AVG Internet Security 2011

Manuel de l'utilisateur

Révision du document 2011.01 (10.9.2010)

Table des matières

1. Introduction

Ce manuel de l'utilisateur constitue la documentation complète du produit **AVG Internet Security 2011**.

Nous vous remercions d'avoir choisi le programme AVG Internet Security 2011.

AVG Internet Security 2011·figure parmi les produits AVG primés et a été conçu pour assurer la sécurité de votre ordinateur et vous permettre de travailler en toute sérénité. Comme toute la gamme des produits AVG, la solution **AVG Internet Security 2011**· a été entièrement repensée, afin de proposer une protection AVG reconnue et certifiée sous une présentation nouvelle, plus conviviale et plus efficace. Votre tout nouveau produit **AVG Internet Security 2011**· bénéficie d'une interface transparente associée à une analyse encore plus approfondie et plus rapide. Davantage de fonctions de sécurité ont été automatisées pour plus de commodité et des options utilisateur « intelligentes » supplémentaires ont été incluses de manière à adapter les fonctions de sécurité à vos activités 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.

Une offre intégrale

- Une protection pertinente par rapport à la manière dont vous utilisez votre ordinateur et l'Internet. Achats et opérations bancaires en ligne, navigation et recherches sur Internet, discussions en ligne et communications par e-mail, téléchargements de fichiers et utilisation des réseaux sociaux : AVG a la solution de sécurité qui correspond à vos besoins.

- Une protection discrète qui a relevé le défi de la sécurité pour plus de 110 millions d'utilisateurs de par le monde et dont le niveau d'excellence est sans cesse maintenu par un réseau international de chercheurs expérimentés.

- Une protection s'appuyant sur une assistance technique spécialisée disponible 24h sur 24

2. Pré-requis à l'installation d'AVG

2.1. Systèmes d'exploitation pris en charge

AVG Internet Security 2011 sert à protéger les postes de travail fonctionnant avec les systèmes d'exploitation suivants :

- Windows XP Edition familiale SP2
- Windows XP Professionnel SP2
- Windows XP Professionnel x64 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 XP x64. Sur ce système d'exploitation, vous pouvez installer AVG Internet Security 2011 sans le composant Identity Protection.*

2.2. Configuration matérielle minimale et recommandée

Configuration matérielle minimale pour **AVG Internet Security 2011** :

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

Configuration matérielle recommandée pour **AVG Internet Security 2011** :

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

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 vous assurer de posséder le dernier fichier d'installation en date d'AVG Internet Security 2011.

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.

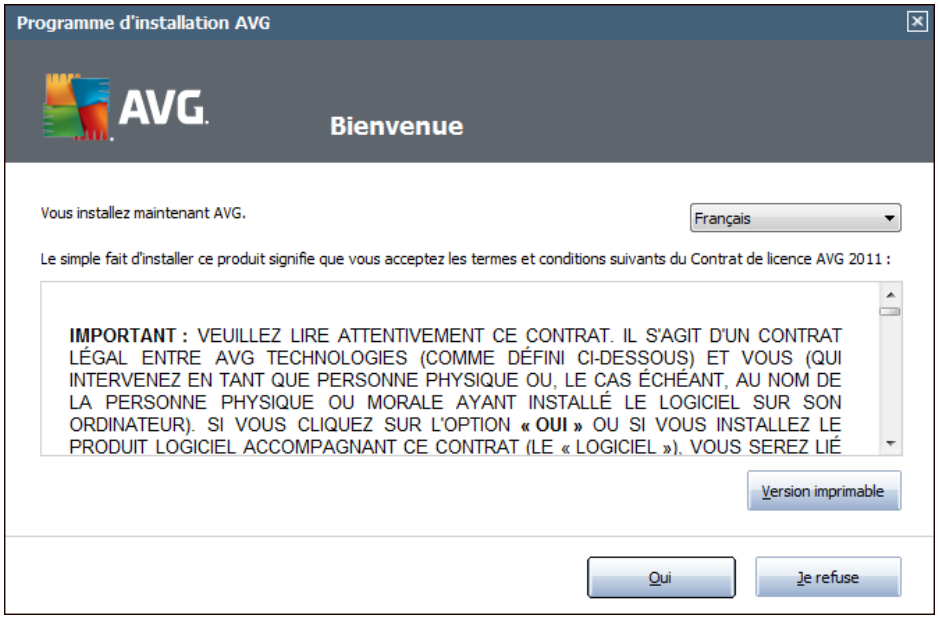
4. Processus d'installation

Pour installer **AVG Internet Security 2011** sur l'ordinateur, vous devez posséder le fichier d'installation le plus récent. Vous pouvez utiliser le fichier d'installation figurant sur le CD et fourni avec votre édition, mais il est fort probable qu'il soit déjà périmé. En conséquence, nous vous recommandons de bien vouloir télécharger de dernier fichier d'installation, depuis Internet. Vous pouvez télécharger le fichier à partir du site Web d'AVG (http://www.avg.com/), section ***Centre de support / Téléchargement.***

L'installation consiste à réaliser une série de tâches décrites à l'intérieur de boîtes de dialogue. Vous trouverez dans ce document une explication de chaque boîte de dialogue :

4.1. Bienvenue

Le processus d'installation démarre dans la fenêtre ***Bienvenue***. Dans cet écran, vous indiquez la langue utilisée par le processus d'installation, et la langue par défaut de l'interface utilisateur AVG. Dans la section supérieure de la fenêtre, recherchez le menu déroulant contenant la liste des langues proposées :



Attention : *vous choisissez ici la langue qui sera utilisée pour l'installation. La langue que vous avez choisi sera installée comme langue par défaut pour l'interface AVG, de même que l'anglais qui est installé systématiquement. Si vous voulez installer d'autres langues pour l'interface utilisateur, indiquez-les dans la boîte de dialogue du programme d'installation* ***Options personnalisées****.*

Par ailleurs, cette boîte de dialogue contient l'intégralité du texte de l'accord de licence AVG. Merci de le lire attentivement. Pour indiquer que vous avez lu, compris et accepté l'accord, cliquez sur le bouton ***Oui***. Si vous n'acceptez pas les termes de la licence, cliquez sur le bouton ***Je refuse*** ; le processus d'installation prendra fin immédiatement.

4.2. Activation de la licence AVG

Dans la boîte de dialogue visant à ***activer votre licence AVG***, indiquez votre numéro de licence dans le champ prévu à cet effet.

Le numéro d'achat se trouve dans le coffret du CD-ROM contenant le programme **AVG Internet Security 2011** . Le numéro de licence figure dans l'e-mail de confirmation que vous avez reçu après avoir acheté le produit **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.

4.3. Sélectionner le type d'installation

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

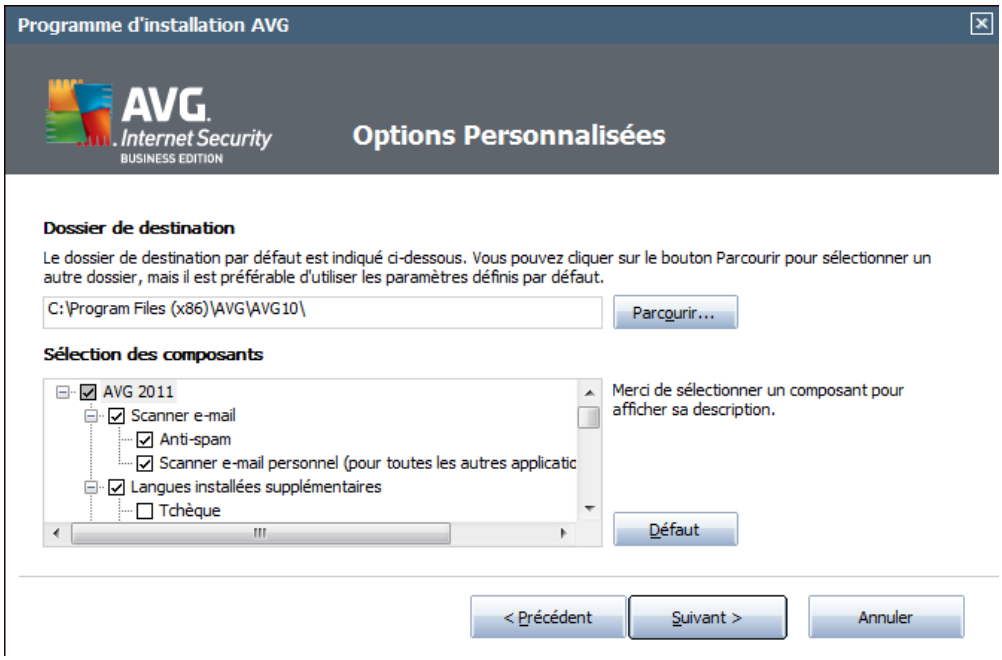
Dans la majorité des cas, il est recommandé d'opter pour l'***installation rapide***, qui installe automatiquement le programme AVG selon les paramètres prédéfinis par l'éditeur du logiciel. Cette configuration allie un maximum de sécurité et une utilisation optimale des ressources. Si besoin est, vous avez toujours la possibilité de modifier directement la configuration dans l'application AVG. Si vous avez sélectionné l'option ***Installation rapide***, cliquez sur le bouton ***Suivant*** pour passer à la boîte de dialogue ***Installer la Barre d'outils de sécurité AVG*** suivante.

L'***installation personnalisée*** est exclusivement réservée aux utilisateurs expérimentés qui ont une raison valable d'installer AVG selon des paramètres non standard. Par exemple, cela leur permet d'adapter le programme à une configuration système spécifique. Après la sélection de cette option, cliquez sur le bouton ***Suivant*** pour ouvrir la boîte de dialogue ***Options personnalisées***.

Dans la partie droite de la boîte de dialogue, vous trouverez la case ***Gadget AVG*** (*prise en charge sous Windows Vista/Windows 7*). Si vous voulez installer ce gadget, cochez la case correspondante. Le ***Gadget AVG*** sera alors accessible par le Volet Windows donnant un accès immédiat aux fonctions les plus importantes du programme **AVG Internet Security 2011** (l'analyse et la mise à jour).

4.4. Options personnalisées

La boîte de dialogue ***Options personnalisées*** permet de configurer deux paramètres de l'installation :



Dossier de destination

Dans la section ***Dossier de destination*** de la boîte de dialogue, vous devez indiquer l'emplacement dans lequel **AVG Internet Security 2011** doit être installé. 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 avant l'installation. Si vous optez pour un autre emplacement, cliquez sur le bouton ***Parcourir*** pour consulter l'arborescence du lecteur, puis sélectionnez le dossier souhaité.

Sélection des composants

La section ***Sélection des composants*** présente tous les composants **AVG Internet Security 2011** pouvant être installés. Si les paramètres par défaut ne vous satisfont pas, vous pouvez supprimer ou ajouter des composants spécifiques.

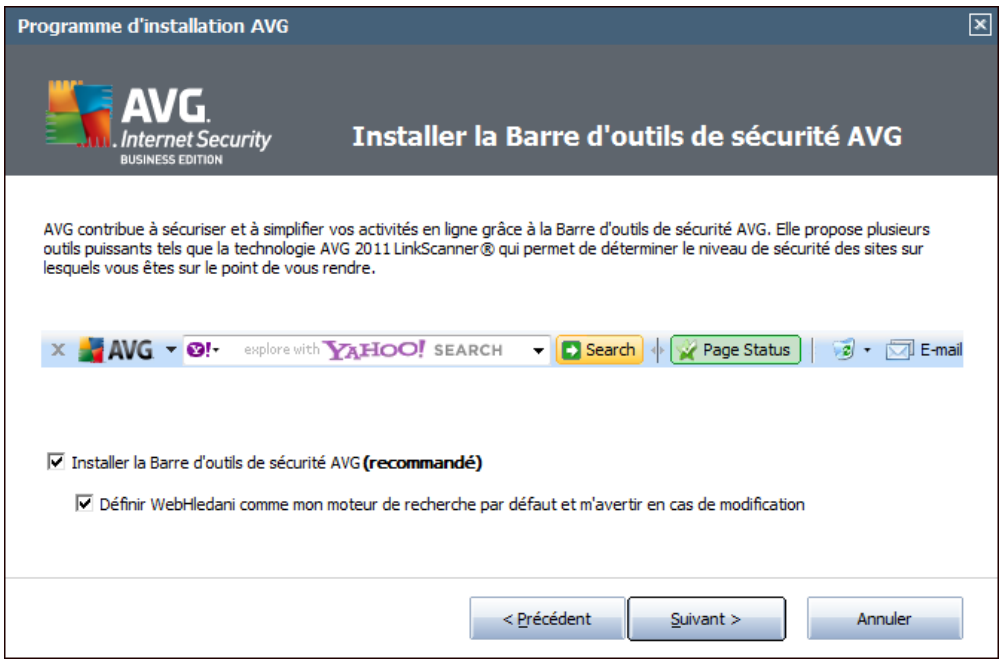
Notez que vous pouvez seulement choisir des composants inclus dans l'Edition AVG dont vous avez acquis les droits.

Mettez en surbrillance un élément de la liste ***Sélection des composants*** : une brève description du composant correspondant s'affiche à droite de la section. Pour plus d'informations sur le rôle de chacun des composants, consultez le chapitre

Présentation des composants de la présente documentation. Pour rétablir la configuration prédéfinie par défaut par l'éditeur du logiciel, cliquez sur le bouton prévu à cet effet.

Cliquez sur le bouton ***Suivant*** pour passer à l'écran suivant.

4.5. Installer la Barre d'outils de sécurité AVG



La boîte de dialogue ***Barre d'outils de sécurité AVG*** offre le choix entre installer ou ne pas installer la fonctionnalité ***Barre de sécurité AVG***. Si vous ne modifiez pas les paramètres par défaut, ce composant sera installé automatiquement dans votre navigateur Internet (*seuls Microsoft Internet Explorer v. 6.0 ou version supérieure et Mozilla Firefox v. 3.0 ou version supérieure sont actuellement pris en charge*) afin de garantir une protection complète sur Internet.

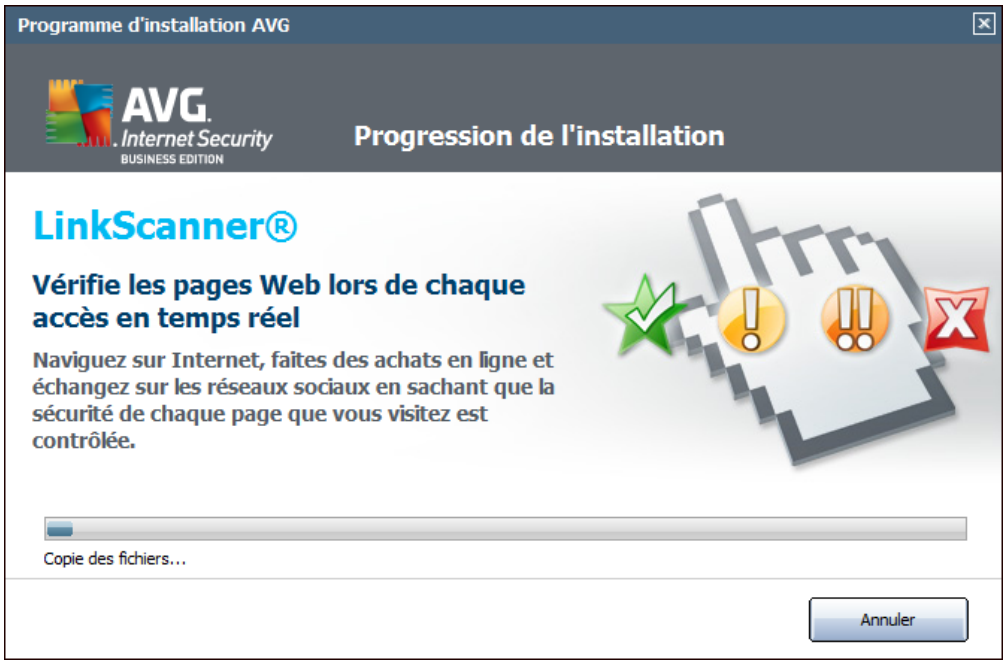
Vous avez également la possibilité de choisir Yahoo! comme moteur de recherche par défaut. Dans ce dernier cas, laissez la case correspondante cochée.

4.6. Fermer les applications en cours d'exécution

La boîte de dialogue ***Fermer les applications en cours d'exécution*** apparaît durant le processus d'installation seulement si des programmes en cours d'utilisation entrent en conflit. En pareil cas, la liste des programmes à fermer de manière à mener à bien l'installation s'affiche. Cliquez sur le bouton ***Quitter*** après avoir sélectionné un élément dans la liste pour arrêter l'application correspondante ou cliquez sur le bouton ***Recommencer*** pour indiquez que vous voulez fermer les applications et passer à l'étape suivante.

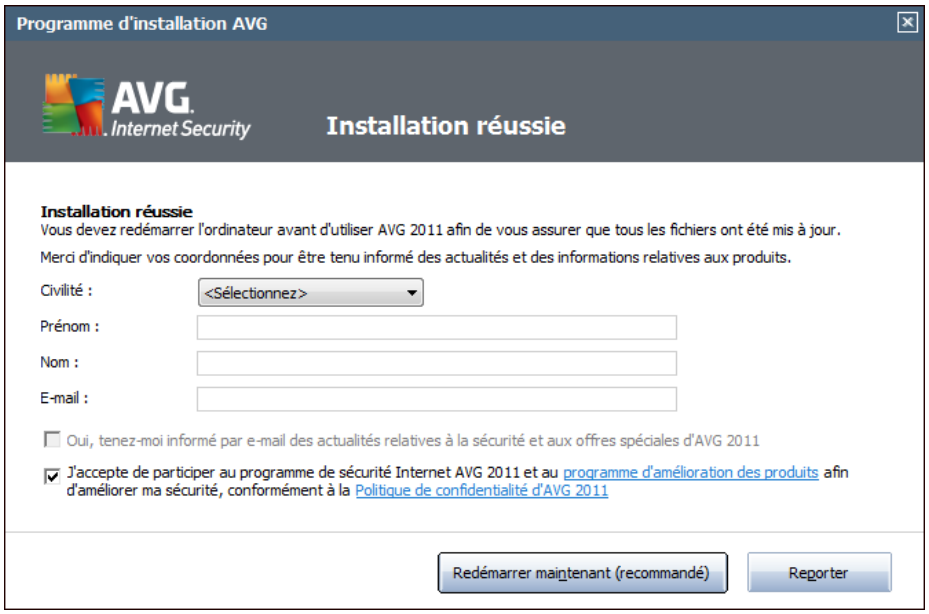
4.7. Progression de l'installation

La boîte de dialogue ***Progression de l'installation*** montre la progression du processus d'installation et ne requiert aucune intervention de votre part :



Lorsque le processus d'installation est terminé, la base de données virale et le programme sont automatiquement mis à jour. Par la suite, vous êtes redirigé vers la boîte de dialogue suivante.

4.8. Installation réussie



La boîte de dialogue ***Installation réussie*** confirme que le programme **AVG Internet Security 2011** est bien installé et configuré.

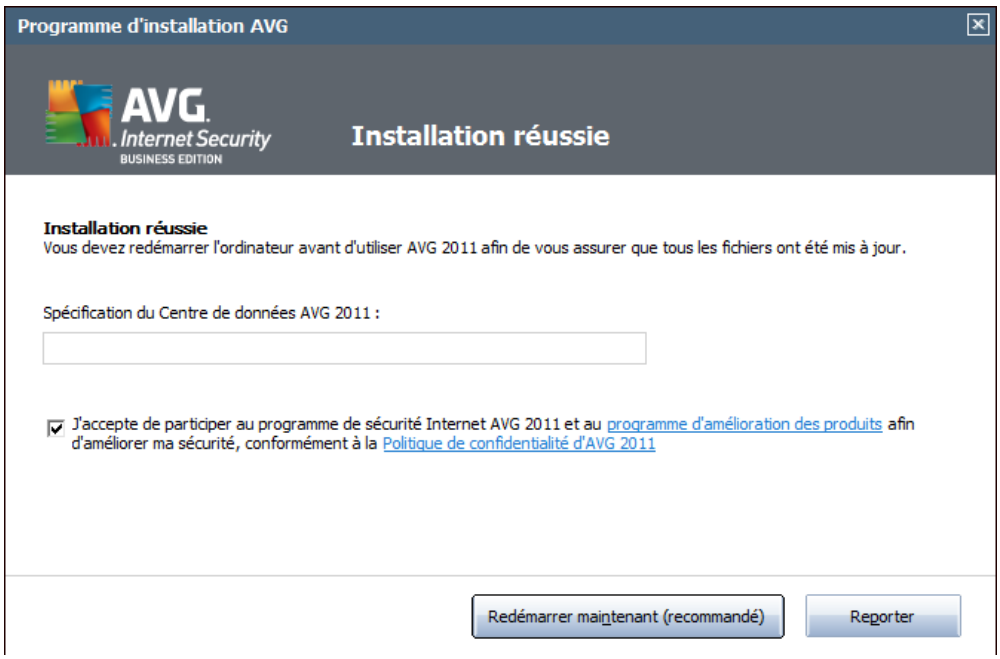
Dans cette boîte de dialogue, indiquez vos coordonnées de manière à pouvoir recevoir toutes les informations sur le produit et sur les nouveautés. Sous la formulaire d'enregistrement, vous trouverez les deux options suivantes :

- ***Oui, tenez-moi informé des actualités relatives à la sécurité et aux offres spéciales d'AVG 2011 par e-mail*** - cochez cette case pour connaître les actualités dans le domaine de la sécurité Internet et les offres promotionnelles, les améliorations ou les mises à niveau des produits AVG, etc.

- ***J'accepte de participer au programme de sécurité Internet AVG 2011 et au programme d'amélioration des produits...*** - cochez cette case si vous désirez apporter votre aide dans le cadre du programme d'amélioration des produits (*pour en savoir plus, voir le chapitre Paramètres avancés d'AVG / Programme d'amélioration des produits*) qui collecte des informations anonymes sur les menaces détectées de manière à accroître le niveau général de la sécurité sur Internet.

Pour terminer le processus d'installation, vous devez redémarrer l'ordinateur. Sélectionnez l'une ou l'autre des options selon ce que vous désirez lancer de suite le redémarrage (***Redémarrer maintenant***) ou le différer (***Redémarrer plus tard***).

> ***Remarque :*** *si vous possédez une licence AVG à usage professionnel et avez précédemment sélectionné l'installation de l'Administration à distance (voir Options personnalisées), la boîte de dialogue indiquant la réussite de l'installation se présente de la manière suivante :*



Vous devez spécifier les paramètres du Centre de données AVG; indiquez la chaîne de connexion au Centre de Données AVG sous la forme serveur:port. Si vous ne disposez pas de cette information pour l'instant, laissez ce champ vide ; vous pourrez définir la configuration ultérieurement dans la boîte de dialogue Paramètres avancés / Administration à distance. Pour plus d'informations sur l'administration à distance AVG, consultez la documentation des Editions Réseau d'AVG (manuel de l'utilisateur) téléchargeable à partir du site Web AVG (http://www.avg.com/).

5. Opérations à effectuer après l'installation

5.1. Enregistrement du produit

Après l'installation d'**AVG Internet Security 2011**, enregistrez votre produit en ligne sur le site Web d'AVG (http://www.avg.com/), page ***Enregistrement*** (*suivez les instructions indiquées sur cette 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.

5.2. Accès à l'interface utilisateur

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

- double-cliquez sur l'***icône de la barre d'état système AVG***
- double-cliquez sur l'icône AVG située sur le Bureau
- double-cliquez sur la ligne d'état figurant dans la section inférieure du ***gadget AVG*** (*s'il a été installé ; prise en charge possible sous Windows Vista / Windows 7*)
- à partir du menu ***Démarrer/ Programmes/AVG 2011/Interface utilisateur AVG***
- à partir de la ***Barre d'outils de sécurité AVG*** et l'option ***Lancer AVG***

5.3. Analyse complète

Le risque de contamination de l'ordinateur par un virus avant l'installation d'**AVG Internet Security 2011** ne doit pas être écarté. C'est pour cette raison qu'il est recommandé d'exécuter 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***.

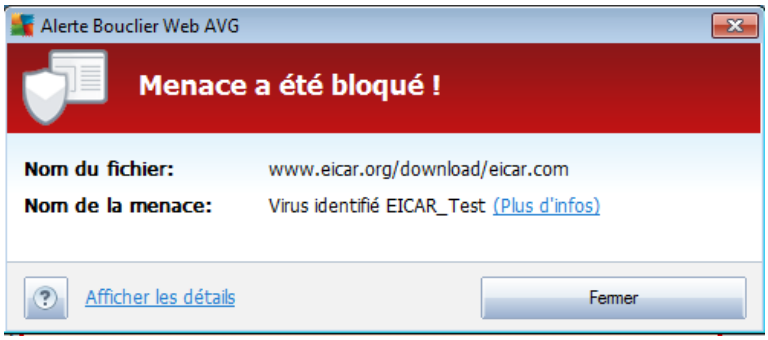
5.4. Test Eicar

Pour confirmer qu'**AVG Internet Security 2011** est bien installé, réalisez 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 Web***réagit en émettant un avertissement. Ce message du Bouclier Web indique qu'AVG est installé correctement sur votre ordinateur.



A partir du site Web http://www.eicar.com, vous pouvez aussi télécharger la version compacte du « virus » EICAR (*sous la forme eicar_com.zip, par exemple*). Le ***Bouclier Web*** permet de télécharger ce fichier et de l'enregistrer sur votre disque local, mais le ***Bouclier résident*** détecte le « virus » au moment où vous décompressez ce fichier. **Si AVG n'identifie pas le fichier test Eicar comme un virus, il est recommandé de vérifier de nouveau la configuration du programme.**

5.5. Configuration AVG par défaut

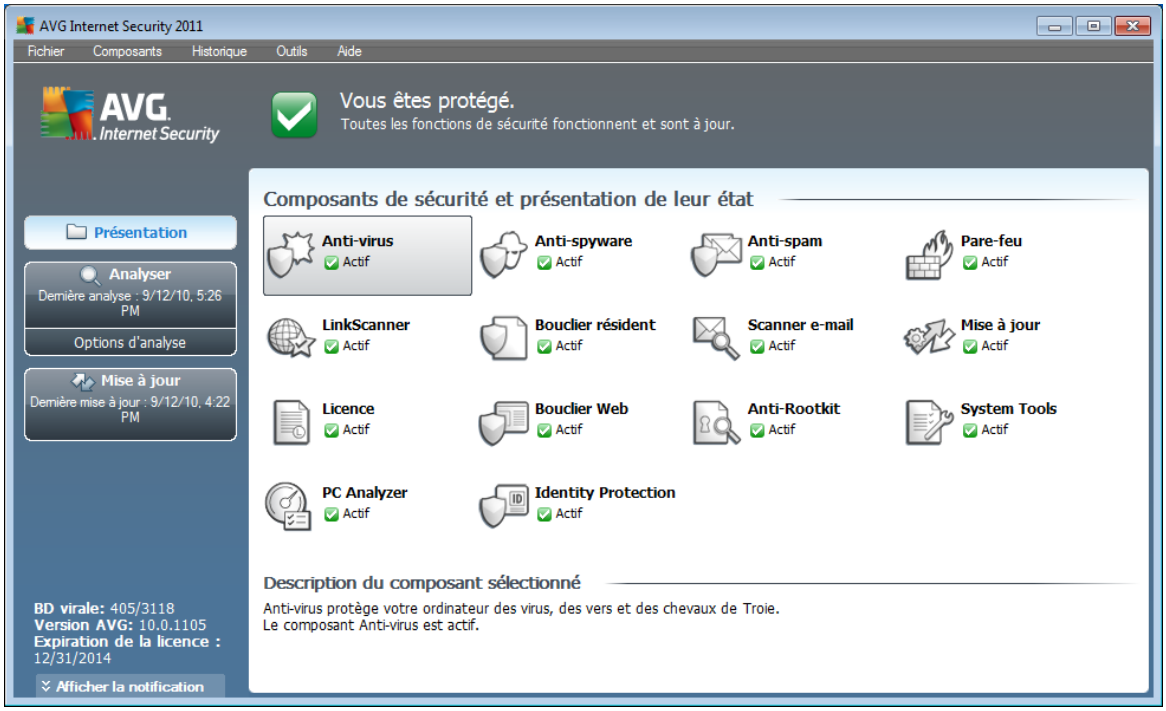
La configuration par défaut (*c'est-à-dire la manière dont l'application est paramétrée à l'issue de l'installation*) d'**AVG Internet Security 2011** est définie par l'éditeur du logiciel de sorte que les composants et les fonctions délivrent leurs performances optimales.

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.

6. Interface utilisateur AVG

AVG Internet Security 2011 affiche 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 >>
- ***Gadget AVG*** *(Volet Windows pour Windows Vista/7)* permet un accès rapide aux analyses et mises à jour AVG - détails >>

6.1. 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 prinicipale du programme **AVG Internet Security 2011**. Servez-vous du menu système pour accéder aux composants, fonctions et services AVG de votre choix.

Le menu système inclut cinq sections principales :

6.1.1. Fichier

- ***Quitter*** - ferme l'interface utilisateur d'**AVG Internet Security 2011**. L'application AVG continue néanmoins de s'exécuter en arrière-plan de sorte que l'ordinateur reste protégé !

6.1.2. 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*** - ouvre l'interface utilisateur par défaut et affiche une présentation générale de tous les composants installés et leur état
- ***Le composant Anti-Virus*** garantit que l'ordinateur est protégé contre les virus essayant de pénétrer dans le système - détails >>
- ***Anti-Spyware*** garantit que l'ordinateur est protégé contre les spywares et les adwares - 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 Scanner e-mail*** vérifie la présence éventuelle de virus dans les mails entrants et sortants - détails >>
- ***Le composant Bouclier résident*** s'exécute en arrière-plan et analyse les fichiers lorsqu'ils sont copiés, ouverts ou enregistrés - détails >>
- ***Le composant Mise à jour*** recherche la présence d'une mise à jour AVG - détails >>
- ***Licence*** affiche le type, le numéro et la date d'expiration de la licence - détails

>>

- ***Bouclier Web*** analyse toutes les données téléchargées par le navigateur Internet - détails >>
- ***Le composant Anti-Rootkit*** détecte les programmes et les technologies cherchant à dissimuler des codes malveillants - détails >>
- Λε χομποσαντ ***System Tools*** décrit de manière détaillée l'environnement AVG et le système d'exploitation - détails >>
- ***PC Analyzer*** renseigne sur l'état de l'ordinateur - détails >>
- ***Identity Protection*** - ce composant est conçu pour empêcher les usurpateurs d'identité de dérober vos ressources numériques personnelles importantes détails >>
- Λεουτιλ ***Administration à distance*** n'apparaît que dans les Editions Réseau d'AVG si vous avez précisez, au cours de l'installation, que vous voulez installer ce composant

6.1.3. Historique

- ***Résultats des analyses*** - affiche 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 Internet Security 2011** 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

6.1.4. 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*** - lance automatiquement le processus de mise à jour du composant **AVG Internet Security 2011**
- ***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 Internet Security 2011** 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***

6.1.5. 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,*** dans laquelle vous obtenez 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/). Merci de compléter le formulaire d'enregistrement ; seuls les clients ayant dûment enregistré leur produit AVG peuvent bénéficier de l'assistance technique gratuite.

Remarque** : si vous utilisez une version d'évaluation* **AVG Internet Security 2011, les deux dernières options sont remplacées par **Acheter maintenant** et **Activer**, ce qui vous permet de vous procurer de suite la version complète du programme. Si le programme* **AVG Internet Security 2011** *est installé à l'aide d'un numéro d'achat, vous avez alors le choix entre les options **Enregistrer** et **Activer**. Pour plus d'informations, consultez la section Licence de cette documentation.*

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

6.2. 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. Vous y trouverez des informations sur l'état actuel de la sécurité du programme **AVG Internet Security 2011**. 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.

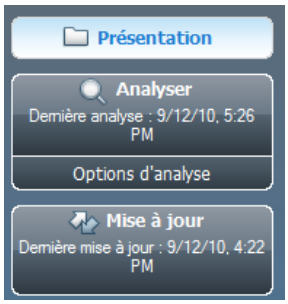
Si AVG n'utilise pas les performances optimales, un nouveau bouton, Corriger (ou Tout corriger si le problème implique plusieurs composants) apparaît près des informations relatives au statut de la sécurité. Cliquez sur le bouton pour lancer le processus automatique de vérification et de configuration du programme. C'est le moyen le simple d'optimiser les performances d'AVG et d'atteindre le plus haut niveau de sécurité.

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.*

6.3. 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 >>***
- ***Analyser*** - par défaut, le bouton vous renseigne sur la dernière analyse effectuée (*type d'analyse, date de la dernière analyse*). Vous pouvez soit exécuter la commande ***Analyser*** pour relancer la même analyse ou cliquer sur le lien ***Analyse de l'ordinateur*** afin d'ouvrir l'interface d'analyse AVG. Celle-ci vous permettra d'exécuter ou de programmer des analyses ou encore d'en modifier les paramètres. Voir chapitre ***Analyse AVG >>***
- ***Mise à jour*** - le lien précise la date de la mise à jour la plus récente. Cliquez sur le lien pour lancer l'interface de mise à jour et exécuter immédiatement le processus de mise à jour AVG. Voir le chapitre ***Mises à jour d'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 l'illustration).

6.4. 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 Internet Security 2011**, 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 >>
- ***Anti-Spyware*** garantit que l'ordinateur est protégé contre les spywares et les adwares - 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 Scanner e-mail*** vérifie la présence éventuelle de virus dans les mails entrants et sortants - détails >>
- ***Le composant Bouclier résident*** s'exécute en arrière-plan et analyse les fichiers lorsqu'ils sont copiés, ouverts ou enregistrés - détails >>
- ***Le composant Mise à jour*** recherche la présence d'une mise à jour AVG - détails >>
- ***Licence*** affiche le type, le numéro et la date d'expiration de la licence - détails >>
- ***Bouclier Web*** analyse toutes les données téléchargées par le navigateur Internet - détails >>
- ***Le composant Anti-Rootkit*** détecte les programmes et les technologies cherchant à dissimuler des codes malveillants - détails >>
- Λε χομποσαντ ***System Tools*** décrit de manière détaillée l'environnement AVG et le système d'exploitation - détails >>
- ***PC Analyzer*** renseigne sur l'état de l'ordinateur - détails >>

- ***Identity Protection*** - ce composant est conçu pour empêcher les usurpateurs d'identité de dérober vos données numériques personnelles importantes détails >>

- Λəουτιλ***Administration à distance***n'apparaît que dans les Editions Réseau d'AVG si vous avez précisez, au cours de l'installation, que vous voulez installer ce composant

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. Double-cliquez sur l'icône d'un composant a pour effet d'ouvrir l'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 l'icône de la barre d'état système.

6.5. 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 :

- ***Base de données virale***- précise la version de la base de données virale actuellement installée

- ***Version AVG*** - indique la version du programme actuellement installée *(le numéro se présente sous la forme 10.0.xxxx. 10.0 désigne la version du produit et xxxx le numéro du build)*

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

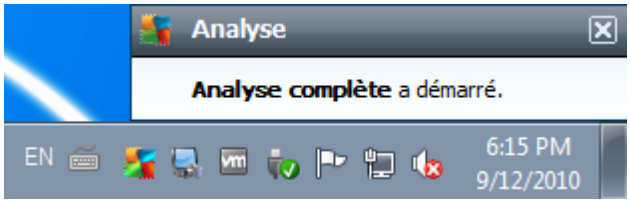
6.6. Icône de la barre d'état système

L'***icône de la barre d'état système*** (*dans la barre des tâches Windows*) signale l'état actuel du programme **AVG Internet Security 2011**. Elle est toujours visible dans la barre d'état, que la fenêtre principale AVG soit ouverte ou fermée :

Lorsqu'elle est 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 est en couleur si AVG signale une erreur mais que vous en avez été averti et avez choisi d'***ignorer l'état du composant***. Une icône marquée d'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 vous renseigne également sur les activités actuelles d'AVG et les possibles modifications d'état du programme (*lancement automatique d'une analyse programmée ou d'une mise à jour. Le profil du pare-feu change en cas de modification de l'état d'un composant, de l'apparition d'une erreur, etc.*). Ce changement est signalé par une fenêtre de l'icône de la barre d'état système 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 :

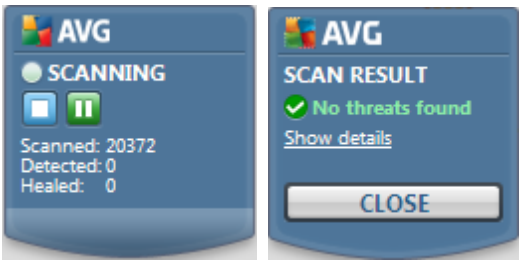
- ***Ouvrir l'Interface utilisateur AVG*** - cette commande permet d'afficher l' interface utilisateur AVG
- ***Analyses*** - cette commande permet d'ouvrir le menu contextuel desanalyses prédéfinies (*Analyse complète*, *Analyse zones sélectionnées*, *Analyse Anti-Rootkit*) et sélectionnez l'analyse requise, elle sera lancée immédiatement
- ***Pare-feu*** - cliquez sur le menu contextuel contenant les options de configuration du Pare-feu permettant de modifier les paramètres principaux : Etat du Pare-feu (*Pare-feu activé/Pare-feu désactivé/Mode Urgence*), activation du mode jeuet profils de Pare-feu
- ***Analyses en cours d'exécution*** - cette option n'est visible que si une analyse est en cours sur l'ordinateur. Vous êtes libre de définir la priorité de ce type d'analyse, de l'interrompre ou de la suspendre. Les options suivantes sont disponibles : *Définir la priorité pour toutes les analyses, Suspendre toutes les analyses* ou *Arrêter toutes les analyses*.
- ***Mise à jour*** - cette option permet de lancer une mise à jour immédiate
- ***Aide*** - ouvre le fichier d'aide à la page d'accueil

6.7. Gadget AVG

Le ***gadget AVG*** s'affiche sur le Bureau de Windows (*Volet Windows*). Cette application n'est compatible qu'avec les systèmes d'exploitation Windows Vista et Windows 7. Le ***gadget AVG*** donne immédiatement accès aux fonctionnalités les plus importantes du programme **AVG Internet Security 2011** , c'est-à-dire aux fonctions d'analyse et de mise à jour :

Le ***gadget AVG*** comporte les options d'accès rapides suivants :

- ***Analyser*** - cliquez sur le lien ***Analyser*** pour lancer directement l'***analyse complète de l'ordinateur*** . Vous pouvez observer la progression d'une analyse dans l'interface utilisateur du gadget. Une brève présentation de statistiques indique le nombre d'objets analysés, de menaces détectées et de menaces réparées. Il est possible de suspendre ou d'interrompre l'analyse en cours. Pour obtenir plus de détails sur les résultats d'analyse, consultez la boîte de dialogue standard ***Résultats d'analyse*** ; l'élément correspondant s'affiche comme ***analyse du gadget du volet***.



