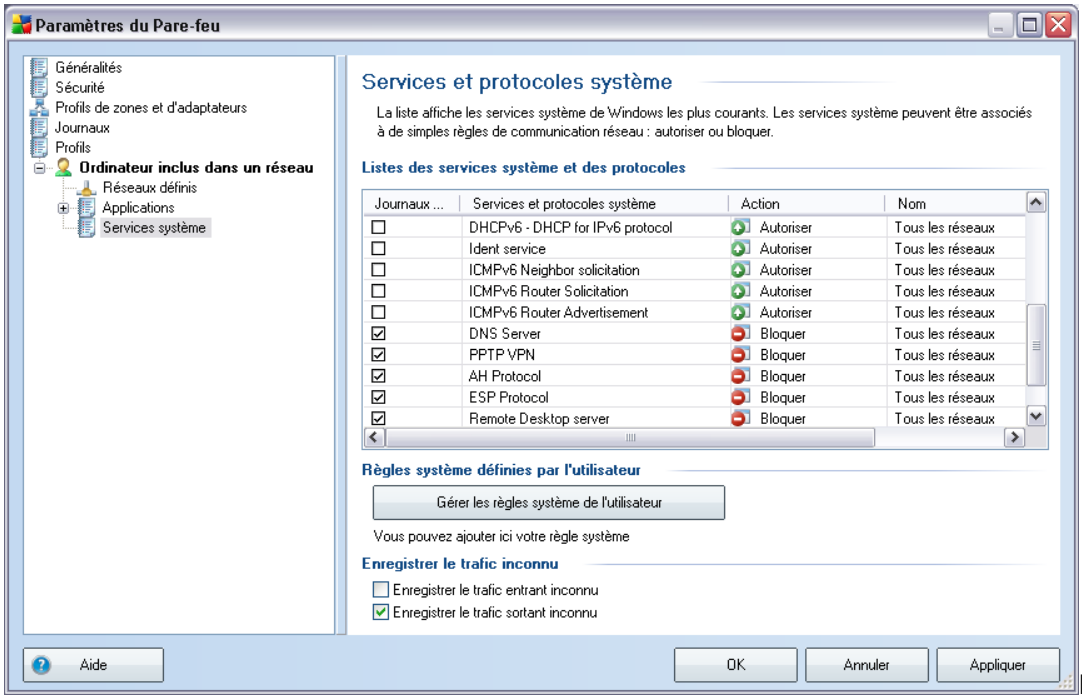
- ***Demander -*** chaque fois que l'application tente de communiquer sur le réseau, vous serez invité à indiquer si cette communication doit être autorisée ou bloquée

- ***Bloquer -*** toutes les tentatives de communication de l'application sont bloquées

- ***Occurrences des journaux de règles*** - cochez cette option pour confirmer votre souhait de consigner dans un journal toutes les actions du ***Pare-feu*** liées à l'application pour laquelle vous avez configuré un ensemble de règles. Les entrées de journal correspondantes se trouvent dans la boîte de dialogue ***Journaux***.

10.5.4. Services système

L'entrée de modifications dans la boîte de dialogue Services et protocoles système ne doit être réservée qu'aux utilisateurs expérimentés !



La boîte de dialogue ***Services et protocoles système*** présente la liste des services et des protocoles du système utilisant le réseau. Sous la liste figurent deux options. Vous pouvez activer ou désactiver ces options pour confirmer votre choix de consigner dans le journal l'ensemble du trafic inconnu (*entrant ou sortant*).

Boutons de commande

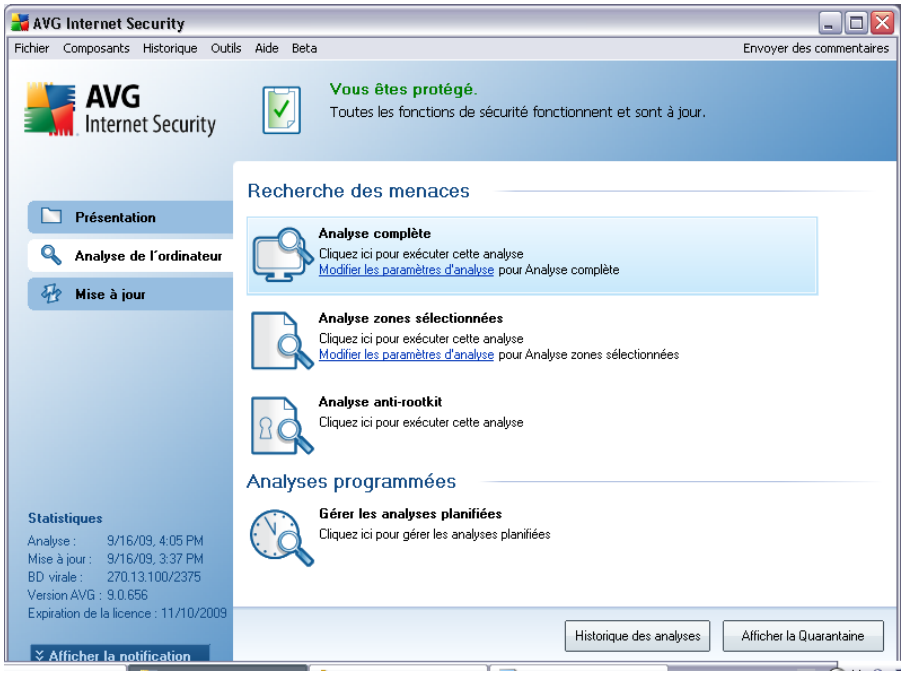
- ***Ajouter / Modifier*** - ces boutons ouvrent la même boîte de dialogue permettant de redéfinir les paramètres des services système. Le bouton ***Ajouter*** ouvre une boîte de dialogue vide et en mode standard (*pas de section pour paramètres avancés, mais cette section est accessible depuis les paramètres avancés de l'action*). Le bouton ***Modifier*** ouvre la même boîte de dialogue mais présente les données déjà saisies concernant le service système sélectionné.

L'entrée de modifications dans la boîte de dialogue Services et protocoles système ne doit être réservée qu'aux utilisateurs expérimentés !

11. Analyse AVG

L'analyse constitue une partie fondamentale de la fonctionnalité d'**AVG 9 Internet Security**. Vous avez la possibilité d'exécuter des analyses à la demande ou de programmer une analyse quotidienne à l'heure qui vous convient le mieux.

11.1. Interface d'analyse



L'interface d'analyse AVG est accessible par ***Analyse de l'ordinateur*** (lien d'accès rapide). Cliquez sur ce lien pour accéder à la boîte de dialogue ***Recherche des menaces***. Dans cette boîte de dialogue, vous trouverez les éléments suivants :

- présentation des analyses prédéfinies - trois types d'analyse (définis par l'éditeur du logiciel) sont prêts à l'emploi sur demande ou par programmation :
    - ***Analyse complète***
    - ***Analyse zones sélectionnées***
    - ***Analyse anti-rootkit***

- programmation de l'analyse - dans cette section, vous définissez de nouvelles analyses et planifiez d'autres programmations selon vos besoins.

Boutons de commande

Les boutons de commande disponibles au sein de l'interface d'analyse sont les suivants :

- ***Historique des analyses*** - affiche la boîte de dialogue Résultats d'analyse relatant l'historique complet des analyses
- ***Afficher la Quarantaine***- ouvre une nouvelle boîte de dialogue intitulée Quarantaine - espace dans lequel les infections sont confinées

11.2. Analyses prédéfinies

Une des principales fonctions d'**AVG 9 Internet Security** est l'analyse à la demande. Ce type d'analyse est prévu pour analyser différentes zones de l'ordinateur en cas de doute concernant la présence éventuelle de virus. Il est vivement recommandé d'effectuer fréquemment de telles analyses même si vous pensez qu'aucun virus ne s'est introduit dans votre système.

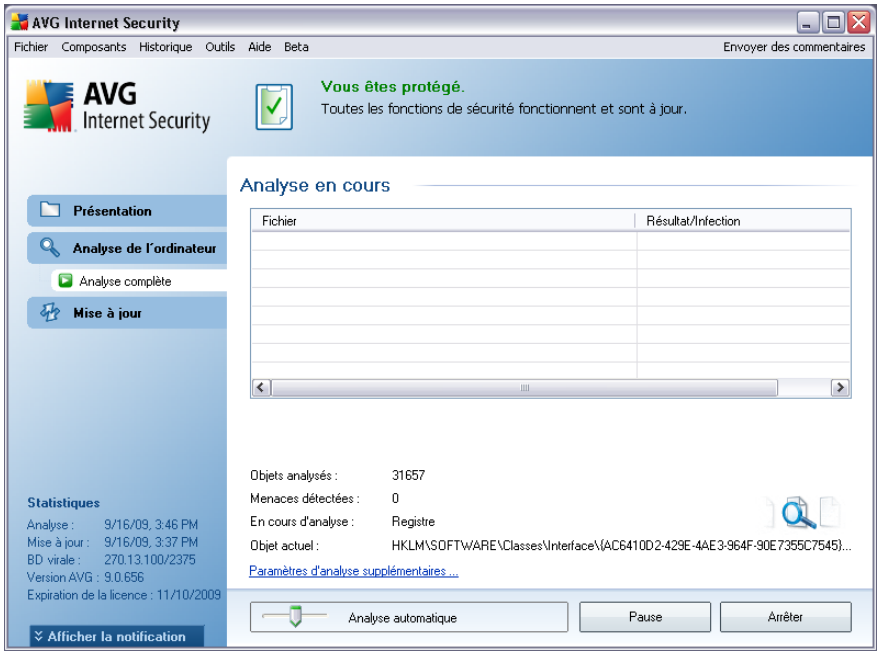
Dans **AVG 9 Internet Security**, vous trouverez deux types d'analyse prédéfinies par l'éditeur du logiciel :

11.2.1. Analyse complète

L'Analyse complète - contrôle l'absence d'infection ainsi que la présence éventuelle de programmes potentiellement dangereux dans tous les fichiers de l'ordinateur. Cette analyse examine les disques durs de l'ordinateur, détecte et répare tout virus ou retire l'infection en la plaçant dans la zone de ***quarantaine***. L'analyse de l'ordinateur doit être exécutée sur un poste de travail au moins une fois par semaine.

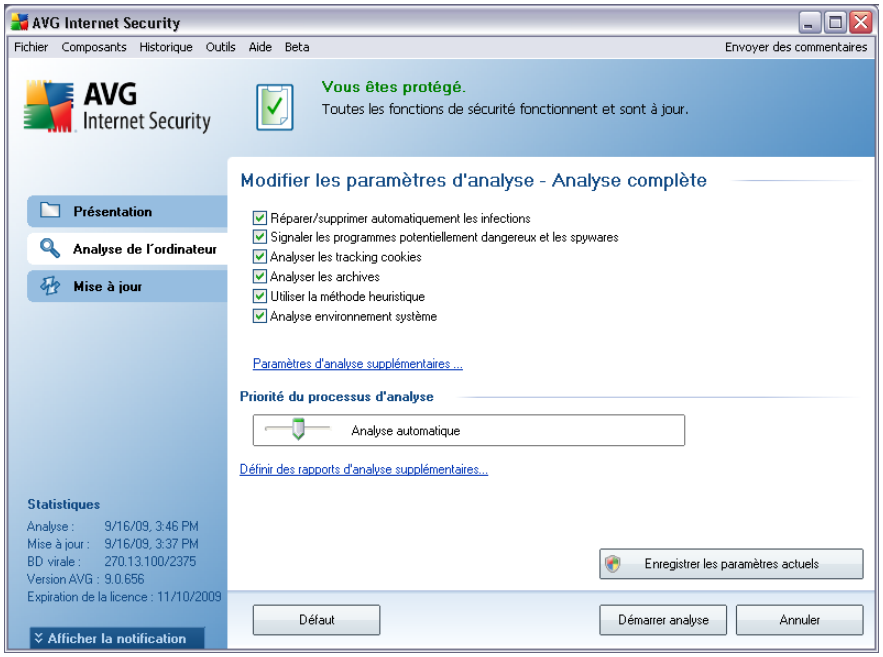
Lancement de l'analyse

L'***Analyse complète*** du contenu d'un ordinateur, peut être lancée directement depuis l'interface d'analyse en cliquant sur l'icône de balayage. Pour ce type d'analyse, il n'est pas nécessaire de configurer d'autres paramètres spécifiques. L'analyse démarre immédiatement dans la boîte de dialogue ***Analyse en cours*** (*voir la capture d'écran*). L'analyse peut être interrompue provisoirement (***Pause***) ou annulée (***Arrêter***) si nécessaire.



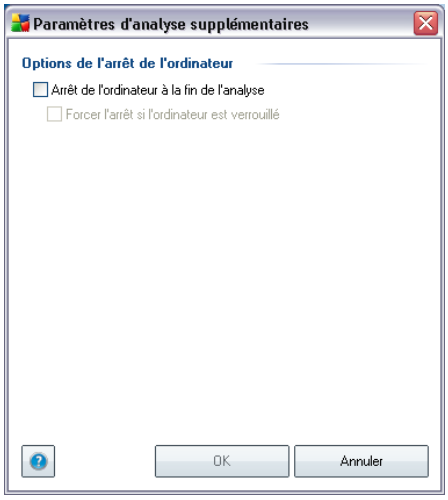
Modification de la configuration de l'analyse

Vous avez la possibilité d'ajuster les paramètres prédéfinis par défaut de l'option ***Analyse complète***. Activez le lien ***Modifier les paramètres d'analyse*** pour accéder à la boîte de dialogue ***Modifier les paramètres d'analyse - Analyse complète***. ***Il est recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité.***



- ***Paramètres d'analyse*** - dans la liste des paramètres d'analyse, vous pouvez activer/désactiver des paramètres spécifiques en fonction de vos besoins. Par défaut, la plupart des paramètres sont activés et seront appliqués automatiquement au cours de l'analyse.

- ***Paramètres d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Paramètres d'analyse supplémentaires*** permettant de spécifier les paramètres suivants :



- ***Options d'arrêt de l'ordinateur*** - indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Une fois l'option ***Arrêt de l'ordinateur à la fin de l'analyse*** confirmée, l'option ***Forcer l'arrêt si l'ordinateur est verrouillé*** s'active et vous permet d'arrêter l'ordinateur même s'il est verrouillé.

- ***Définir les types de fichiers à analyser*** - vous devez également choisir d'analyser :

  - ***Tous les types de fichier*** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers (séparées par des virgules) à ne pas analyser ; ou

  - ***Types de fichier sélectionnés*** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'infection ne sont pas analysés ; il s'agit par exemple de fichiers de texte brut ou de certains types de fichier non exécutables*), notamment les fichiers multimédia (*vidéo, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par des virus.*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.

  - Vous pouvez également choisir l'option ***Analyser les fichiers sans extension*** - cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent

toujours faire l'objet d'une analyse.

- ***Priorité du processus d'analyse*** - le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, le niveau de priorité attribué est moyen (*Analyse automatique*), qui applique le meilleur compromis entre le processus d'analyse et l'utilisation des ressources système. Vous pouvez aussi choisir le processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse)*) ; ou rapide, qui utilise plus de ressources système (*convient notamment quand vous quittez temporairement votre poste de travail*).

- ***Définir des rapports d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Rapports d'analyse*** qui permet de sélectionner les types de résultats à signaler :

Avertissement : *ces paramètres d'analyse sont identiques à ceux d'une nouvelle analyse, comme indiqué dans le chapitre* ***AVG Analyse / Programmation de l'analyse / Comment faire l'analyse****. Si vous décidez de modifier la configuration par défaut de l'****Analyse complète****, vous avez la possibilité d'enregistrer ces nouveaux paramètres en tant que configuration par défaut et de les appliquer à toute analyse complète de l'ordinateur.*

11.2.2. Analyse zones sélectionnées

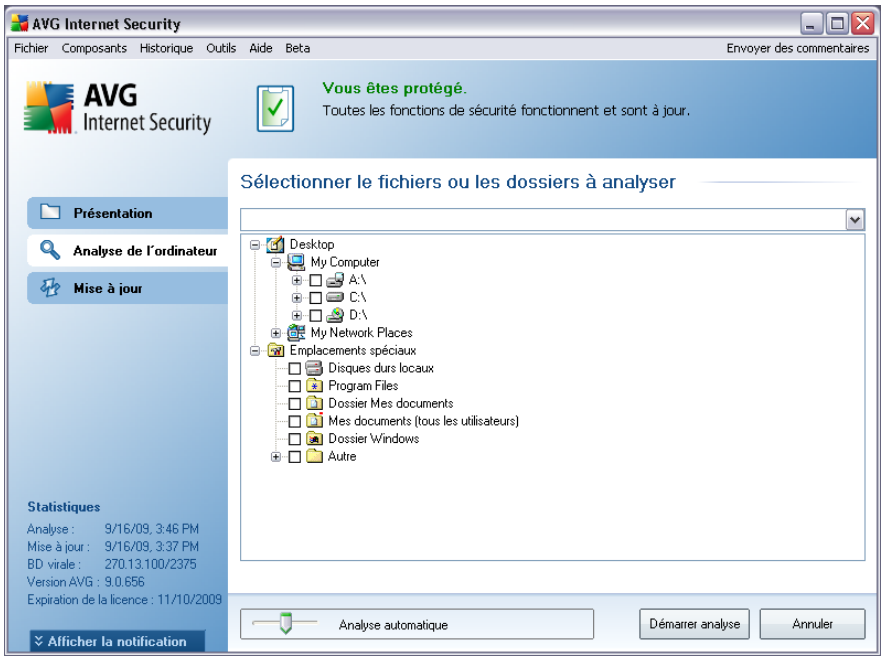
Analyse zones sélectionnées - analyse seulement les zones de l'ordinateur que vous avez sélectionnées en vue d'une analyse (*dossiers, disque durs, disquettes, CD, etc.)*). Le déroulement de l'analyse en cas de détection virale, ainsi que la solution appliquée, est le même que pour une analyse complète de l'ordinateur ***: tout virus détecté est réparé ou déplacé en quarantaine***. L'analyse zones sélectionnées permet de configurer vos propres analyses et de les programmer en fonction de vos besoins.

Lancement de l'analyse

L'***analyse zones sélectionnées***peut être lancée directement depuis l'interface d'analyse en cliquant sur l'icône associée. La boîte de dialogue ***Sélectionner les fichiers ou les dossiers à examiner***s'ouvre. Dans l'arborescence de votre ordinateur, sélectionnez les dossiers que vous souhaitez analyser. Le chemin d'accès à chaque dossier sélectionné est généré automatiquement et apparaît dans la zone de texte située dans la partie supérieure de la boîte de dialogue.

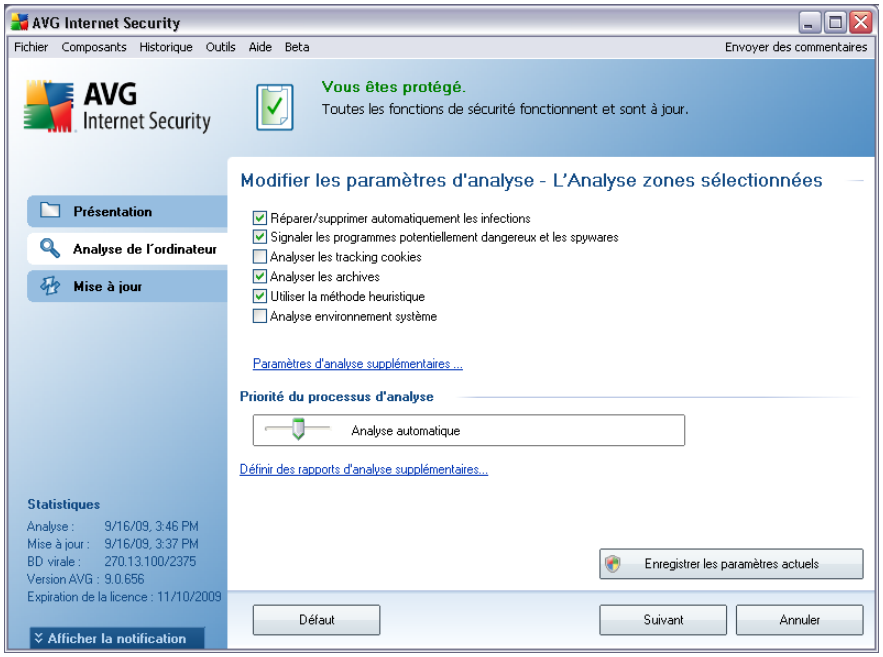
Il est aussi possible d'analyser un dossier spécifique et d'exclure tous ses sous-dossiers du processus. Pour ce faire, il suffit d'insérer le signe moins "**-**" avant le chemin d'accès généré automatiquement (*voir la capture d'écran*). Pour exclure un dossier complet de l'analyse, utilisez le paramètre la case "!" paramètre.

Pour exécuter l'analyse, cliquez sur le bouton ***Démarrer l'analyse*** ; le processus est fondamentalement identique à celui d'une analyse complète de l'ordinateur.



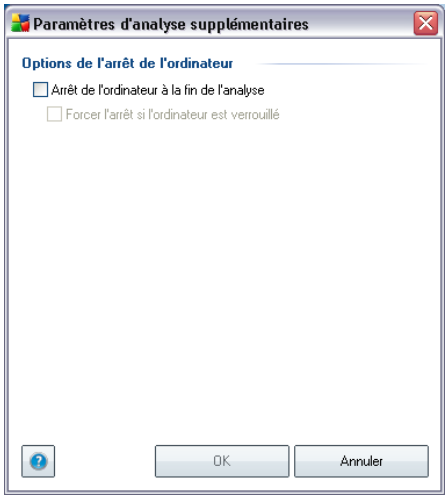
Modification de la configuration de l'analyse

Vous pouvez modifier les paramètres prédéfinis par défaut de l'option ***Analyse zones sélectionnées***. Activez le lien ***Modifier les paramètres d'analyse*** pour accéder à la boîte de dialogue ***Modifier les paramètres d'analyse - Analyse zones sélectionnées***. ***Il est toutefois recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité.***



- ***Paramètres de l'analyse*** - dans la liste des paramètres de l'analyse, vous pouvez activer/désactiver des paramètres spécifiques en fonction de vos besoins *(pour une description détaillée de ces paramètres, consultez le chapitre Paramètres avancés AVG/ Analyses / Analyses zones sélectionnées)*.

- ***Paramètres d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue Paramètres d'analyse supplémentaires permettant de spécifier les paramètres suivants :



- ***Options de l'arrêt de l'ordinateur*** - indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Une fois l'option ***Arrêt de l'ordinateur à la fin de l'analyse*** confirmée, l'option ***Forcer l'arrêt si l'ordinateur est verrouillé*** s'active et vous permet d'arrêter l'ordinateur même s'il est verrouillé.

- ***Définir les types de fichier à analyser*** - Ensuite, vous pouvez choisir d'analyser :

  - ***Tous les types de fichier*** avec la possibilité de définir les éléments à ne pas inclure dans l'analyse en dressant une liste d'extensions de fichiers séparées par des virgules et exclues de l'analyse ; ou les

  - ***Types de fichier sélectionnés*** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'infection ne sont pas analysés ; il s'agit par exemple de fichiers de texte brut ou de certains types de fichier non exécutables*), y compris les fichiers média (*video, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par des virus.*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.

  - Vous pouvez également choisir l'option ***Analyser les fichiers sans extension*** - celle-ci est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent

toujours faire l'objet d'une analyse.