- ***Mise à jour*** - cliquez sur le lien ***Mise à jour*** pour lancer directement la mise à jour AVG à partir du gadget :

- ***Lien Twitter*** - ouvre une nouvelle interface du ***gadget AVG*** qui présente les derniers posts d'AVG publiés sur Twitter. Suivez le lien ***Afficher tous les posts d'AVG sur Twitter*** pour ouvrir votre navigateur Internet dans une nouvelle fenêtre et vous serez redirigé vers le site Web Twitter et notamment à la page consacrée aux actualités de la société AVG :

- ***Lien Facebook*** - ouvre le site Web Facebook dans votre navigateur Internet, à la page ***Communauté AVG***
- ***PC Analyzer*** - ouvre l'interface utilisateur du composant ***PC Analyzer***

7. Composants AVG

7.1. Anti-Virus

7.1.1. Principes de l'Anti-Virus

Le moteur d'analyse du logiciel anti-virus examine les fichiers et l'activité liée aux fichiers (ouverture, fermeture, 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.

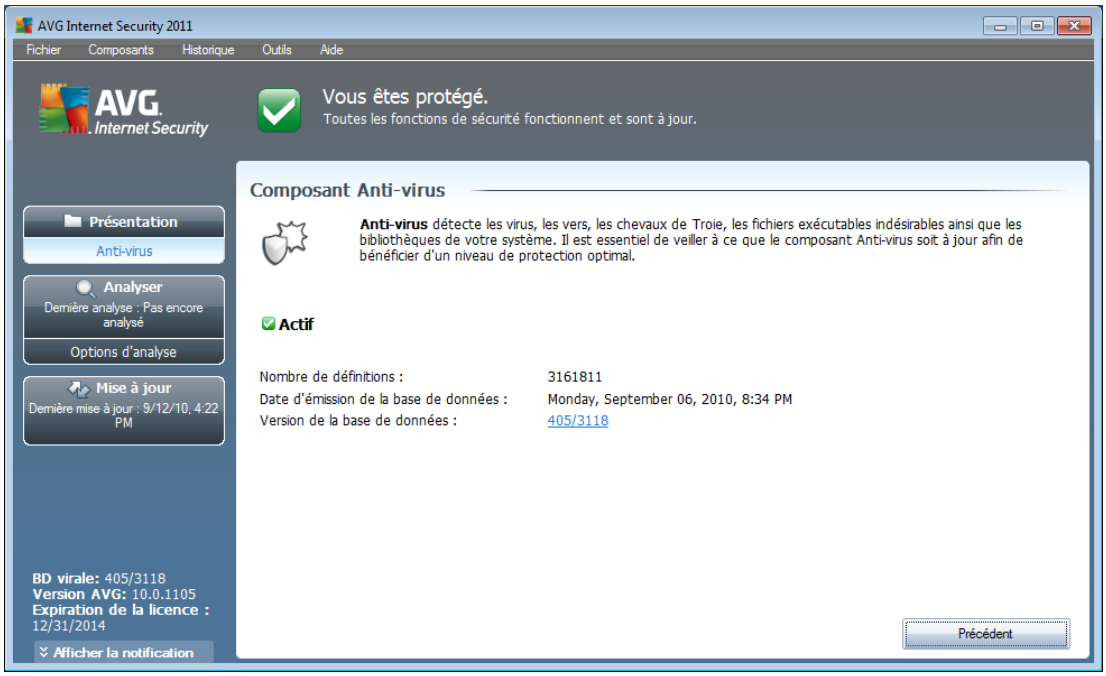
Rappelons que la fonction essentielle d'une protection anti-virus consiste à empêcher l'exécution de tout virus inconnu sur l'ordinateur.

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.

7.1.2. 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*** :

- ***Nombre de définitions*** - indique le nombre de virus définis dans la dernière version à ce jour de la base de données virale
- ***Date d'émission 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*** - indique le numéro de la version de la base de données virale actuellement installée; ce chiffre 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*).

7.2. Anti-Spyware

7.2.1. Principes de l'Anti-Spyware

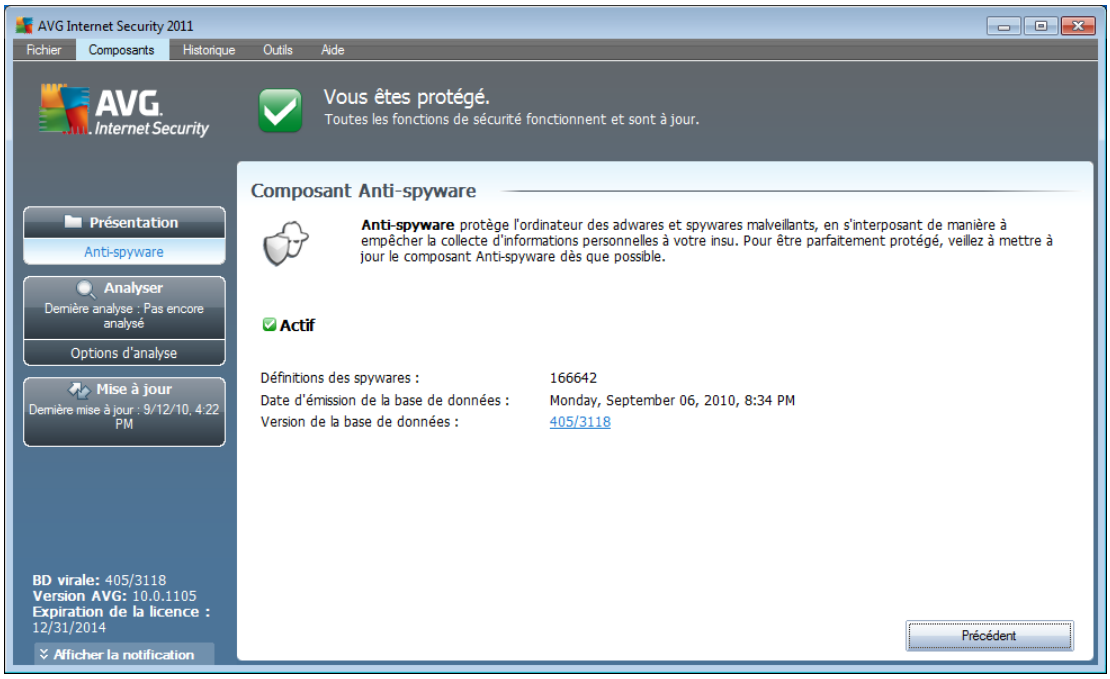
Le terme spyware désigne généralement un code malicieux et plus précisément un logiciel qui collecte des informations depuis l'ordinateur d'un utilisateur, à l'insu de celui-ci. Certains spywares installés volontairement peuvent contenir des informations

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 et du programme **AVG Internet Security 2011** ***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).

7.2.2. 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 et certaines statistiques ***Anti-Spyware*** :

- ***Définitions des spywares*** - indique le nombre de spywares définis dans la dernière version de la base de données
- ***Date d'émission 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*).

7.3. Anti-Spam

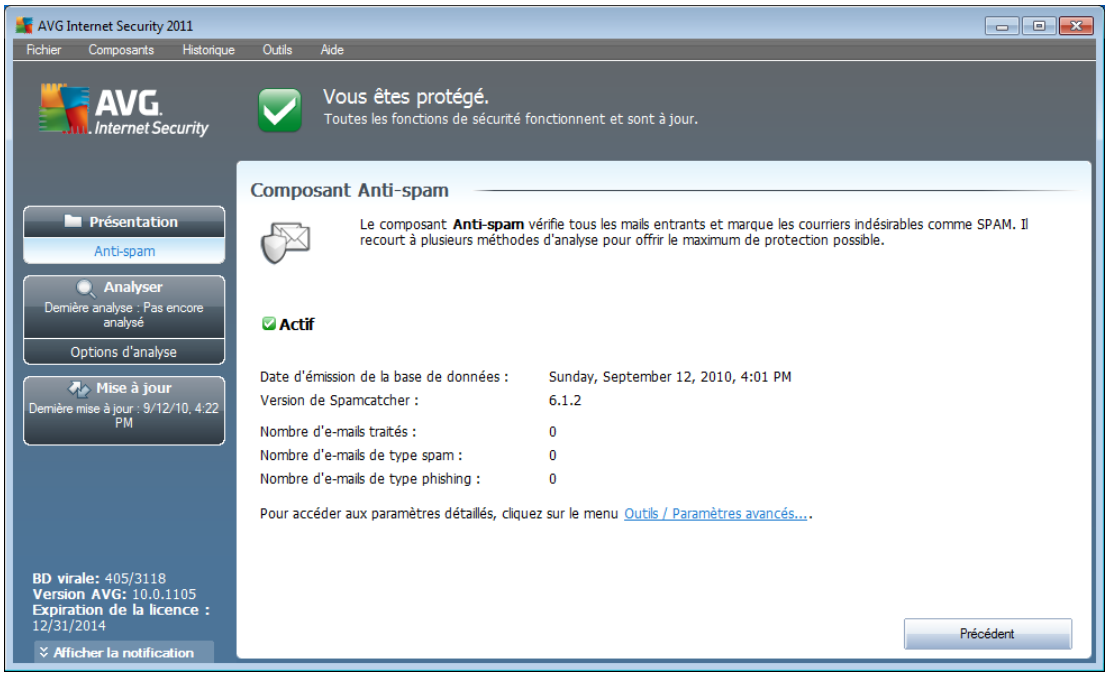
Le terme « spam » désigne un message indésirable ; il s'agit généralement d'un produit ou d'un service à caractère publicitaire envoyé en masse à de nombreuses adresses électroniques ayant pour conséquence d'encombrer les boîtes aux lettres des destinataires. Il faut distinguer le spam des autres messages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

7.3.1. 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*).

7.3.2. Interface de l'Anti-Spam



La boîte de dialogue du composant ***Anti-spam*** fournit une brève description du fonctionnement du composant, des informations sur son état actuel et les 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
- ***Nombre d'e-mails traités*** - indique le nombre d'e-mails analysés depuis la dernière exécution du moteur anti-spam
- ***Nombre d'e-mails de type spam*** - indique le nombre d'e-mails signalés comme indésirables par rapport au nombre d'e-mails analysés
- ***Nombre d'e-mails de type phishing*** - indique le nombre d'e-mails signalés comme étant à l'origine d'une tentative de phishing par rapport au nombre d'e-mails analysés

La boîte de dialogue ***Anti-Spam*** inclut également un lien ***Outils/Paramètres avancés. Ce lien permet d'être redirigé vers l'environnement de la configuration avancée de l'ensemble des composants **AVG Internet Security 2011** .

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. Toute modification de ces paramètres doit être*

réalisée par un utilisateur expérimenté.

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*).

7.4. 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.*

7.4.1. 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 :

- Autoriser ou bloquer automatiquement les tentatives de communication des applications connues ou demander votre confirmation
- Utiliser des profils complets avec des règles prédéfinies en fonction de vos besoins
- Changer automatiquement de profil lors de la connexion à différents réseaux ou de l'utilisation de divers adaptateurs réseau

7.4.2. 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 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***:
  - ***Directement connecté à Internet*** – recommandé pour les ordinateurs domestiques directement reliés 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.

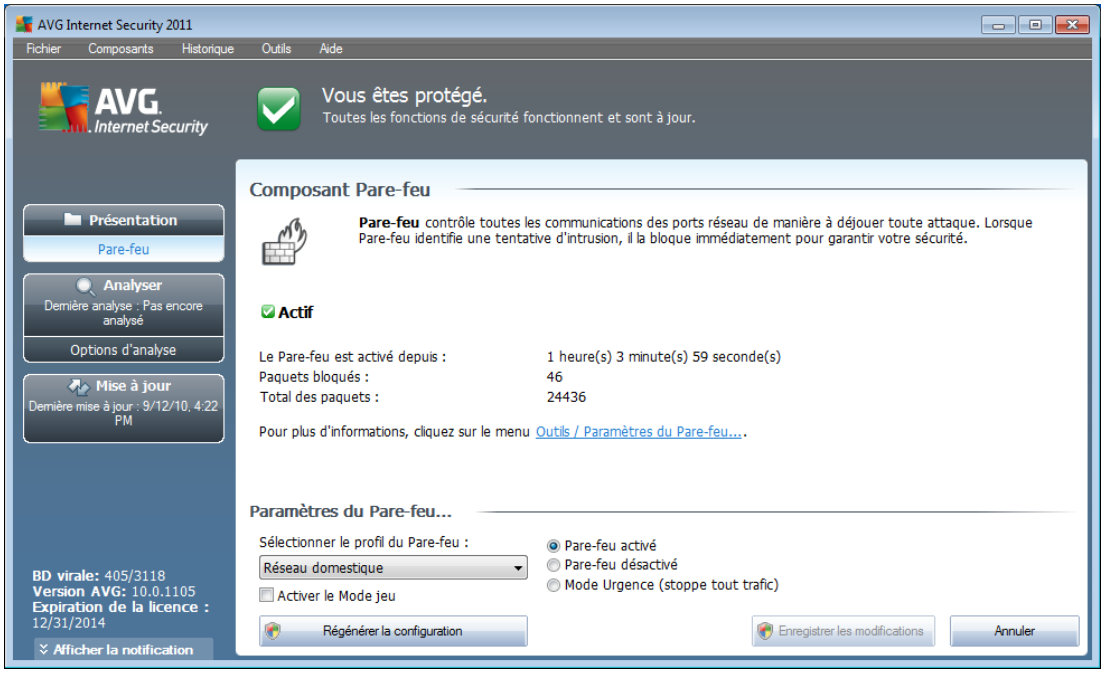
Changement de profil

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* .

7.4.3. Interface du Pare-feu



L'interface du composant ***Pare-feu*** donne des informations de base sur la fonctionnalité du composant, son état, 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

Paramètres - Pare-feu

- ***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 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. En mode jeu, toutes les tâches programmées (*analyses, mises à jour*) sont reportées jusqu'à la fermeture de l'application.

- ***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 vise à bloquer l'ensemble du trafic sur chaque port réseau; le ***Pare-feu*** fonctionne, mais aucun trafic réseau n'est stoppé

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 apparaît.*

Boutons de commande

- ***Regénérer la configuration*** - cliquez sur ce bouton pour remplacer la configuration du ***Pare-feu*** et rétablir la configuration par défaut selon la détection automatique.
- ***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 (*avec la présentation générale des composants*)

7.5. LinkScanner

7.5.1. Principes de LinkScanner

LinkScanner est conçu pour lutter contre les menaces d'un jour sans cesse plus nombreuses; ces dernières disparaissent dès le lendemain de leur apparition sur Internet. Ces menaces peuvent infiltrer n'importe quel type de site Web, des sites gouvernementaux aux sites des PME en passant par ceux de marques bien connues. Elles ne s'attardent rarement plus de 24 heures sur un site. Pour vous protéger, le ***LinkScanner*** analyse les pages Web indiquées par les liens de la page que vous consultez et vérifie qu'elles sont sûres au moment crucial, c'est-à-dire lorsque vous

êtes sur le point de cliquer sur un lien.

La technologie du ***LinkScanner*** se base sur deux fonctions, ***Search-Shield*** et ***Surf-Shield*** :

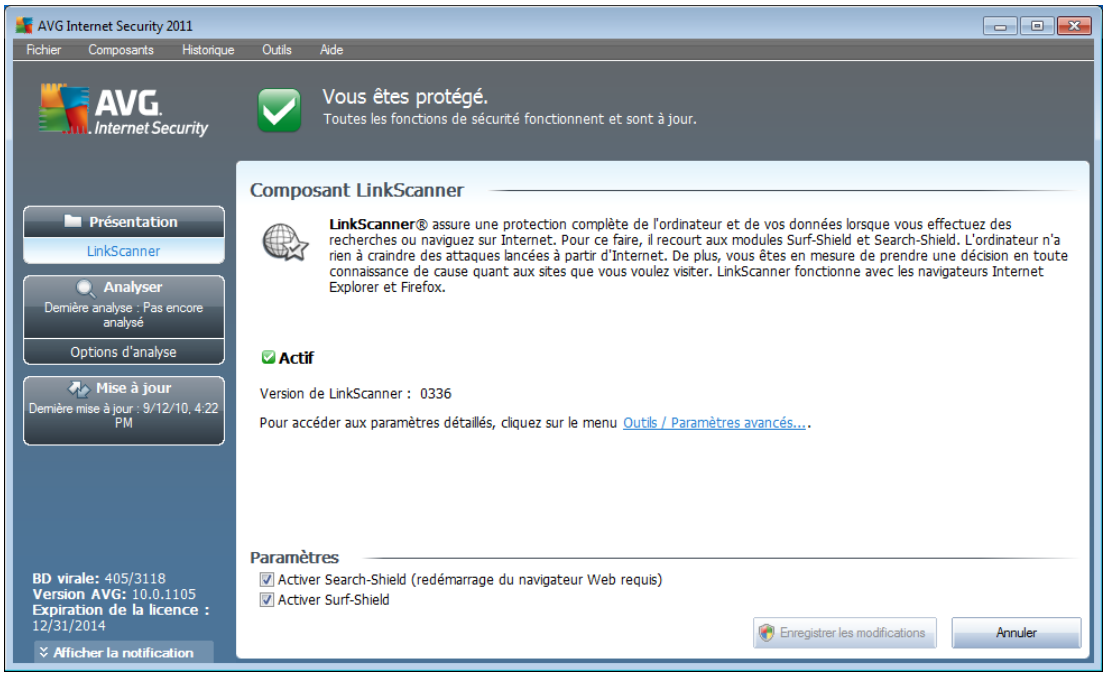
- ***Search-Shield*** contient une liste de sites Web (*adresses URL*) connus pour leur dangerosité. Lors d'une recherche sur Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg ou SlashDot, les résultats de recherche sont comparés à cette liste, puis une icône rendant un verdict sur la sécurité s'affiche (*sur Yahoo!, seules les icônes indiquant que le site Web est piraté s'affichent*).

- ***Surf-Shield***analyse le contenu des sites Web que vous visitez, quelle que soit leur adresse. Même si ***Search-Shield*** ne détecte pas un site Web donné (*par exemple lorsqu'un nouveau site malveillant est créé ou lorsqu'un site officiel est contaminé*), ***Surf-Shield*** le détecte et le bloque si vous essayez d'y accéder.

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

7.5.2. Interface de LinkScanner

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



Paramètres LinkScanner

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

- ***Activer Search-Shield*** - (*option activée par défaut*) : icônes de notification portant sur les recherches effectuées à l'aide des moteurs Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, ou SlashDot après vérification préalable du contenu des sites renvoyés par le moteur de recherche.

- ***Activer Surf-Shield*** : (*option activée par défaut*) : protection active (*en temps réel*) contre les sites hébergeant 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*).

7.5.3. Search-Shield

Lorsque vous effectuez des recherches sur Internet et que le module ***Search-Shield*** est activé, tous les résultats de recherche renvoyés par les moteurs de recherche les plus courants (*Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg et SlashDot*) sont évalués pour définir la dangerosité de leurs liens. Grâce à cette vérification des liens et au signalement des mauvais liens, ***AVG LinkScanner*** signale les liens dangereux ou suspects 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. Lorsque l'évaluation du risque est terminée, l'icône d'information correspondante 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 n'est pas fiable ou contient des liens menant à des pages dont les résultats d'analyse sont positifs ou dont le code est suspect, même s'il n'est pas directement lié pour le moment à des menaces.

La page liée 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.

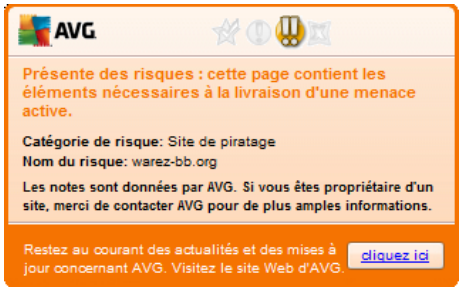
Le fait de placer le pointeur sur une icône d'évaluation permet d'obtenir des

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 :

7.5.4. 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, ***AVG Link Scanner*** n'autorisera pas votre navigateur à l'afficher.

Si vous rencontrez un site Web malveillant, ***AVG Link Scanner*** vous le signalera dans votre navigateur en affichant un écran comparable à celui-ci :



L'accès à un tel site Web s'effectue à vos risques et périls et est fortement déconseillé !

7.6. Bouclier résident

7.6.1. 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 pas la possibilité au virus de

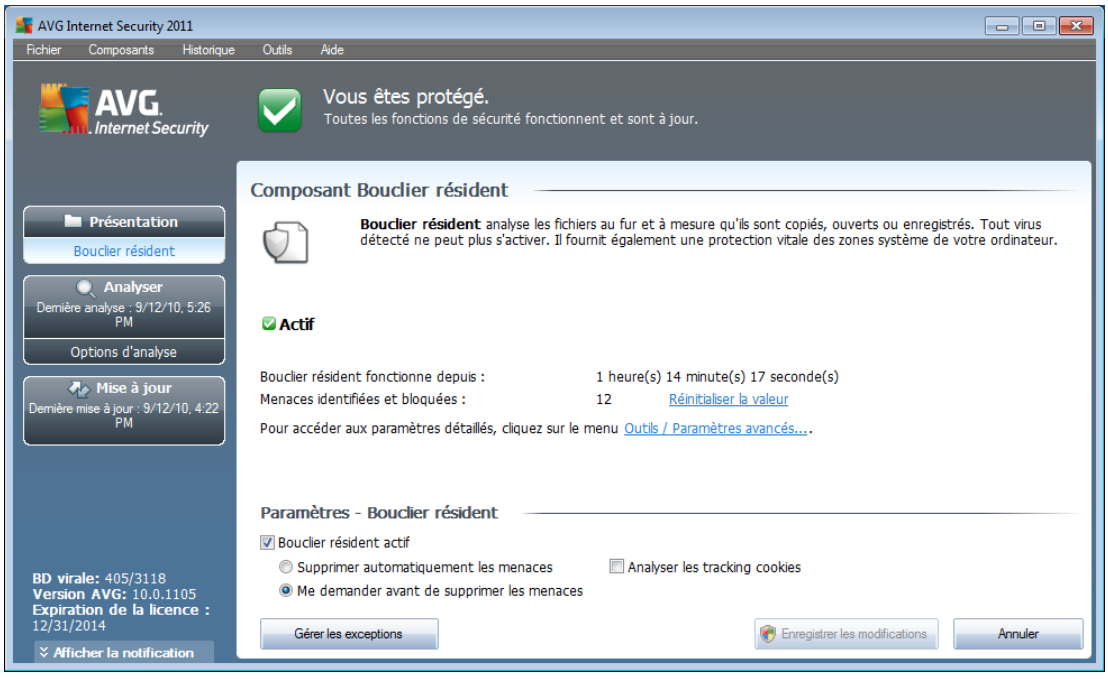
s'activer. Généralement, vous ne remarquez pas ce processus, car il fonctionne "en arrière-plan". Vous êtes seulement averti en cas de détection de menaces, tandis que le ***Bouclier résident*** bloque l'activation de la menace et l'éradique. Le ***Bouclier résident*** est chargé dans la mémoire de votre ordinateur au démarrage du système.

Actions possibles du Bouclier résident :

- Recherche de types spécifiques de menaces possibles
- *Analyse des supports amovibles (clés USB, etc.)*
- Analyse des fichiers ayant une extension déterminée ou sans précision d'extension
- Autorisation d'exceptions pour l'analyse – des fichiers ou des dossiers spécifiques qui ne doivent jamais être analysés

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

7.6.2. Interface du Bouclier résident



Outre une présentation du fonctionnement du composant ***Bouclier résident*** et des informations sur son état, l'interface du ***Bouclier résident*** fournit quelques données statistiques :

- ***Le Bouclier résident est actif depuis***- indique le temps écoulé depuis le dernier lancement du composant
- ***Menaces identifiées et bloquées*** - indique le nombre d'infections détectées

dont l'exécution ou l'ouverture a été bloquée (*il est possible de réinitialiser cette valeur, si besoin est, à des fins statistiques par exemple - Réinitialiser la valeur*)

Paramètres - Bouclier résident

Dans la partie inférieure de la boîte de dialogue figure la section ***Paramètres du Bouclier résident***, dans lequel vous pouvez modifier certains paramètres de base de la fonctionnalité du composant (*comme pour tous les autres composants, la configuration détaillée est accessible via l'élément Outils/Paramètres avancés du menu système*).

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 de l'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 : 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 leur panier d'achat électronique*).

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 :

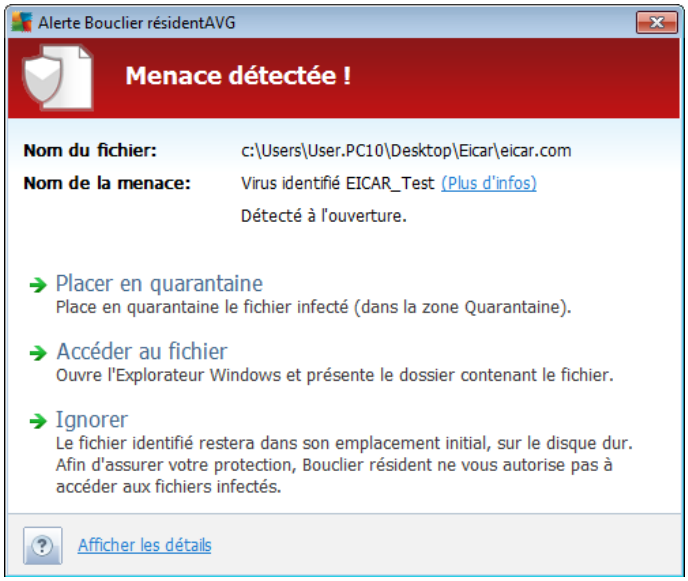
- ***Gérer les exceptions*** - ouvre la boîte de dialogue ***Bouclier résident - Eléments exclus*** où vous pouvez définir les dossiers à ne pas inclure dans l'analyse du ***Bouclier résident***

- ***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 (*avec la présentation générale des composants*)

7.6.3. 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 :



Dans cette fenêtre d'avertissement, vous trouverez des informations sur le fichier qui a été détecté et défini comme étant infecté (*Nom du fichier*), le nom de l'infection reconnue (*Nom de la menace*) ainsi qu'un lien renvoyant à l'***Encyclopédie des virus*** contenant de plus amples détails sur l'infection, le cas échéant (*Plus d'infos*).

Par la suite, vous devez décider la mesure à appliquer ; vous avez le choix entre les options suivantes :

Notez que, dans certaines conditions (type de fichier infecté et emplacement du fichier), certaines de ces options ne sont pas actives !

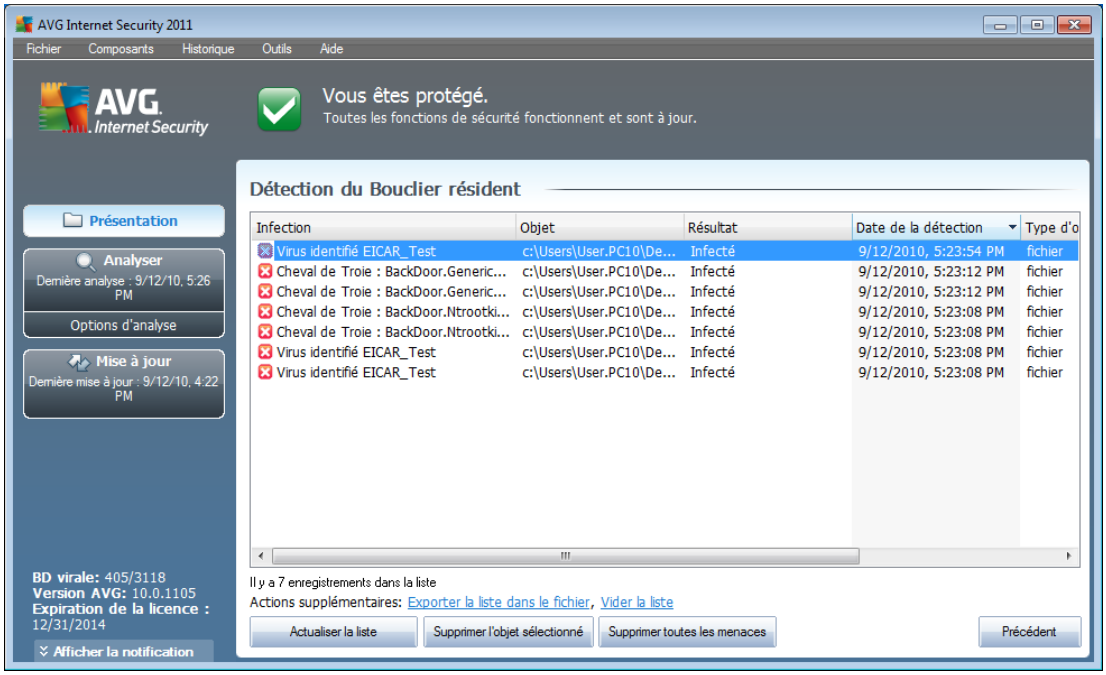
- ***Supprimer la menace en tant qu'utilisateur avancé*** - cochez cette case si, en tant que simple utilisateur, vous pensez ne pas disposer des droits suffisants pour supprimer la menace. Les utilisateurs avec pouvoirs ont des droits d'accès étendus. Si la menace est située dans un dossier système déterminé, vous pouvez avoir besoin de cocher cette case pour la supprimer.

- ***Réparer*** - ce bouton ne s'affiche que si une solution permettant de traiter l'infection décelée existe. Dans ce cas, elle élimine l'infection et rétablit l'état initial du fichier. Si le fichier lui-même est un virus, cette fonction le supprime (*en plaçant le fichier dans la zone* ***Quarantaine***)

- ***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 !

Dans la section inférieure de la boîte de dialogue, vous trouverez le lien ***Afficher les détails***. Cliquez dessus pour ouvrir la fenêtre contenant des informations détaillées sur le processus en cours lorsque l'infection a été détectée et l'identification du processus.

Vous trouverez des informations sur la présentation des menaces détectées par le ***Bouclier résident*** dans la boîte de dialogue ***Détection par le Bouclier résident*** accessible par la barre de menus ***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
- ***Date 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*** permet de revenir dans l'***interface utilisateur AVG*** par défaut (*présentation des composants*).

7.7. 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 offrent un risque élevé de réception de messages électroniques 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 leurs données personnelles (*adresse e-mail, par exemple*) dans des formulaires en ligne, ces usagers contribuent à augmenter les risques 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.

7.7.1. Principes du Scanner e-mail

Le Scanner e-mail analyse automatiquement les messages entrants et sortants. Vous pouvez l'utiliser avec les clients de messagerie qui ne possèdent pas leurs propres plug-ins AVG (*mais, il peut également être utilisé pour lire les mails des clients de messagerie qu'AVG prend en charge au moyen d'un plug-in donné (Microsoft Outlook, The Bat*, par exemple). Il est principalement destiné au applications telles que Outlook Express, Thunderbird, 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, 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.

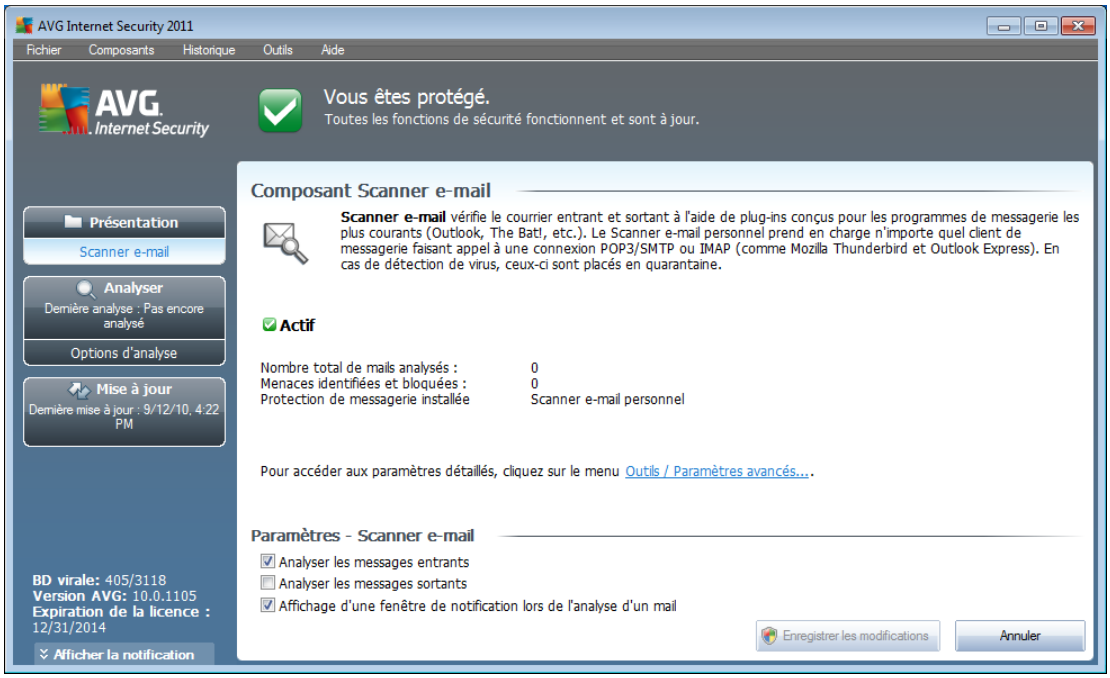
- ***Message entrant :*** lorsque vous recevez un message du serveur, le composant ***Scanner e-mail*** vérifie s'il ne contient pas de virus, supprime les pièces jointes infectées (le cas échéant) et ajoute la certification. Lorsque des virus sont détectés, ils sont immédiatement placés en ***Quarantaine***.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

7.7.2. Interface du Scanner e-mail



La boîte de dialogue du composant ***Scanner e-mail*** décrit précisément le fonctionnement du composant et indique son état actuel. Elle fournit aussi les informations statistiques suivantes :

- ***Nombre total de mails analysés*** - nombre de messages analysés depuis le démarrage du ***Scanner e-mail*** (*il est éventuellement possible de réinitialiser cette valeur, à des fins statistiques par exemple*)
- ***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

Paramètres - Scanner e-mail

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.

- ***Affichage d'une fenêtre de notification lors de l'analyse d'un mail***- cochez cette case pour qu'une info-bulle de notification s'affiche au-dessus de l'icône AVG dans la barre d'état système au cours de l'analyse du message par le composant ***Scanner e-mail***. Par défaut, la case est activée et il est recommandé de ne pas modifier ce paramètre.