- ***Priorité du processus d'analyse*** - le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, le niveau de priorité attribué est moyen (*Analyse automatique*), qui applique le meilleur compromis entre le processus d'analyse et l'utilisation des ressources système. Vous pouvez aussi choisir le processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse)*) ; ou rapide, qui utilise plus de ressources système (*convient notamment quand vous quittez temporairement votre poste de travail*).

- ***Définir des rapports d'analyse supplémentaires*** - ce lien ouvre la boîte de dialogue ***Rapports d'analyse*** où vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :

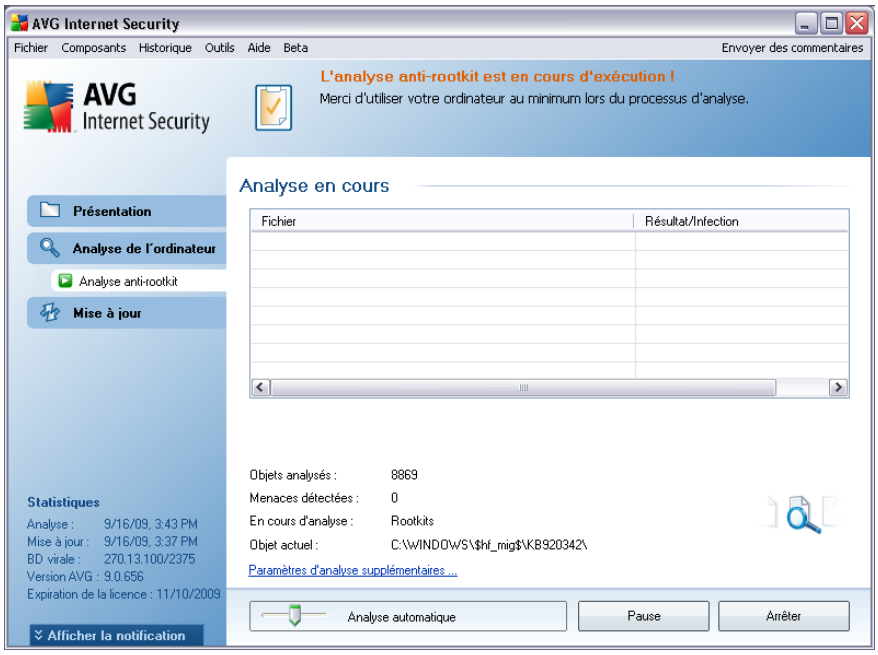
Avertissement : *ces paramètres d'analyse sont identiques à ceux d'une nouvelle analyse, comme indiqué dans le chapitre* ***AVG Analyse / Programmation de l'analyse / Comment faire l'analyse****. Si vous décidez de modifier la configuration* ***Analyse zones sélectionnées*** *par défaut, vous pouvez enregistrer les paramètres modifiés en tant que configuration par défaut et les appliquer aux analyses ultérieures de fichiers ou de dossiers spécifiques. De plus, cette configuration sera utilisée comme modèle des nouvelles analyses programmées (toutes les analyses personnalisées basées sur la configuration actuelle de l'analyse des zones sélectionnées).*

11.2.3. Analyse Anti-Rootkit

L'analyse anti-rootkit permet de vérifier si votre ordinateur contient des rootkits (*programmes et technologies destinés à cacher l'activité de programmes malveillants sur l'ordinateur*). Si un rootkit est détecté, cela ne veut pas forcément dire que votre ordinateur est infecté. Dans certains cas, des pilotes spécifiques ou des sections d'applications régulières peuvent être considérés, à tort, comme des rootkits.

Lancement de l'analyse

L'analyse anti-rootkit peut être lancée directement depuis l'interface d'analyse en cliquant sur l'icône d'analyse. Pour ce type d'analyse, il n'est pas nécessaire de configurer d'autres paramètres spécifiques. L'analyse démarre immédiatement dans la boîte de dialogue ***Analyse en cours*** (*voir la capture d'écran*). L'analyse peut être interrompue provisoirement (***Interrompre***) ou annulée (***Arrêter***) si nécessaire.

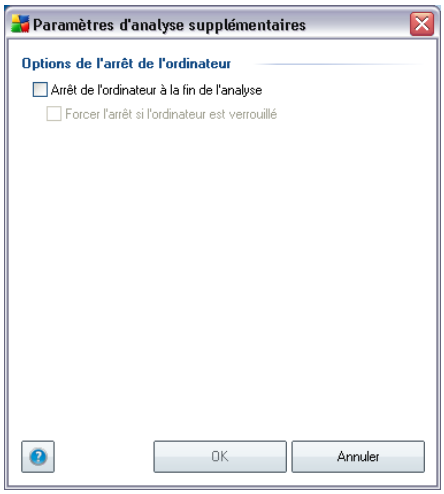


Modification de la configuration de l'analyse

L'analyse anti-rootkit est toujours lancée avec les paramètres par défaut et les paramètres d'analyse ne peuvent être modifiés que dans la boîte de dialogue ***Paramètres avancés d'AVG / Anti-Rootkit***. Dans l'interface d'analyse, seule la configuration suivante est disponible :

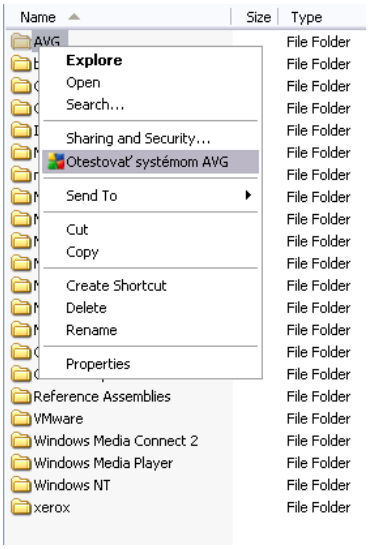
- ***Analyse automatique*** - le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, le niveau de priorité attribué est moyen (*Analyse automatique*), qui applique le meilleur compromis entre le processus d'analyse et l'utilisation des ressources système. Vous pouvez aussi choisir le processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse)*) ; ou rapide, qui utilise plus de ressources système (*convient notamment quand vous quittez temporairement votre poste de travail*).

- ***Paramètres d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Paramètres d'analyse supplémentaires*** où vous pouvez définir les conditions de l'arrêt de l'ordinateur relatives à l'***analyse anti-rootkit*** (***Arrêt de l'ordinateur à la fin de l'analyse*** *ou éventuellement* ***Forcer l'arrêt si l'ordinateur est verrouillé***) :



11.3. Analyse contextuelle

Outre les analyses prédéfinies et exécutées sur l'ensemble de l'ordinateur ou sur des zones sélectionnées, **AVG 9 Internet Security** permet d'analyser rapidement l'objet de votre choix dans l'environnement de l'Explorateur Windows. Si vous désirez ouvrir un fichier inconnu dont le contenu est incertain, vous pouvez le vérifier à la demande. Procédez comme suit :



- Dans l'Explorateur Windows, mettez le fichier (ou le dossier) en surbrillance
- Cliquez avec le bouton droit de la souris sur l'objet pour afficher le menu contextuel
- Choisissez la commande ***Analyse par AVG*** pour faire analyser le fichier par AVG

11.4. Analyse depuis la ligne de commande

Dans **AVG 9 Internet Security**, il est possible de lancer l'analyse depuis la ligne de commande. Vous apprécierez cette possibilité sur les serveurs, par exemple, ou lors de la création d'un script de commandes qui doit s'exécuter automatiquement après l'initialisation de l'ordinateur. La plupart des paramètres proposés dans l'interface utilisateur graphique sont disponibles à partir de la ligne de commande.

Pour lancer l'analyse AVG depuis la ligne de commande, exécutez la commande suivante depuis le dossier où AVG est installé :

- ***avgscanx*** pour un système d'exploitation 32 bits
- ***avgscana*** pour un système d'exploitation 64 bits

Syntaxe de la commande

La syntaxe de la commande est la suivante :

- ***avgscanx /paramètre***... par exemple, ***avgscanx /comp*** pour l'analyse complète de l'ordinateur
- ***avgscanx /paramètre /paramètre*** .. si plusieurs paramètres sont précisés, les entrer à la suite, séparés par un espace et une barre oblique
- si un paramètre requiert la saisie de valeurs spécifiques (par exemple, le paramètre ***/scan*** requiert de savoir quelles zones de votre ordinateur ont été sélectionnées afin d'être analysées et vous devez indiquer un chemin exact vers la section sélectionnée), il faut séparer les valeurs éventuelles par une virgule, par exemple : ***avgscanx /scan=C:\,D:***

Emplacement des fichiers à vérifier

Pour afficher la liste complète des paramètres disponibles, tapez la commande concernée ainsi que le paramètre /? ou /HELP (ex : ***avgscanx /?***). Le seul paramètre obligatoire est /SCAN pour lequel il est nécessaire de spécifier les zones de l'ordinateur à analyser. Pour une description détaillée des options, voir la liste des paramètres de ligne de commande.

Pour exécuter l'analyse, appuyez sur ***Entrée***. Pendant l'analyse, vous pouvez arrêter le processus en appuyant sur ***Ctrl+C*** ou ***Ctrl+Pause***.

Analyse CMD lancée depuis l'interface d'analyse

Lorsque vous exécutez l'ordinateur en mode sans échec de Windows, il est également possible de faire appel à la ligne de commande à partir de l'interface utilisateur graphique. L'analyse à proprement parler sera lancée à partir de la ligne de commande, la boîte de dialogue ***Editeur de ligne de commande*** permet seulement de préciser la plupart des paramètres d'analyse dans l'interface graphique plus conviviale.

Etant donné que cette boîte de dialogue est seulement accessible en mode sans échec de Windows, consultez le fichier d'aide accessible à partir de cette boîte de dialogue si vous avez besoin de renseignements supplémentaires.

11.4.1. Paramètres d'analyse CMD

Vous trouverez ci-après la liste de tous les paramètres disponibles pour lancer une analyse depuis la ligne de commande :

- ***/SCAN*** Analyse de fichiers ou de dossiers spécifiques / SCAN=chemin;chemin (ex. : /SCAN=C:\;D:\)
- ***/COMP*** Analyse complète
- ***/HEUR*** Utiliser l'analyse heuristique
- ***/EXCLUDE*** Fichiers ou chemin exclus de l'analyse
- ***/@*** Fichier de commande /nom du fichier/
- ***/EXT*** Analyser ces extensions /par exemple EXT=EXE,DLL/
- ***/NOEXT*** Ne pas analyser ces extensions /par exemple NOEXT=JPG/
- ***/ARC*** Analyser les archives
- ***/CLEAN*** Nettoyer automatiquement
- ***/TRASH*** Mettre les fichiers en Quarantaine
- ***/QT*** Analyse rapide
- ***/MACROW*** Signaler les macros
- ***/PWDW*** Signaler les fichiers protégés par un mot de passe
- ***/IGNLOCKED*** Ignorer les fichiers verrouillés
- ***/REPORT*** Reporter dans le fichier /nom du fichier/
- ***/REPAPPEND*** Inclure dans le fichier de rapport
- ***/REPOK*** Avertir l'utilisateur des fichiers non infectés
- ***/NOBREAK*** Ne pas autoriser CTRL-PAUSE pour arrêter
- ***/BOOT*** Activer la vérification MBR/BOOT

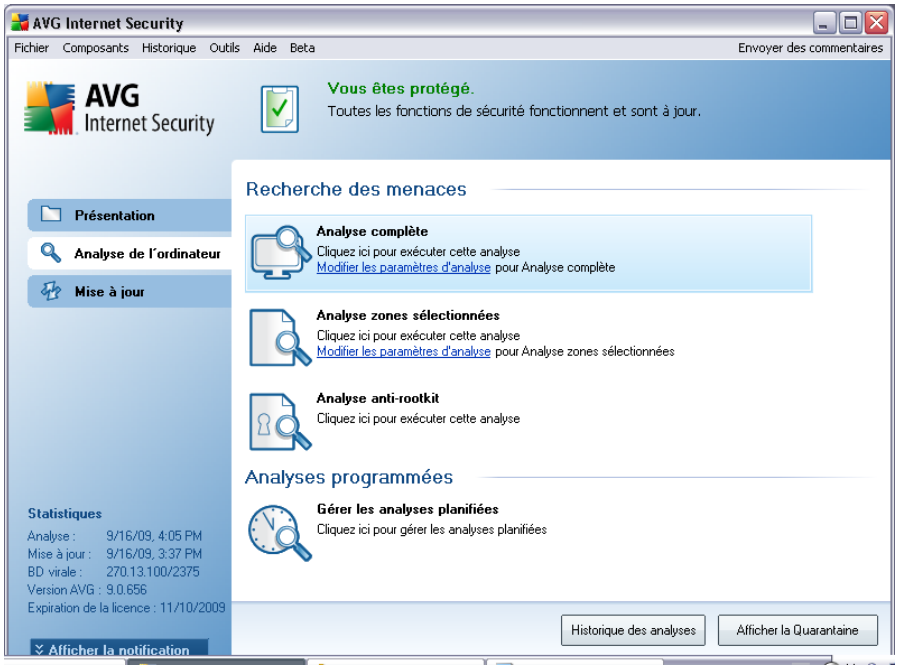
- ***/PROC*** Analyser les processus actifs
- ***/PUP*** Signaler les "programmes potentiellement dangereux"
- ***/REG*** Analyser la base de registre
- ***/COO*** Analyser les cookies
- ***/?*** Affichage de l'aide sur un sujet
- ***/HELP*** Affichage de l'aide sur un sujet
- ***/PRIORITY*** Définir la priorité de l'analyse /Faible, Auto, Elevée (voir Paramètres avancés / Analyses)
- ***/SHUTDOWN*** Arrêt de l'ordinateur à la fin de l'analyse
- ***/FORCESHUTDOWN*** Forcer l'arrêt de l'ordinateur à la fin de l'analyse
- ***/ADS*** Analyser les flux de données NTFS uniquement

11.5. Programmation de l'analyse

Avec **AVG 9 Internet Security**, vous pouvez effectuer une analyse à la demande (par exemple, lorsque vous soupçonnez une infection par un virus dans votre ordinateur) ou selon un programme défini. Il est vivement recommandé d'exécuter des analyses planifiées. Vous serez ainsi assuré que votre ordinateur sera protégé de tout risque d'infection et vous n'aurez plus à vous soucier de la gestion des analyses.

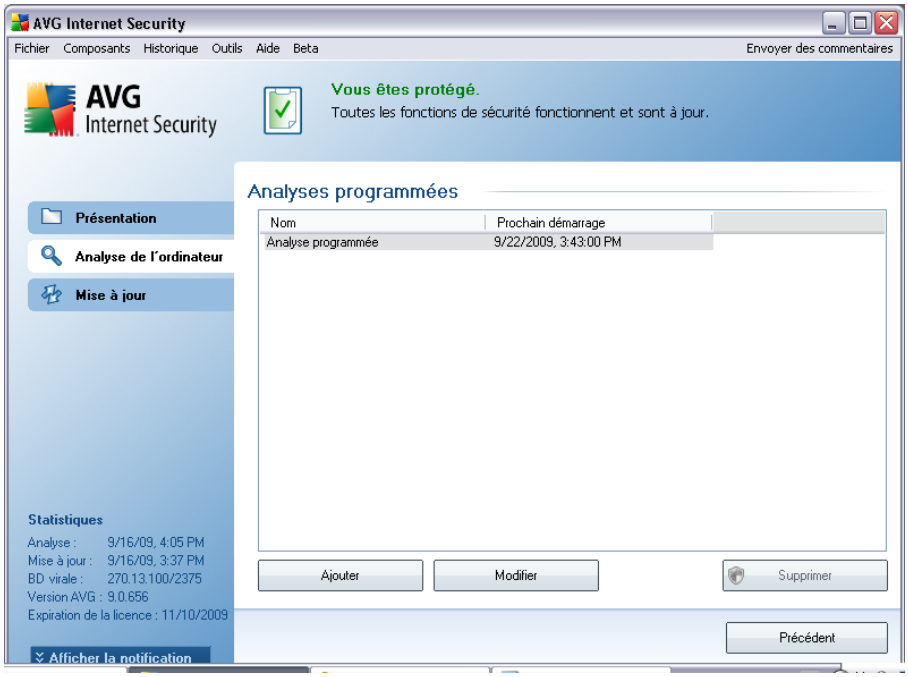
Vous devez effectuer une***Analyse complète*** régulièrement, au moins une fois par semaine. Si possible, faites aussi une analyse complète l'ordinateur une fois par jour, comme configuré par défaut dans la programmation de l'analyse. Si l'ordinateur est toujours sous tension, vous pouvez programmer l'analyse en dehors de vos heures de travail. Si l'ordinateur est parfois hors tension, programmez une analyse au démarrage de l'ordinateur lorsqu'elle n'a pas pu être effectuée.

Pour créer de nouvelles programmations d'analyse, consultez l'interface d'analyse AVG , dans la section du bas, ***Analyses programmées*** :



Analyses programmées

Cliquez sur l'icône située dans la section ***Analyses programmées*** pour ouvrir une nouvelle boîte de dialogue ***Analyses programmées*** présentant une liste de toutes les analyses actuellement programmées :



Vous pouvez modifier / ajouter des analyses à l'aide des boutons de commande suivants :

- ***Ajouter*** - le bouton ouvre la boîte de dialogue ***Paramètres de l'analyse programmée***, onglet ***Paramètres de la programmation***. Dans cette boîte de dialogue, définissez les paramètres de la nouvelle analyse.

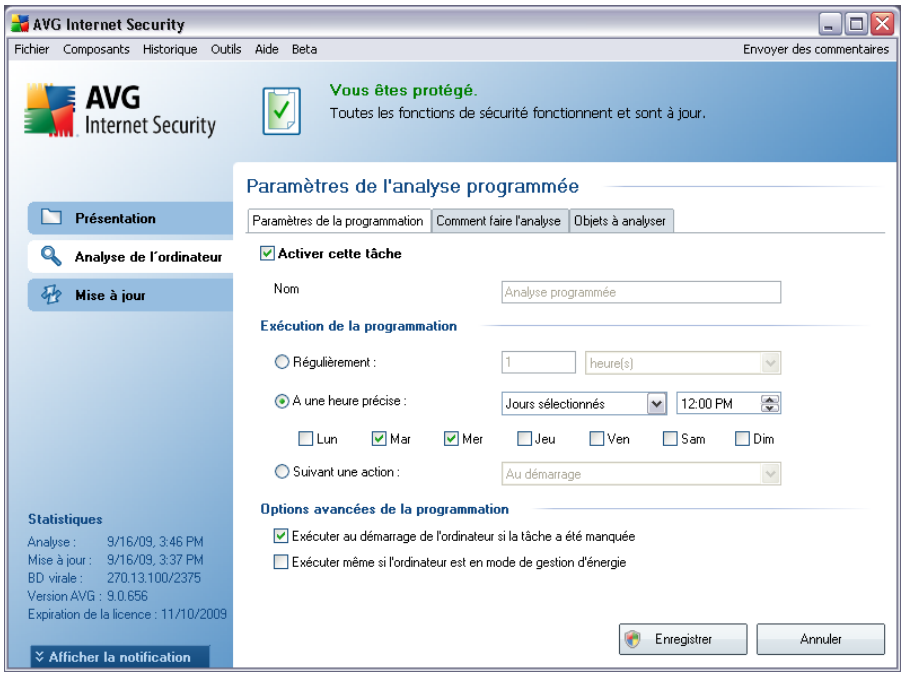
- ***Modifier*** - ce bouton n'est actif que si vous avez déjà sélectionné une analyse existante dans la liste des analyses programmées. Dans ce cas, le bouton est accessible ; il suffit de cliquer dessus pour accéder à la boîte de dialogue ***Paramètres de l'analyse programmée***, onglet ***Paramètres de la programmation***. Les paramètres de l'analyse sélectionnée sont pré-renseignés et peuvent être modifiés.

- ***Supprimer*** - ce bouton est actif si vous avez déjà sélectionné une analyse existante dans la liste des analyses programmées. Cette analyse peut ensuite être supprimée de la liste en cliquant sur ce bouton. Notez néanmoins que vous ne pouvez supprimer que vos propres analyses. Les analyses de type ***Programmation de l'analyse complète de l'ordinateur*** prédéfinies par défaut ne peuvent jamais être supprimées.

- ***Précédent*** - permet de revenir à l'interface d'analyse d'AVG

11.5.1. Paramètres de la programmation

Pour programmer une nouvelle analyse et définir son exécution régulière, ouvrez la boîte de dialogue ***Paramètres de l'analyse programmée*** (*cliquez sur le bouton* ***Ajouter une programmation de l'analyse*** *situé dans la boîte de dialogue* ***Analyses programmées***). Cette boîte de dialogue comporte trois onglets : ***Paramètres de la programmation*** - *voir l'illustration ci-dessous* (*il s'agit de l'onglet qui s'affiche par défaut et de façon automatique à l'ouverture de la boîte de dialogue*), ***Paramètres de l'analyse*** et ***Objets à analyser***.



Dans l'onglet ***Paramètres de la programmation***, vous pouvez cocher/décocher la case ***Activer cette tâche*** pour désactiver temporairement l'analyse programmée et la réactiver au moment opportun.

Donnez ensuite un nom à l'analyse que vous voulez créer et programmer. Saisissez le nom dans la zone de texte figurant à côté de l'option ***Nom***. Veillez à utiliser des noms courts, descriptifs et appropriés pour distinguer facilement les différentes analyses par la suite.

Exemple : *il n'est pas judicieux d'appeler l'analyse "Nouvelle analyse" ou "Mon analyse", car ces noms ne font pas référence au champ réel de l'analyse. A l'inverse, "Analyse des zones système" est un nom descriptif précis. Il est également nécessaire de spécifier dans le nom de l'analyse si l'analyse concerne l'ensemble de l'ordinateur*

ou une sélection de fichiers ou de dossiers. Notez que les analyses personnalisées sont toujours basées sur l'Analyse zones sélectionnés.

Dans cette boîte de dialogue, vous définissez encore plus précisément les paramètres de l'analyse :

- ***Exécution de la programmation*** - spécifiez l'intervalle entre chaque exécution de la nouvelle analyse. Il est possible de répéter le lancement de l'analyse après un laps de temps donné (***Régulièrement***), d'en définir la date et l'heure précises (***A une heure précise***) ou encore de définir l'évènement auquel sera associé le lancement de l'analyse (***Suivant une action***).