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 est réservée aux 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.*

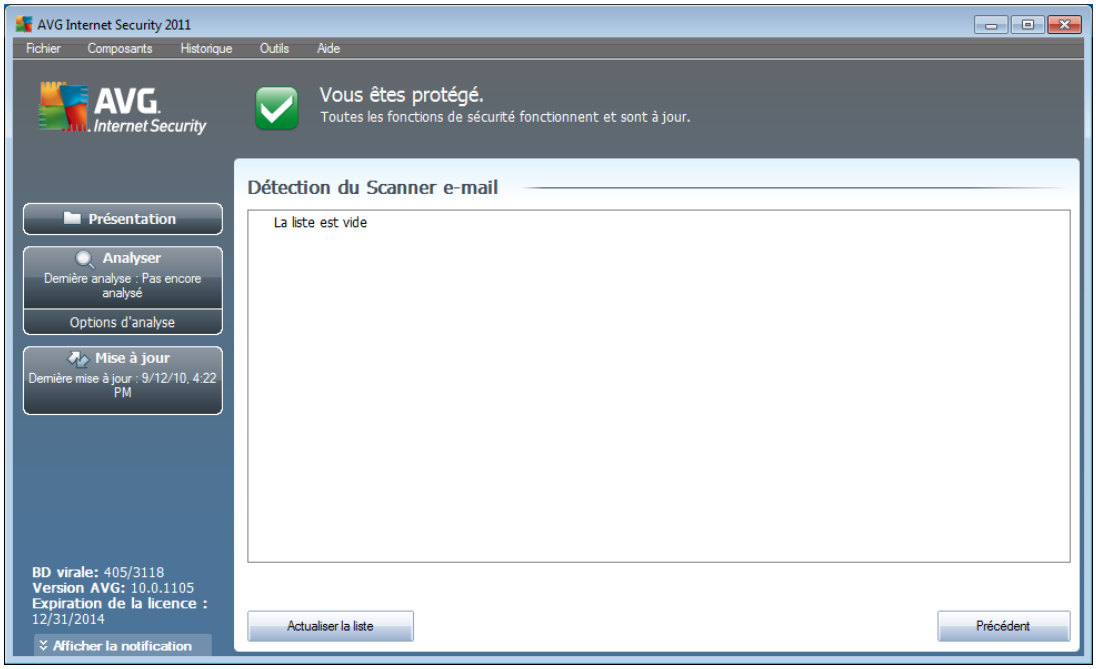
Boutons de commande

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 (*avec la présentation générale des composants*)

7.7.3. Détection du Scanner e-mail



Dans la boîte de dialogue ***Détection du Scanner E-mail*** (*accessible par le menu Historique / Détection du Scanner E-mail*), vous accédez à 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
- ***Précédent*** - revient à la boîte de dialogue précédente

7.8. Mise à jour

7.8.1. Principes du composant Mise à jour

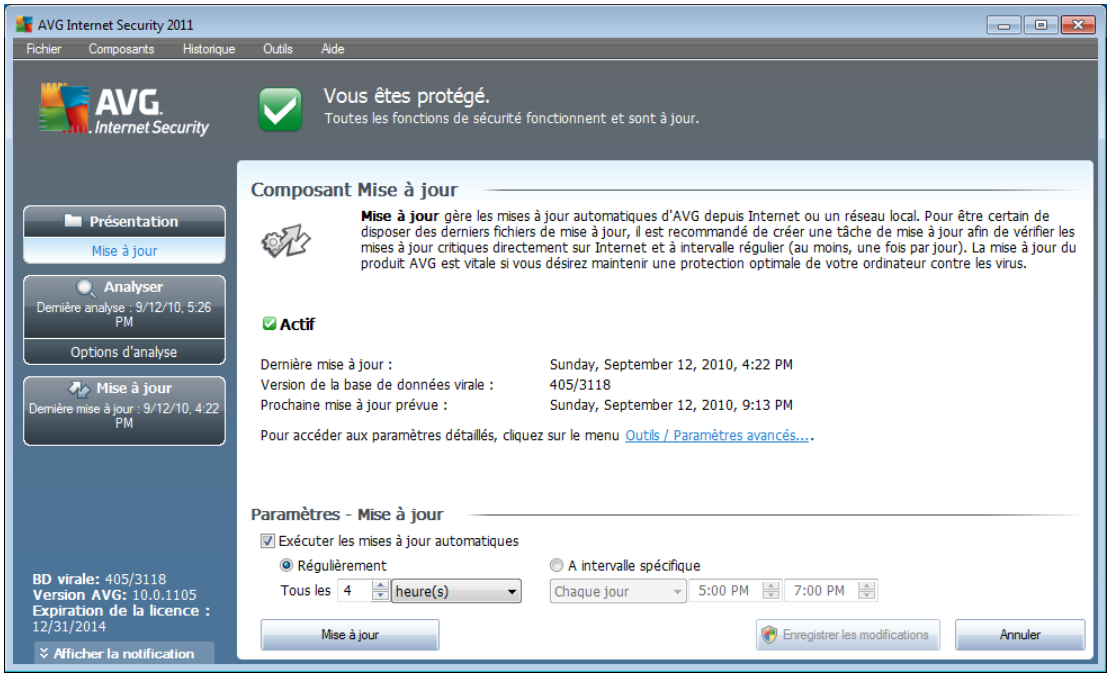
Aucun logiciel de sécurité ne peut garantir une protection fiable contre la diversité des menaces à moins d'une mise à jour régulière. Les auteurs de virus sont toujours à l'affût de nouvelles failles des logiciels ou des systèmes d'exploitation. Chaque jour apparaissent de nouveaux virus, malwares et 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 d'AVG pour plus d'informations sur les différents types et niveaux de mises à jour.*

7.8.2. Interface du composant Mise à jour



L'interface ***Mise à jour*** affiche des informations sur la fonctionnalité du composant, sur son état actuel et certaines 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*** - indique le numéro de la version de la base de données virale actuellement installée; 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

Paramètres - Mise à jour

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

- o ***A intervalle spécifique*** - précisez l'heure exacte à laquelle la mise à jour doit avoir lieu

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.

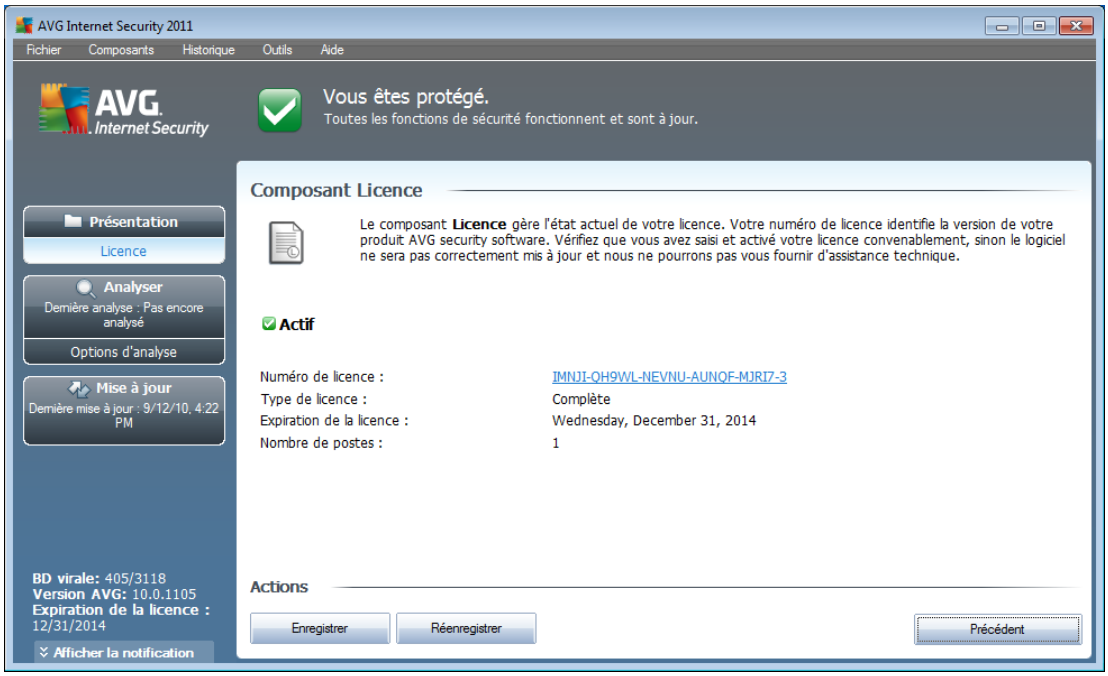
Remarque : *l'éditeur du logiciel a configuré tous les composants AVG de manière à obtenir des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté. Si vous devez 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 de ***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 (*avec la présentation générale des composants*)

7.9. Licence



L'interface du composant ***Licence*** décrit brièvement le fonctionnement du composant, indique son état actuel et fournit les informations suivantes :

- ***Numéro de licence*** - désigne la forme abrégée de votre numéro de licence (*pour des raisons de sécurité, les quatre derniers caractères sont absents*). Lorsque vous saisissez un numéro de licence, vous devez le saisir exactement tel qu'il est affiché. Par conséquent, nous vous conseillons vivement de toujours procéder par "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 Internet Security 2011** après cette date, il est nécessaire de renouveler votre licence. Le renouvellement peut être réalisé en ligne sur le site Web d'AVG.

- ***Nombre de postes*** - nombre de postes de travail sur lequel vous êtes autorisé à installer le produit **AVG Internet Security 2011**.

Boutons de commande

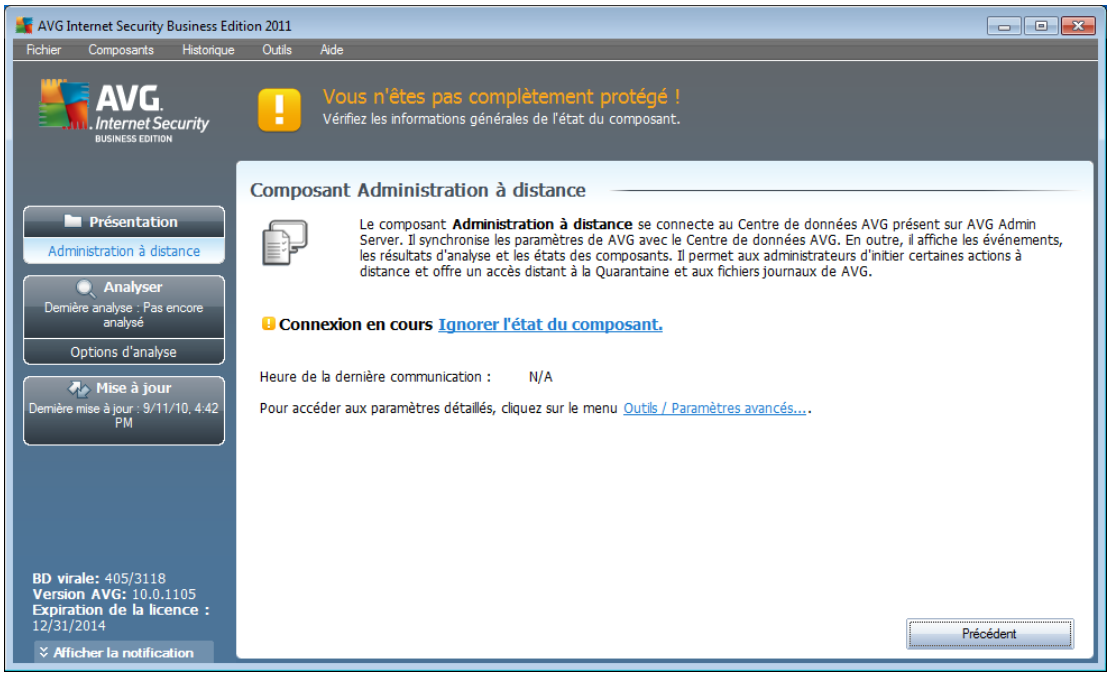
- ***Enregistrer*** - renvoie à la page d'enregistrement du site Web d'AVG (http://www.avg.com/). Merci de compléter le formulaire d'enregistrement ; seuls les clients ayant dûment enregistré leur produit AVG peuvent bénéficier de l'assistance technique gratuite.

- ***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*).

Remarque : si vous utilisez une version d'évaluation *AVG Internet Security 2011* **, les boutons qui s'affichent sont** *Acheter maintenant* ***et*** *Activer et vous permettent de vous procurer de suite la version complète du programme. Si le programme* **AVG Internet Security 2011** *est installé à l'aide d'un numéro d'achat, vous avez alors le choix entre les* ***Enregistrer*** *et* ***Activer***.

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

7.10. Administration à distance



Le composant ***Administration à distance*** s'affiche seulement dans l'interface utilisateur **AVG Internet Security 2011** lorsque vous avez installé l'Edition Réseau du produit (*voir le composant* ***Licence***). Dans la boîte de dialogue ***Administration à distance***, vous pouvez savoir si le composant est actif et connecté au serveur. Tous les paramètres du composant ***Administration à distance*** doivent être définis dans ***Paramètres avancés / Administration à distance***.

Pour obtenir une description détaillée des options et de la fonctionnalité du composant dans le système AVG, reportez-vous à la documentation spécifique consacrée à ce sujet. Cette documentation est téléchargeable à partir du site Web d'AVG (www.avg.com), section ***Centre de Support / Téléchargement / Documentation*** .

Boutons de commande

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

7.11. Bouclier Web

7.11.1. Principes du Bouclier Web

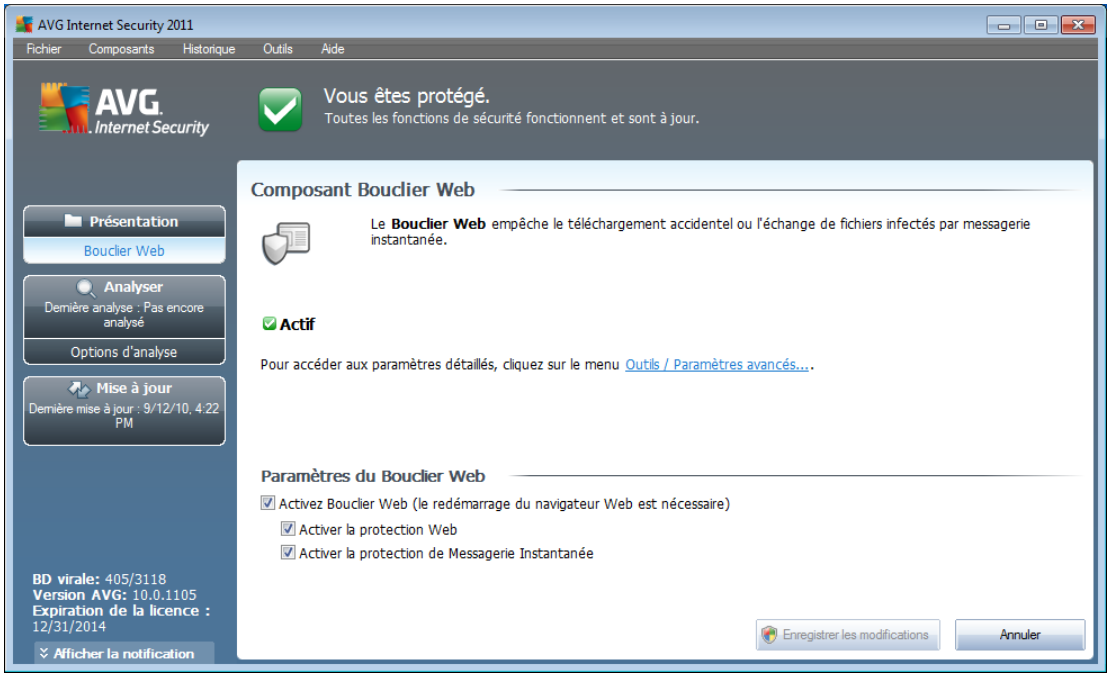
Le ***Bouclier Web*** est une protection résidente en temps réel ; il analyse le contenu des pages Web visitées (*et les fichiers qu'elles contiennent*) avant que celles-ci ne s'affichent dans le navigateur ou ne soient téléchargées sur l'ordinateur.

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 !*

7.11.2. Interface du Bouclier Web

L'interface du composant ***Bouclier Web*** décrit le fonctionnement de ce type de protection. Vous y trouverez également des informations sur le statut du composant. Dans la partie inférieure de la boîte de dialogue, vous trouverez des options d'édition élémentaires pour ce composant:



Paramètres du Bouclier Web

En premier lieu, vous êtes libre 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. Si la case est cochée et que le ***Bouclier Web*** est actif, deux autres options de configuration sont disponibles :

- ***Activer la Protection Web*** - cette option confirme que le ***Bouclier Web*** doit analyser le contenu des pages Web.

- ***Activer le Bouclier de messagerie instantanée*** - cochez cette option si vous voulez que le ***Bouclier Web*** contrôle l'absence de virus dans les communications de la messagerie instantanée (*ICQ, MSN Messenger, 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

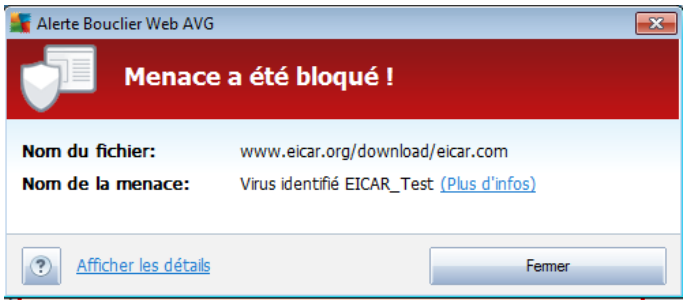
Les boutons de commande disponibles dans l'interface du ***Bouclier Web*** sont :

- ***Enregistrer 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*)

7.11.3. Détection du Bouclier Web

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



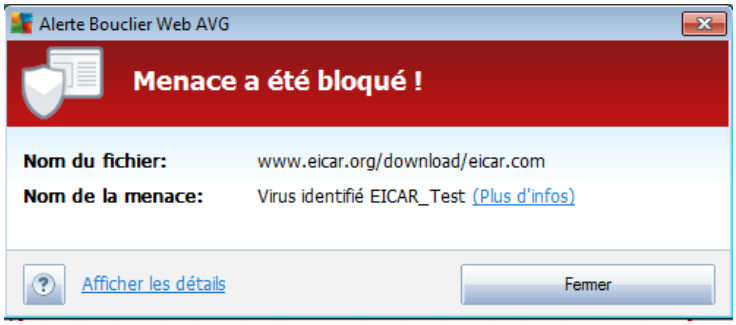
Dans cette boîte de dialogue d'avertissement, vous trouverez des informations sur le fichier qui a été détecté et défini comme infecté (*Nom du fichier*), le nom de l'infection reconnue (*Nom de la menace*) ainsi qu'un lien renvoyant à l'***Encyclopédie des virus*** contenant de plus amples détails sur l'infection (*le cas échéant*). Cette boîte de dialogue présente les boutons de fonction suivantes :

- ***Afficher les détails*** - cliquez sur le bouton ***Afficher les détails*** pour ouvrir une fenêtre contenant des informations détaillées sur le processus en cours lorsque

l'infection a été détectée et l'identification du processus.

- ***Fermer*** - cliquez sur le bouton pour fermer la boîte de dialogue.

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 rafraîchir la liste des menaces détectées par le ***Bouclier Web***. Le bouton ***Précédent*** permet de revenir dans l'***interface utilisateur AVG*** par défaut (*présentation des composants*).

7.12. Anti-Rootkit

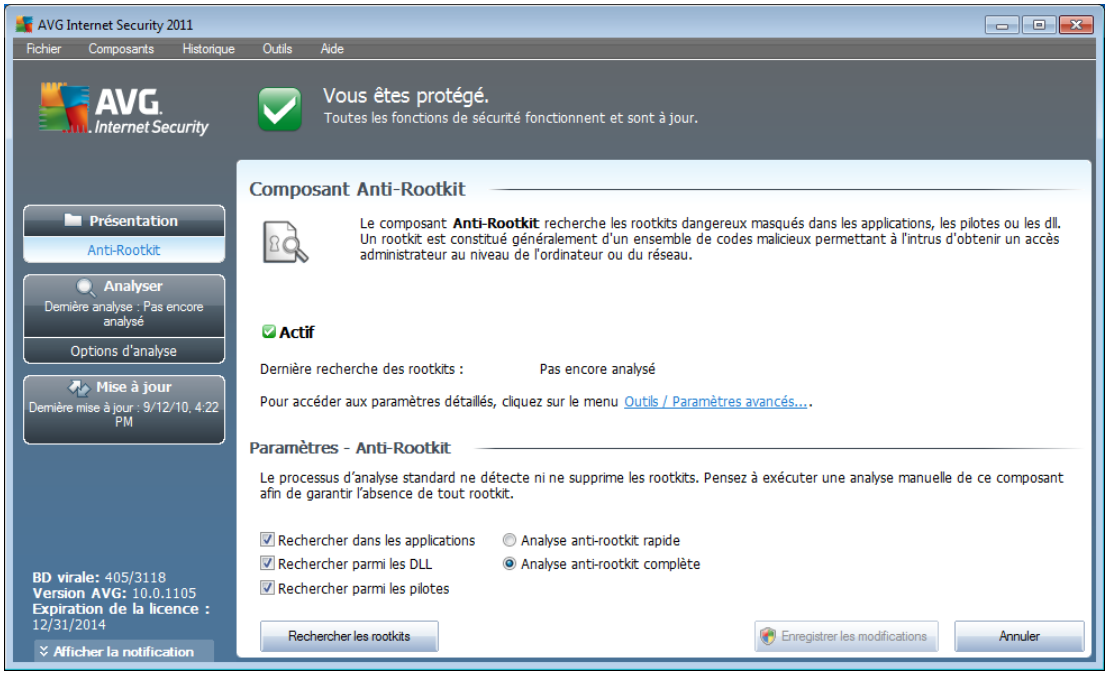
Un rootkit est un programme conçu pour prendre le contrôle du système, sans l'autorisation de son propriétaire et de son administrateur légitime. Un accès matériel est rarement nécessaire car un rootkit est prévu pour s'introduire dans le système d'exploitation exécuté sur le matériel. En règle générale, les rootkits dissimulent leur présence dans le système en dupant ou en contournant les 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.

7.12.1. 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.

7.12.2. Interface de l'Anti-Rootkit



L'interface utilisateur ***Anti-Rootkit*** décrit brièvement le rôle du composant , indique l'état actuel du composant et fournit des informations sur la dernière analyse effectuée par le module ***Anti-Rootkit*** (***Dernière recherche des rootkits***). La boîte de dialogue ***Anti-Rootkit*** inclut également un lien ***Outils/Paramètres avancés***. Ce lien permet d'être redirigé vers l'environnement de la configuration avancée du composant ***Anti-Rootkit***.

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.*

Paramètres - Anti-Rootkit

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 tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows*)
- ***Analyse anti-rootkit complète*** - analyse tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows généralement*), ainsi que tous les disques locaux (*y compris le disque flash, mais pas les lecteurs de disquettes ou de CD-ROM*)

Boutons de commande

- ***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

7.13. System Tools

System Tools désignent les outils offrant une vue détaillée de l'environnement **AVG Internet Security 2011** et du système d'exploitation. Le composant présente :

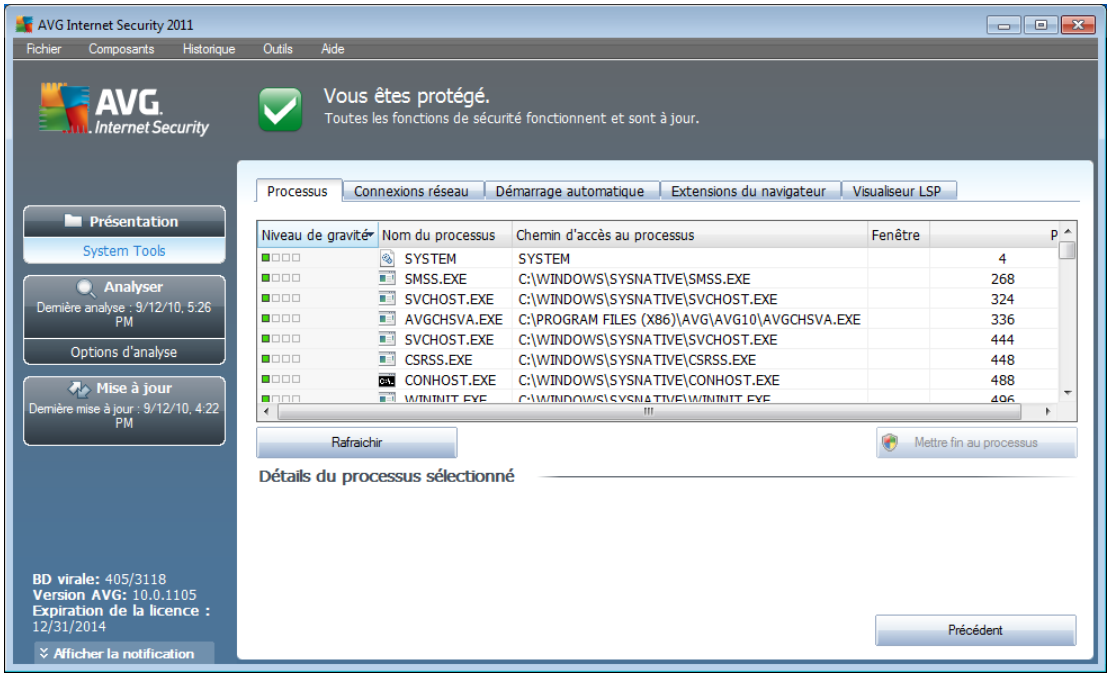
- Processus - liste des processus (*applications en cours d'exécution*) actifs sur votre ordinateur
- Connexions réseau - liste des connexions actives
- Démarrage automatique - liste des applications qui s'exécutent au démarrage

de Windows

- Extensions du navigateur - liste des plug-ins (*applications*) installés dans 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 !

7.13.1. 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 :

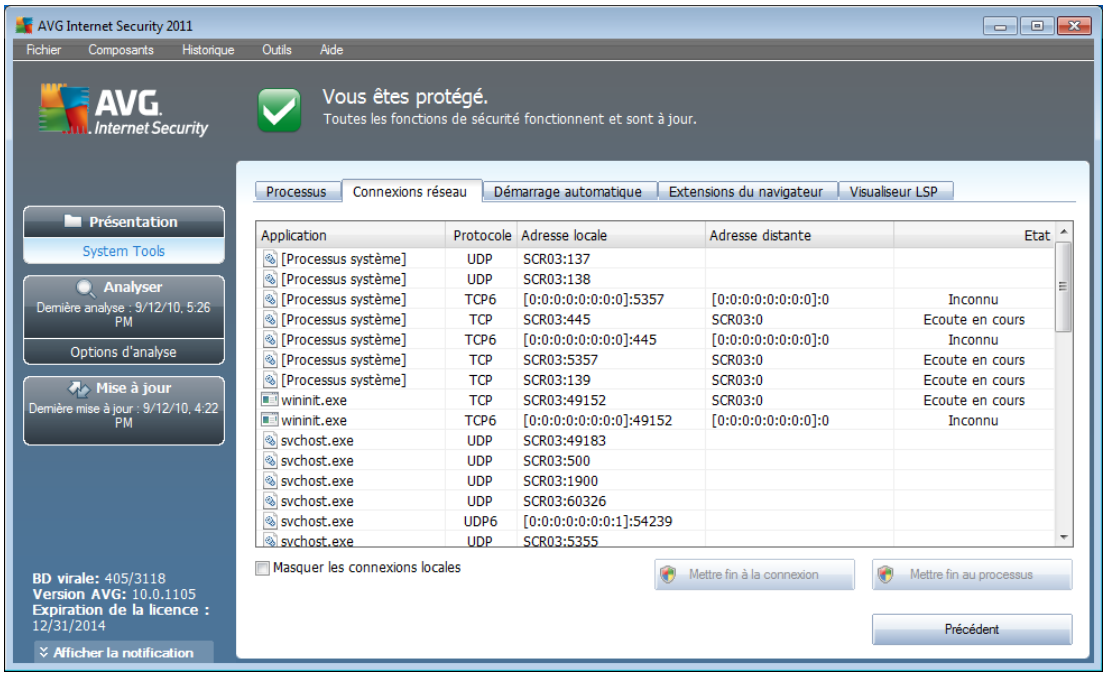
- ***Niveau de gravité*** – identification graphique de la gravité du processus en cours sur quatre niveaux allant du moins dangereux (■□□□) au plus grave (■■■■)
- ***Nom du processus*** - nom du processus en cours
- ***Chemin d'accès au processus*** - chemin d'accès physique menant à un processus actif
- ***Fenêtre*** - indique, le cas échéant, le nom de la fenêtre de l'application
- ***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!***
- ***Précédent*** - permet de revenir à l'interface utilisateur AVG par défaut (*présentation des composants*).

7.13.2. Connexions réseau



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

- ***Application*** - nom de l'application liée à la connexion (*sauf pour Windows 2000 pour lequel les informations ne sont pas disponibles*)
- ***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.

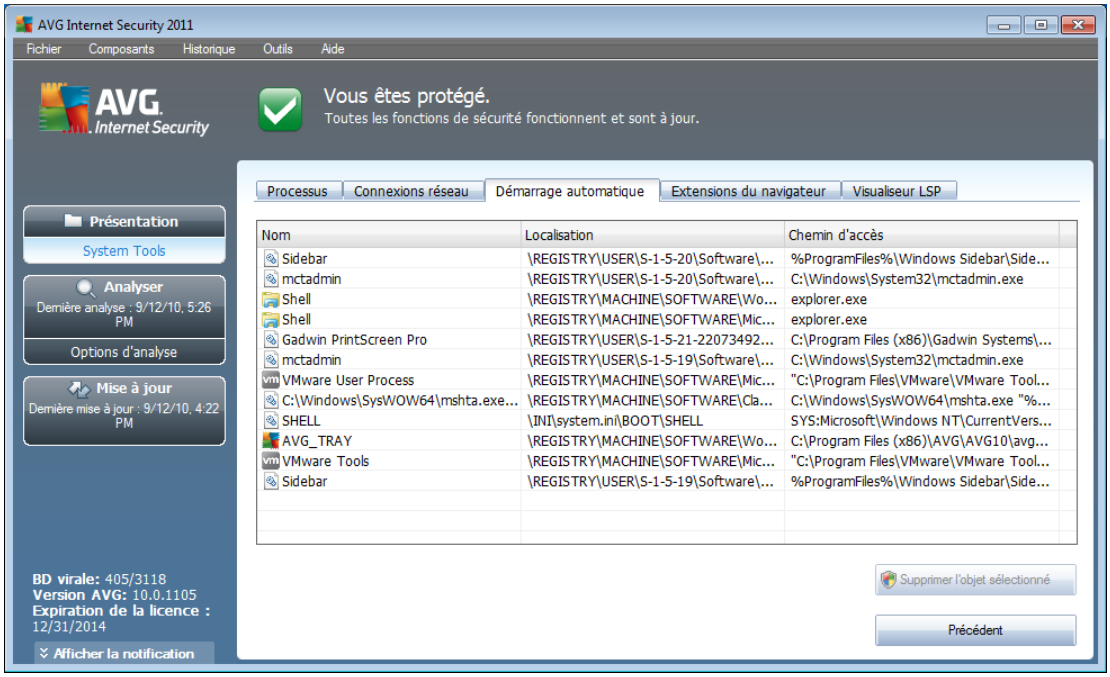
Boutons de commande

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 associées aux connexions sélectionnées dans la liste
- ***Précédent*** - permet de revenir à l'***interface utilisateur AVG*** par défaut (présentation 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.

7.13.3. Démarrage automatique

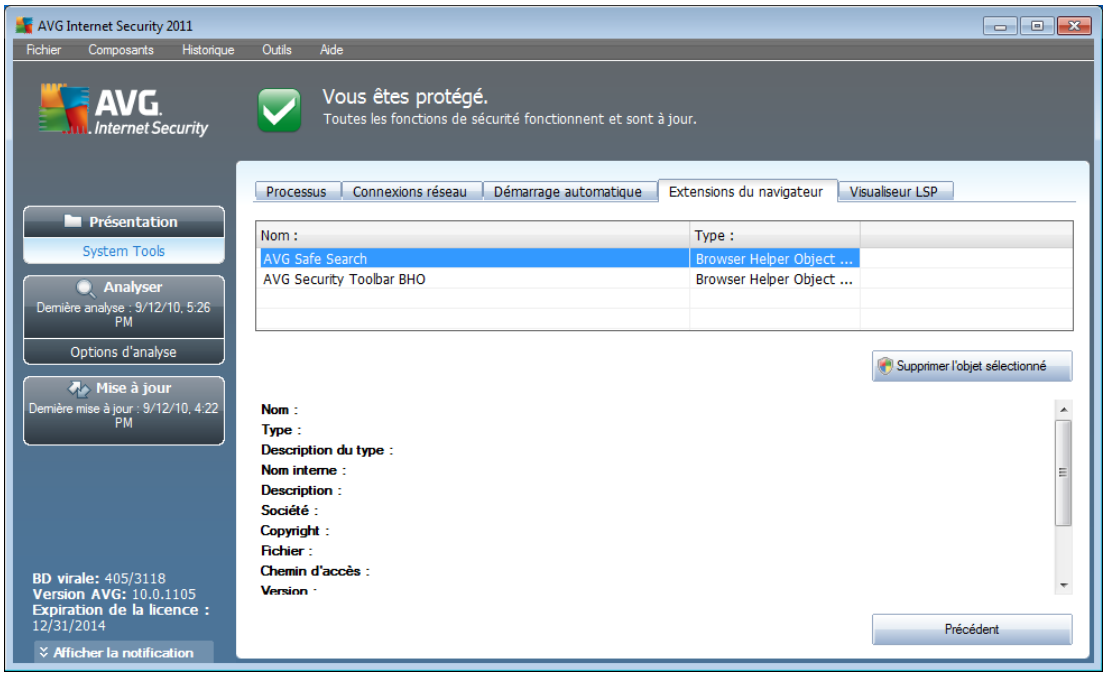


La boîte de dialogue de ***démarrage automatique*** indique toutes les applications qui sont exécutées lors du démarrage système de Windows. Très souvent, des applications malveillantes se greffent sur l'entrée de la base de registre de démarrage.

Vous pouvez supprimer une ou plusieurs entrées en les sélectionnant, puis en cliquant sur le bouton ***Supprimer la sélection.*** Le bouton ***Précédent*** permet de revenir dans l' interface utilisateur AVG par défaut (*présentation des composants*).

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

7.13.4. Extensions du navigateur



La boîte de dialogue***Extensions du navigateur*** contient la liste des plug-ins (*ou applications*) qui sont installés dans votre navigateur Internet. Cette liste est constituée des plug-ins 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.

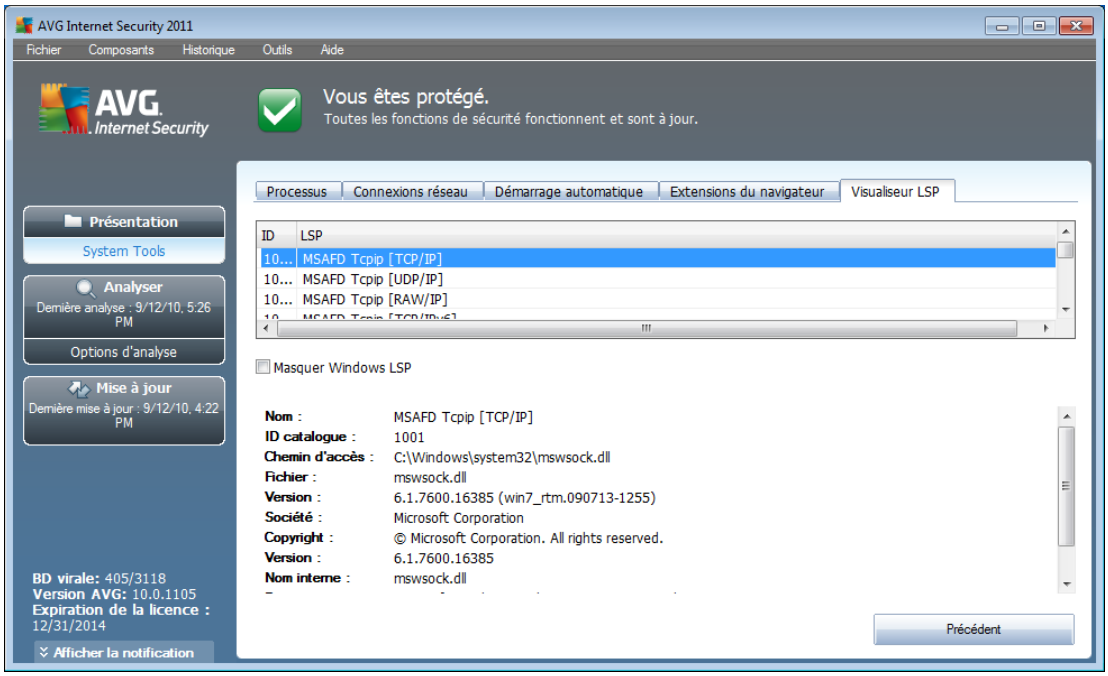
Boutons de commande

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 !***

- ***Précédent*** - permet de revenir à l'interface utilisateur AVG ***par défaut (présentation des composants).***

7.13.5. 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 entrent 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, l'examen minutieux de la liste permet de repérer les menaces LSP potentielles.

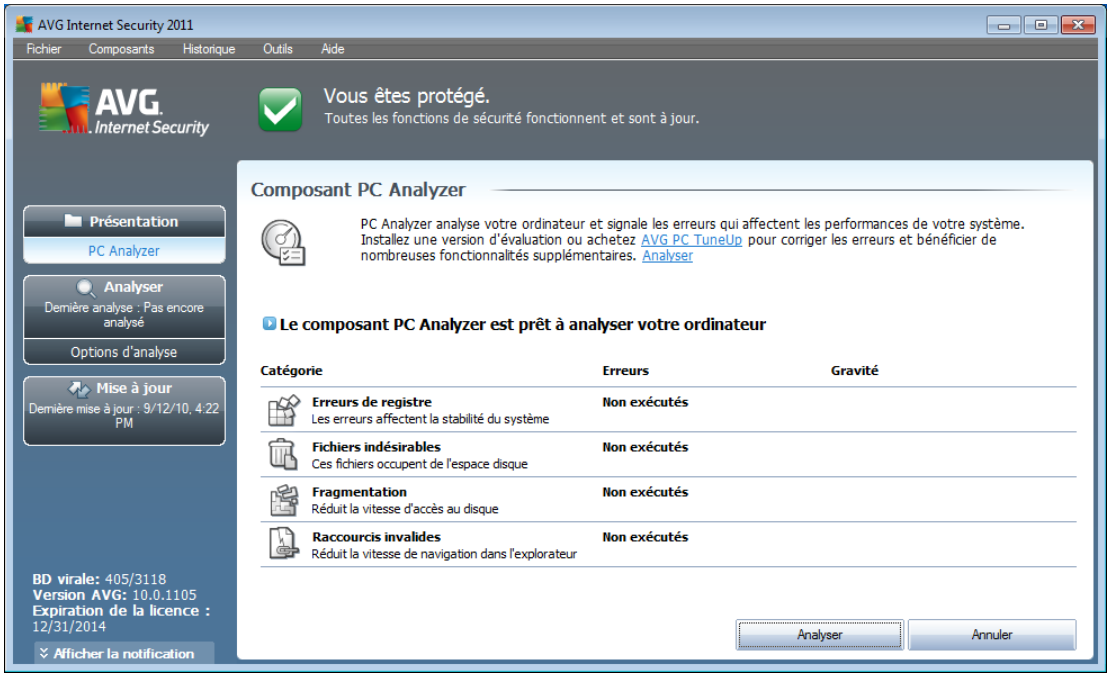
Dans certaines conditions, il est également possible de réparer certains LSP dont le lien est interrompu (*notamment si un fichier est supprimé alors que les entrées correspondantes dans la base de registre sont conservées en l'état*). Un nouveau bouton permettant de résoudre ce genre de problème s'affiche 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*** permet de revenir dans l'***interface utilisateur AVG*** par défaut (*présentation des composants*).