- ***Options avancées de la programmation*** - cette section permet de définir dans quelles conditions l'analyse doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

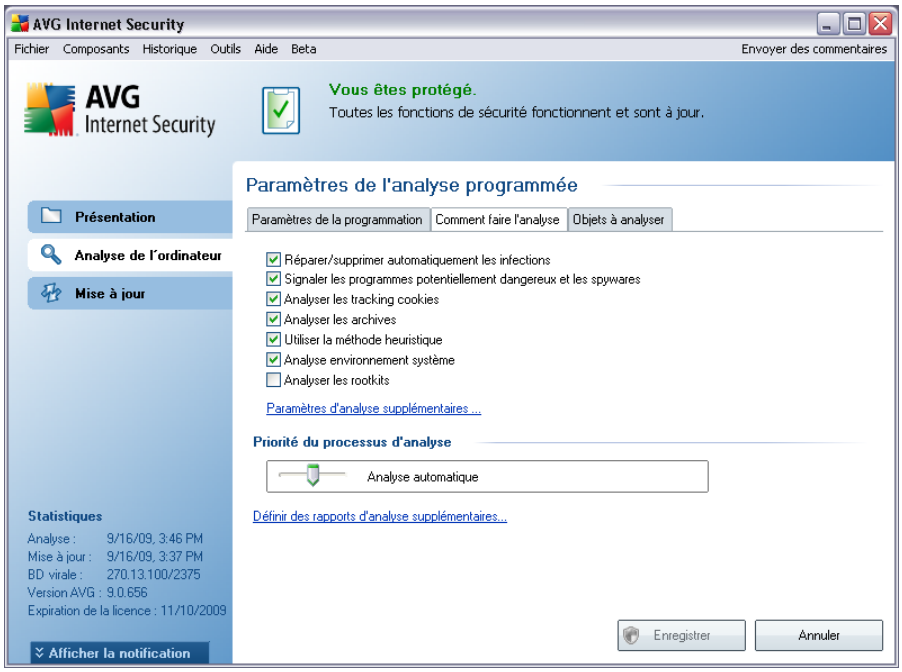
Boutons de commande de la boîte de dialogue Paramètres de l'analyse programmée

Deux boutons de commande figurent sur les trois onglets de la boîte de dialogue ***Paramètres de l'analyse programmée*** (***Paramètres de la programmation***, ***Paramètres de l'analyse*** et ***Objets à analyser***). Ils ont la même fonctionnalité :

- ***Enregistrer*** - enregistre toutes les modifications apportées dans l'onglet courant ou dans un autre onglet de cette boîte de dialogue et revient à la boîte de dialogue par défaut de l'interface d'analyse AVG. Par conséquent, si vous voulez configurer les paramètres d'analyse répartis sous tous les onglets, cliquez sur ce bouton uniquement après avoir défini tous vos choix.

- ***Annuler*** - annule toutes les modifications entrées sous l'onglet actif ou un autre onglet de cette boîte de dialogue et affiche la boîte de dialogue par défaut de l'interface d'analyse AVG.

11.5.2. Comment faire l'analyse



Sous l'onglet ***Comment faire l'analyse***, vous trouverez une liste de paramètres d'analyse qui peuvent être activés ou désactivés. Par défaut, la plupart des paramètres sont activés et appliqués lors de l'analyse. Aussi est-il recommandé de ne pas modifier la configuration prédéfinie d'AVG sans motif valable:

- ***Réparer/supprimer automatiquement les infections*** – (*option activée par défaut*) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement si une solution le permet . Si la désinfection automatique du fichier n'est pas possible (ou si cette option est désactivée), un message de détection de virus s'affiche. Il vous appartient alors de déterminer le traitement à appliquer à l'infection. L'action recommandée consiste à confiner le fichier infecté en ***quarantaine***.

- ***Signaler les programmes potentiellement dangereux et les spywares*** - (*option activée par défaut*) : ce paramètre contrôle la fonctionnalité ***Anti-Virus*** qui détecte les programmes potentiellement dangereux (*fichiers exécutables fonctionnant comme des spywares ou des adwares*) afin de les bloquer ou de les supprimer.

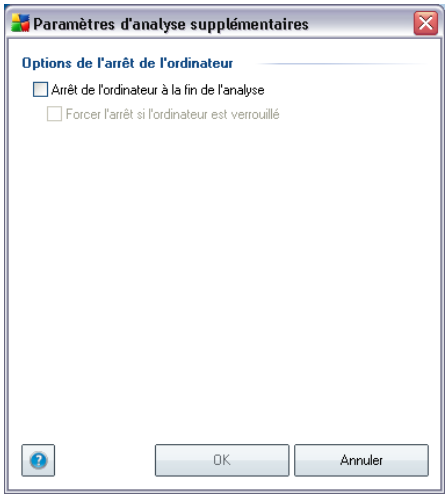
- ***Analyser les tracking Cookies*** - (*option activée par défaut*) : ce paramètre du composant ***Anti-Spyware*** définit les cookies qui pourront être détectés au

cours de l'analyse (*les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leurs paniers d'achat électronique*).

- ***Analyser les archives*** - (*option activée par défaut*) :ce paramètre indique que l'analyse doit examiner tous les fichiers, même ceux comprimés dans certains types d'archives (archives ZIP ou RAR, par exemple).
- ***Utiliser la méthode heuristique*** - (*option activée par défaut*) : l'analyse heuristique (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*) est l'une des méthodes employées pour détecter des virus pendant l'analyse.
- ***Analyser environnement système*** - (*option activée par défaut*) : l'analyse vérifie les fichiers système de l'ordinateur.
- ***Analyser les rootkits*** – cochez cette option si vous souhaitez inclure la détection de rootkits dans l'analyse complète de l'ordinateur. La détection seule de rootkits est aussi proposée dans le composant ***Anti-Rootkit;***

Ensuite, vous pouvez modifier les paramètres de l'analyse en procédant comme suit :

- ***Paramètres d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Paramètres d'analyse supplémentaires*** permettant de spécifier les paramètres suivants :



  - ***Options de l'arrêt de l'ordinateur*** - indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Une fois

l'option ***Arrêt de l'ordinateur à la fin de l'analyse*** confirmée, l'option ***Forcer l'arrêt si l'ordinateur est verrouillé*** s'active et vous permet d'arrêter l'ordinateur même s'il est verrouillé.

- ***Définir les types de fichier à analyser*** - ensuite, vous pouvez choisir d'analyser :
  - ***Tous les types de fichier*** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers (séparées par des virgules) à ne pas analyser ; ou les
  - ***Types de fichier sélectionnés*** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers média (*video, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par des virus.*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.
  - Vous pouvez également choisir l'option ***Analyser les fichiers sans extension*** - celle-ci est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.

- ***Priorité du processus d'analyse*** - le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, le niveau de priorité attribué est moyen (*Analyse automatique*), qui applique le meilleur compromis entre le processus d'analyse et l'utilisation des ressources système. Vous pouvez aussi choisir le processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse)*) ; ou rapide, qui utilise plus de ressources système (*convient notamment quand vous quittez temporairement votre poste de travail*).

- ***Définir des rapports d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Rapports d'analyse***, où vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :

Remarque : *par défaut, l'analyse est configurée pour bénéficier de performances optimales. Sauf raison valable, il est fortement conseillé de conserver la configuration telle qu'elle est prédéfinie. Seuls les utilisateurs expérimentés peuvent modifier la configuration. Pour accéder à d'autres options de configuration de l'analyse, consultez la boîte de dialogue* ***Paramètres avancés*** *accessible par la commande du menu système* ***Outils/ Paramètres avancés****.*

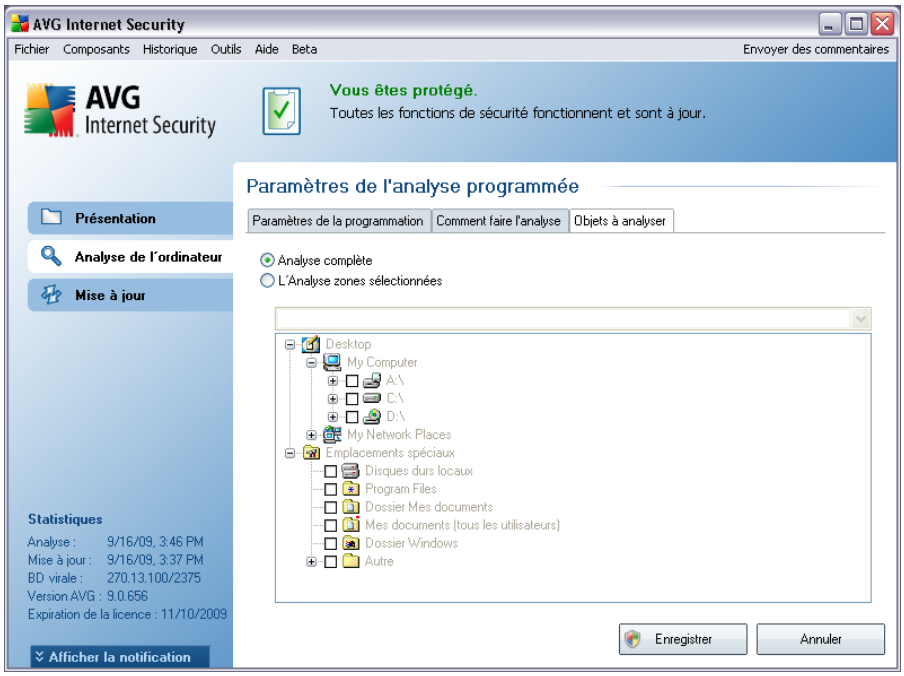
Boutons de commande

Deux boutons de commande sont proposés sous les trois onglets de la boîte de dialogue ***Paramètres de l'analyse programmée*** (***Paramètres de la programmation***, ***Comment faire l'analyse*** et ***Objets à analyser***). Ils ont la même fonctionnalité :

- ***Enregistrer*** - enregistre toutes les modifications entrées sous cet onglet ou un autre onglet de cette boîte de dialogue et affiche la boîte de dialogue par défaut de l'interface d'analyse AVG. Par conséquent, si vous voulez configurer les paramètres d'analyse répartis dans tous les onglets, cliquez sur ce bouton uniquement après avoir défini tous vos choix.

- ***Annuler*** - annule toutes les modifications faites dans l'onglet actif ou un autre onglet de cette boîte de dialogue et affiche la boîte de dialogue par défaut de l'interface d'analyse AVG.

11.5.3. Objets à analyser



Sous l'onglet ***Objets à analyser***, indiquez si vous voulez programmer l'analyse complète de l'ordinateur ou l'analyse de fichiers ou de dossiers spécifiques. Si vous optez pour la deuxième solution, la structure de l'arborescence affichée dans la partie inférieure de la boîte de dialogue devient active et permet de définir les dossiers qui vous intéressent.

Boutons de commande de la boîte de dialogue Paramètres de l'analyse programmée

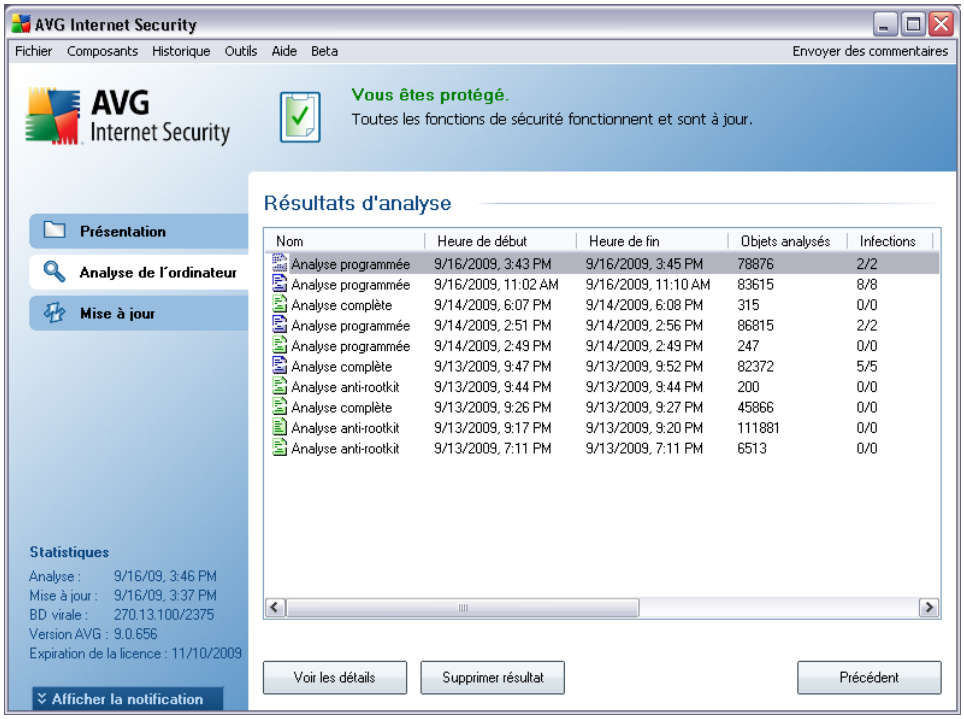
Deux boutons de commande figurent sur les trois onglets de la boîte de dialogue ***Paramètres de l'analyse programmée*** (***Paramètres de la programmation***, ***Comment faire l'analyse et*** Objets à analyser). Ils ont la même fonctionnalité :

- ***Enregistrer*** - enregistre toutes les modifications entrées sous l'onglet en cours ou un autre onglet de cette boîte de dialogue et affiche la boîte de dialogue par défaut de l'interface d'analyse AVG. Par conséquent, si vous voulez configurer les paramètres d'analyse répartis sous tous les onglets, cliquez sur ce bouton uniquement après avoir défini tous vos choix.