7.14. PC Analyzer

Le composant ***PC Analyzer*** est en mesure de déceler des défaillances système sur l'ordinateur et d'afficher une présentation claire des éléments à l'origine de la diminution des performances générales de l'ordinateur. Dans l'interface utilisateur du

composant, vous pouvez observer un graphique comptant quatre lignes se rapportant aux catégories correspondantes : erreurs de registre, fichiers inutiles, fragmentation et raccourcis corrompus :



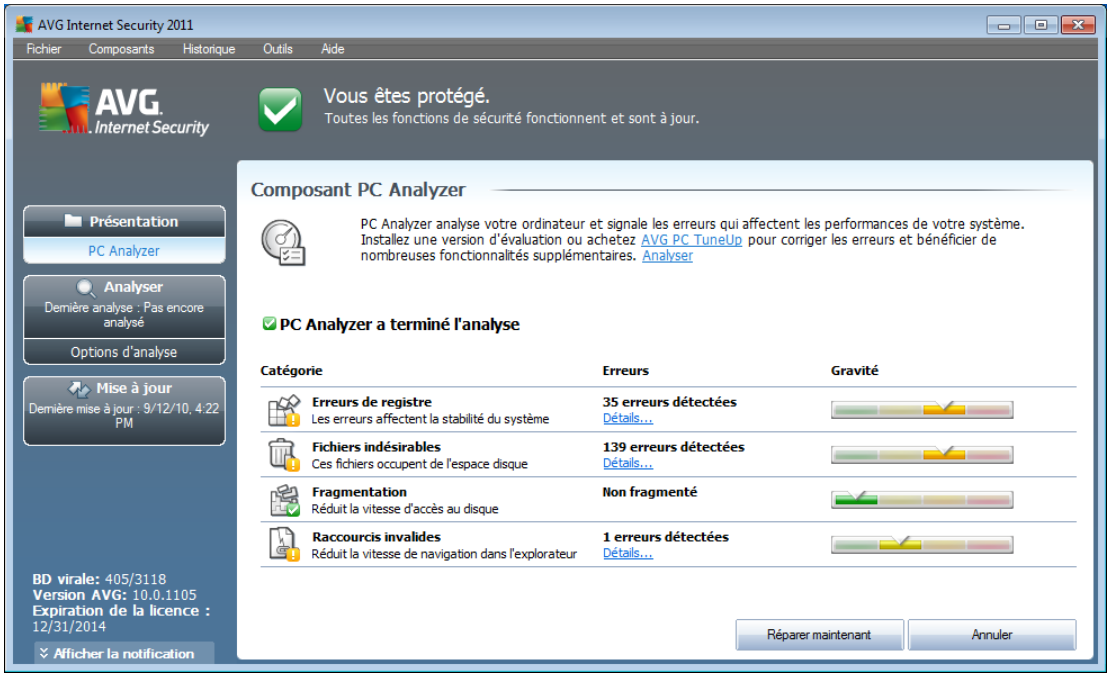
- ***Erreurs de registre*** : indique le nombre d'erreurs dans le Registre Windows. Nous vous déconseillons d'essayer de réparer le registre vous-même, car c'est une tâche qui nécessite des connaissances avancées.

- ***Fichiers indésirables*** : indique le nombre de fichiers probablement inutiles. Généralement, il s'agit de nombreux types de fichiers temporaires et des fichiers qui se trouvent dans la Corbeille.

- ***Fragmentation*** : calcule le pourcentage de l'espace du disque dur qui a été fragmenté, c'est-à-dire utilisé sur une longue durée de sorte que plusieurs fichiers se trouvent éparpillés sur différents volumes du disque physique. Un outil de défragmentation permet de remédier à ce gaspillage.

- ***Raccourcis corrompus*** : indique les raccourcis qui ne fonctionnent plus, mènent à des emplacements inexistants, etc.

Pour lancer l'analyse du système, cliquez sur le bouton ***Analyser***. Vous serez en mesure de suivre la progression de l'analyse et d'examiner ses résultats dans le graphique qui apparaîtra :



Les résultats indiquent le nombre et le type de défaillances système détectées (***Erreurs***) selon les catégories évaluées. Les résultats d'analyse se présentent également sous la forme d'un graphique (axe de la colonne ***Gravité***).

Boutons de commande

- ***En savoir plus*** - cliquez sur ce bouton pour accéder au site Web d'AVG (http://www.avg.com/) à la page fournissant des informations détaillées et à jour sur le composant ***PC Analyzer***

- ***Analyser*** (*à l'écran avant le début de l'analyse*) - ce bouton permet de lancer une analyse immédiate de l'ordinateur

- ***Réparer maintenant*** (*ce bouton apparaît après l'analyse*) - le bouton permet de se rendre sur le site Web d'AVG (http://www.avg.com/) à la page fournissant des informations détaillées et à jour sur le composant ***PC Analyzer***

- ***Annuler*** - cliquez sur ce bouton pour arrêter l'analyse en cours ou pour revenir à l'écran par défaut de l'***interface utilisateur AVG*** (*présentation des composants*) si l'analyse est terminée

7.15. 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

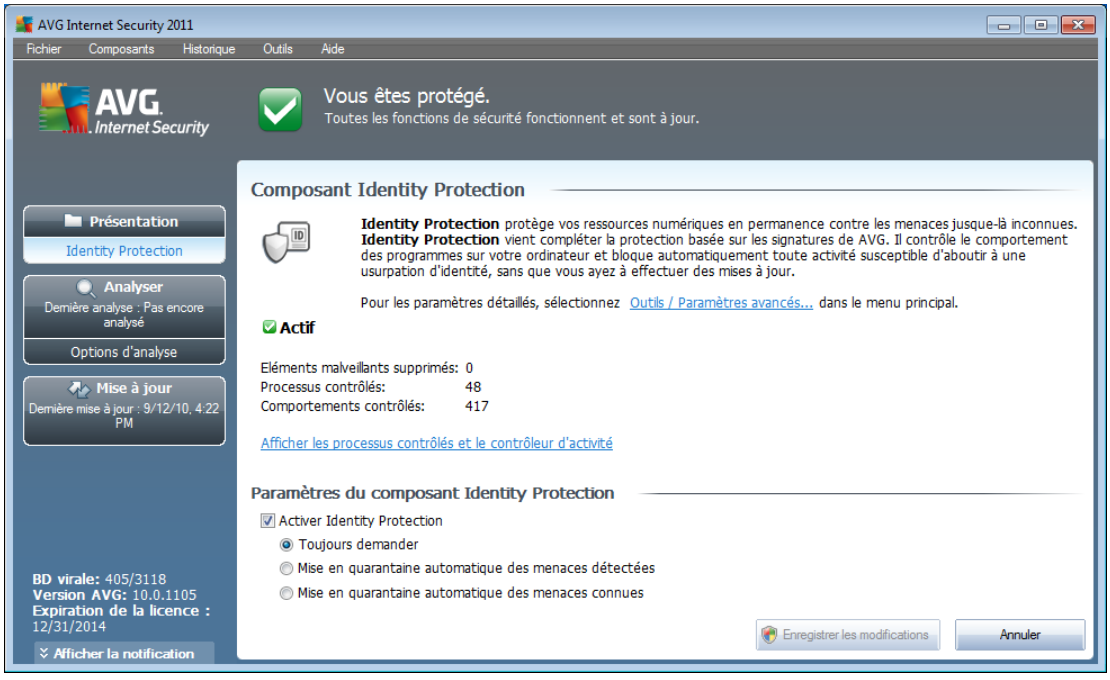
fonctionnent correctement. ***AVG Identity Protection*** détecte et bloque de façon permanente les comportements suspects et protège votre ordinateur contre tous les nouveaux contenus malveillants.

7.15.1. 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.

7.15.2. Interface d'Identity Protection



L'interface du composant ***Identity Protection*** présente brièvement la fonctionnalité du composant, son état et quelques données statistiques :

- ***Eléments 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

Vous trouverez au-dessous le lien ***Afficher les processus contrôlés et le contrôleur d'activité*** qui affiche l'interface utilisateur du composant ***System Tools***. Ce dernier présente de manière détaillée tous les processus sous surveillance.

Paramètres du composant Identity Protection

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 :

- ***Activer Identity Protection*** - (*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 une application est identifiée comme malveillante, le programme vous invite à la bloquer (*cette option est activée par défaut et il est recommandé de ne pas modifier ce paramètre sauf absolue nécessité*)

  - ***Mise en quarantaine automatique des menaces détectées*** - toutes les applications détectées comme des programmes malveillants sont automatiquement bloquées

  - ***Mise en quarantaine automatique des menaces connues*** - toutes les applications dont vous êtes certain qu'elles seront détectées comme des programmes malveillants sont automatiquement bloquées

Boutons de commande

Les boutons de commande disponibles dans l'interface ***Identity Protection*** sont :

- ***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 (*avec la présentation générale des composants*)

8. Barre d'outils de sécurité AVG

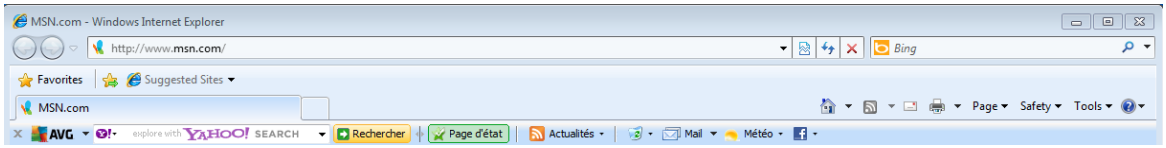
La ***Barre d'outils de sécurité AVG*** est un nouvel outil qui fonctionne en association avec le composant ***LinkScanner***. La ***Barre d'outils de sécurité AVG*** permet également de contrôler les fonctions du composant ***LinkScanner*** et de corriger le comportement de ce dernier.

Si vous installez cette barre d'outils lors de l'installation du produit **AVG Internet Security 2011**, elle est automatiquement ajoutée à votre navigateur Web (*Internet Explorer 6.0 ou version supérieure et Mozilla Firefox 3.0 ou version supérieure*). Les autres navigateurs Internet ne sont pas encore pris en charge.

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

8.1. Interface de la barre d'outils de sécurité AVG

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 3.0 ou supérieure*). Une fois que vous avez décidé d'installer la ***Barre d'outils de sécurité AVG****(le processus d'installation d'AVG vous a demandé si vous vouliez installer le composant ou non*), le composant apparaît sous la barre d'adresse de votre navigateur :



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

8.1.1. Bouton du logo AVG

Ce bouton permet d'accéder aux éléments généraux de la barre d'outils. Cliquez sur le logo afin d'être redirigé vers le site Web d'AVG. Cliquer sur le pointeur situé au regard de l'icône AVG donne accès aux éléments suivants :

- ***Informations sur la barre d'outils*** - lien menant à 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***
- ***Lancer AVG*** - ouvre l'**AVG Internet Security 2011*interface utilisateur***
- ***Actualités sur AVG*** - ouvre un menu contextuel comportant les liens suivants renvoyant à des informations importantes sur la sécurité d'**AVG Internet Security 2011** :
    - *Niveau de menace actuel* - ouvre le site Web d'AVG à la page donnant des informations importantes sur les menaces principales, les recommandations en matière de suppression de virus, la mise à jour du

programme AVG, l'accès à la base de données virale et d'autres informations utiles

- *Actualités sur AVG* - ouvre la page Web répertoriant les derniers communiqués de presse portant sur AVG
- *Niveau de menace actuel* - ouvre la page Web donnant une représentation graphique du niveau de menace actuel sur le Web
- *Laboratoire des menaces AVG* - ouvre le site Web à la page Rapports du site AVG dans laquelle vous pouvez rechercher la menace qui vous intéresse par son nom et obtenir des informations détaillées

- ***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 de la barre d'outils de sécurité AVG***
- ***Supprimer l'historique*** - grâce à la ***barre d'outils de sécurité AVG***, vous pouvez supprimer l'historique complet ou supprimer, au choix, l'historique de navigation, l'historique de téléchargement ou les 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, d'envoyer des commentaires sur le produit ou de consulter les informations sur la version actuelle de la barre d'outils

8.1.2. Zone de recherche du moteur Yahoo!

La zone de recherche Yahoo! constitue un moyen facile et sécurisé pour effectuer une recherche sur le Web à l'aide du moteur Yahoo!. Sasissez un mot ou une expression dans la zone de recherche, puis cliquez sur ***Rechercher*** ou appuyez sur ***Entrée***. La recherche démarre 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 ***Search-Shield***.

Dans la zone de recherche, vous pouvez aussi accéder à Wikipedia ou à un autre service de recherche. Voir l'illustration :

8.1.3. Niveau de protection

Le bouton ***Protection totale/Protection limitée/Aucune protection*** vérifie l'état des composants ***Surf-Shield*** et ***Search-Shield***. *Protection totale* indique que les deux composants sont actifs. *Protection limitée* indique qu'un seul des composants est actif tandis que *Aucune protection* signale que les deux sont désactivés. Ce bouton ouvre l'onglet ***Sécurité*** de la boîte de dialogue ***Options de la barre d'outils***, qui vous permet d'affecter la fonctionnalité de la ***Barre d'outils de sécurité AVG*** à appliquer.

8.1.4. Statut de la page

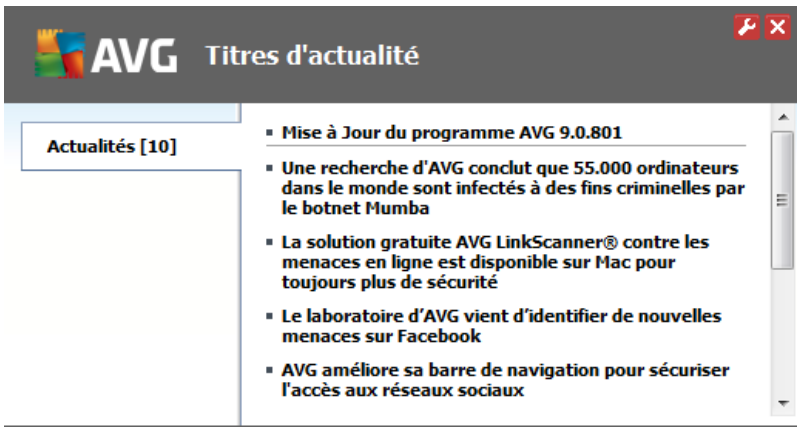
Intégré à la barre d'outils, ce bouton affiche l'évaluation de la page Web actuellement à l'écran en fonction des critères du composant ***Surf-Shield*** :

- - La page associée au lien est exempte de virus
- La page est suspecte.
- - La page contient des liens vers des pages dont le contenu est dangereux.
- - La page associée au lien contient des menaces actives ! Pour votre propre sécurité, vous n'êtes pas autorisé à visiter la page.
- - La page associée au lien n'est pas accessible et n'a pas pu être vérifiée.

Cliquez sur le bouton pour ouvrir un panneau d'informations sur les détails de la page Web concernée.

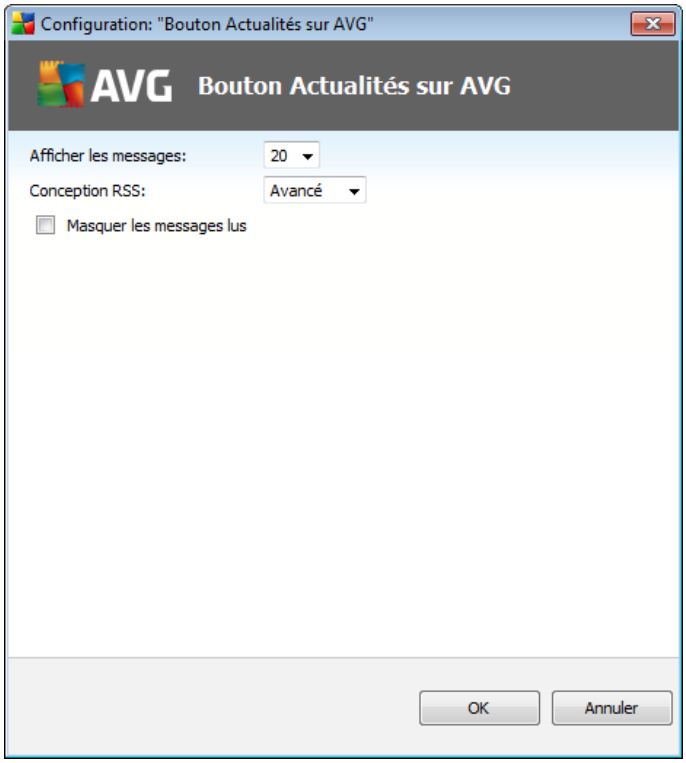
8.1.5. Actualités AVG

Placé dans la ***barre d'outils de sécurité AVG***, ce bouton ouvre une présentation des ***dernières actualités***relatives à AVG. Il s'agit d'articles parus dans la presse ou de communiqués de presse de la société :



Dans le coin supérieur droit, deux boutons rouges sont accessibles :

- - le bouton ouvre une boîte de dialogue dans laquelle vous définissez les paramètres du bouton ***Actualités AVG*** figurant dans la ***barre d'outils de sécurité AVG*** :

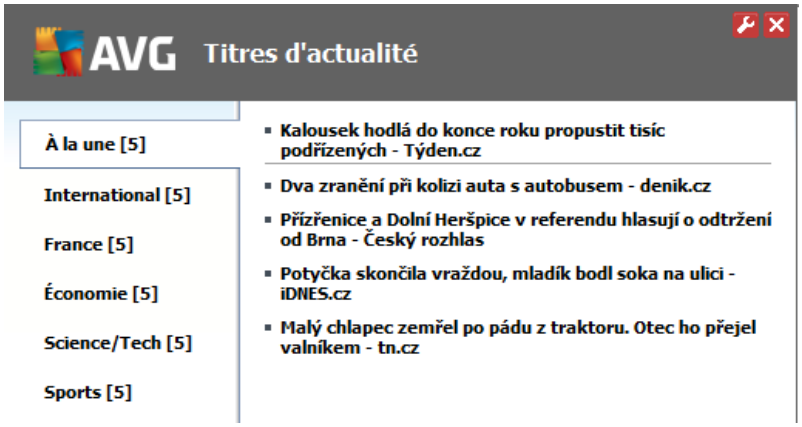


- ***Afficher les messages*** - permet de choisir le nombre de messages à afficher
- ***Conception RSS*** - sélectionnez le mode avancé ou le mode standard de l'affichage des actualités (*le mode avancé est sélectionné par défaut, voir l'illustration ci-dessus*)
- ***Masquer les messages lus*** - cochez cette option pour ne plus afficher les messages lus afin de permettre la remise de nouveaux messages

- - cliquez sur ce bouton pour fermer la page des actualités actuellement consultées

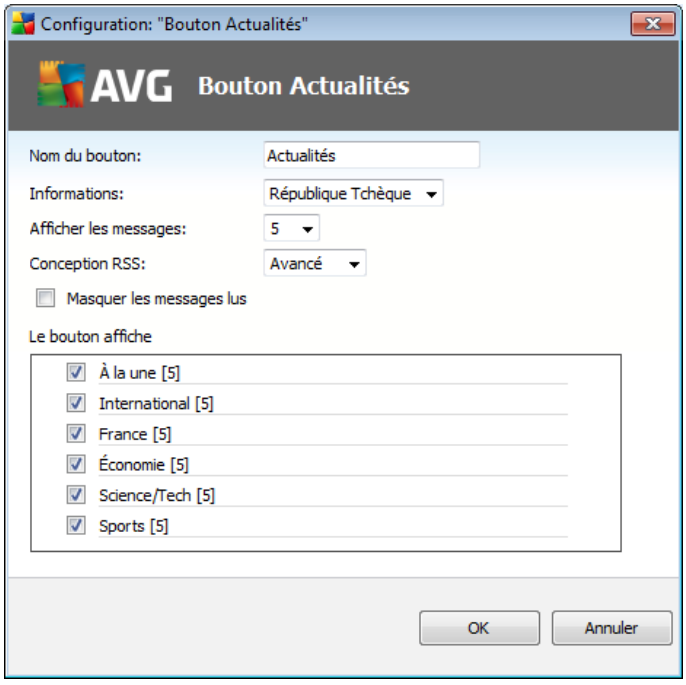
8.1.6. Actualités

De la même manière, dans la ***Barre d'outils de sécurité AVG***, ce bouton permet d'accéder aux dernières actualités diffusées par le média sélectionné ; la fenêtre qui s'affiche comprend plusieurs sections :



Dans le coin supérieur droit, deux boutons rouges sont visibles :

- - le bouton ouvre une boîte de dialogue dans laquelle vous définissez les paramètres du bouton ***Actualités*** figurant dans la ***barre d'outils de sécurité AVG*** :



- ***Nom du bouton*** - vous avez la possibilité de renommer le bouton affiché dans la ***barre d'outils de sécurité AVG***

- ***Informations***- choisissez le pays dans la liste dont vous voulez consulter les actualités

- ***Afficher les messages*** - permet de choisir le nombre de messages à afficher

- ***Conception RSS*** - permet de passer du mode standard au mode avancé et vice-

versa pour sélectionner la présentation des actualités (***le mode avancé est défini par défaut, voir illustration ci-dessus***)

- ***Masquer les messages lus*** - sélectionnez cette option pour confirmer que tout message lu ne doit plus figurer dans la présentation des actualités et doit être remplacée par une nouvelle actualité

- ***Le bouton affiche***- dans ce champ, vous devez définir le type d'informations à afficher dans la présentation des actualités de la ***Barre d'outils de sécurité AVG***

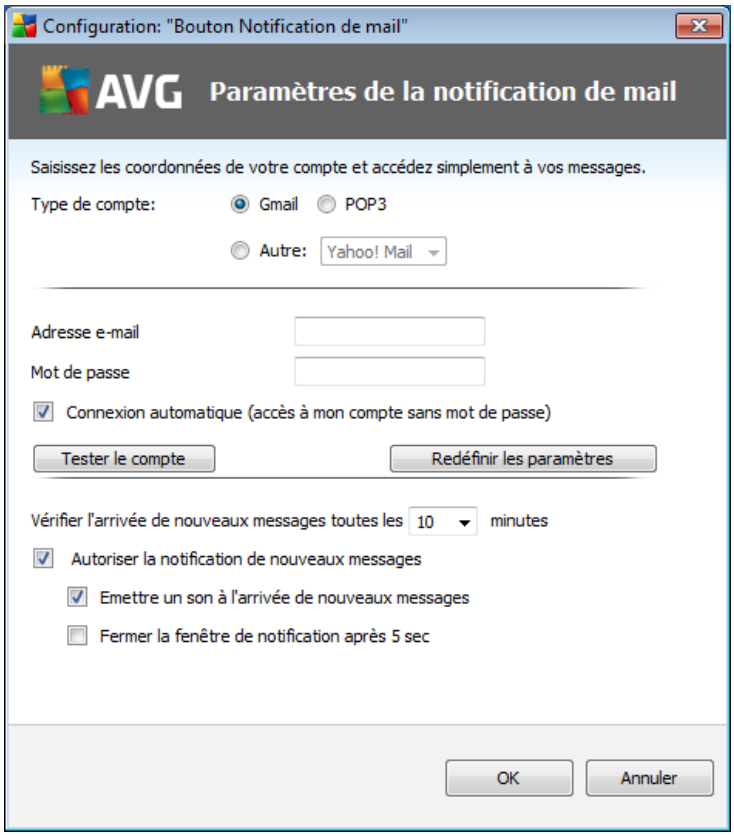
  - - cliquez sur ce bouton pour fermer la page des actualités actuellement consultées

8.1.7. Supprimer l'historique

Ce bouton permet de supprimer l'historique du navigateur de la même manière que via ***logo AVG -> Supprimer l'historique***.

8.1.8. Notification de mail

Le bouton ***Notification de mail*** permet d'activer l'option visant à signaler l'arrivée de nouveaux messages directement dans l'interface ***Barre d'outils de sécurité AVG***. Le bouton ouvre la boîte de dialogue de modification suivante dans laquelle vous définissez les paramètres de votre compte de messagerie et les règles d'affichage des e-mails. Conformez-vous aux instructions figurant dans la boîte de dialogue :



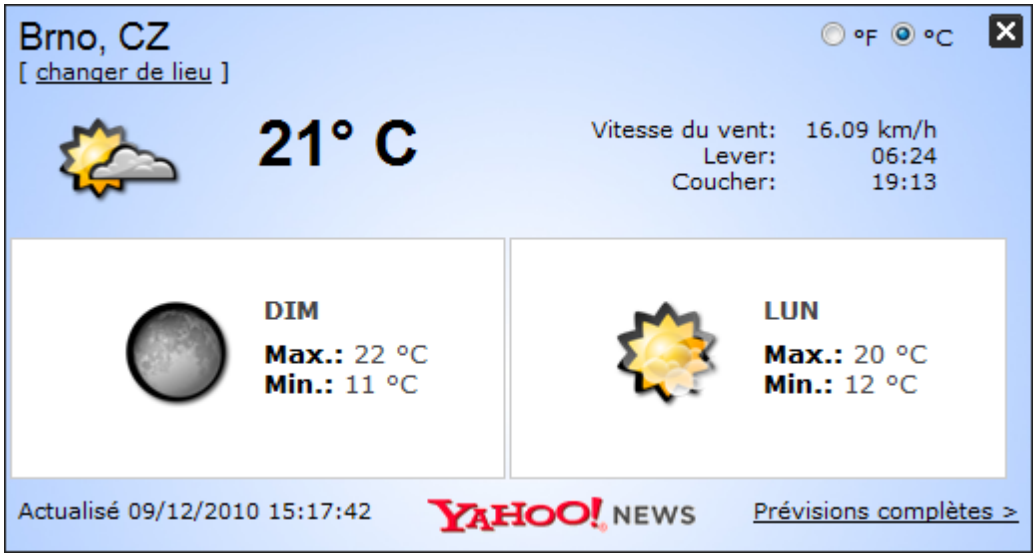
- ***Type de compte*** - indiquez le type de protocole que votre compte de messagerie emploie. Vous avez le choix entre les protocoles suivants : *Gmail*, *POP3* ou sélectionnez le nom du serveur dans le menu déroulant de l'option *Autre* (*pour le moment, vous pouvez utiliser cette option pour Yahoo! Mail et Hotmail*). Si vous ne connaissez pas le type de serveur de messagerie que votre compte utilise, contactez votre fournisseur de messagerie électronique ou votre fournisseur d'accès Internet pour obtenir ce renseignement.

- ***Connexion*** - Dans la section Connexion, saisissez scrupuleusement votre *adresse e-mail* et le *mot de passe* associé. Laissez l'option *Connexion automatique* cochée afin de mémoriser ces informations.

- ***Vérifier l'arrivée de nouveaux messages toutes les ... minutes*** - Définissez l'intervalle de vérification des messages (*entre 5 et 120 minutes*) et précisez si vous désirez être averti de l'arrivée d'un nouveau message et les modalités de cette notification.

8.1.9. Bulletin météo

Le bouton ***Météo*** indique la température actuelle (*actualisée toutes les 3 à 6 heures*) de la ville sélectionnée dans l'interface de la ***barre d'outils de sécurité AVG***. Cliquez sur le bouton pour ouvrir un nouveau panneau d'informations contenant les détails du bulletin météo :



Voici la liste des options :

- ***Changer de lieu*** - cliquez sur ***Changer de lieu*** pour afficher une nouvelle boîte de dialogue intitulée ***Rechercher votre ville***. Indiquez le nom de la ville qui vous intéresse dans la zone de texte et cliquez sur le bouton ***Rechercher***. Ensuite dans la liste des villes de même nom, sélectionnez la destination recherchée. Le panneau d'informations s'affiche à nouveau et donne les renseignements météorologiques sur le lieu sélectionné.

- ***Convertisseur Fahrenheit / Celsius***- dans le coin supérieur droit du panneau d'informations, vous pouvez choisir entre degrés Fahrenheit et degrés Celsius. Les températures s'afficheront ensuite dans la mesure définie.

- ***Prévisions complètes***- si vous êtes intéressé par un bulletin météo complet, cliquez sur le lien ***Prévisions complètes*** pour visiter le site Web météo spécialisé qui se trouve à l'adresse http://weather.yahoo.com/

8.1.10. Facebook

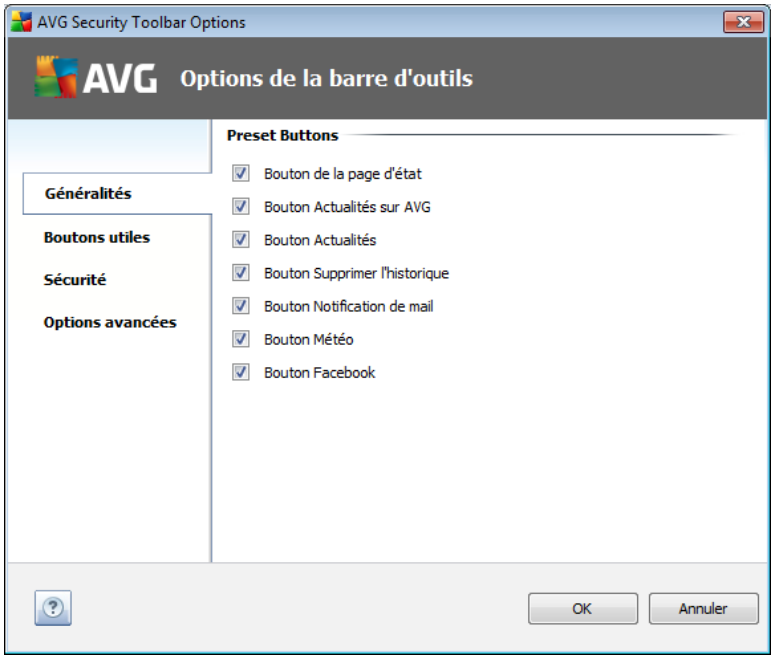
Le bouton ***Facebook*** permet de vous connecter au réseau social Facebook à partir de la ***barre d'outils de sécurité AVG***. Cliquez sur le bouton et l'invite de connexion s'affiche ; cliquez à nouveau pour ouvrir l'***écran de connexion Facebook***. Identifiez-vous et cliquez sur le bouton ***Connexion***. Si vous ne possédez pas de compte Facebook, vous pouvez en créer un en cliquant sur le lien ***S'inscrire sur Facebook***.

Lors du processus d'inscription Facebook, vous serez invité à autorisé l'application ***AVG Social Extension***. Cette application est essentielle pour la connexion de la barre d'outils à Facebook. Par conséquent, il est recommandé d'autoriser son fonctionnement. La connexion Facebook est ensuite activée et le bouton ***Facebook*** figurant dans la ***barre d'outils de sécurité AVG*** offre les options standard du menu Facebook.

8.2. 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 via le menu de la barre d'outils *AVG / Options* dans une nouvelle boîte de dialogue appelée ***Options de la barre d'outils*** divisée en trois parties :

8.2.1. Onglet Général

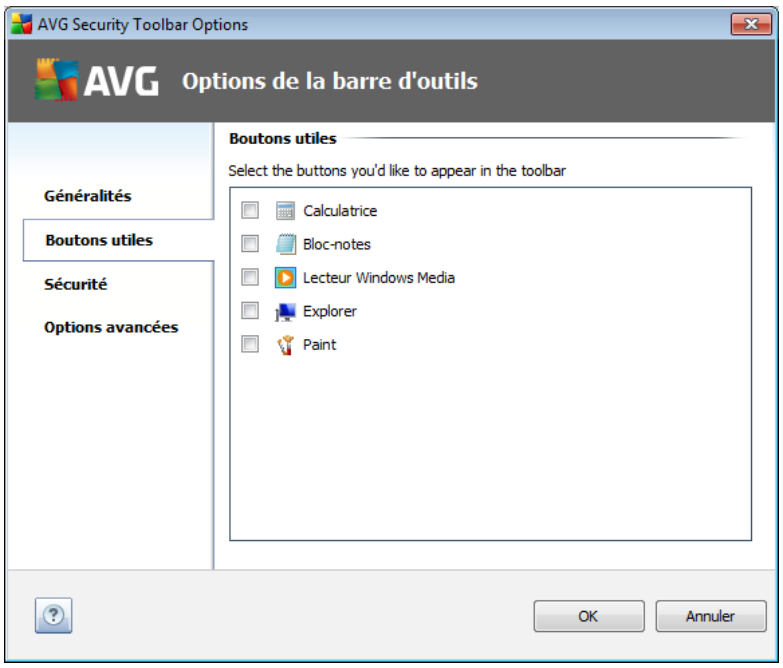


Dans cet onglet vous pouvez spécifier les boutons de commande à afficher et masquer dans le panneau de la ***barre d'outils de sécurité AVG***. Cochez l'option qui convient pour afficher le bouton correspondant. Voici la description de la fonctionnalité de chacun des boutons de la barre d'outils :

- ***Bouton Statut de la page -*** le bouton a pour objectif d'afficher le niveau de sécurité de la page actuellement ouverte dans la ***barre d'outils de sécurité AVG***
- ***Bouton Actualités AVG*** - le bouton ouvre une page Web répertoriant les derniers communiqués de presse sur AVG.
- ***Bouton Titres d'actualité*** - le bouton permet de consulter les titres de grands quotidiens
- ***Bouton Effacer l'historique*** - ce bouton permet d'effectuer les actions suivantes : Supprimer tout l'historique, Supprimer l'historique des recherches, Supprimer l'historique du navigateur, Supprimer l'historique de téléchargement ou Supprimer les cookies directement à partir du panneau Barre d'outils de sécurité AVG
- ***Bouton Notification de mail***- ce bouton permet d'indiquer l'arrivée de nouveaux messages dans l'interface de la ***barre d'outils de sécurité AVG***
- ***Bouton Météo*** - ce bouton livre des informations immédiates sur les conditions météorologiques de la ville sélectionnée
- ***Bouton Facebook*** - ce bouton vous connecte directement au réseau social

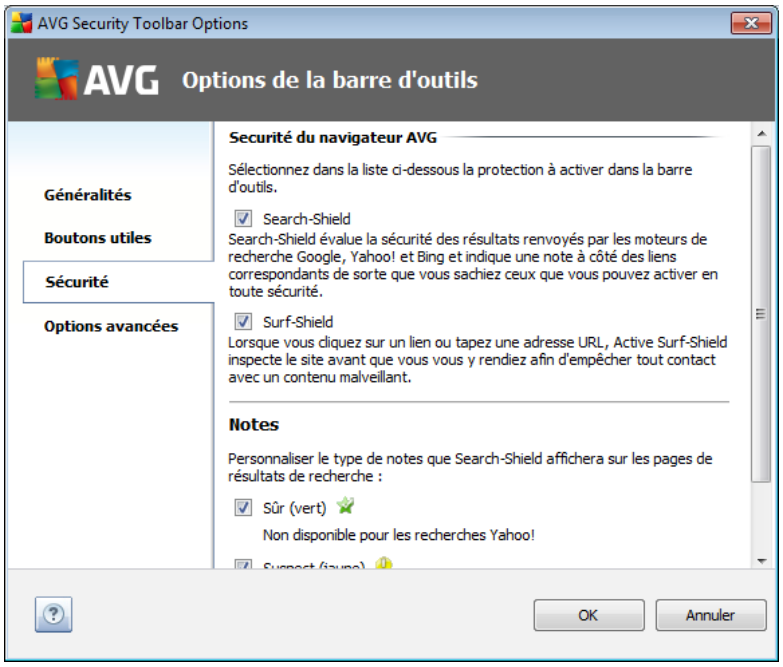
Facebook

8.2.2. Onglet Boutons utiles



L'onglet ***Boutons utiles*** permet de sélectionner des applications parmi une liste d'applications et d'afficher leur icône dans l'interface de la barre d'outils. L'icône sert alors de lien d'accès rapide destiné à démarrer immédiatement l'application associée.

8.2.3. Onglet Sécurité



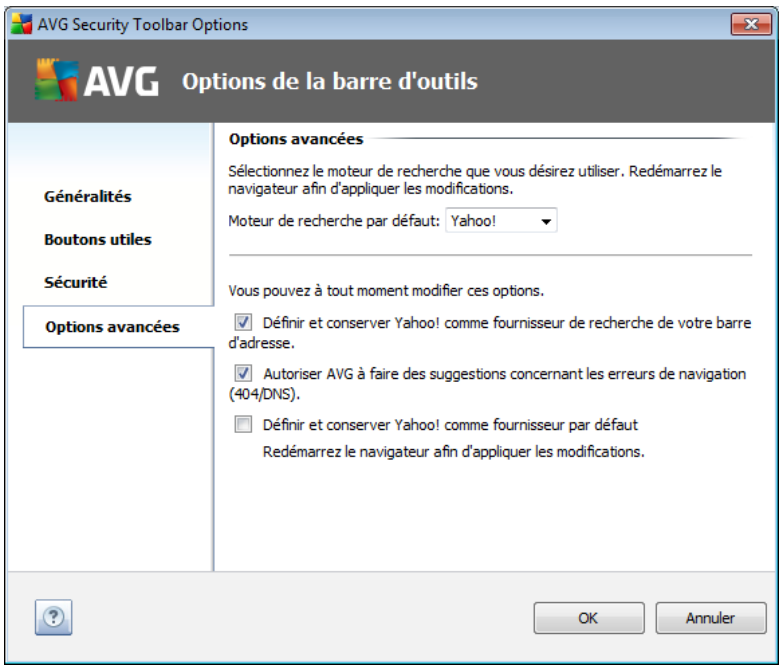
L'onglet de ***Sécurité*** est divisé en deux sections, ***Sécurité du navigateur AVG*** et ***Notes***. Vous pouvez cocher les cases souhaitées pour définir les fonctionnalités de la ***barre d'outils de sécurité AVG*** que vous voulez utiliser :

- ***Sécurité du navigateur*** - cochez cette case pour activer ou désactiver le service ***AVG Search-Shield*** et/ou le service ***Surf-Shield***
- ***Notes*** - permet de sélectionner les symboles graphiques utilisés pour les notes des résultats de recherche par le composant ***Search-Shield*** que vous voulez utiliser
  - o la page est exempte de virus
  - o la page est suspecte
  - o la page contient des liens vers des pages dont le contenu est dangereux
  - o la page contient des menaces actives
  - o la page n'est pas accessible et ne peut pas faire l'objet d'une analyse

Cochez l'option voulue pour confirmer que vous voulez être informé sur ce niveau de menace particulier. Toutefois, il est impossible de désactiver l'affichage de la coche rouge attribué aux pages contenant des menaces actives et dangereuses. ***Il est recommandé de garder la configuration par défaut et de***

ne la changer qu'en cas d'absolue nécessité.