- ***Annuler*** - annule toutes les modifications entrées sous l'onglet actif ou un

autre onglet de cette boîte de dialogue et affiche la boîte de dialogue par défaut de l'interface d'analyse AVG.

11.6. Résultats d'analyse



La boîte de dialogue ***Résultats d'analyse*** est accessible depuis l'interface d'analyse AVG via le bouton ***Historique / Résultats des analyses***. Elle contient la liste de toutes les analyses précédemment exécutées ainsi que les informations suivantes sur les résultats :

- ***Nom*** - désignation de l'analyse ; il s'agit soit du nom d'une analyse prédéfinie soit d'un nom que vous avez attribué à une analyse personnalisée . Chaque nom inclut une icône indiquant le résultat de l'analyse :

  - une icône de couleur verte signale l'absence d'infection

  - une icône de couleur bleue indique l'absence d'infection, mais la suppression automatique d'un objet infecté

  - une icône de couleur rouge vous alerte sur la présence d'une infection qui a été détectée lors de l'analyse et qui n'a pas pu être

traitée.

Les icônes sont entières ou brisées - l'icône entière représente une analyse exécutée et correctement terminée ; l'icône brisée désigne une analyse annulée ou interrompue.

Remarque : *pour plus d'informations sur une analyse, consultez la boîte de dialogue* ***Résultats des analyses****, par le biais du bouton* ***Voir les détails*** *(partie inférieure de la boîte de dialogue).*

- ***Heure de début*** - date et heure d'exécution de l'analyse
- ***Heure de fin*** - date et heure de fin de l'analyse
- ***Objets analysés*** - nombre d'objets qui ont été vérifiés
- ***Infections*** - nombre d'infections détectées / supprimées
- ***Spywares*** - nombre de spywares détectés / supprimés
- ***Informations sur le journal d'analyse*** - informations sur le déroulement de l'analyse et sur les résultats (finalisation ou interruption du processus)

Boutons de commande

Les boutons de contrôle de la boîte de dialogue ***Résultats d'analyse*** sont les suivants :

- ***Voir les détails*** - ce bouton est actif seulement si une analyse donnée est sélectionnée dans la vue générale ; cliquer sur le bouton a pour effet d'afficher la boîte de dialogue ***Résultats des analyses***, qui fournit des détails sur l'analyse en question
- ***Supprimer résultat*** - ce bouton est actif seulement si une analyse donnée est sélectionnée dans la présentation ; cliquer sur le bouton a pour effet de supprimer l'analyse sélectionnée des résultats d'analyse
- ***Précédent*** - permet de revenir à la boîte de dialogue par défaut de l'interface d'analyse AVG

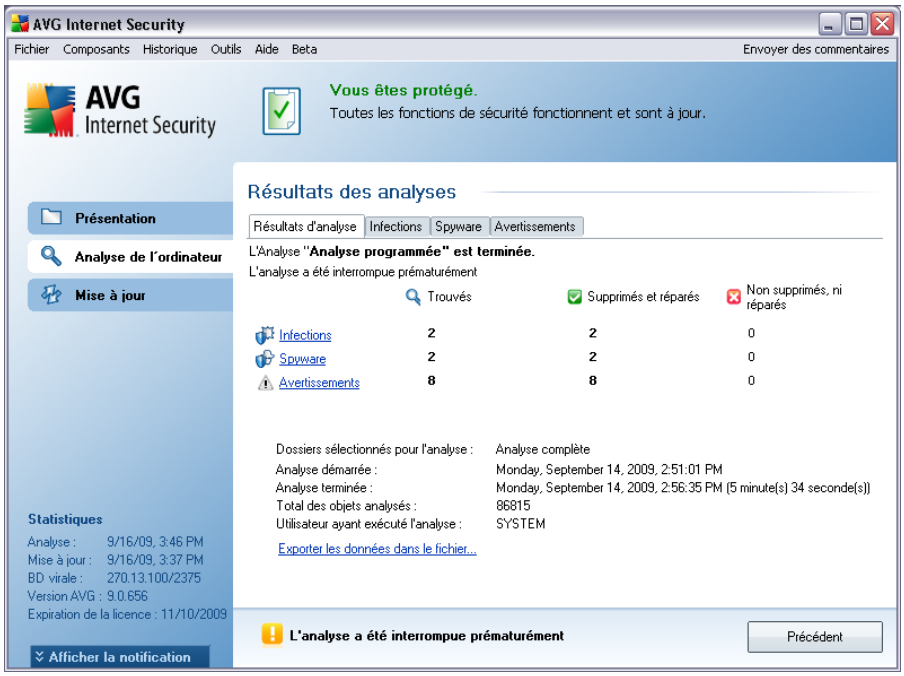
11.7. Détails des résultats d'analyse

Si, dans la boîte de dialogue ***Résultats d'analyse***, une analyse donnée est sélectionnée, cliquer sur le bouton ***Voir les détails*** a pour effet d'afficher la boîte de dialogue ***Résultats des analyses*** fournissant des détails sur la progression et le résultat de cette analyse.

La boîte de dialogue est subdivisée en plusieurs onglets :

- ***Résultats d'analyse*** - l'onglet est toujours affiché et délivre des informations statistiques sur le déroulement de l'analyse
- ***Infections*** - l'onglet s'affiche seulement en cas d'infection virale, détectée lors de l'analyse
- ***Spyware*** - l'onglet s'affiche seulement si un spyware a été trouvé lors de l'analyse
- ***Avertissements*** - l'onglet s'affiche seulement si certains objets n'ont pu être analysé lors de la vérification
- ***Rootkits*** - l'onglet s'affiche seulement si un rootkit a été trouvé lors de l'analyse
- ***Informations*** **-** l'onglet s'affiche seulement si certaines menaces potentielles ont été détectées et ne peuvent pas être rangées dans une des catégories mentionnées. Un message d'avertissement lié à l'objet trouvé s'affiche également

11.7.1. Onglet Résultats d'analyse



Sur la page de l'onglet ***Résultats des analyses***, vous trouverez des statistiques détaillées portant sur :

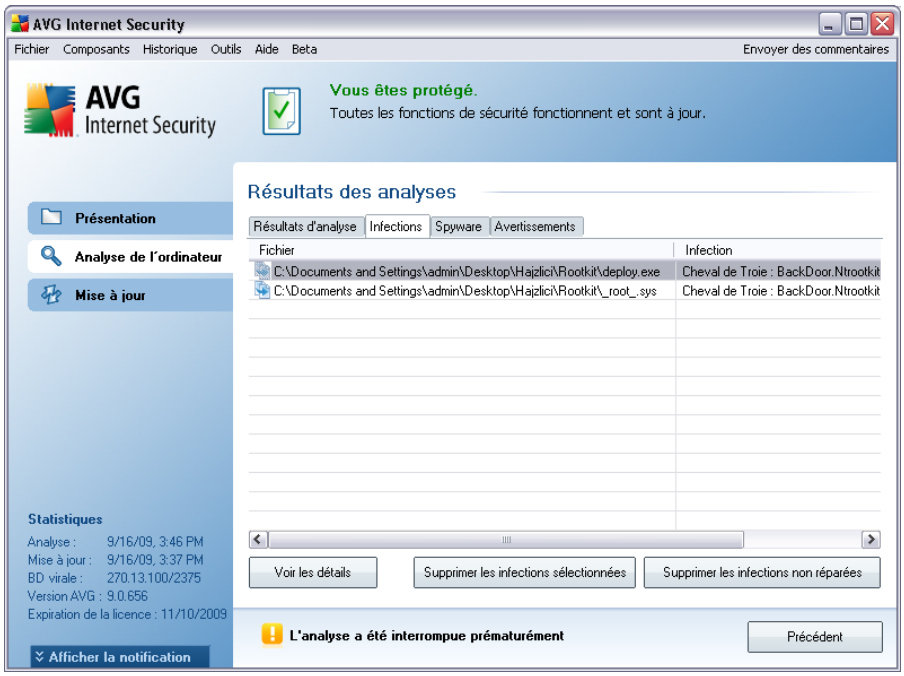
- les infections / spywares détectés
- les infections / spywares supprimés
- le nombre d'infections / de spywares qui n'ont pu être supprimés ou réparés

De plus, l'onglet signale la date et l'heure exactes du début de l'analyse, le nombre total d'objets analysés, la durée de l'analyse et le nombre d'erreurs qui se sont produites au cours de l'analyse.

Boutons de commande

Cette boîte de dialogue comporte un seul bouton de commande. Le bouton ***Fermer résultats***, qui vous renvoie à la boîte de dialogue ***Résultats d'analyse***.

11.7.2. Onglet Infections



L'onglet ***Infections*** apparaît dans la boîte de dialogue ***Résultats des analyses*** seulement si une infection virale est identifiée au cours de l'analyse. L'onglet comporte trois parties contenant les informations suivantes :

- ***Fichier*** - chemin complet vers l'emplacement d'origine de l'objet infecté
- ***Infections*** - nom du virus détecté (*pour plus de détails sur un virus particulier, consultez l'Encyclopédie des virus en ligne*)
- ***Résultat*** - indique l'état actuel de l'objet infecté détecté :
  - ***Infecté*** - l'objet infecté détecté a été laissé à son emplacement d'origine (*si, par exemple, vous avez désactivé l'option de réparation automatique pour une analyse spécifique*)
  - ***Réparé*** - l'objet infecté détecté a été réparé et conservé à son emplacement d'origine
  - ***Placé en quarantaine*** - l'objet infecté a été transféré en ***Quarantaine***
  - ***Supprimé*** - l'objet infecté a été supprimé

- ***Ajouté aux exceptions PUP*** - l'objet détecté est considéré comme une exception et est inclus dans la liste des exceptions PUP (*liste configurée dans la boîte de dialogue* ***Exceptions PUP*** *des paramètres avancés*)

- ***Fichier verrouillé -*** non vérifié - l'objet considéré est verrouillé, AVG ne peut donc pas l'analyser

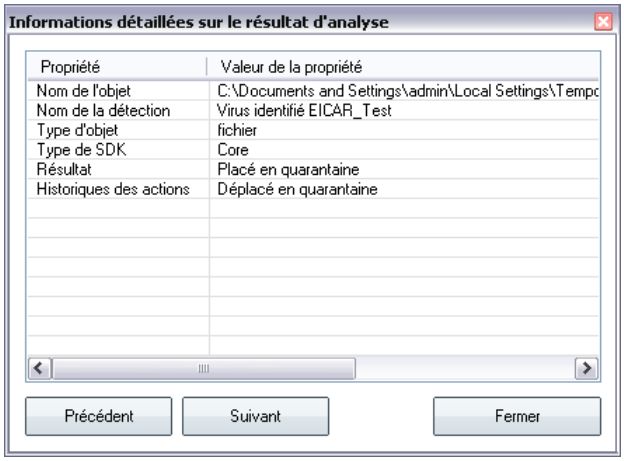
- ***Objet potentiellement dangereux*** - l'objet est considéré comme potentiellement dangereux, mais n'est pas infecté (*il contient par exemple des macros*) ; cette information est fournie à titre d'avertissement uniquement

- ***Un redémarrage de l'ordinateur est nécessaire pour terminer l'opération*** - l'objet infecté ne peut pas être supprimé ; pour ce faire, il faut redémarrer l'ordinateur

Boutons de commande

Cette boîte de dialogue compte trois boutons de commande :

- ***Voir les détails*** - le bouton ouvre la boîte de dialogue, ***Informations détaillées sur le résultat d'analyse*** :



Cette boîte de dialogue fournit des informations sur l'emplacement de l'objet infecté (***Nom de la propriété***). Les boutons ***Précédent*** et ***Suivant*** vous donnent accès aux informations sur des résultats spécifiques. Le bouton ***Fermer*** permet de quitter la boîte de dialogue.