8.2.4. Onglet Options avancées



Sous l'onglet ***Options avancées***, sélectionnez d'abord le moteur de recherche à utiliser par défaut. Vous avez le choix entre *Yahoo!, Baidu, WebHledani* et *Yandex*. Après toute modification, redémarrez le navigateur Internet pour que le changement soit pris en compte.

Par ailleurs, vous pouvez activer ou désactiver d'autres paramètres spécifiques de la ***barre d'outils de sécurité AVG*** *(la capture présente les paramètres par défaut de Yahoo!)* :

- ***Définir et conserver Yahoo! comme moteur de recherche de votre barre d'adresse*** - si vous la cochez, cette option 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.

- ***Autoriser AVG à faire des suggestions concernant les erreurs de navigation (404/DNS)*** - lorsque vous effectuez une recherche sur Internet aboutissant à une page non existante ou impossible à afficher (erreur 404), vous êtes automatiquement redirigé vers une page Web qui vous propose une liste de pages en rapport avec le sujet traité.

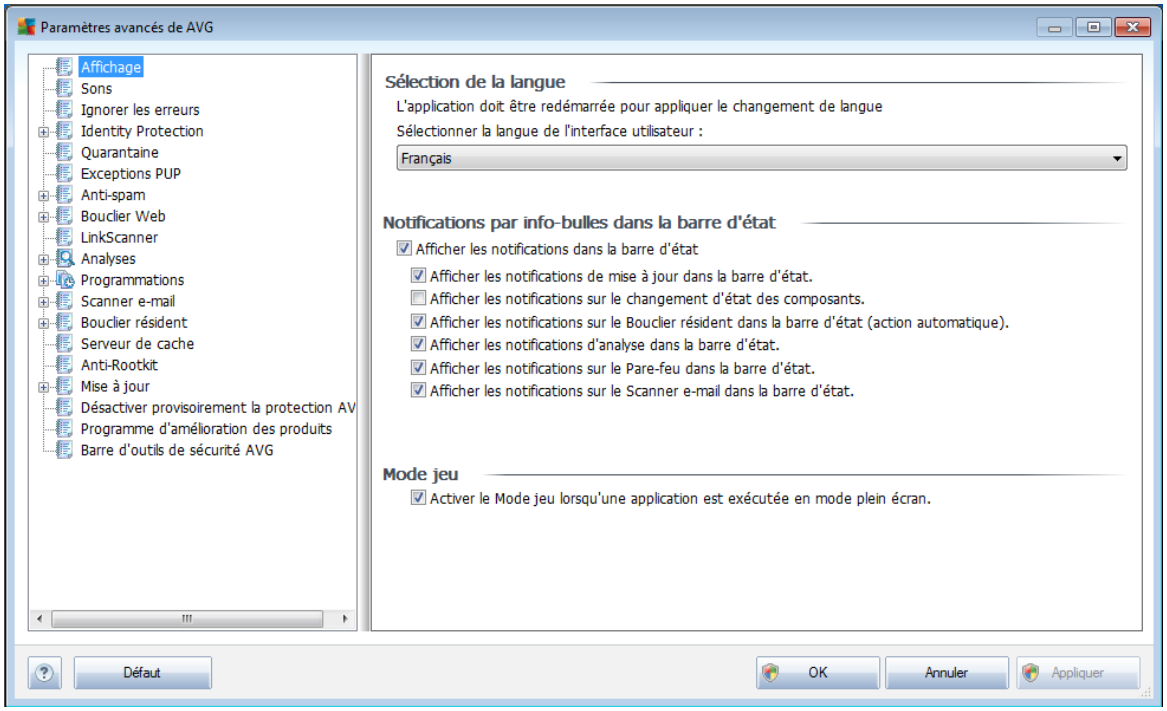
- ***Définir et conserver Yahoo! comme moteur de recherche*** - Yahoo! est le moteur de recherche par défaut pour la recherche Web dans la ***Barre d'outils de sécurité AVG***. Lorsque vous l'activez, cette option peut également devenir votre moteur de recherche par défaut.

9. Paramètres avancés d'AVG

La boîte de dialogue de configuration avancée d'**AVG Internet Security 2011** 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 modifier 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 :

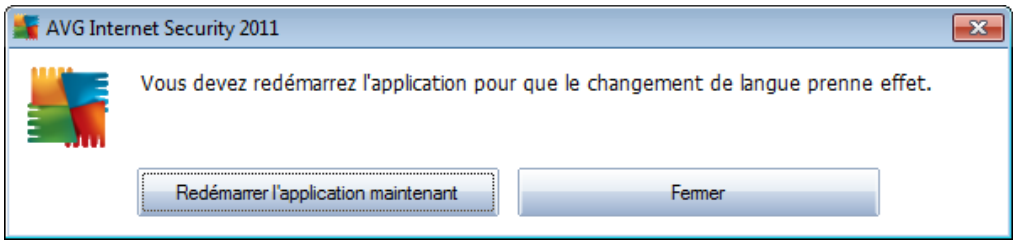


Sélection de la langue

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. Le menu déroulant ne propose que les langues que vous avez sélectionnées au cours du processus d'installation (*voir chapitre Options personnalisées*) en plus de l'anglais (*langue installée par défaut*). 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)

- Cliquez 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 les notifications de mise à jour*** dans la barre d'état - 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 sur 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 une anomalie d'un composant, elle remplit la même fonction d'information que l'icône dans la barre d'état système (changement de couleur) indiquant un problème lié à un composant AVG.
  - ***Afficher les notifications sur le Bouclier résident dans la barre d'état (action automatique)*** - indiquez s'il faut afficher ou supprimer les informations sur les processus d'enregistrement, de copie et d'ouverture de fichier (*cette configuration est applicable seulement si l'option Réparer automatiquement du Bouclier résident est activée*).

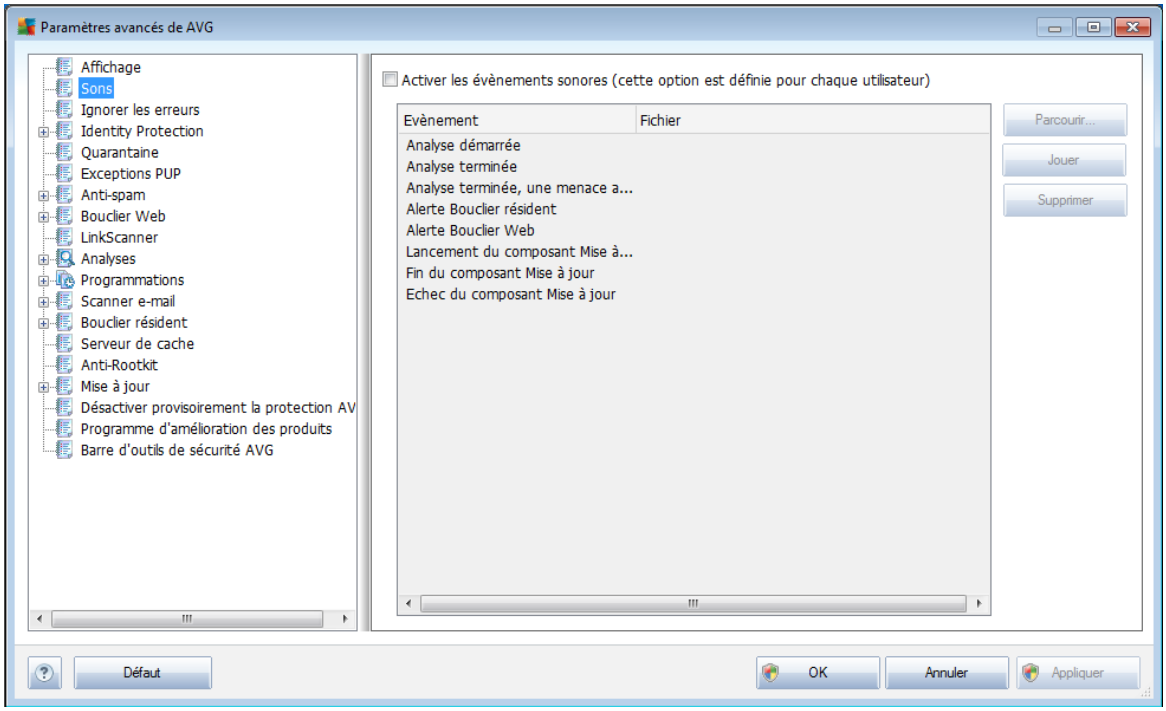
- ***Afficher les notifications d'analyse*** dans la barre d'état - indiquez s'il faut afficher les informations sur le lancement automatique de l'analyse programmée, sa progression et ses résultats.
- ***Afficher les notifications sur le Pare-feu dans la barre d'état*** *** - décidez s'il faut afficher 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 les notifications sur le Scanner e-mail dans la barre d'état*** *** - indiquez s'il faut afficher les informations sur l'analyse de tous les messages entrants et sortants.

Mode jeu

Cette fonction est conçue pour des applications plein écran pour lesquelles les éventuelles notifications d'information AVG (*qui s'affichent après le démarrage d'une analyse programmée*) seraient perturbantes (*elles risquent de réduire l'application ou de corrompre les images*). 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.

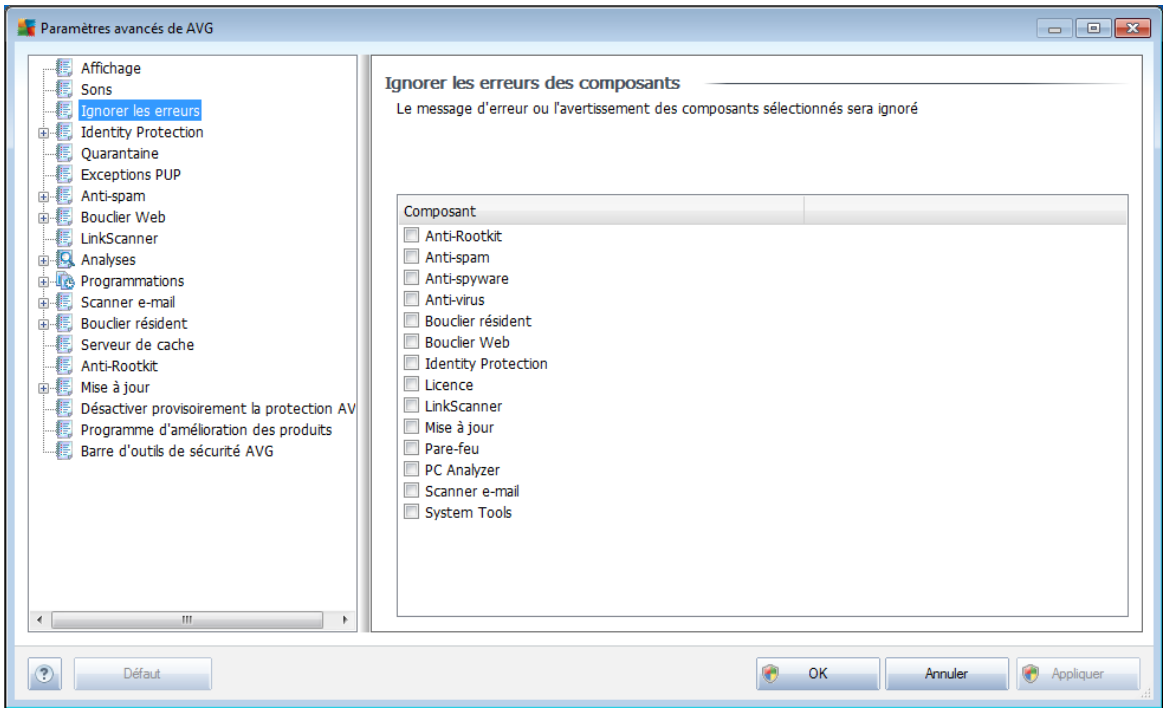


Ainsi, sélectionnez l'évènement correspondant à partir de la liste et recherchez (***Parcourir***) un son approprié que vous souhaitez affecter à cet évènement. Pour écouter le son sélectionné, mettez en surbrillance l'évènement dans la liste et cliquez sur le bouton ***Jouer***. Utilisez le bouton ***Supprimer***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

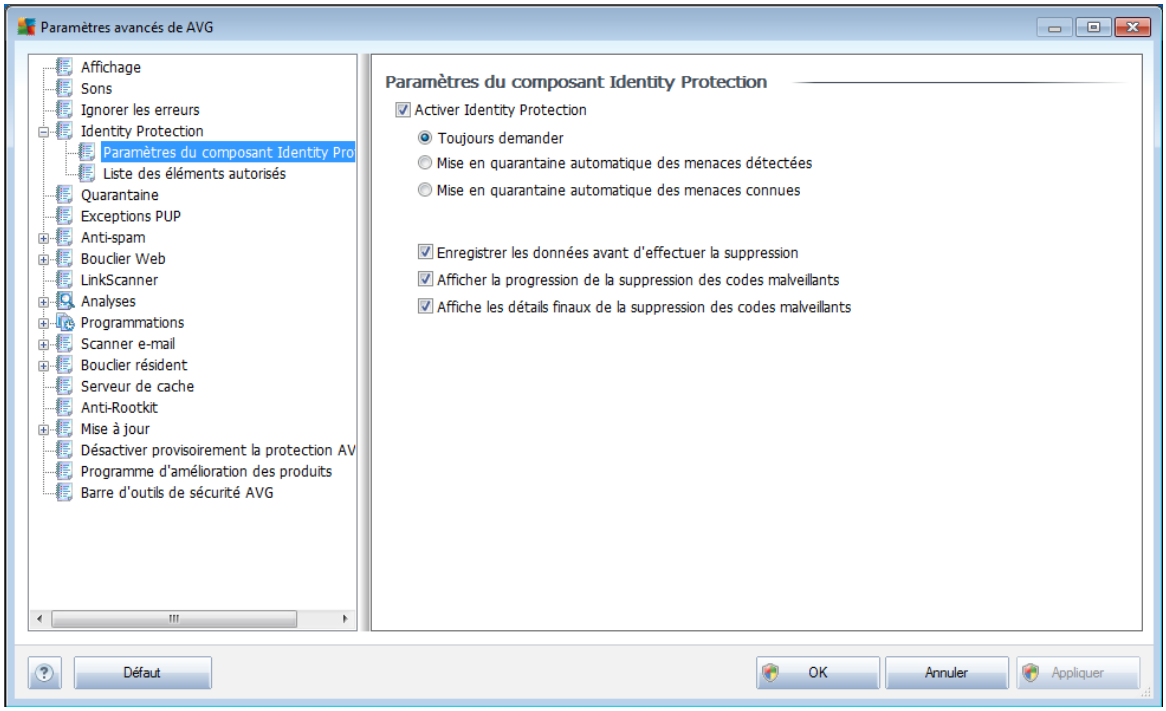
Aussi, dans la boîte de dialogue ci-dessus, sélectionnez les composants qui risquent de présenter une erreur (*composants désactivés*) dont vous voulez ignorer l'état. Une

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*** :



Activer Identity Protection (*option activée par défaut*) – désélectionnez cette case pour désactiver le composant ***Identity Protection***.

Nous recommandons vivement de ne pas le faire, sauf en cas d'absolue nécessité.

Si le composant ***Identity Protection*** est activé, vous pouvez indiquer l'opération à effectuer lorsqu'une menace est détectée :

- ***Toujours demander*** (*option activée par défaut*) - 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.
- ***Mise en quarantaine automatique des menaces détectées*** - cochez cette

case pour indiquer que vous voulez placer immédiatement 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.

- ***Mise en quarantaine automatique des menaces connues*** - laissez cette option activée si vous voulez que toutes les applications identifiées comme potentiellement malveillantes soient immédiatement confinées dans ***Quarantaine AVG***.

Par ailleurs, vous pouvez choisir d'autres options pour utiliser éventuellement d'autres options ***Identity Protection*** :

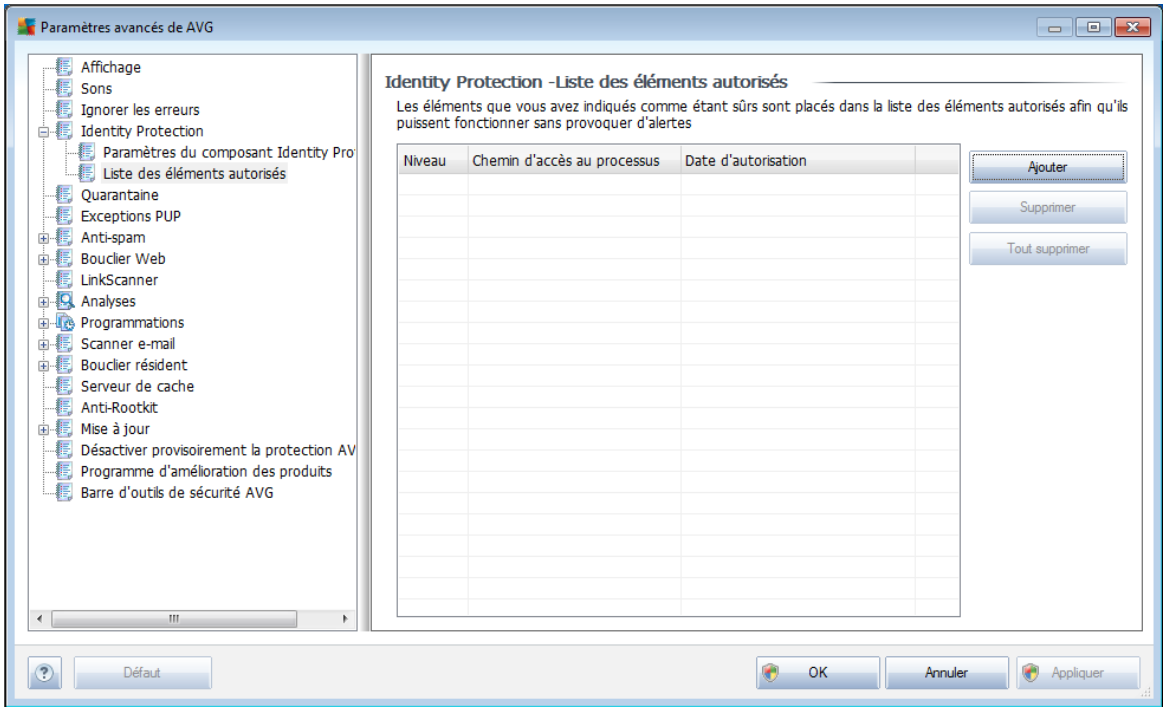
- ***Enregistrer les données avant d'effectuer la suppression*** - (*option activée par défaut*) - laissez cette case cochée si vous souhaitez être averti lorsque la quarantaine d'une application détectée comme potentiellement malveillante est levée. Au cas où vous seriez en train de travailler sur l'application, vous devez enregistrer votre travail pour ne pas le perdre. Par défaut, la case est activée et il est recommandé de ne pas modifier ce paramètre.

- ***Afficher la progression de la suppression des codes malveillants*** - (*option activée par défaut*) - lorsqu'un programme potentiellement dangereux est détecté, cette option (activé) permet d'afficher une nouvelle boîte de dialogue indiquant la progression de la mise en quarantaine du programme malveillant.

- ***Afficher les détails finaux de la suppression des codes malveillants*** - (*option activée par défaut*) - lorsque cette option est activée, affiche des informations détaillées sur chaque objet mis en quarantaine (*niveau de gravité, emplacement, etc.*).

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 ***Mise en quarantaine automatique des 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 des éléments autorisés d'Identity Protection*** et n'est plus signalée comme élément potentiellement dangereux :



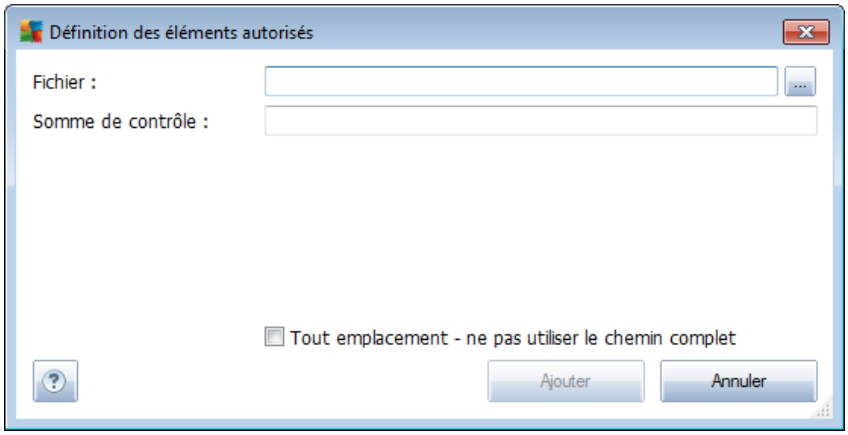
La ***liste des éléments autorisée d'Identity Protection*** fournit les informations suivantes sur chaque processus :

- ***Niveau*** - représentation 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 :

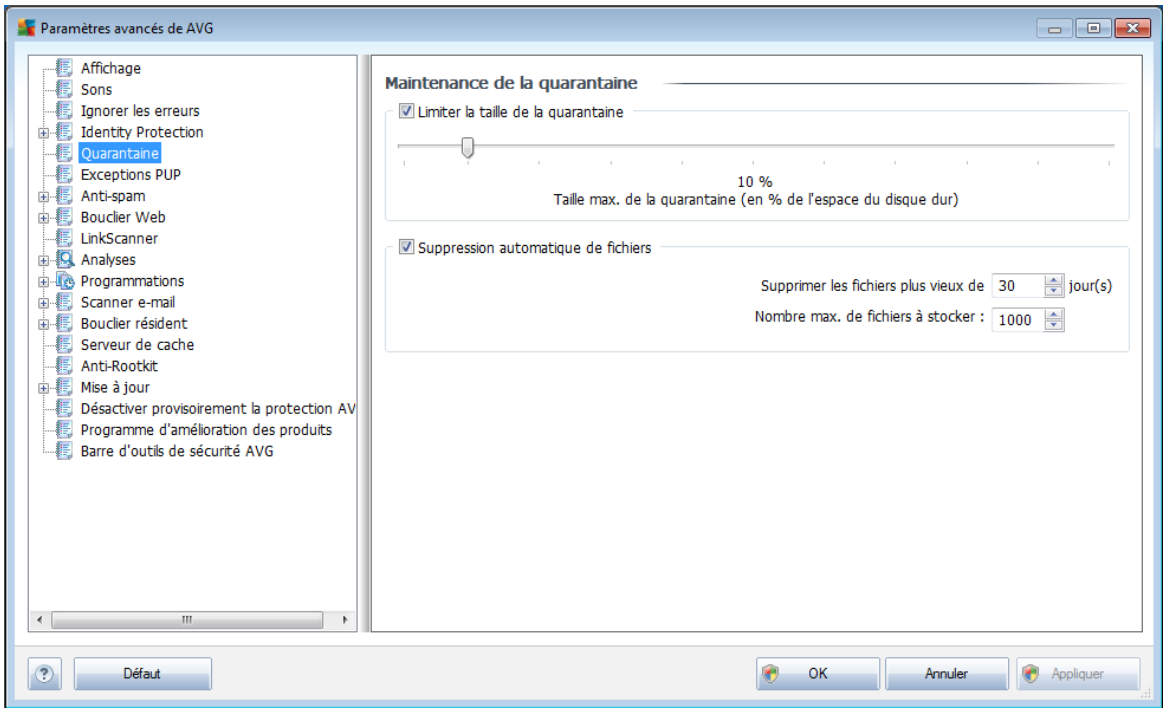
- ***Ajouter*** - cliquez sur ce bouton pour ajouter un élément à la liste autorisée. La boîte de dialogue suivante s'affiche :



- ***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 le fichier comme étant une exception pour un emplacement spécifique, ne cochez pas cette case.

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

9.5. Quarantaine

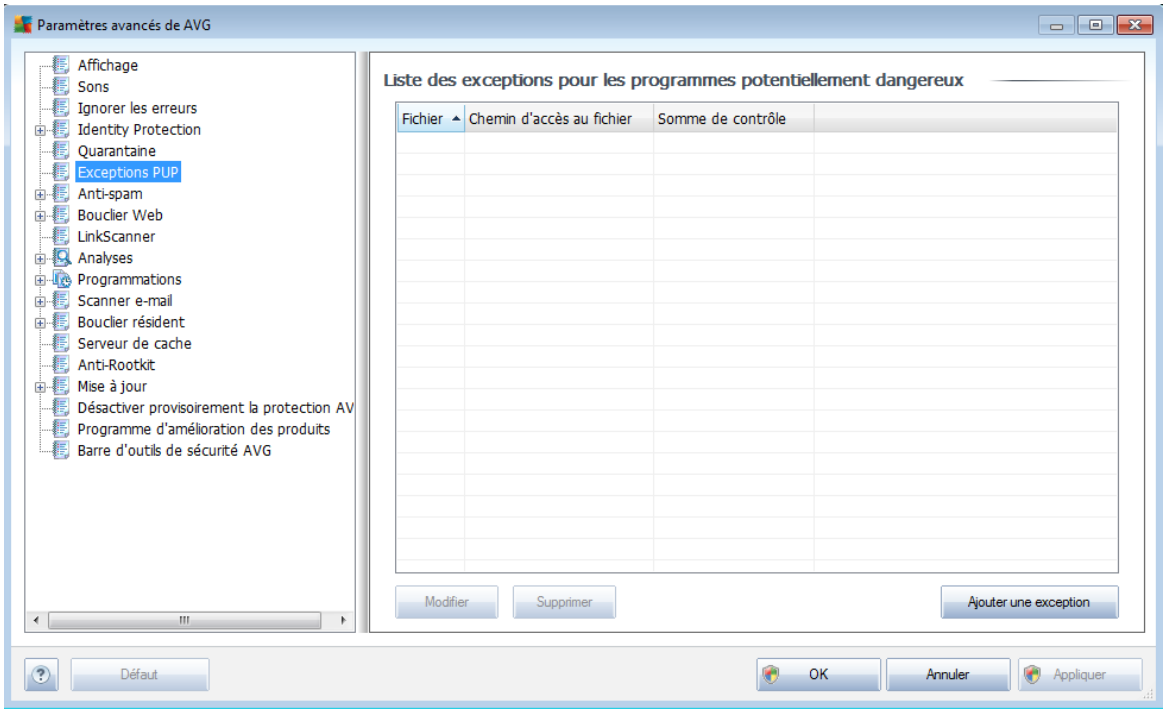


La boîte de dialogue ***Maintenance de la quarantaine*** permet de définir plusieurs paramètres liés à l'administration des objets stockés dans le module ***Quarantaine*** :

- ***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 Internet Security 2011 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 l'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 :

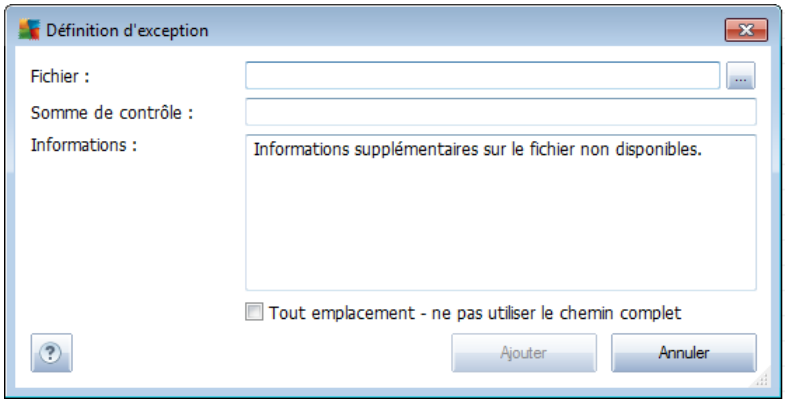


La boîte de dialogue ***Liste des exceptions pour les programmes potentiellement dangereux*** dresse la liste des exceptions déjà définies et actuellement valides par rapport aux programmes indésirables. Vous pouvez modifier la liste, supprimer des éléments existants ou ajouter une nouvelle exception.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

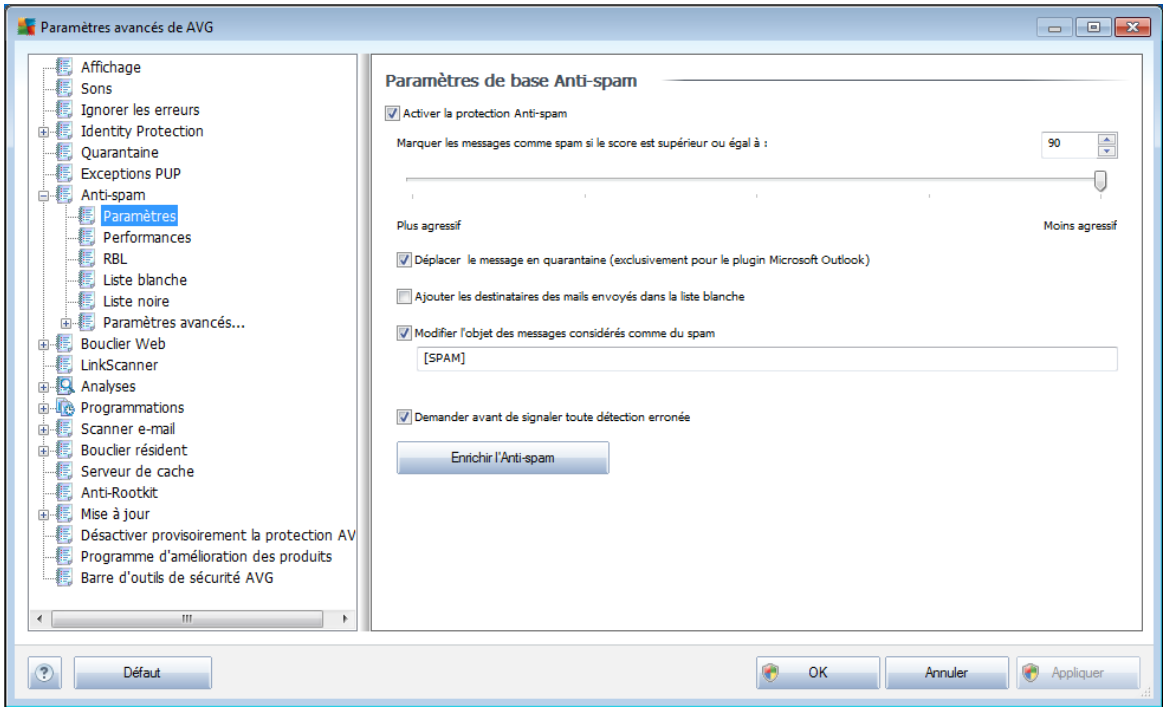
- ***Somme de contrôle*** - affiche la "signature" unique du fichier choisi. Il s'agit d'une chaîne de caractères générée automatiquement, qui permet à AVG de distinguer sans risque d'erreur ce fichier parmi tous les autres. La somme de contrôle est générée et affichée une fois le fichier ajouté.

- ***Informations*** - affiche des informations supplémentaires sur le fichier (*licence, version, etc.*)

- ***Tout emplacement - ne pas utiliser le chemin complet*** - si vous souhaitez définir ce fichier comme une exception uniquement pour un emplacement spécifique, veillez à ne pas cocher cette case. Si la case est cochée, le fichier mentionné est défini en tant qu'exception indifféremment de son emplacement (*vous devez malgré tout indiquer le chemin d'accès complet du fichier ; le fichier servira alors d'exemple unique au cas où deux fichiers portant le même nom existent dans le système*).

9.7. Anti-spam

9.7.1. Paramètres



Dans la boîte de dialogue ***Paramètres de base anti-spam***, désélectionnez 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 régler le paramètre ***Marquer les messages comme spams si le score est supérieur à***, saisissez le score qui convient ou faites glisser le curseur vers la gauche ou vers la droite (*seules les valeurs entre 50 et 90 sont acceptées*).

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 80-90*** - les messages susceptibles d'être du spam sont identifiés par le filtre. Il est possible toutefois que certains messages valides soient détectés à tort comme du spam.
- ***Valeur 60-79*** - ce type de configuration est particulièrement strict. Tous les messages susceptibles d'être du spam sont identifiés par le filtre. Il est fort probable que certains messages anodins soient également rejetés.
- ***Valeur 50-59*** - ce type de configuration est très restrictif. Les messages qui ne sont pas du spam ont autant de chances d'être rejetés que ceux qui en

sont vraiment. Ce seuil n'est pas recommandé dans des conditions normales d'utilisation.

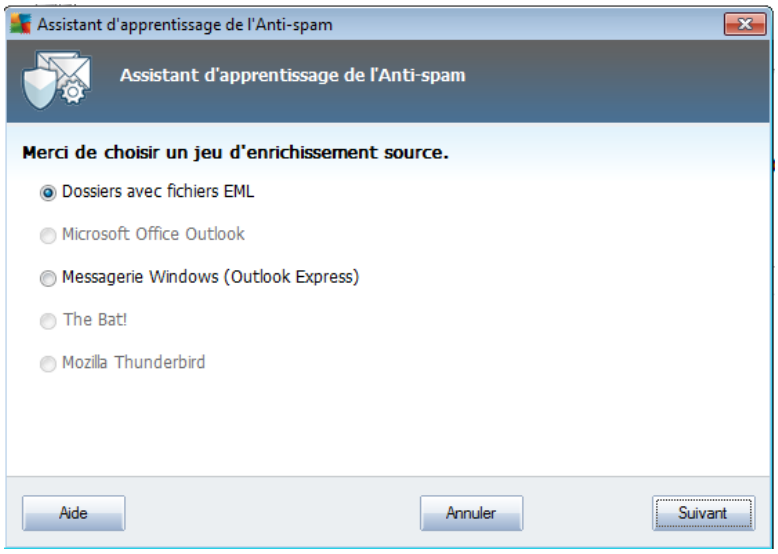
Dans la boîte de dialogue ***Paramètres standard anti-spam***, vous pouvez aussi définir la façon dont les messages indésirables doivent être traités :

- ***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*** – cochez 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.
- ***Demander avant de signaler toute détection erronée*** - option activée si, au cours de l'installation, vous avez accepté de participer au ***Programme d'amélioration des produits***. En pareil cas, vous avez autorisé le signalement des menaces détectées à AVG. La procédure de signalement est entièrement automatisée. Toutefois, vous pouvez cocher cette case pour confirmer que vous voulez être interrogé avant qu'un spam détecté soit signalé à AVG afin de vous assurer que le message en question a bien lieu d'être classé dans la catégorie du spam.

Boutons de commande

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

La première boîte de dialogue de l'***Assistant d'enrichissement de l'anti-spam*** vous invite à sélectionner la source des messages que vous souhaitez utiliser pour l'enrichissement. En général, vous utiliserez des mails signalés par erreur comme spam ou des messages indésirables qui n'ont pas été reconnus comme spam.



Plusieurs choix sont proposés :

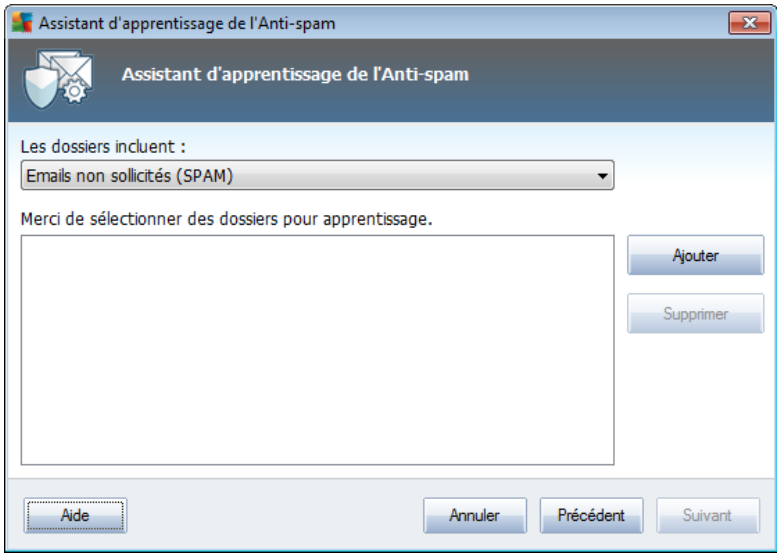
- ***un client de messagerie spécifique*** - si vous utilisez un des clients répertoriés (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), sélectionnez l'option correspondante
- ***Dossiers avec fichiers EML*** - si vous utilisez un autre programme de messagerie, commencez par enregistrer les messages dans un dossier 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



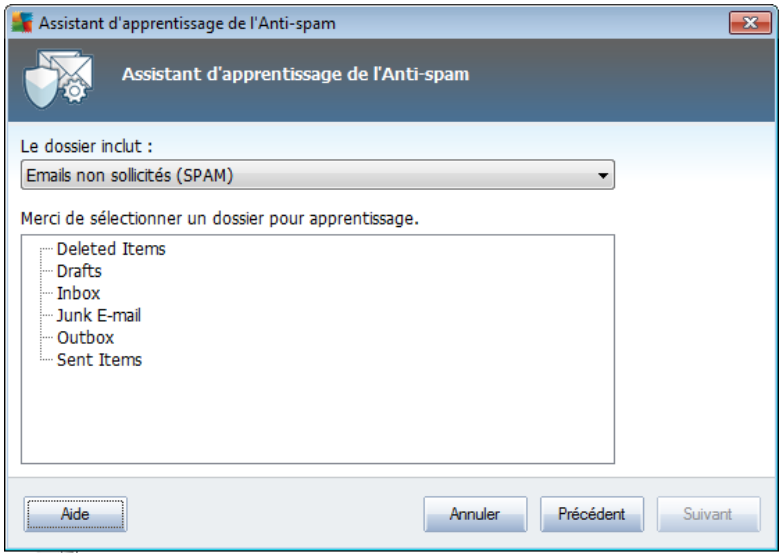
Dans cette boîte de dialogue, sélectionnez le dossier contenant les messages à utiliser pour la procédure d'enrichissement. Cliquez sur le bouton ***Ajouter*** pour localiser le dossier contenant les fichiers .eml (*messages e-mail enregistrés*). Le dossier sélectionné apparaît dans la boîte de dialogue.

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***.

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

Client de messagerie spécifique

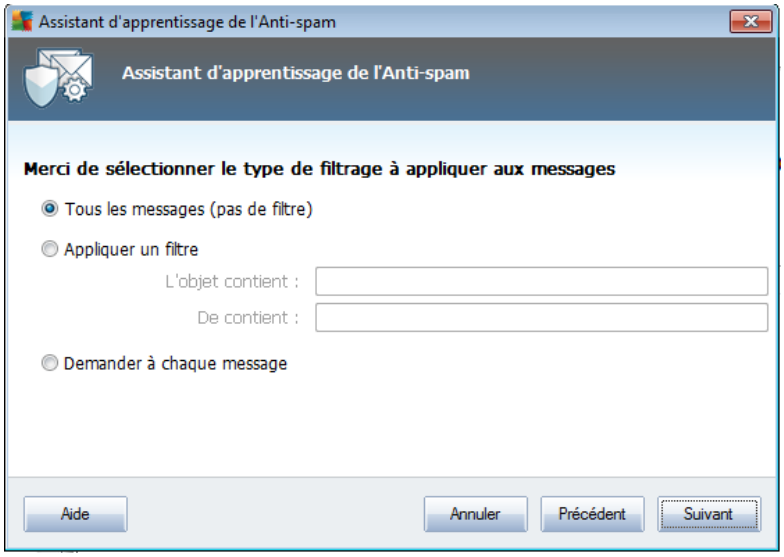
Lorsque vous avez choisi une option, une nouvelle boîte de dialogue apparaît.



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

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

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



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

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

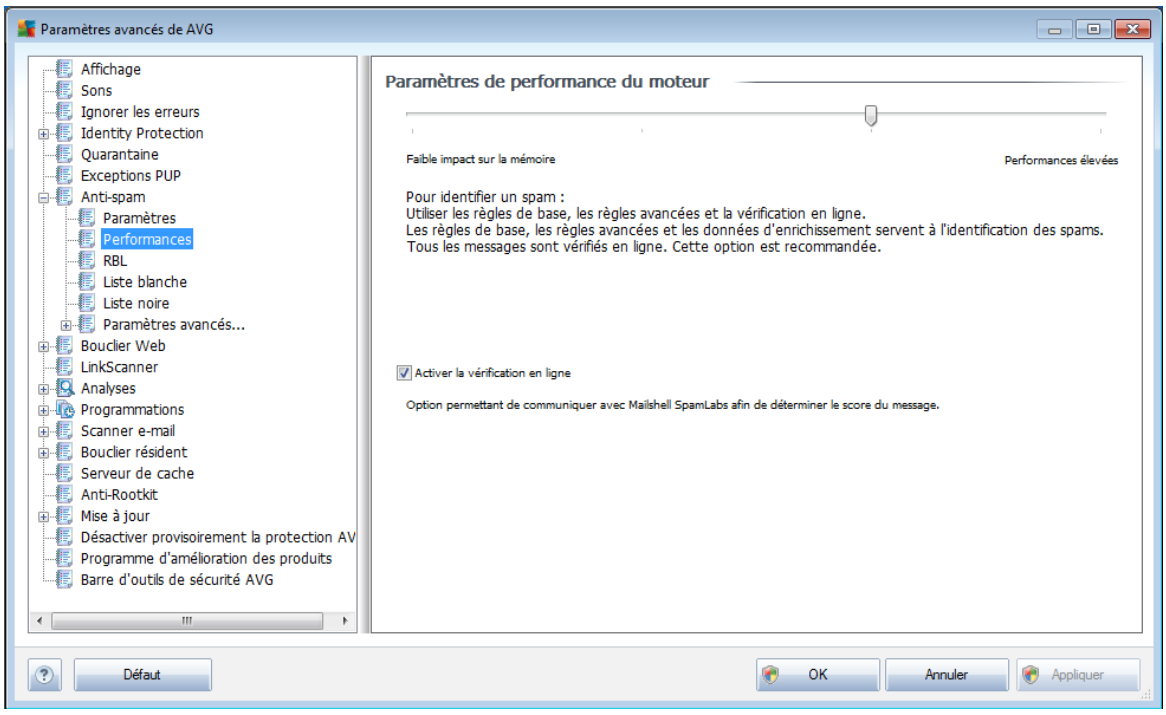
En cas de doute sur le contenu du dossier ou si vous voulez que l'assistant vous interroge pour chaque message (de manière à décider si le message en question contribue à l'enrichissement ou non de l'anti-spam), sélectionnez l'option ***Demander à chaque message***.

Pour d'autres paramètres avancés de filtrage, sélectionnez 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.

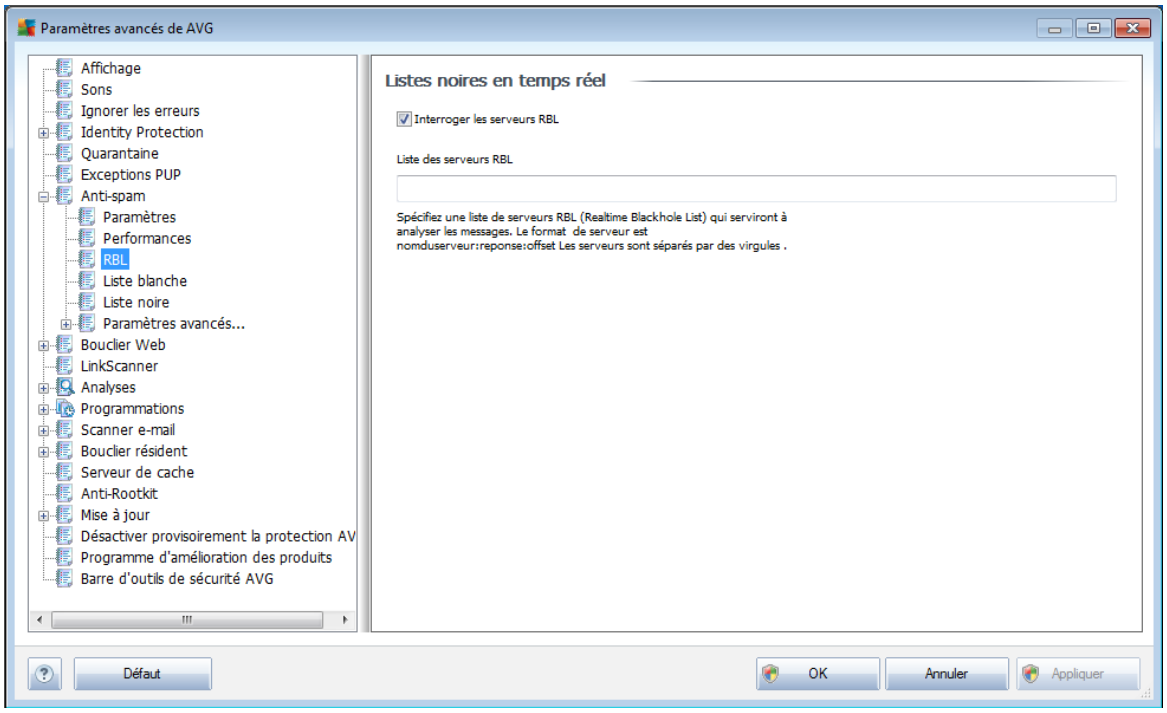
- ***Performances élevées*** - Ce mode exige une quantité de mémoire importante. Pendant l'analyse destinée à identifier le spam, les fonctions suivantes seront utilisées : règles et cache de base de données de spam, règles standard et avancées, adresses IP et bases de données de l'expéditeur de spam.

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.

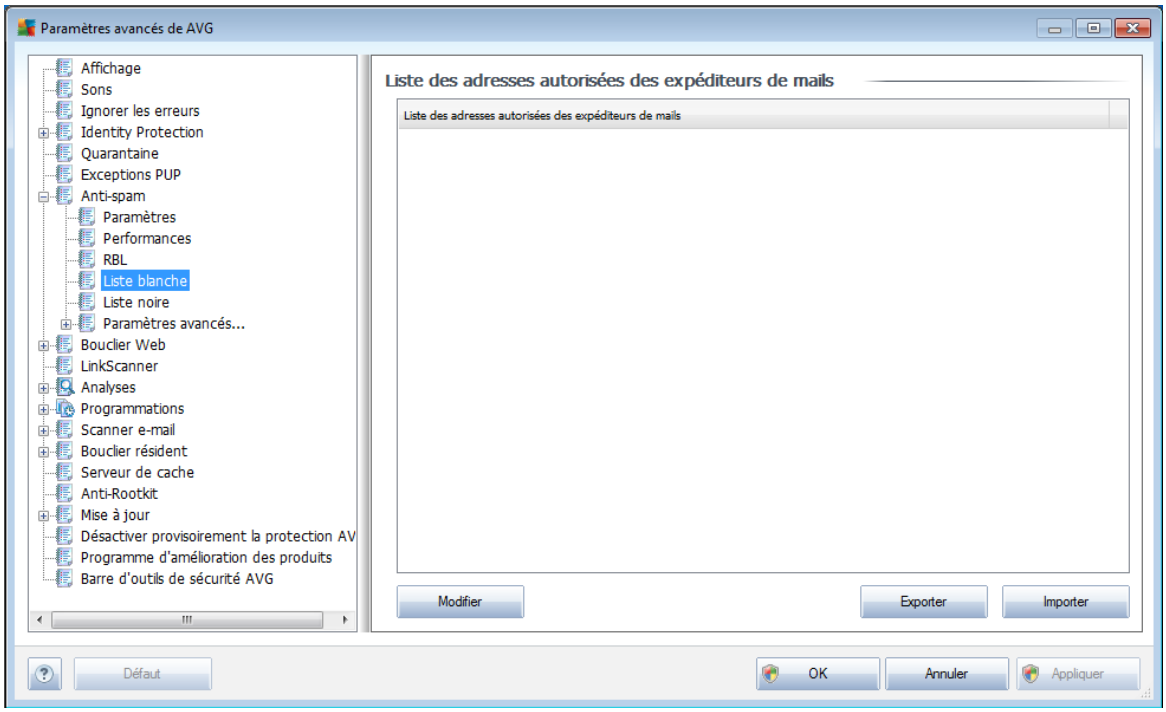
La ***liste des serveurs RBL*** permet de définir les emplacements des serveurs RBL.

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

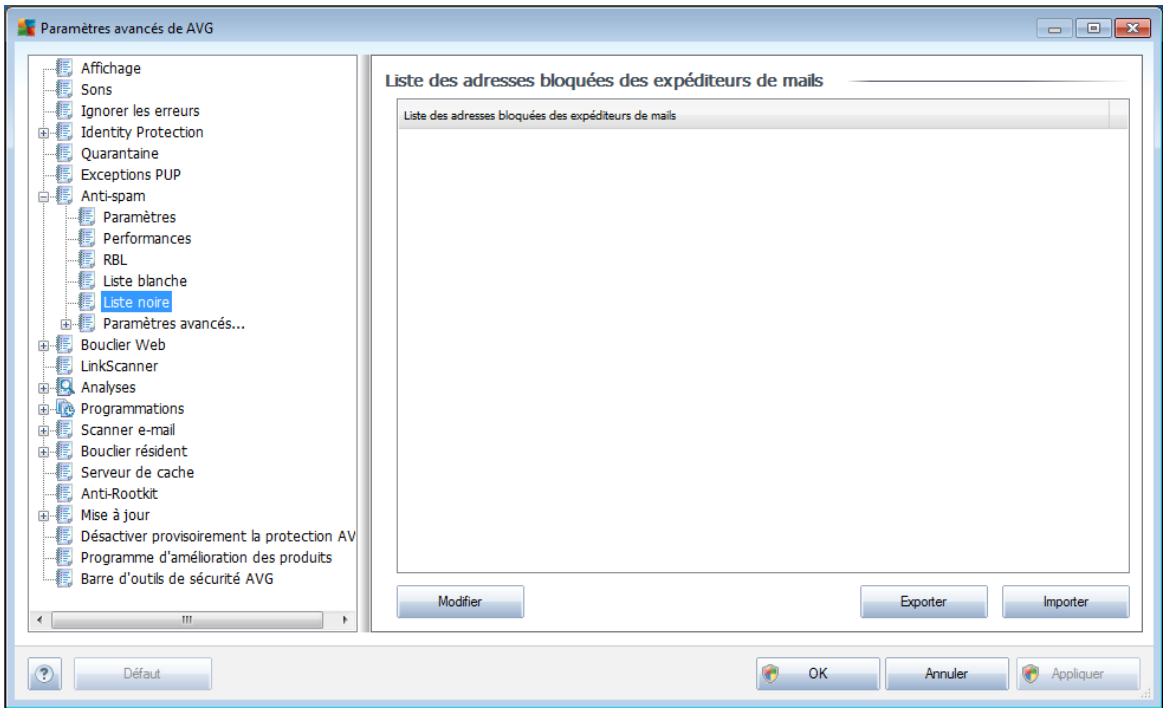
pouvez dresser une liste de noms de domaine complets (*avgfrance.com*, par exemple) dont vous avez la certitude qu'ils ne diffusent pas de messages indésirables.

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 : 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.

9.7.6. Paramètres avancés

La catégorie Paramètres avancés contient les options de configuration détaillées du composant Anti-Spam. Ces paramètres sont destinés aux utilisateurs expérimentés et plus particulièrement aux administrateurs réseau, qui doivent paramétrer plus finement la protection anti-spam et garantir la protection la plus complète des serveurs de messagerie. Pour cette raison, aucune aide supplémentaire n'est fournie au sein des boîtes de dialogue. Néanmoins, l'interface utilisateur affiche une brève description de chaque option associée.

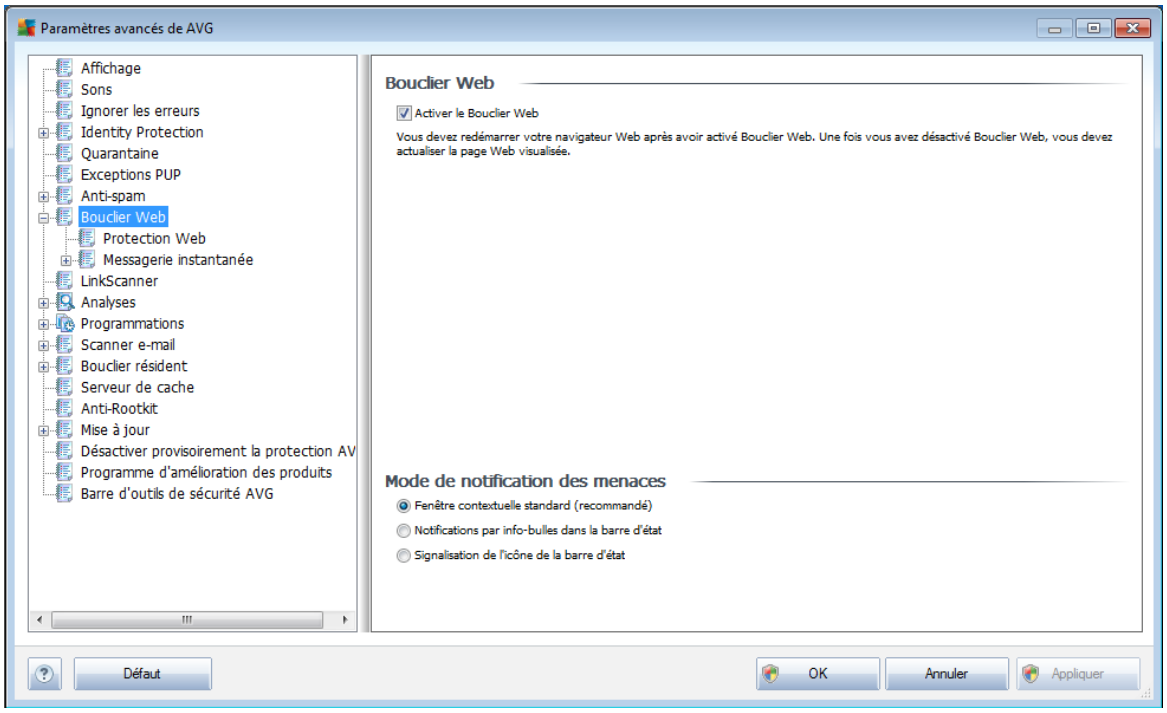
Nous vous conseillons vivement de ne pas modifier ces paramètres, à moins de maîtriser complètement les paramètres avancés de Spamcatcher (MailShell Inc.). Toute modification incorrecte risque de dégrader les performances ou de provoquer un dysfonctionnement du composant.

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

- ***Cache*** - signature, réputation du domaine, réputation légitime
- ***Enrichissement*** - nombre maximum de mots à entrer, seuil d'apprentissage automatique, pondération
- ***Filtrage*** - liste des langues, liste des pays, adresses IP approuvées, adresses IP bloquées, pays bloqués, caractères bloqués, expéditeurs usurpés

- ***RBL*** - serveurs RBL, résultats multiples, seuil, délai, IP max.
- ***Connexion Internet*** - délai, serveur proxy, authentification du proxy

9.8. Bouclier Web



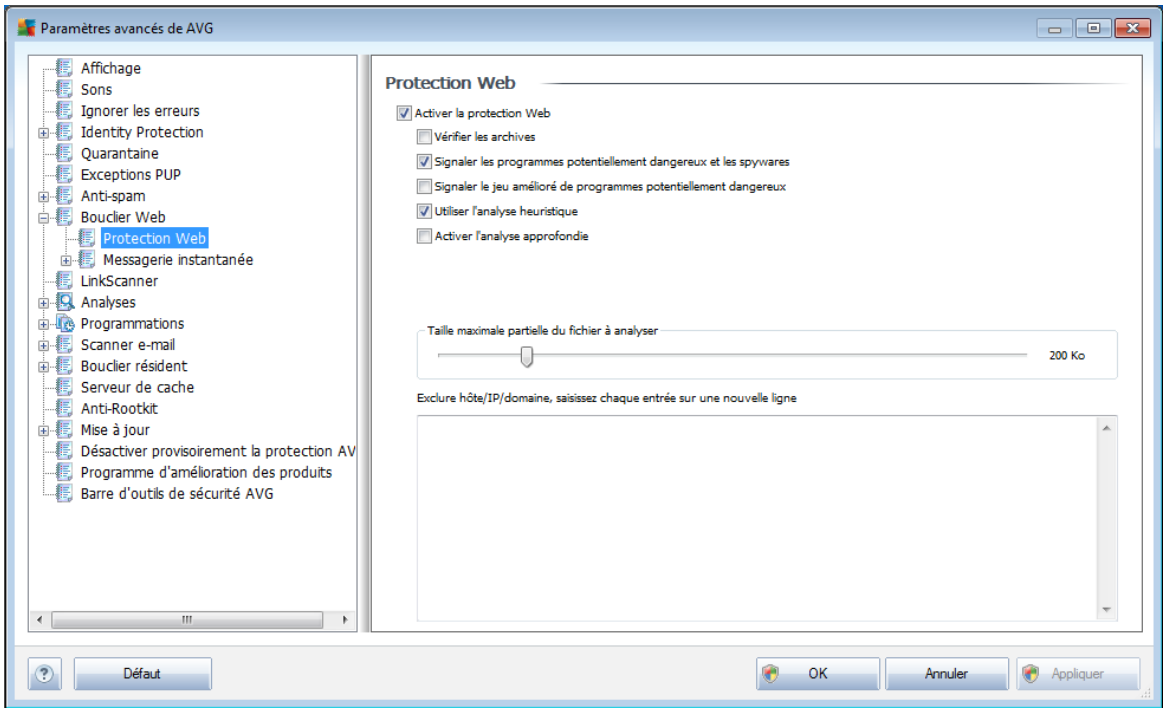
La boîte de dialogue ***Bouclier Web*** permet d'activer ou de désactiver totalement le composant ***Bouclier Web*** via l'option ***Activer le Bouclier Web*** (*activée par défaut*). Pour accéder aux paramètres avancés de ce composant, utilisez les boîtes de dialogue suivantes, comme indiqué dans l'arborescence 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 la 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*** (option désactivée par défaut*) :*analyse le contenu des archives éventuelles contenues dans la page Web à afficher.

  - ***Signaler les programmes potentiellement dangereux et les spywares*** (*activé par défaut*) : cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

  - ***Signaler le jeu amélioré de programmes potentiellement dangereux*** (*(option désactivée par défaut*) : permet de détecter le jeu étendu des spywares qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes

légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

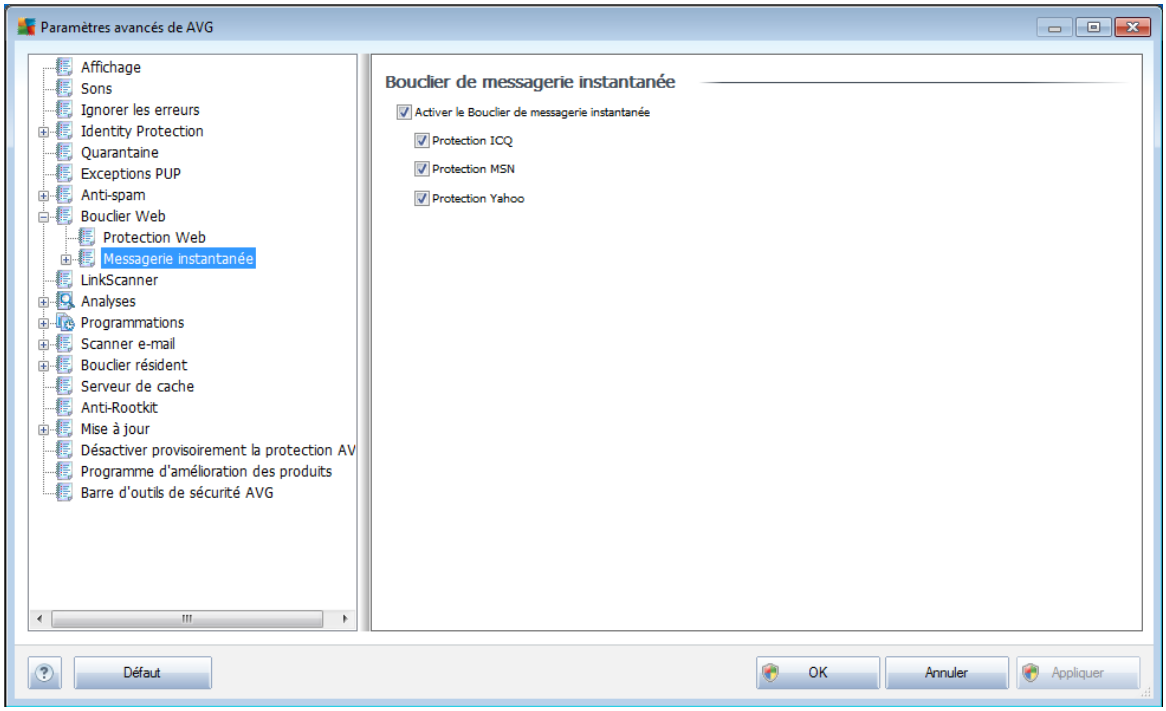
- ***Utiliser l'analyse heuristique*** (*option activée par défaut*) : analyse le contenu de la page à afficher en appliquant la méthode heuristique (*l'émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*).

- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*suspicion d'une infection de l'ordinateur*), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

- ***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 taille maximale spécifiée, 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

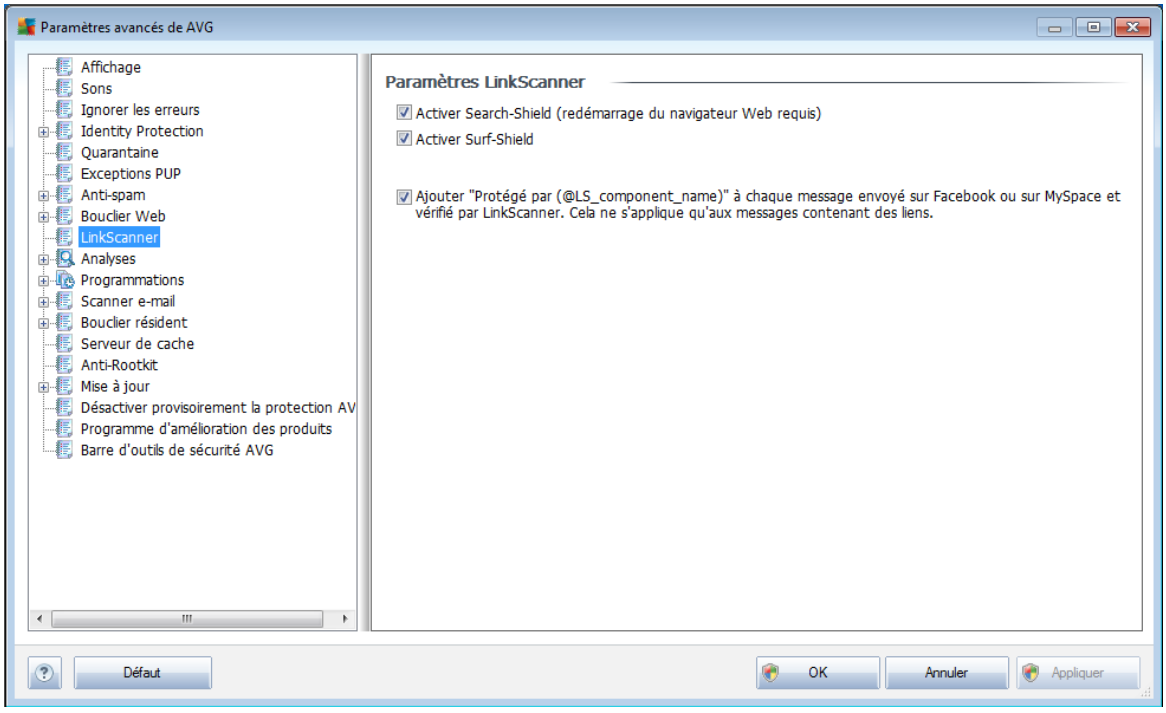


La boîte de dialogue ***Bouclier de messagerie instantanée*** permet de modifier les paramètres du composant ***Bouclier Web*** dans le cadre de l'analyse de la messagerie instantanée. Actuellement, seuls trois programmes de messagerie instantanée sont pris en charge : ***ICQ***, ***MSN*** et ***Yahoo***. 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 du LinkScanner*** permet d'activer ou de désactiver les fonctions essentielles du composant ***LinkScanner*** :



- ***Activer*** Search-Shield - *(*option activée par défaut
- ***Activer Surf-Shield*** : (*option activée par défaut*) : protection active (*en temps réel*) contre les sites hébergeant des exploits, lorsque vous y accédez. 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*).
- ***Ajouter "Protégé par LinkScanner..."*** - cochez cette case pour insérer une mention de certification relative à la vérification ***Link Scanner*** dans les messages contenant des liens hypertexte envoyés par les réseaux sociaux Facebook et MySpace.

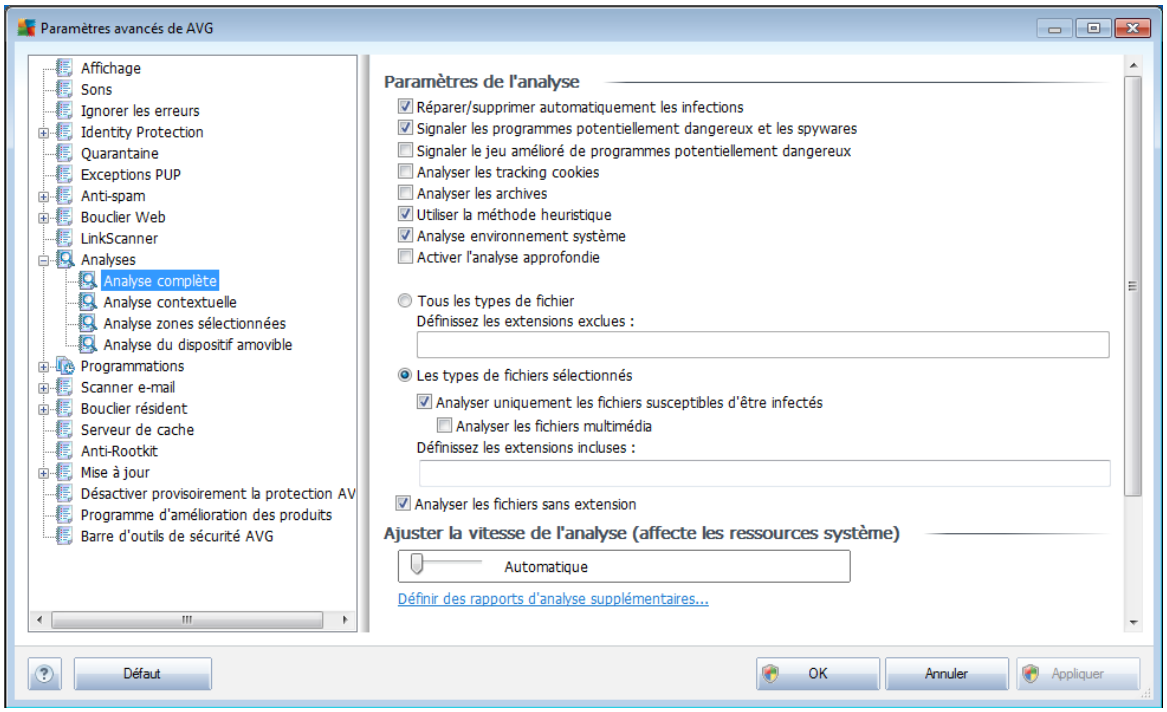
9.10. Analyses

Les paramètres d'analyse avancés sont répartis en quatre catégories selon le type d'analyse spécifique tel qu'il a été défini par l'éditeur 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 du dispositif amovible*** : 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*** (*option activée par défaut*) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement dans la mesure du possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en ***quarantaine***.

- ***Signaler les programmes potentiellement dangereux et les spywares*** (*activé par défaut*) : cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** *(option désactivée par défaut*) : permet de détecter le jeu étendu des spywares*** qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

- ***Analyser les tracking cookies*** (*option désactivée 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 leur panier d'achat électronique*).

- ***Analyser les archives*** (*option désactivée par défaut*) : ce paramètre indique que l'analyse examine 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.

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

- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*suspicion d'une infection de l'ordinateur*), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

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

(*après enregistrement de la liste, les virgules sont remplacées par des points-virgules*) à ne pas analyser ; ou les

- ***Les types de fichiers 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 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 un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.

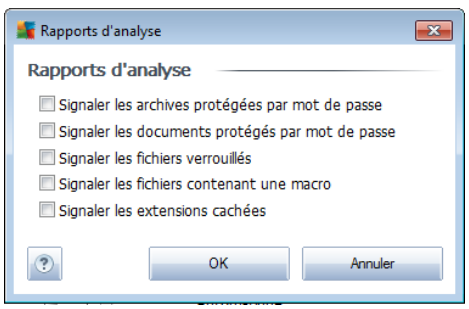
- Vous pouvez également choisir l'option ***Analyser les fichiers sans extension*** - cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une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

Ajuster la vitesse de l'analyse

Dans la section ***Ajuster la vitesse de l'analyse***, il est possible de régler la vitesse d'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.

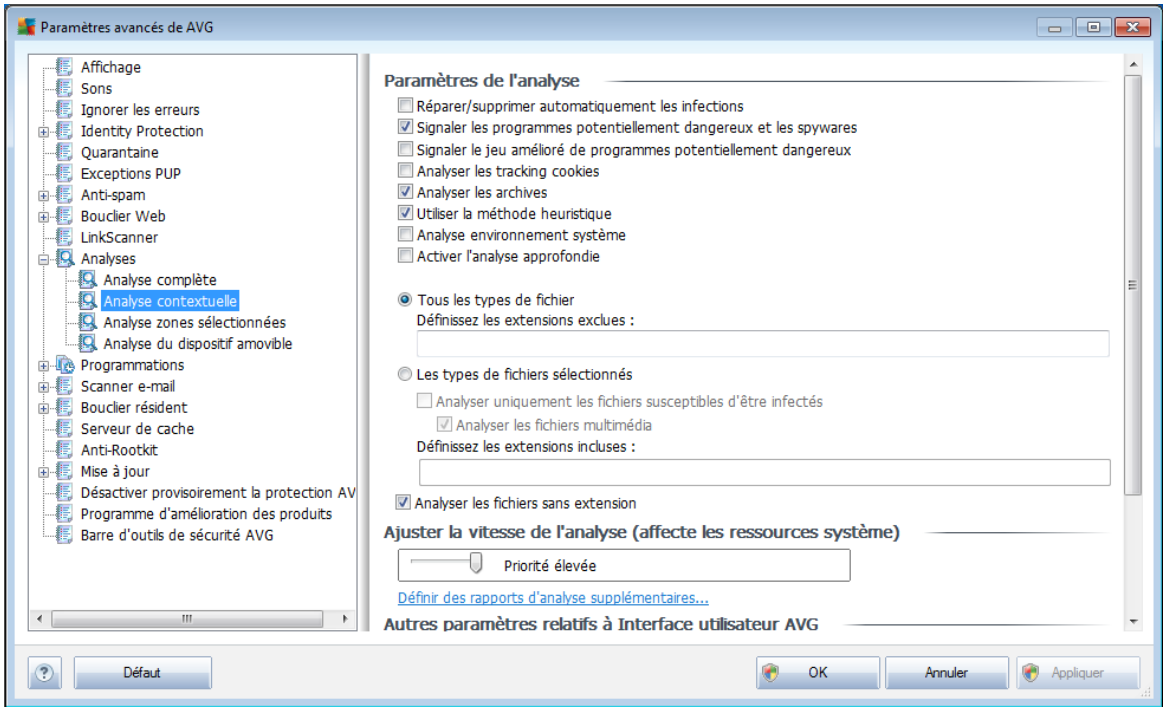
Définir des rapports d'analyse supplémentaires...

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



9.10.2. Analyse contextuelle

Similaire à l'option précédente ***Analyse complète***, l'option ***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*** :



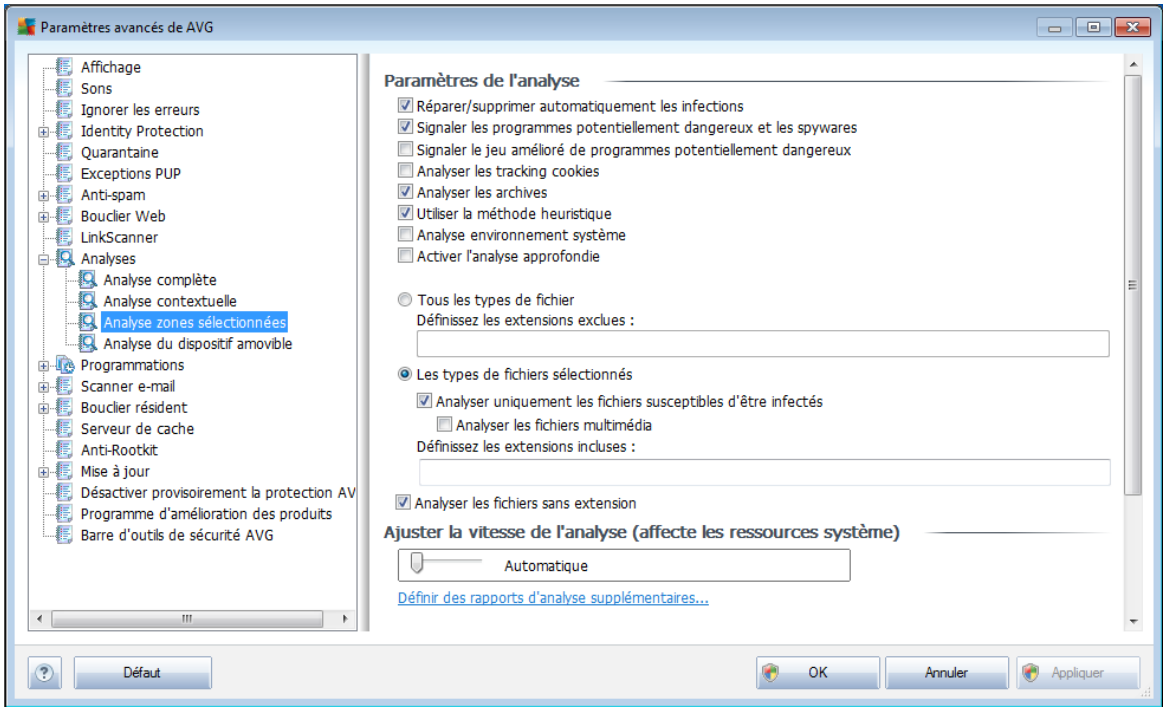
La liste des paramètres correspond à celle proposée pour l'***analyse complète***. Cependant, les paramètres par défaut diffèrent (*par exemple, l'analyse complète par défaut ne vérifie pas les archives, mais analyse l'environnement système à l'inverse de l'analyse contextuelle*).