- ***Supprimer les infections sélectionnées*** - servez-vous de ce bouton pour mettre les objets trouvés en ***quarantaine***

- ***Supprimer toutes les infections non réparées*** - ce bouton supprime tous les objets trouvés qui ne peuvent être désinfectés, ni placés en ***quarantaine***

- ***Fermer résultats*** - met fin aux informations détaillées et renvoie la boîte de dialogue ***Résultats d'analyse***

11.7.3. Onglet Spywares

L'onglet ***Spyware*** apparaît dans la boîte de dialogue ***Résultats des analyses*** seulement si un spyware (ou code espion) a été détecté au cours de l'analyse. L'onglet comporte trois parties contenant les informations suivantes :

- ***Fichier*** - chemin complet vers l'emplacement d'origine de l'objet infecté

- ***Infections*** - nom du spyware détecté (*pour plus de détails sur un virus particulier, consultez l'****Encyclopédie des virus*** *en ligne*)

- ***Résultat*** - indique l'état actuel de l'objet infecté détecté :

    - ***Infecté*** - l'objet infecté détecté a été conservé à son emplacement d'origine (si, par exemple, vous avez désactivé l'option de réparation automatique dans des paramètres d'analyse particuliers)

    - ***Réparé*** - l'objet infecté détecté a été réparé et conservé à son emplacement d'origine

    - ***Placé en quarantaine*** - l'objet infecté a été déplacé en ***Quarantaine***

    - ***Supprimé*** - l'objet infecté a été supprimé

    - ***Ajouté aux exceptions PUP*** - l'objet détecté est considéré comme une exception et est inclus dans la liste des exceptions PUP (*liste configurée dans la boîte de dialogue* ***Exceptions PUP*** *des paramètres avancés*)

    - ***Fichier verrouillé - non vérifié*** - l'objet considéré est verrouillé, AVG ne peut donc pas l'analyser

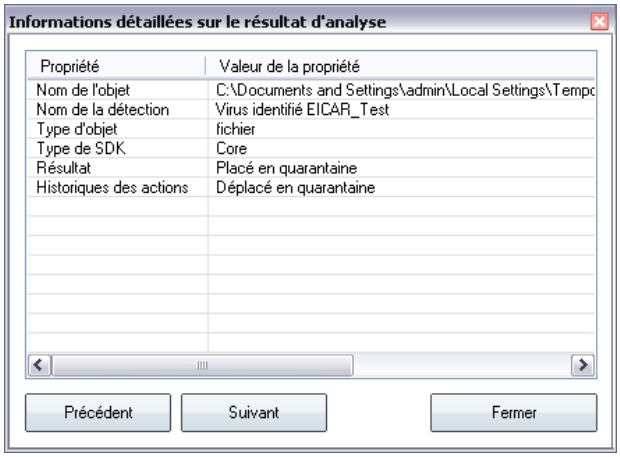
    - ***Objet potentiellement dangereux*** - l'objet est considéré comme potentiellement dangereux, mais n'est pas infecté (il contient par exemple des macros) ; cette information est fournie à titre d'avertissement uniquement

- o ***Un redémarrage de l'ordinateur est nécessaire pour terminer l'opération*** - l'objet infecté ne peut pas être supprimé ; pour ce faire, il faut redémarrer l'ordinateur

Boutons de commande

Cette boîte de dialogue compte trois boutons de commande :

- ***Voir les détails - le bouton ouvre la boîte de dialogue,*** Informations détaillées sur le résultat d'analyse :

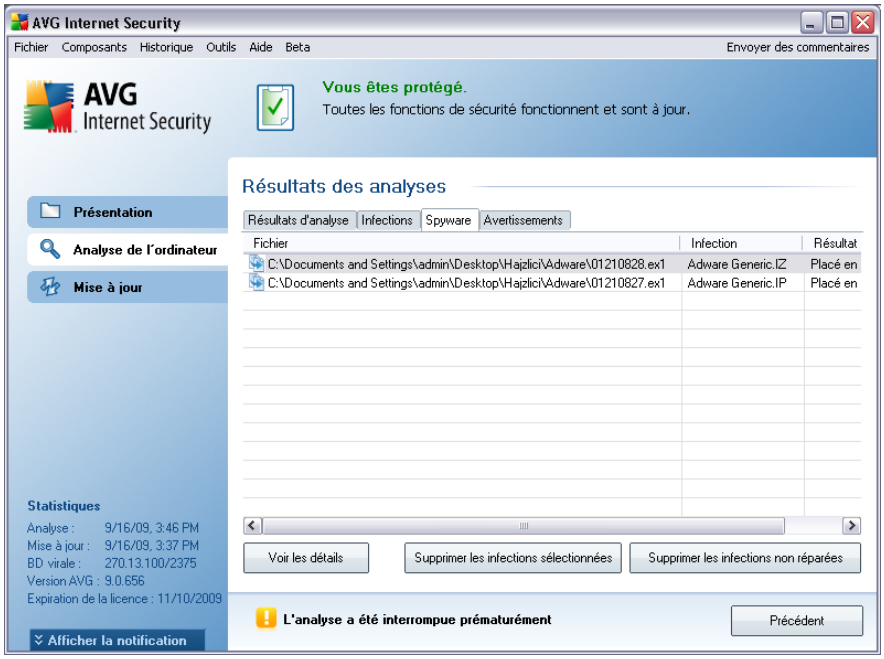


  Dans cette boîte de dialogue, vous trouverez des informations sur l'emplacement de l'objet infecté (***Nom***). Les boutons ***Précédent*** et ***Suivant*** vous donnent accès aux informations sur des résultats spécifiques. Le bouton ***Fermer*** permet de quitter la boîte de dialogue.

- ***Supprimer les infections sélectionnées*** - servez-vous de ce bouton pour mettre les objets trouvés en ***quarantaine***
- ***Supprimer toutes les infections non réparées*** - ce bouton supprime tous les objets trouvés qui ne peuvent être désinfectés, ni placés en ***quarantaine***
- ***Fermer résultats*** - met fin aux informations détaillées et renvoie la boîte de dialogue ***Résultats d'analyse***

11.7.4. Onglet Avertissements

L'onglet ***Avertissements*** affiche des informations sur les objets "suspects" (*généralement des fichiers*) trouvés au cours de l'analyse. Lorsqu'ils sont détectés par le ***Bouclier résident***, l'accès à ces fichiers est bloqué. Voici des exemples types de ce genre d'objets : fichiers masqués, cookies, clés de registre suspectes, documents protégés par un mot de passe, archives, etc. De tels fichiers ne présentent pas de menace directe pour l'ordinateur ou sa sécurité. Les informations relatives à ces fichiers sont généralement utiles lorsque la présence d'adwares ou de spywares est décelée dans votre ordinateur. Si l'analyse AVG ne détecte que des avertissements, aucune action n'est nécessaire.



Cette rubrique décrit brièvement les exemples les plus courants de tels objets :

- ***Fichiers masqués*** - Les fichiers masqués sont, par défaut, non visibles et certains virus ou autres menaces peuvent empêcher leur détection en stockant leurs fichiers avec cet attribut. Si AVG signale un fichier masqué que vous soupçonnez d'être dangereux, vous pouvez le confiner en ***Quarantaine***.

- ***Cookies*** - Les cookies sont des fichiers texte bruts utilisés par les sites Web pour stocker des informations propres à l'utilisateur. Elles permettent ultérieurement de charger un contenu personnalisé d'un site Web, de saisir automatiquement le nom d'utilisateur, etc.

- ***Clés de registre suspectes*** - Certains programmes malveillants stockent leurs informations dans la base de registre de Windows. De cette manière, elles sont chargées au démarrage ou peuvent s'immiscer dans le système d'exploitation.

11.7.5. Onglet Rootkits

L'onglet ***Rootkits*** affiche des informations sur les rootkits détectés au cours de l'analyse si vous avez lancé le composant ***Analyse Anti-Rootkit***, ou ajouté manuellement l'option d'analyse anti-rootkit dans l'option ***Analyse de la totalité de l'ordinateur*** (*cette option est désactivée par défaut*).

Un ***rootkit*** est un programme conçu pour prendre le contrôle du système, sans l'autorisation de son propriétaire et de son administrateur légitime. Un accès matériel est rarement nécessaire car un rootkit est prévu pour s'introduire dans le système d'exploitation exécuté sur le matériel. En règle générale, les rootkits dissimulent leur présence dans le système en contournant ou en ne se conformant pas aux mécanismes de sécurité standard du système d'exploitation. Souvent, ils prennent la forme de chevaux de Troie et font croire aux utilisateurs que leur exécution est sans danger pour leurs ordinateurs. Pour parvenir à ce résultat, différentes techniques sont employées : dissimulation de processus aux programmes de contrôle ou masquage de fichiers ou de données système, au système d'exploitation.

La structure de cet onglet est quasiment la même que celle de l'***onglet Infections*** ou de l'***onglet Spyware***.

11.7.6. Onglet Informations

L'onglet ***Informations*** contient des renseignements sur des "objets trouvés" qui ne peuvent pas être classés dans les catégories infections, spywares, etc. Il est impossible de les désigner comme positivement dangereux, mais ils réclament malgré tout votre attention. L'analyse AVG permet de détecter des fichiers qui ne sont peut-être pas infectés mais malicieux. Ces fichiers sont signalés comme un ***avertissement*** ou comme une ***information***.

Les raisons suivantes peuvent expliquer la gravité des ***informations*** :

- ***Mode de compression*** - Le fichier a été compressé avec l'un des systèmes de compression les moins connus, peut-être dans le but d'en empêcher l'analyse par AVG. Cependant, il n'est pas dit qu'un tel résultat indique que ce fichier contienne un virus.

- ***Mode de compression récursif*** - Identique au précédent, mais moins fréquent parmi les logiciels les plus connus. Ces fichiers sont malicieux et leur suppression ou envoi à AVG pour analyse doit être envisagé.

- ***Archive ou document protégé par mot de passe*** - Les fichiers protégés par mot de passe ne peuvent pas être analysés par AVG (*ou par d'autres programmes anti-malwares*).