Remarque : *pour obtenir la description des paramètres qui vous intéressent, consultez le chapitre* ***Paramètres avancés d'AVG / Analyses / Analyse complète****.*

Comme la boîte de dialogue ***Analyse complète*** , celle de l'***analyse contextuelle*** inclut la section ***Autres paramètres relatifs à l'interface utilisateur AVG***, dans laquelle vous indiquez si vous voulez que la progression de l'analyse et ses résultats soient accessibles à partir de l'interface utilisateur AVG. Vous pouvez aussi définir que les résultats d'analyse n'apparaissent qu'en cas d'infection détectée.

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***.

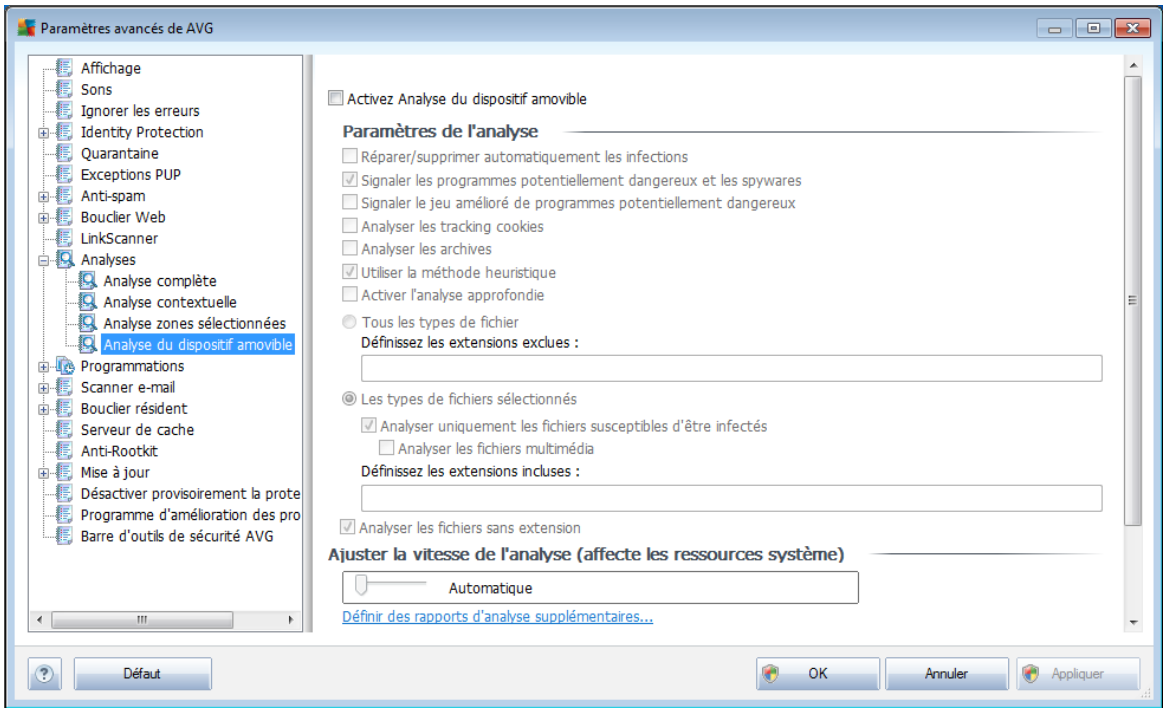


Tous les paramètres définis dans cette boîte de dialogue de configuration s'appliquent uniquement aux zones sélectionnées pour analyse dans le cadre de l'option ***Analyse zones sélectionnées***.

Remarque : *pour obtenir la description des paramètres qui vous intéressent, consultez le chapitre* ***Paramètres avancés d'AVG / Analyses / Analyse complète***.

9.10.4. Analyse du dispositif amovible

L'interface de configuration de l'***analyse du dispositif amovible*** ressemble beaucoup à celle intitulée ***Analyse complète*** :



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 la description des paramètres qui vous intéressent, consultez le chapitre* ***Paramètres avancés d'AVG / Analyses / Analyser complète***.

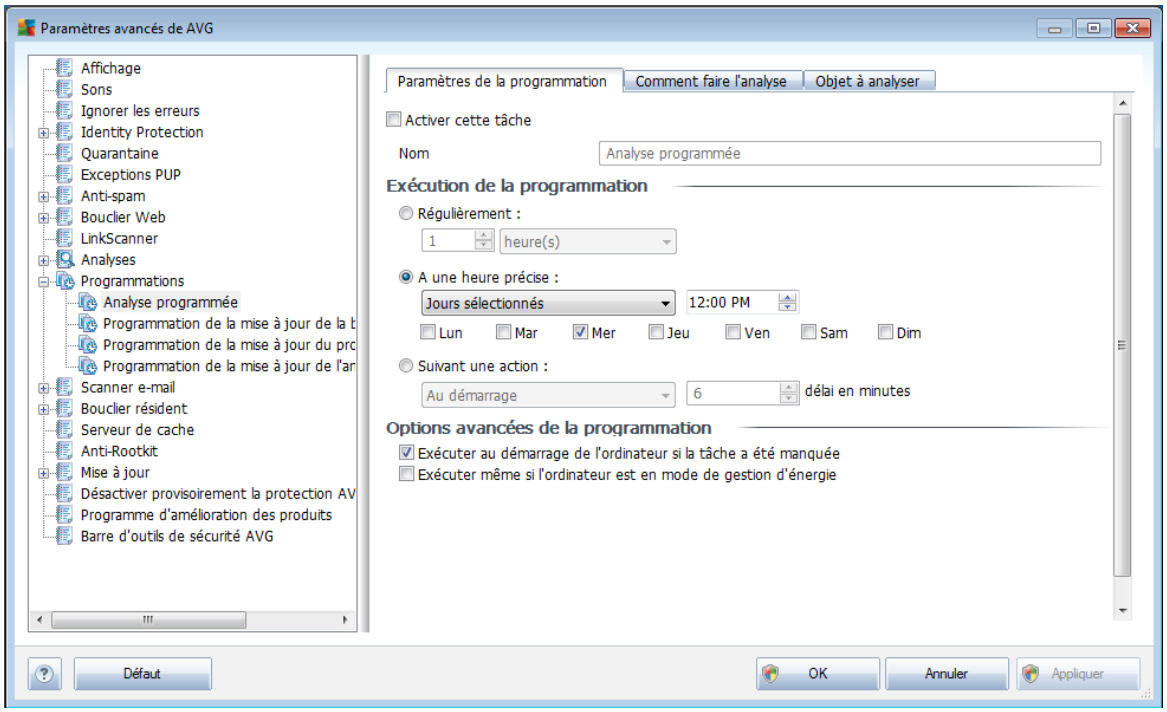
9.11. Programmations

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

- Analyse programmée
- 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/désélectionner 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 :

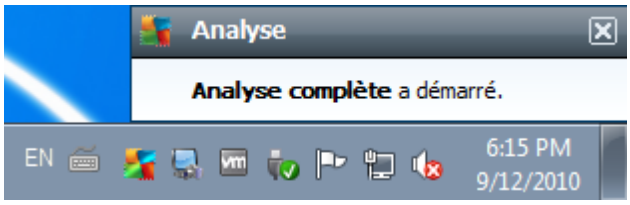
Exécution de la programmation

Ici, spécifiez l'intervalle entre chaque exécution de la nouvelle analyse. 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 lancement de l'analyse (***Suivant une action***).

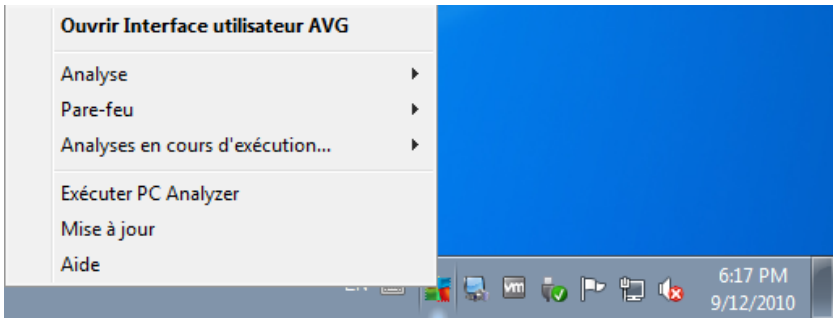
Options avancées de la programmation

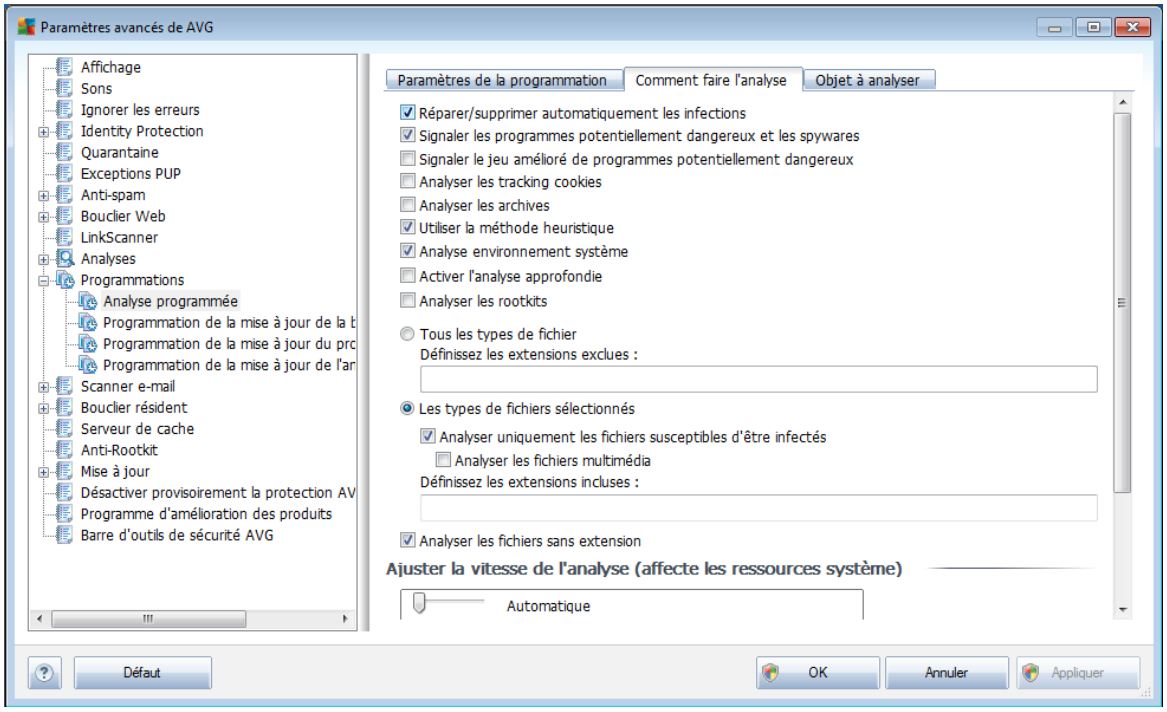
Cette section permet de définir dans quelles conditions l'analyse doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

Lorsque l'analyse programmée est exécutée à l'heure spécifiée, une fenêtre vous en informe par le biais d'une note 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 clignotantes*) et signale qu'une analyse programmée est en cours. Cliquez avec le bouton droit de la souris sur l'icône AVG de l'analyse en cours : un menu contextuel s'affiche dans lequel vous choisissez d'interrompre momentanément ou définitivement l'analyse et pouvez également modifier la priorité de l'analyse en cours d'exécution :





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 dans la mesure du possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en ***quarantaine***.

- ***Signaler les programmes potentiellement dangereux et les spywares*** *(option activée par défaut) :* cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** *(option désactivée par défaut)* : permet de détecter le jeu étendu des spywares*** qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

- ***Analyser les tracking cookies*** (*option désactivée par défaut*) : ce paramètre du composant ***Anti-Spyware*** définit que les cookies devront 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 leur panier d'achat électronique*).

- ***Analyser les archives*** (*option désactivée par défaut*) : ce paramètre indique que l'analyse examine tous les fichiers même ceux stockés dans des formats d'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.

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

- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*suspicion d'une infection de l'ordinateur*), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

- ***Analyser les rootkits*** (*option désactivée par défaut*) : 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 exclure de l'analyse en répertoriant les extensions de fichiers séparées par des virgules (*après enregistrement de la liste, les virgules sont remplacées par des points-virgules*) à ne pas analyser ; ou les

- ***Types de fichiers 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 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 un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.

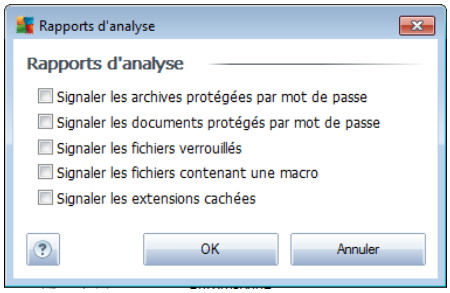
- Vous pouvez également choisir l'option ***Analyser les fichiers sans extension*** - cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une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

Ajuster la vitesse de l'analyse

Dans la section ***Ajuster la vitesse de l'analyse***, il est possible de régler la vitesse d'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.

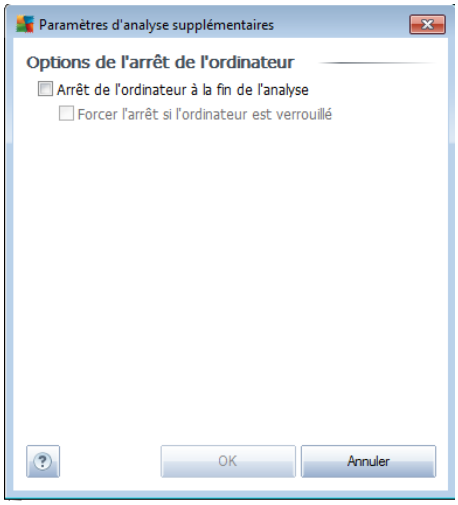
Définir des rapports d'analyse supplémentaires

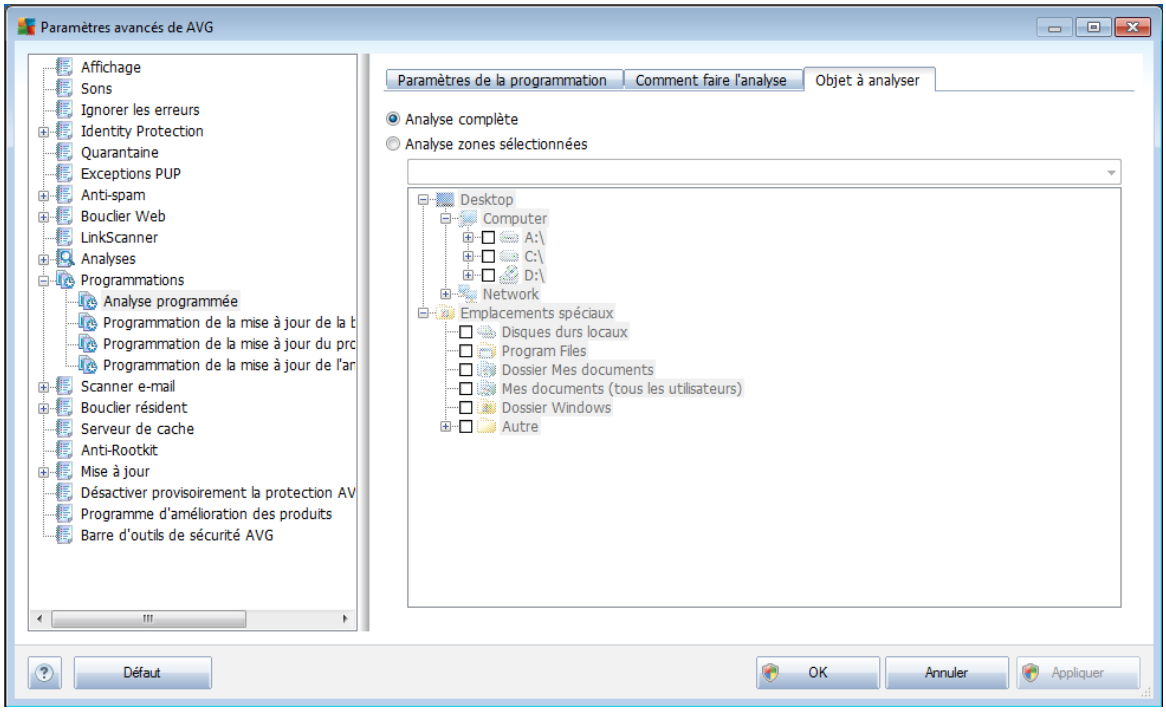
Cliquez sur le lien ***Définir des rapports d'analyse supplémentaires*** pour ouvrir la boîte de dialogue ***Rapports d'analyse*** dans laquelle vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :



Paramètres d'analyse supplémentaires

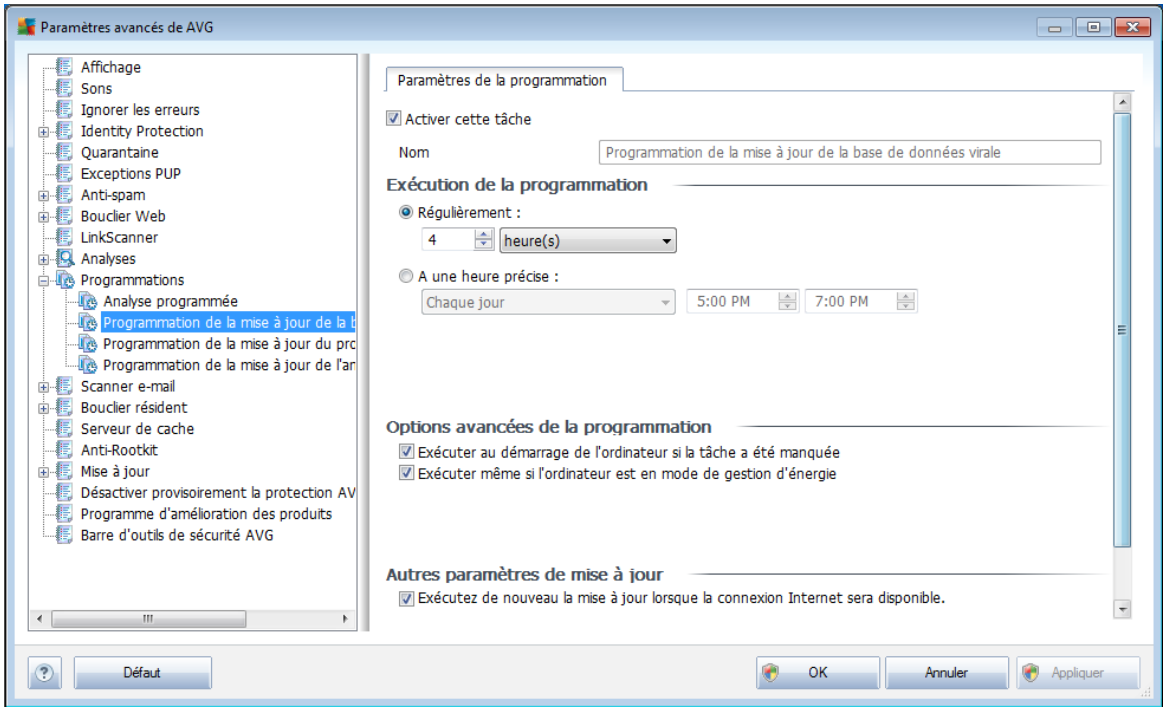
Cliquez sur ***Paramètres d'analyse supplémentaires*** pour ouvrir la boîte de dialogue ***Options de l'arrêt de l'ordinateur*** dans laquelle vous indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Si l'option ***Arrêt de l'ordinateur à la fin de l'analyse*** est activée, l'option ***Forcer l'arrêt si l'ordinateur est verrouillé*** devient disponible et 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/désélectionner 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***. Dans la boîte de dialogue correspondante, vous spécifiez en détail 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 programmation par le fournisseur du programme.

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 le lancement de la mise à jour après un laps de temps donné (***Régulièrement***) ou d'en définir la date et l'heure précises (***A une heure précise***).

Options avancées de la programmation

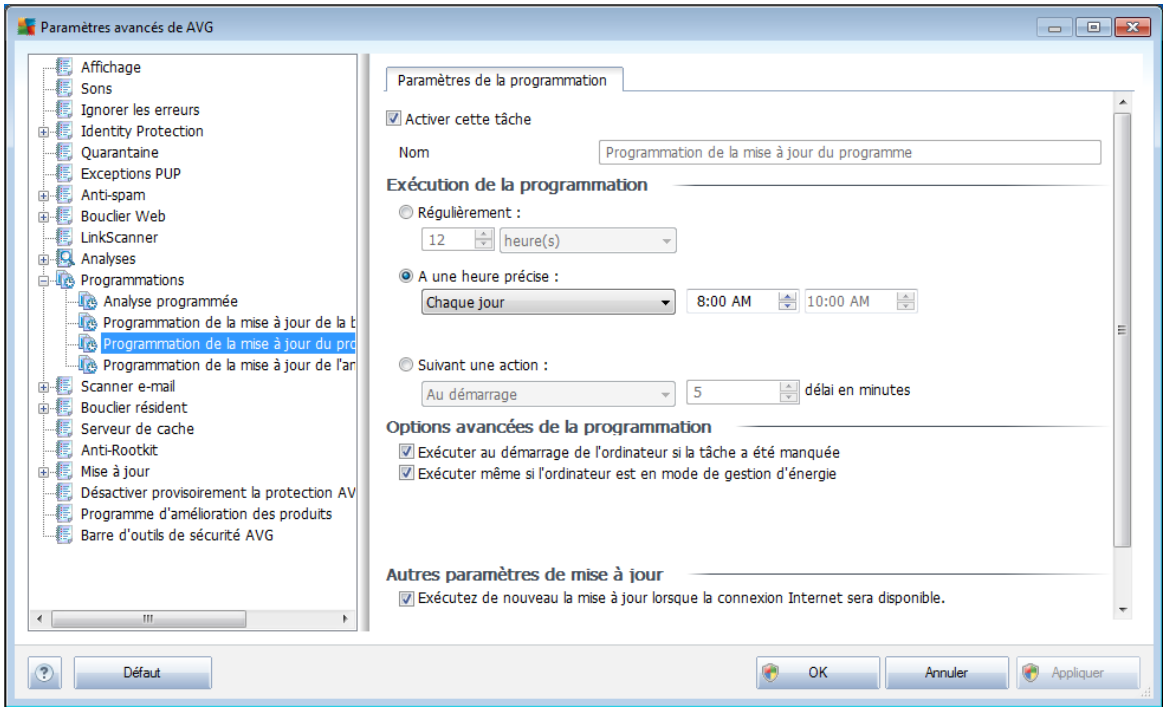
Cette section permet de définir dans quelles conditions la mise à jour de la base de données virale doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

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 cocher/désélectionner 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 l'éditeur du programme.

Exécution de la programmation

Ici, spécifiez l'intervalle entre chaque exécution de la mise à jour de l'application programmée. Il est possible de répéter l'exécution de la mise à jour 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 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.

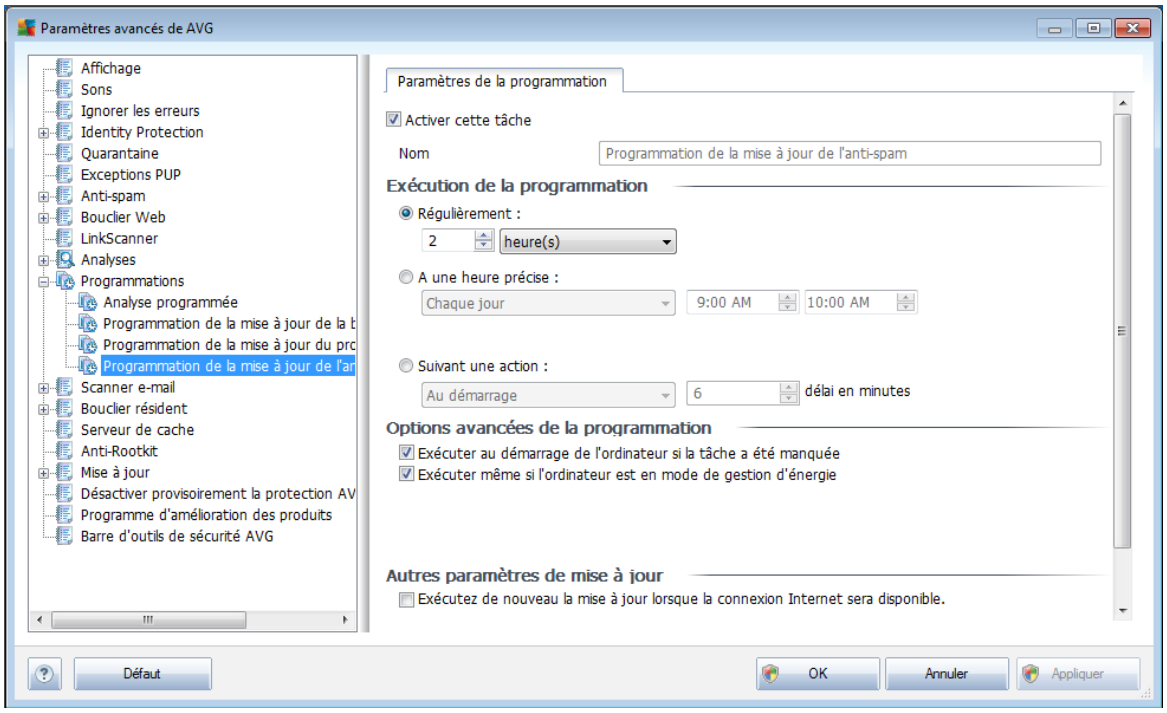
Autres paramètres de mise à jour

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***).

Remarque : *si une mise à jour planifiée du programme coïncide avec une analyse programmée, le processus de mise à jour a priorité sur l'analyse qui est interrompue.*

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



Dans l'onglet ***Paramètres de la programmation***, vous pouvez cocher/désélectionner

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 standard 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.

Exécution de la programmation

Ici, spécifiez la fréquence de mise à jour du composant ***Anti-Spam***. Il est possible de répéter le lancement de la mise à jour ***anti-spam***après un laps de temps donné (***Régulièrement***), de définir une heure et une date précises (***A une heure précise***) ou encore de définir 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 hors tension ou en mode d'économie d'énergie.

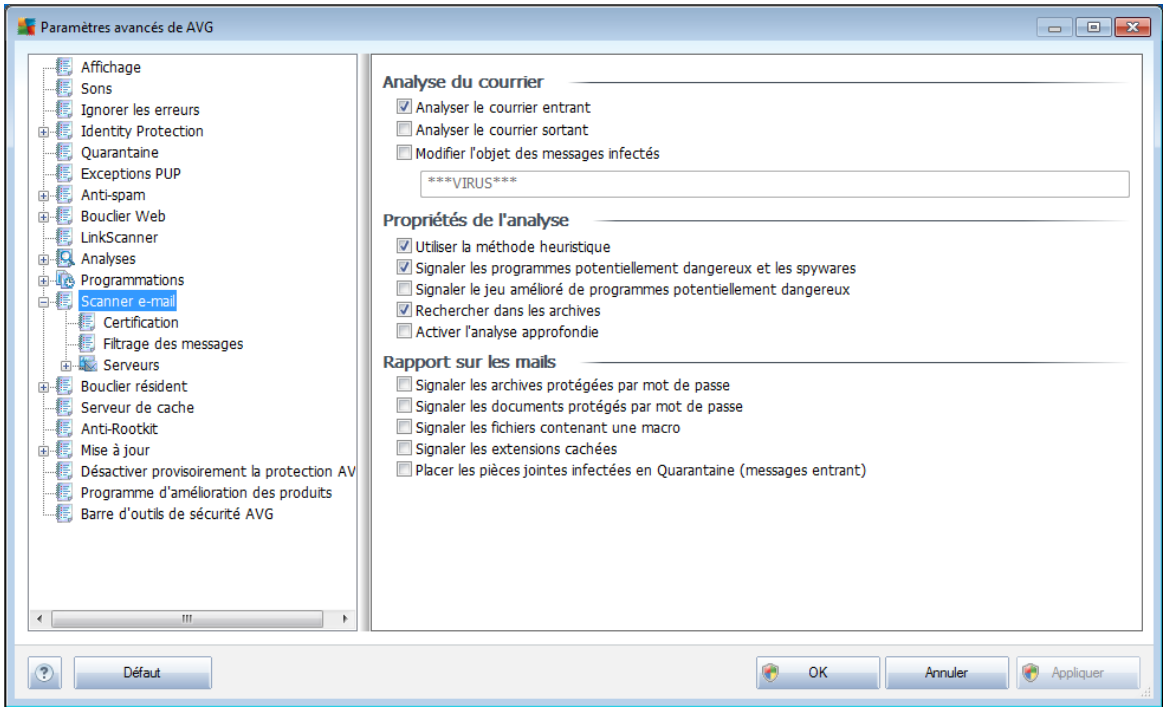
Autres paramètres de mise à jour

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*** comporte trois parties :



Analyse du courrier

Dans cette section, vous définissez la configuration standard des messages entrants et/ou sortants :

- ***Analyser le courrier entrant*** (*option activée par défaut*) - cette option permet d'activer ou de désactiver l'analyse des e-mails remis à votre client de messagerie
- ***Analyser le courrier sortant*** (*option désactivée par défaut*) - cette option permet d'activer ou de désactiver l'analyse des e-mails envoyés par votre compte
- ***Modifier l'objet des messages infectés*** (*option désactivée par défaut*) - si vous voulez être averti que le message est infecté , cochez cette case et indiquez le texte à afficher dans le champ prévu à cet effet. Ce texte sera alors inséré dans l'objet de chaque mail infecté, pour une identification et un filtrage plus faciles. Nous vous recommandons de conserver la valeur par défaut : ***VIRUS***.

Propriétés de l'analyse

Dans cette section, vous choisissez les modalités de l'analyse des messages :

- ***Utiliser la méthode heuristique*** (*option activée par défaut*) - cochez cette option pour appliquer la méthode heuristique à l'analyse des messages. Lorsque cette option est active, vous pouvez filtrer les pièces jointes, non seulement selon leur extension, mais aussi selon leur contenu. Le filtrage peut être défini dans la boîte de dialogue ***Filtrage des messages***.

- ***Signaler les programmes potentiellement dangereux et les spywares*** (*option activée par défaut*) : cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** - *(option désactivée par défaut*) : permet de détecter le jeu étendu des spywares qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

- ***Rechercher dans les archives*** (*option activée par défaut*) - cochez la case pour analyser le contenu des archives jointes aux messages.

- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*exemple : suspicion de présence d'un virus ou d'un exploit sur l'ordinateur*) vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

Signalisation des pièces jointes

Dans cette section, vous pouvez définir des rapports supplémentaires sur les fichiers potentiellement dangereux ou suspects. Notez qu'aucun avertissement ne sera affiché, seul un texte de certification sera ajouté à la fin du message et tous les rapports associés seront recensés dans la boîte de dialogue Détection du scanner e-mail.

- ***Signaler les archives protégées par mot de passe*** – archives (*ZIP, RAR, etc.*) qui sont protégées par mot de passe et qui, à ce titre, ne peuvent pas faire l'objet d'une recherche de virus. Cochez cette case pour les signaler comme étant potentiellement dangereuses.

- ***Signaler les documents protégés par mot de passe*** – les documents protégés par mot de passe ne peuvent pas faire l'objet d'une recherche de virus. Cochez cette case pour les signaler comme étant potentiellement

dangereux.

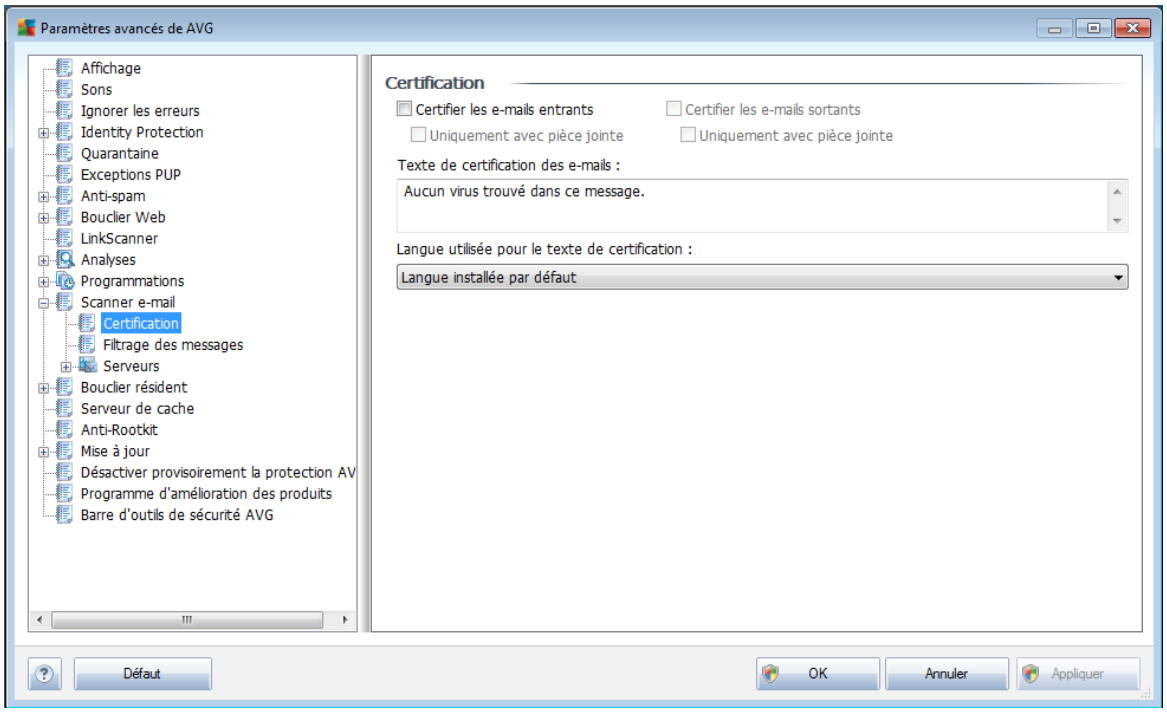
- ***Signaler les fichiers contenant une macro*** – *une macro est une séquence prédéfinie d'étapes destinées à faciliter certaines tâches pour l'utilisateur (les macros MS Word en sont un exemple bien connu*). A ce titre, une macro peut contenir des instructions potentiellement dangereuses. Vous pouvez cocher cette case pour garantir que les fichiers contenant des macros seront signalés comme suspects.

- ***Signaler les extensions cachées*** – masquer les extensions qui peuvent présenter un fichier exécutable suspect "objet.txt.exe" sous la forme d'un fichier texte "objet.txt" inoffensif. Cochez cette case pour signaler ces fichiers comme étant potentiellement dangereux.

- ***Placer les pièces jointes signalées dans Quarantaine*** – 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

Dans la boîte de dialogue ***Certification***, vous pouvez saisir le texte de certification pour les mails entrants et sortants ainsi que la langue dans laquelle il est rédigé :



Le texte de certification se compose de deux parties : la partie utilisateur et la partie système. Dans l'exemple suivant, la première ligne représente la partie utilisateur, le reste est généré automatiquement :

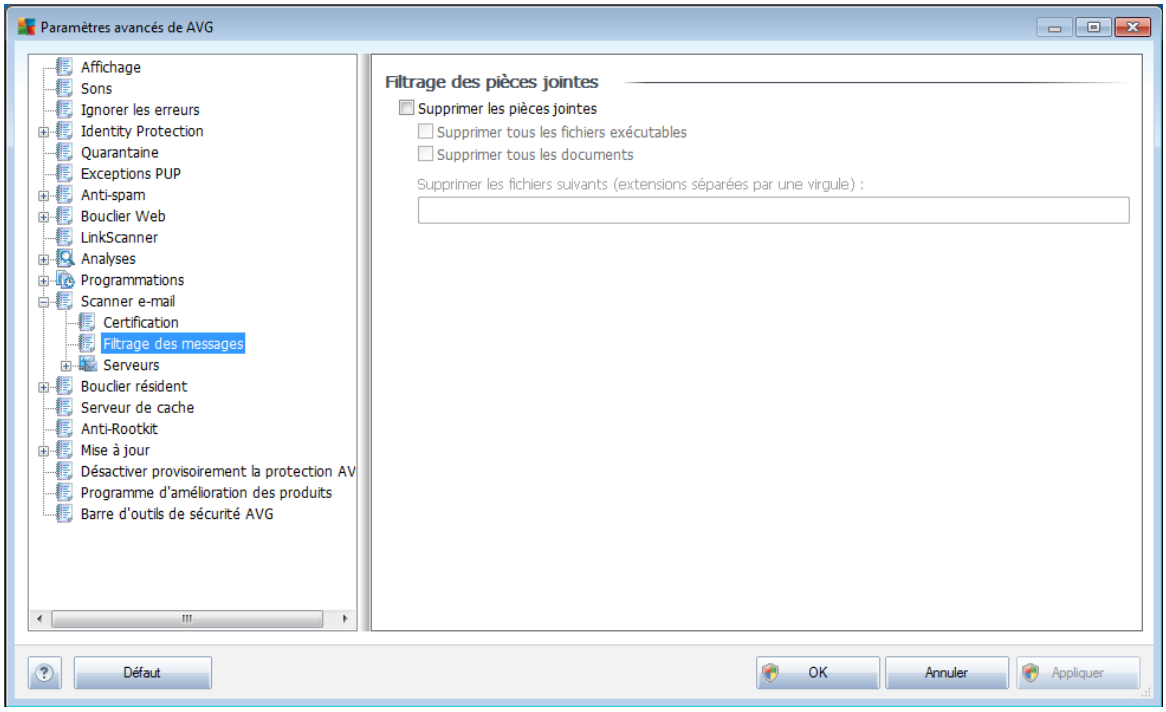
Aucun virus trouvé dans ce message.