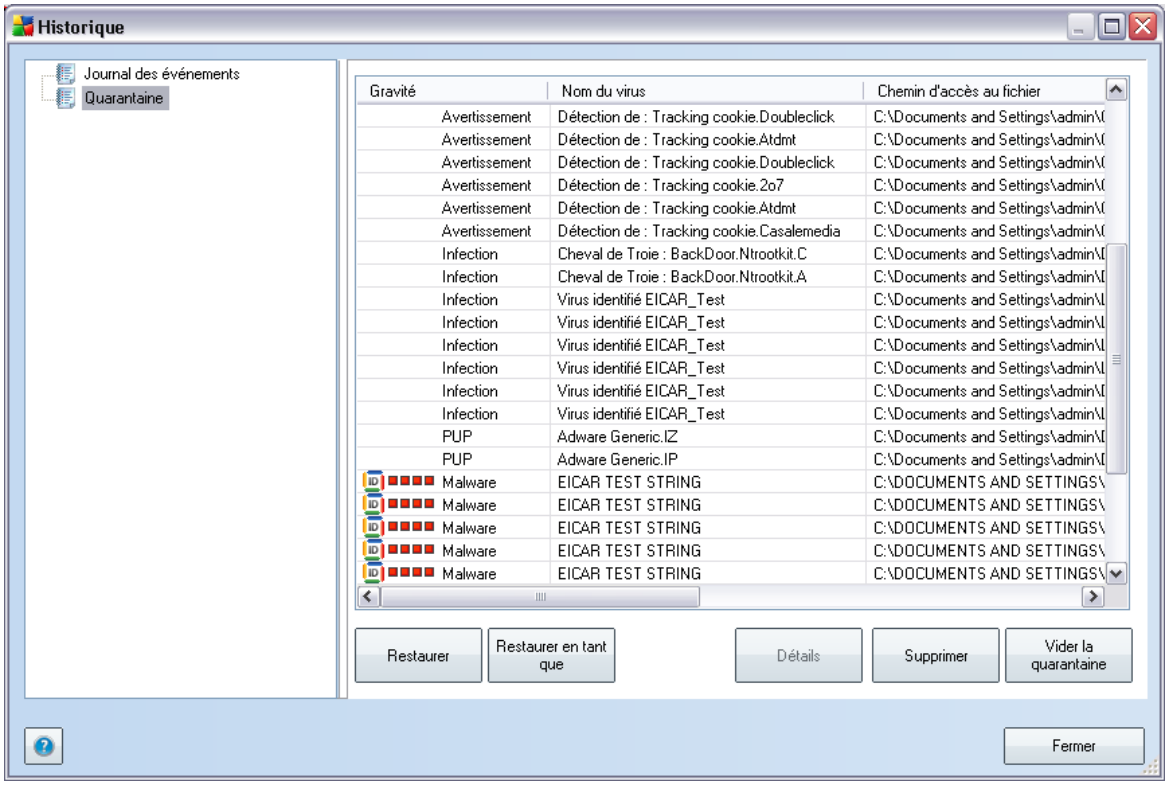
- ***Document contenant des macros*** - Le document signalé contient des macros potentiellement dangereuses.

- ***Extension cachée*** - Les fichiers munis d'une extension cachée peuvent apparaître comme des images alors qu'en réalité ils sont des fichiers exécutables (*exemple : image.jpg.exe*). Par défaut, la deuxième extension n'est pas visible sur Windows et AVG signale ce genre de fichiers afin d'empêcher leur ouverture accidentelle.

- ***Chemin d'accès au fichier incorrect*** - Si un fichier système important est exécuté à partir d'un chemin d'accès autre que celui par défaut (*exemple : winlogon.exe exécuté à partir d'un dossier autre que Windows*), AVG signale cette contradiction. Dans certains cas, les virus utilisent des noms de processus système standards pour que leur présence sur le système soit moins visible.

- ***Fichier verrouillé*** - Le fichier signalé est verrouillé et, de ce fait, AVG ne peut pas l'analyser. En général, il s'agit d'un fichier qui est constamment utilisé par le système (*par exemple, un fichier d'échange*).

11.8. Quarantaine



La Quarantaine offre un environnement parfaitement sûr pour la manipulation des objets infectés ou susceptibles de l'être, détectés au cours des analyses AVG. Lorsqu'un objet infecté est repéré par l'analyse et qu'AVG n'est pas en mesure de le réparer automatiquement, un message vous invite à indiquer la mesure à prendre. Il est recommandé de placer l'objet en***Quarantaine*** afin de le traiter ultérieurement.

L'interface ***Quarantaine*** s'affiche dans une fenêtre différente et présente des informations générales sur les objets infectés et déplacés en quarantaine :

- ***Gravité*** - offre une identification graphique de la gravité des résultats respectifs sur quatre niveaux allant du moins dangereux (■□□□) au plus grave (■■■■)
- ***Type d'infection*** - différencie les types d'objets trouvés selon l'importance de leur infection (*les objets répertoriés sont potentiellement infectés ou réellement infectés*)

- ***Nom du virus*** - spécifie le nom de l'infection décelée conformément à l' Encyclopédie des virus (disponible en ligne)
- ***Chemin d'accès au fichier*** - chemin d'accès menant à l'origine du fichier infectieux
- ***Nom original de l'objet*** - tous les objets détectés figurant dans la liste portent un nom standard attribué par AVG au cours du processus d'analyse. Si le nom initial de l'objet est connu (*telle qu'une pièce jointe qui ne correspond pas au contenu véritable de la pièce jointe*), il sera indiqué dans cette colonne.
- ***Date de l'enregistrement*** - date et heure à laquelle le fichier a été trouvé et placé en***quarantaine***

Boutons de commande

Les boutons de commande suivants sont accessibles depuis l'interface ***Quarantaine*** :

- ***Restaurer*** - rétablit le fichier infecté à sa place d'origine sur le disque
- ***Restaurer en tant que*** - si vous décidez de transférer l'objet infecté détecté depuis la zone de ***Quarantaine*** vers un dossier de votre choix, servez-vous de ce bouton. L'objet suspect détecté sera enregistré sous son nom d'origine. Si le nom d'origine n'est pas connu, le nom standard sera utilisé.
- ***Supprimer*** - supprime définitivement le fichier infecté de la ***Quarantaine***
- ***Vider la quarantaine*** - Vider intégralement le contenu de la***Quarantaine***

12. Mises à jour d'AVG

Il est essentiel de mettre régulièrement à jour votre programme anti-virus de manière à assurer une détection rapide des virus récemment découverts. Les mises à jour AVG ne sont pas diffusées selon un programme précis, mais sont plutôt la réaction à la détection d'un grand nombre de menaces ou de menaces sérieuses. C'est pourquoi, il est recommandé de vérifier au moins une fois par jour l'existence d'une éventuelle mise à jour. L'option de vérification toutes les 4 heures garantit la protection optimale par la base virale AVG tout au long de la journée .

12.1. Niveaux de mise à jour

AVG présente deux niveaux de mise à jour :

- ***La mise à jour des définitions*** inclut les modifications nécessaires à une protection efficace contre les virus, le spam et les programmes malveillants. En règle générale, cette action ne s'applique pas au code. Seule la base de données de définition est concernée. Il est conseillé d'effectuer cette mise à jour dès qu'elle est disponible.

- ***La mise à jour du programme*** contient diverses modifications, corrections et améliorations.

Lorsque vous programmez une mise à jour, il est possible de sélectionner le niveau de priorité voulu lors du téléchargement et de l'application de la mise à jour.

12.2. Types de mises à jour

Il existe deux types de mises à jour :

- ***Mise à jour à la demande*** - une mise à jour immédiate d'AVG que vous exécutez dès que vous en voyez l'utilité.

- ***Mise à jour programmée*** - AVG permet également de définir à l'avance un plan de mise à jour. La mise à jour planifiée est alors exécutée de façon périodique en fonction de la configuration choisie. Chaque fois que de nouveaux fichiers de mise à jour sont présents à l'emplacement indiqué, ils sont téléchargés directement depuis Internet ou à partir d'un répertoire du réseau. Lorsqu'aucune mise à jour n'est disponible, le processus n'a pas lieu.

12.3. Processus de mise à jour

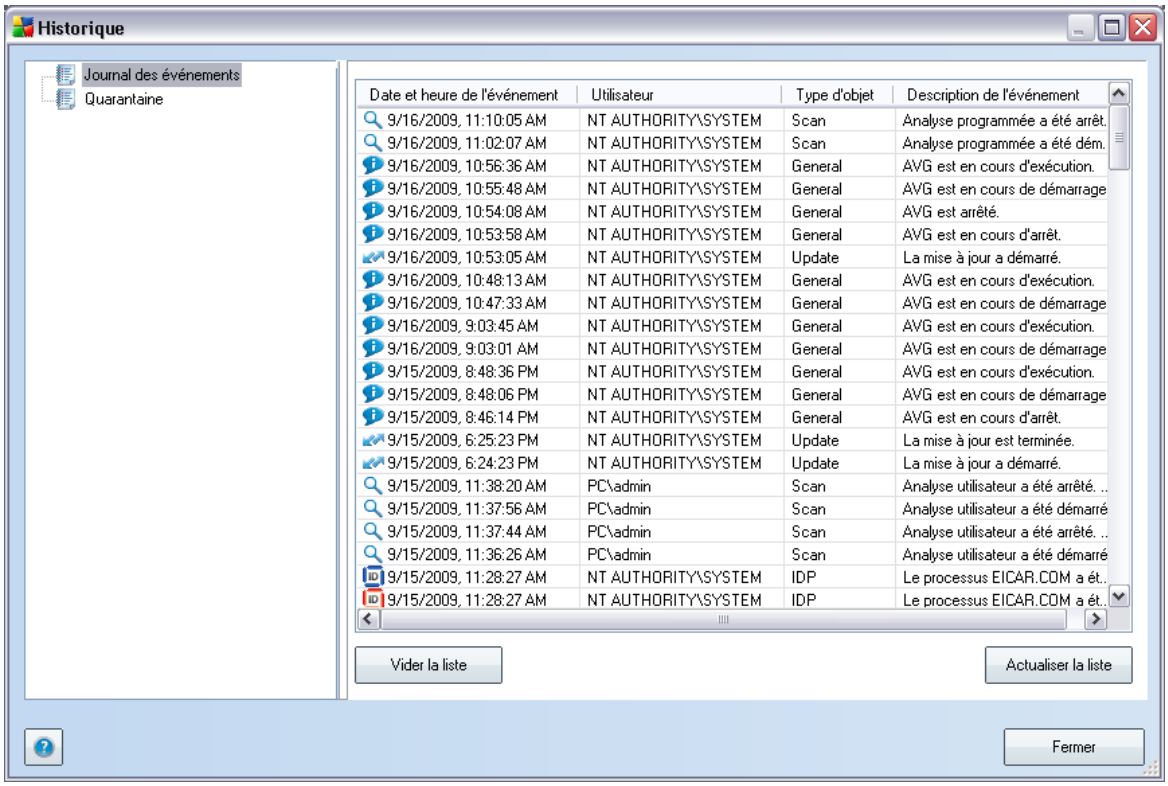
Le processus de mise à jour peut être lancé aussi souvent que nécessaire en cliquant sur ***Mise à jour*** (lien d'accès rapide). Ce lien est constamment disponible, quelle que soit la boîte de dialogue ouverte dans l'interface utilisateur AVG. Il est toutefois

particulièrement recommandé d'effectuer des mises à jour fréquentes comme établi par défaut dans le composant Mise à jour.

Lorsque vous lancez la mise à jour, AVG vérifie en premier lieu si de nouveaux fichiers de mise à jour sont disponibles. Le cas échéant, AVG télécharge et exécute ces mises à jour. Pendant ce processus, l'interface ***Mise à jour*** s'affiche et vous présente le déroulement de l'opération sous une forme graphique avec des données statistiques explicites (*taille du fichier de mise à jour, données reçues, vitesse du téléchargement, temps écoulé...*).

***Remarque** : avant l'exécution de la mise à jour du programme AVG, un point de restauration est créé. En cas d'échec de la mise à jour et de blocage de votre système d'exploitation, vous avez alors la possibilité de restaurer le système d'exploitation tel qu'il était configuré à partir de ce point. Cette option est disponible dans le menu Démarrer / Tous les programmes / Accessoires / Outils système / Restauration du système. Option destinée aux utilisateurs expérimentés seulement !*

13. Journal des évènements



La boîte de dialogue ***Journal des événements*** est accessible par le menu système, commande ***Historique/Journal des événements***. Dans cette boîte de dialogue, vous trouverez un résumé des événements les plus importants survenus pendant l'exécution du programme **AVG 9 Internet Security**. La commande ***Journal des événements*** enregistre les types d'événements suivants :

- Informations au sujet des mises à jour de l'application AVG
- Heure de début, de fin ou d'interruption de l'analyse (y compris pour les analyses effectuées automatiquement)
- Evènements liés à la détection des virus (par le Bouclier résident ou résultant de l'analyse) avec indication de l'emplacement des occurrences
- Autres événements importants

Boutons de commande

- ***Vider la liste*** - supprime toutes les entrées de la liste d'événements
- ***Actualiser la liste*** - met à jour toutes les entrées de la liste d'événements

14. FAQ et assistance technique

En cas de problème technique ou commercial avec votre produit AVG, consultez la section ***FAQ*** du site Web d'AVG (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***.