Analyse effectuée par AVG.

Version : x.y.zz / Base de données virale : xx.y.z - Date : 12/9/2010

Si vous décidez d'insérer un texte de certification aux messages entrants ou sortants, vous pouvez en définir les termes exacts dans la boîte de dialogue (***Texte de certification des e-mails***) et choisir la langue de la deuxième partie du texte qui est générée automatiquement (***Langue du texte de certification***).

9.12.2. Filtrage des messages

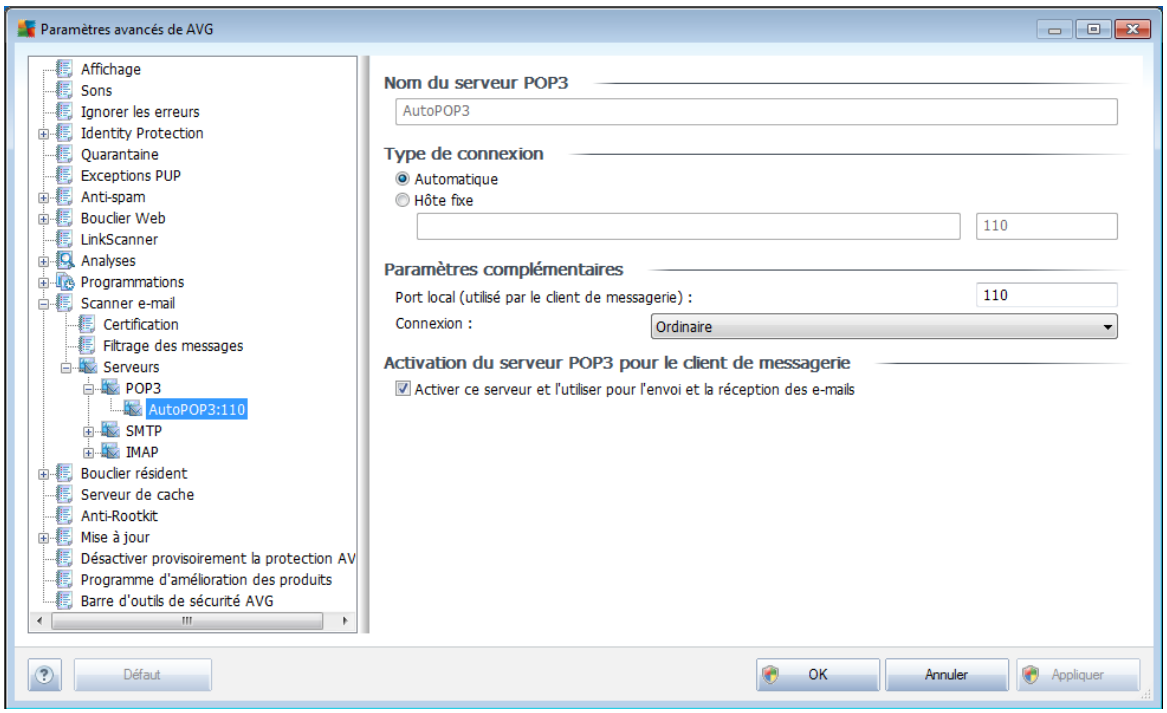


La boîte de dialogue ***Filtrage des pièces jointes*** est destinée à vous aider à définir les paramètres de l'analyse des pièces jointes aux mails. Par défaut, l'option ***Supprimer les pièces jointes*** est désactivée. Si vous décidez de l'activer, toutes les pièces jointes signalées comme infectées 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, *.docx, *.xls, *.xlsx 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. 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*** - dans ce champ, vous pouvez spécifier le nom des serveurs récemment ajoutés (*pour ajouter un serveur POP3, cliquez avec le bouton droit sur l'option POP3 du menu de navigation gauche*). Dans le cas d'un serveur créé automatiquement (serveur "AutoPOP3"), ce champ est désactivé.

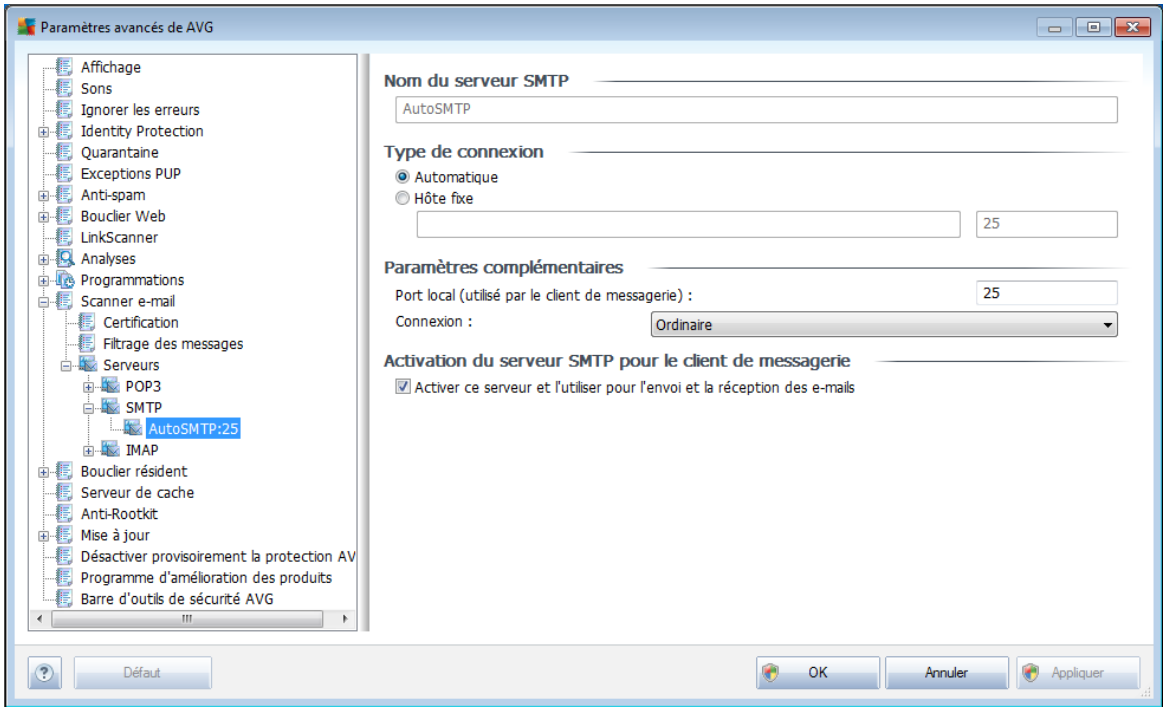
- ***Type de connexion*** - définissez la méthode de sélection du serveur de messagerie pour les mails entrants.

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

    - ***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. En guise de 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 143.

- ***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.
  - ***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*** - cochez/désélectionnez cette case pour activer ou désactiver le serveur POP3 spécifié

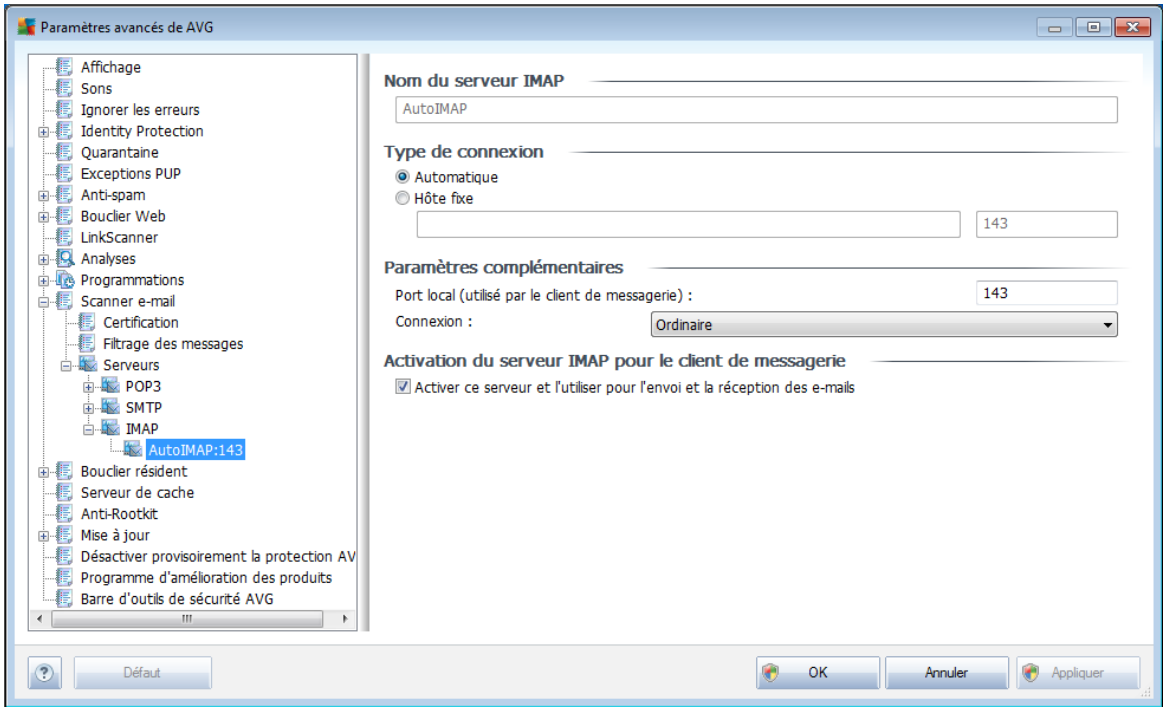


Dans cette boîte de dialogue (*ouverte grâce à la commande* ***Serveurs / SMTP***), vous configurez un nouveau serveur ***Scanner e-mail*** à l'aide du protocole SMTP pour les messages sortants :

- ***Nom du serveur SMTP*** - dans ce champ, vous pouvez spécifier le nom des

serveurs récemment ajoutés (*pour ajouter un serveur SMTP, cliquez avec le bouton droit sur l'option SMTP du menu de navigation gauche*). Dans le cas d'un serveur créé automatiquement (serveur "AutoSMTP"), ce champ est désactivé.

- ***Type de connexion*** - définissez la méthode de sélection du serveur de messagerie pour les mails sortants :
    - ***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 de votre 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*** - 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 SMTP.
    - ***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.
- ***Activation du serveur SMTP pour le client de messagerie*** - cochez/ désélectionnez cette case pour activer ou désactiver le serveur SMTP spécifié ci-dessus



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

- ***Nom du serveur IMAP*** - dans ce champ, vous pouvez spécifier le nom des serveurs récemment ajoutés (*pour ajouter un serveur IMAP, cliquez avec le bouton droit sur l'option IMAP du menu de navigation gauche*). Dans le cas d'un serveur créé automatiquement (serveur "AutoIMAP"), ce champ est désactivé.

- ***Type de connexion*** - définissez la méthode de sélection du serveur de messagerie pour les mails sortants :

  - ***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 de votre 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 (*imap.acme.com:8200, par exemple*). Le port standard des communications SMTP est le port 25.

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

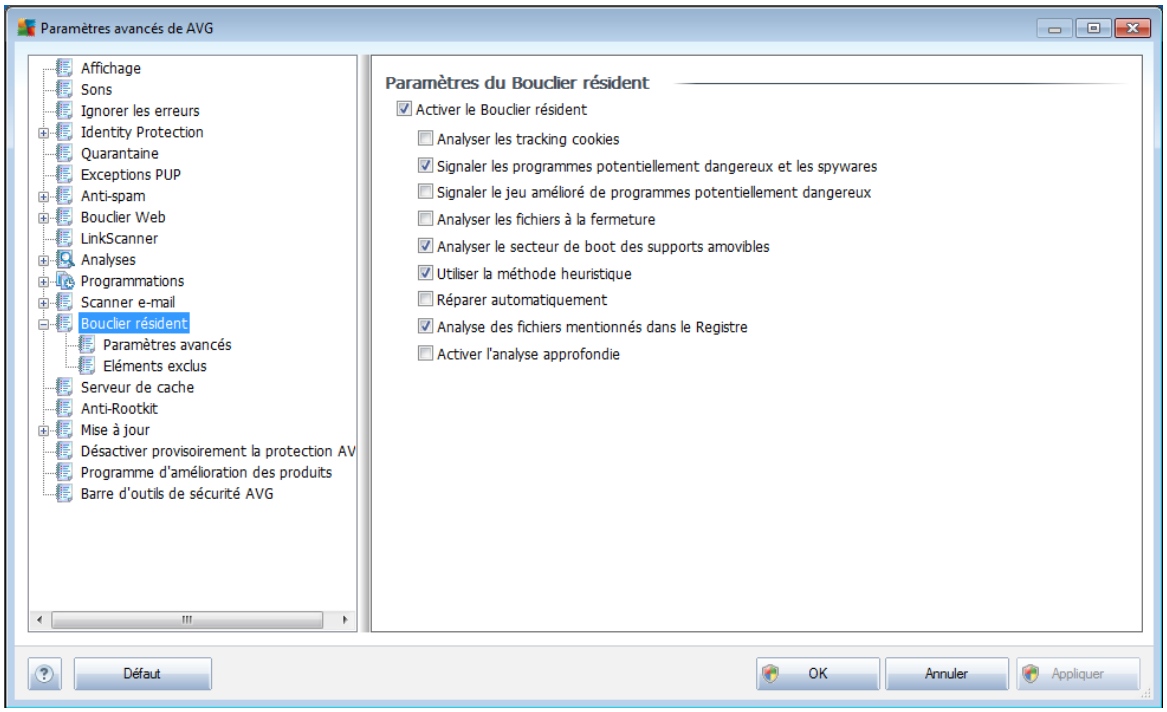
- **_Port local_** - indique le port sur lequel transitent les communications provenant de l'application de messagerie. Vous devez alors indiquer, dans votre programme de messagerie, que ce port sert pour les communications IMAP.

- **_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.

- ***Activation du serveur IMAP pour le client de messagerie*** - cochez/ désélectionnez cette case pour activer ou désactiver le serveur SMTP spécifié ci-dessus

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 tracking cookies*** - ce paramètre indique que l'analyse doit détecter les cookies. (*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 leur panier d'achat électronique).

- ***Signaler les programmes potentiellement dangereux et les spywares*** – (*activé par défaut*) : cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** (*option désactivée par défaut*) : permet de détecter le jeu étendu des spywares qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

- ***Analyser les fichiers à la fermeture*** (*option désactivée par défaut*) - 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 de 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*)

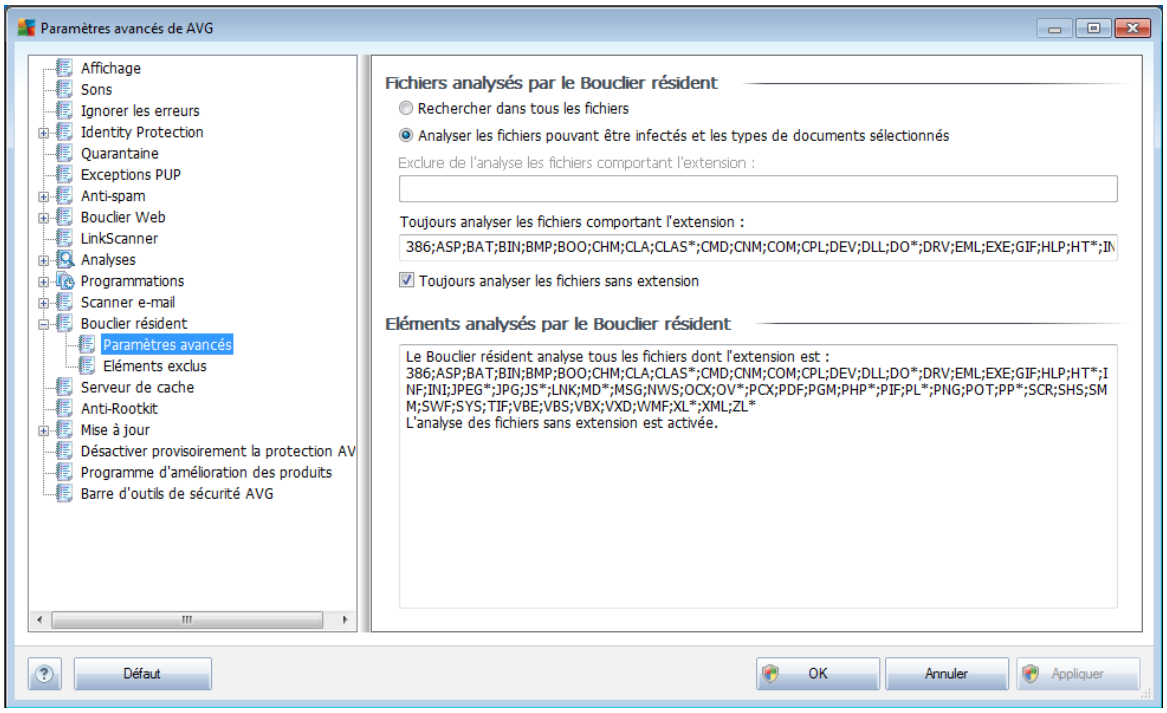
- ***Réparer automatiquement*** (*option désactivée par défaut*) - toute infection détectée sera réparée automatiquement dans la mesure où un traitement existe ; les infections incurables seront supprimées.

- ***Analyse de fichiers mentionnés dans le Registre*** (*option activée par défaut*) - ce paramètre indique qu'AVG analyse les fichiers exécutables ajoutés au registre de démarrage pour éviter l'exécution d'une infection connue au démarrage suivant de l'ordinateur.

- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*urgence*), vous pouvez cocher cette case afin d'activer les algorithmes les plus rigoureux qui examineront au peigne fin tous les objets représentant de près ou de loin une menace. Gardez à l'esprit que cette méthode prend énormément de temps.

9.13.1. Paramètres avancés

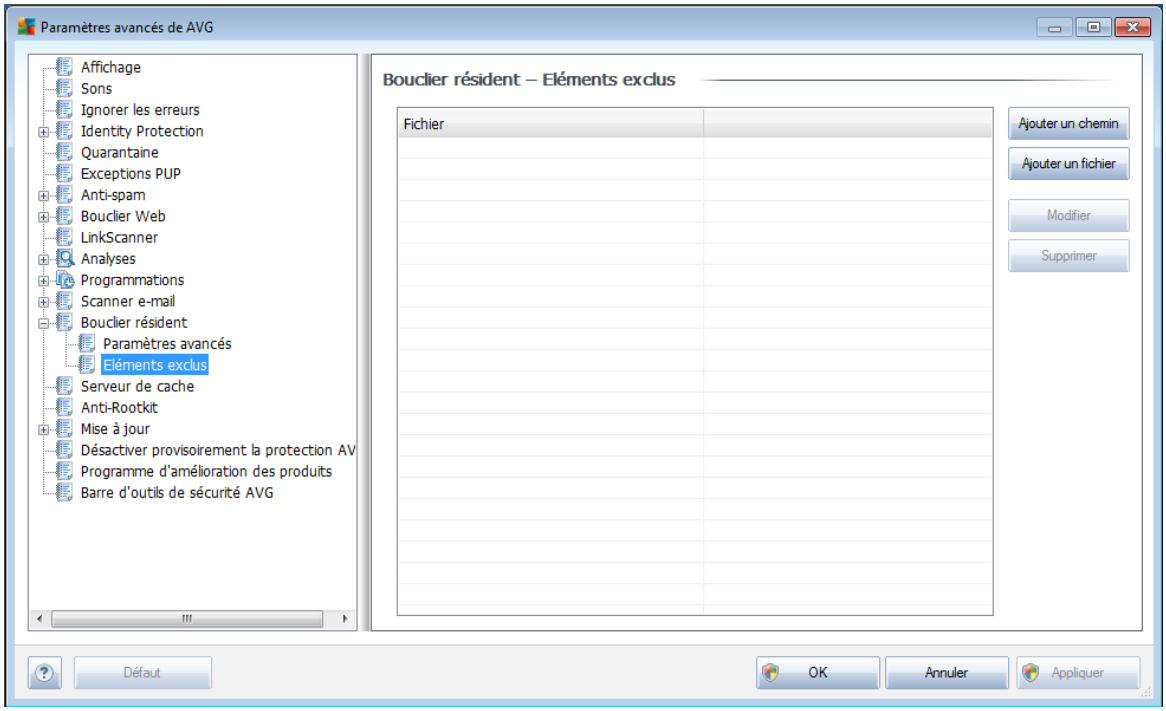
Dans la boîte de dialogue ***Fichiers analysés par le Bouclier résident***, il est possible de spécifier les fichiers à analyser (*en fonction de leurs extensions*) :



Choisissez si vous voulez analyser tous les fichiers ou seulement ceux qui sont susceptibles d'être infectés. 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.

La section en dessous appelée ***Eléments analysés par le Bouclier résident*** récapitule les paramètres actuels et donne des informations détaillées sur les éléments examinés par le Bouclier résident.

9.13.2. Eléments exclus



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

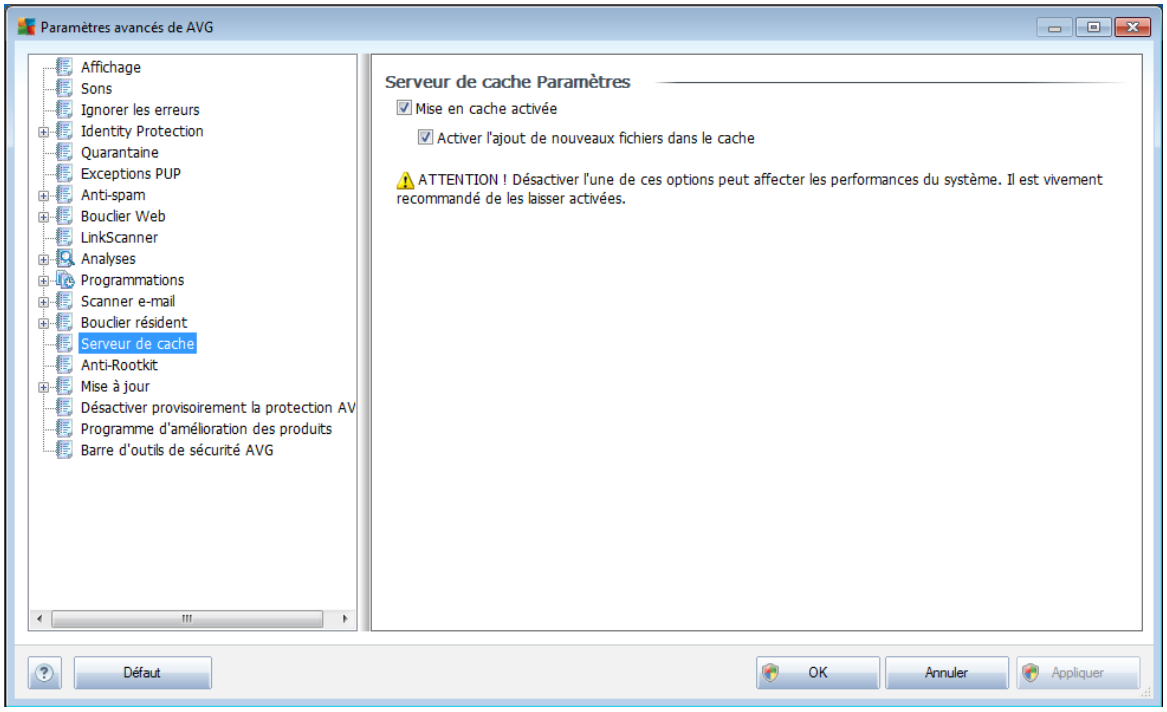
Il est vivement recommandé de n'exclure aucun fichier, sauf en cas d'absolue nécessité !

Cette boîte de dialogue présente les boutons de fonction suivantes :

- ***Ajouter un chemin*** – ce bouton permet de spécifier un répertoire ou des répertoires que vous souhaitez exclure de l'analyse en les sélectionnant un à un dans l'arborescence de navigation du disque local
- ***Ajouter un fichier*** – ce bouton permet de spécifier les fichiers que vous souhaitez exclure de l'analyse en les sélectionnant un à un dans l'arborescence de navigation du disque local
- ***Modifier***- ce bouton permet de modifier le chemin d'accès à un fichier ou dossier sélectionné
- ***Supprimer***– ce bouton permet de supprimer le chemin d'accès à un objet sélectionné dans la liste

9.14. Serveur de cache

Le ***serveur de cache*** est un processus conçu pour accélérer toutes les analyses (*analyses à la demande, analyses de l'ordinateur programmée ou analyses du Bouclier résident*). Il rassemble et conserve les informations des fichiers dignes de confiance (*fichiers système dotés d'une signature numérique, etc.).*). Ces fichiers, jugés sans danger, sont par la suite ignorés pendant l'analyse.



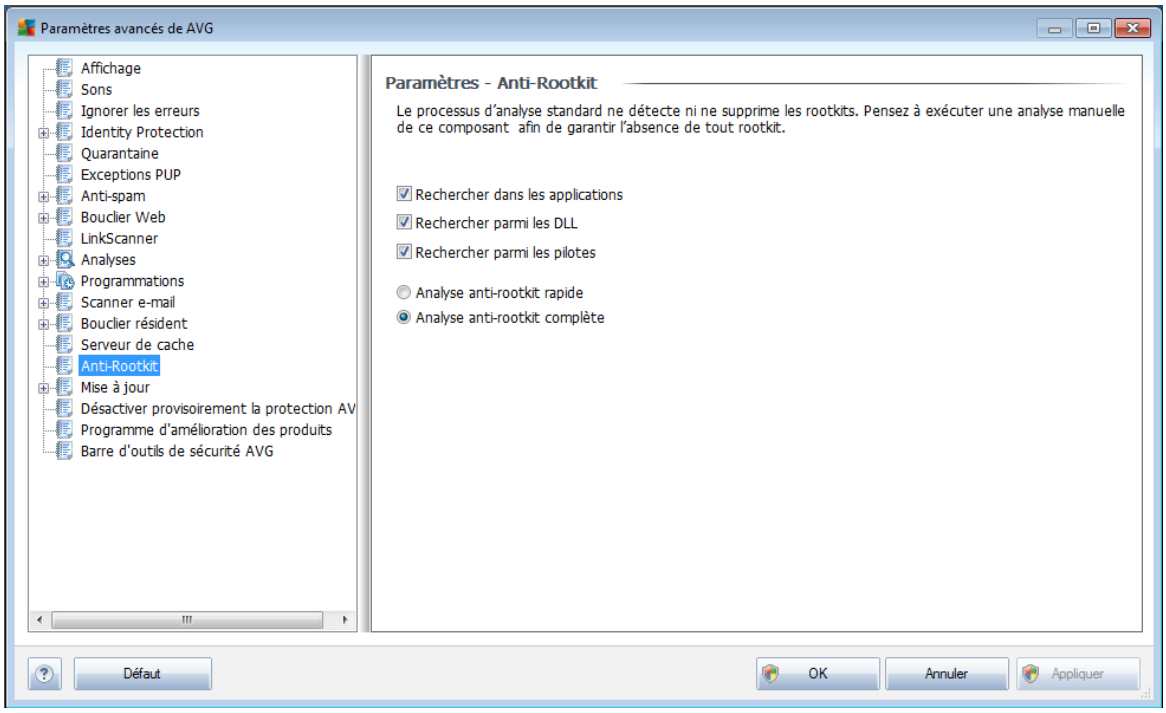
La boîte de dialogue des paramètres propose deux options :

- ***Mise en cache activée*** (*option activée par défaut*) – désélectionnez la case pour désactiver le ***serveur de cache*** et videz la mémoire de mise en cache. Notez que l'analyse risque de durer plus longtemps et que les performances de l'ordinateur risquent d'être diminuées étant donné que chaque fichier en cours d'utilisation fera d'abord l'objet d'une analyse anti-virale et anti-spyware préalable.

- ***Activer l'ajout de nouveaux fichiers dans le cache*** (*option activée par défaut*) – désélectionnez la case pour mettre fin à l'ajout de fichiers dans la mémoire cache. Tout fichier déjà mis en cache sera conservé et utilisé jusqu'à ce que la mise en cache soit complètement désactivée ou jusqu'à la prochaine mise à jour de la base de données virale.

9.15. Anti-rootkit

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



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

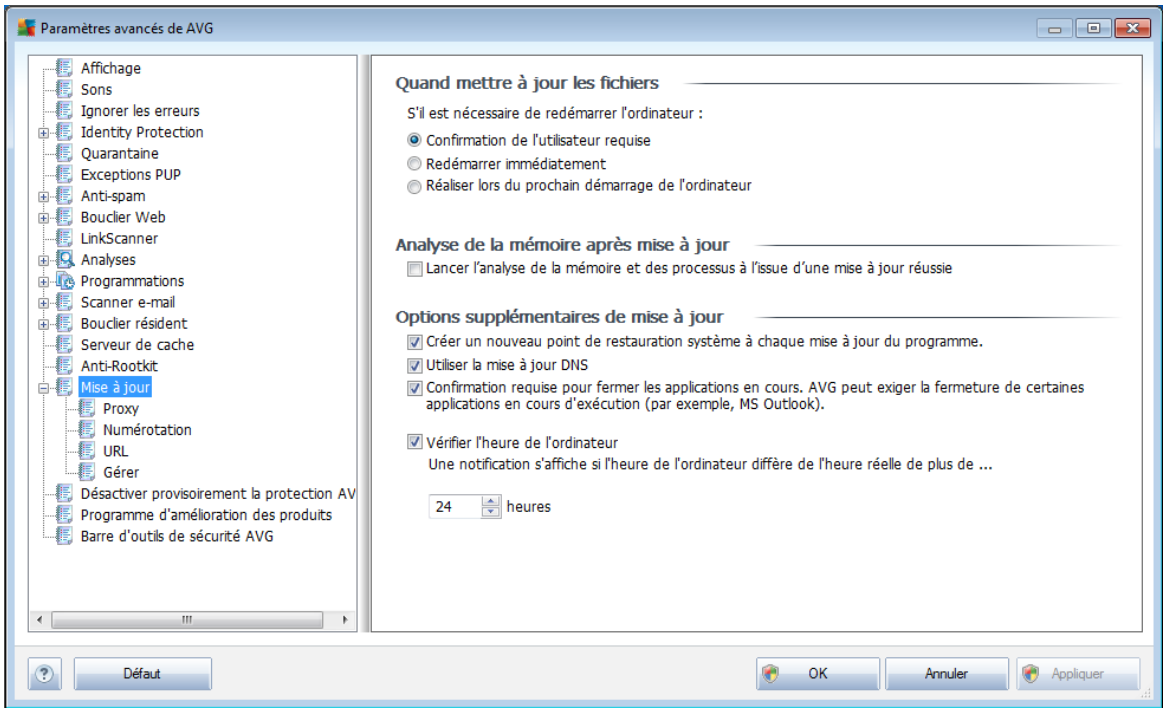
Cochez tout les cases permettant d'indiquer les objets à analyser :

- ***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 tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows*)
- ***Analyse anti-rootkit complète*** - analyse tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows généralement*), ainsi que tous les disques locaux (*y compris le disque flash, mais pas les lecteurs de disquettes ou de CD-ROM*)

9.16. 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 redémarré (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 exécuter 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

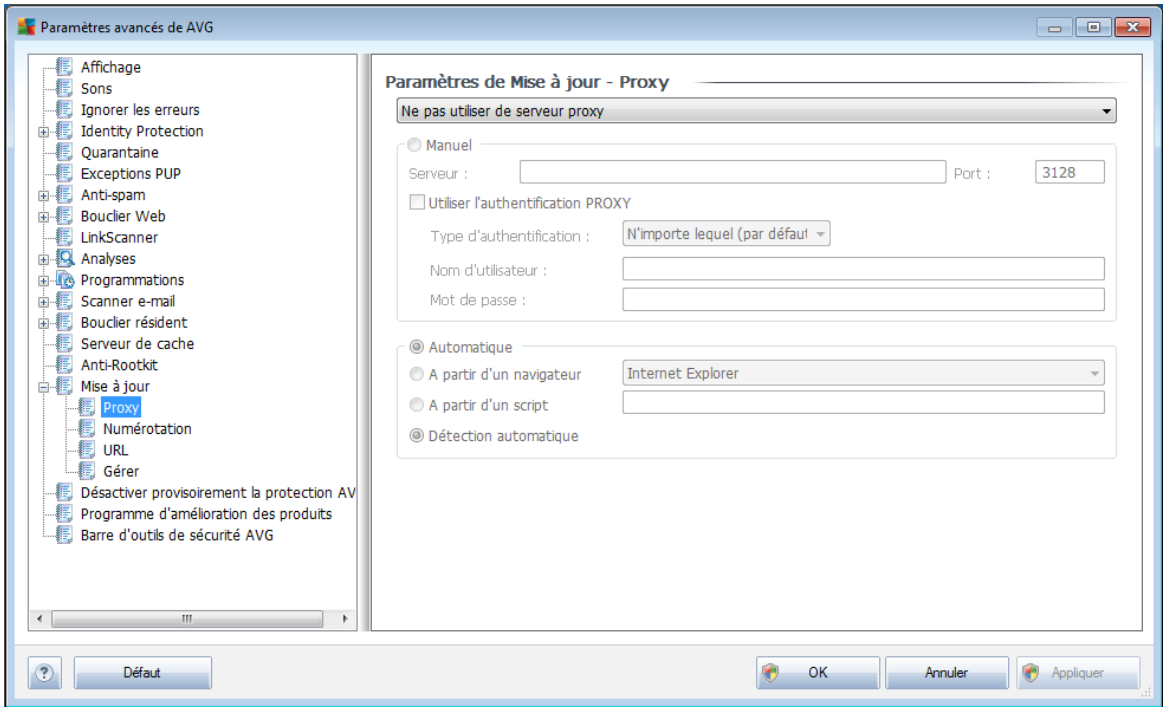
- ***Créer un nouveau point de restauration après chaque nouvelle mise à jour du programme*** : un point de restauration est créé avant le lancement d'une mise à jour du programme AVG. En cas d'échec de la mise à jour et de blocage de votre système d'exploitation, vous avez alors la possibilité de restaurer 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. Option réservée aux utilisateurs expérimentés. 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.

9.16.1. 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 choisir parmi les options suivantes :

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

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)

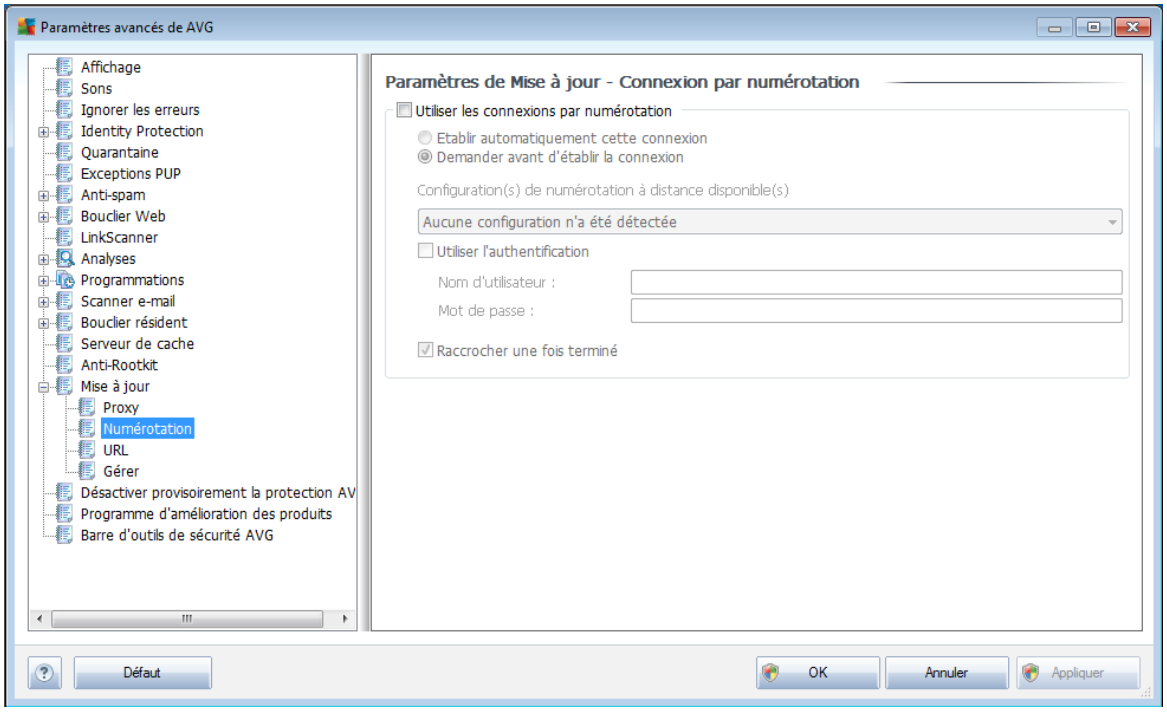
Il est aussi possible de définir des règles spécifiques à chaque utilisateur pour le serveur proxy. Si votre serveur proxy est configuré de cette manière, cochez l'option ***Utiliser l'authentification PROXY*** pour vous assurer que votre nom d'utilisateur et votre mot de passe sont valides pour établir 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 du 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 du proxy
- ***Détection automatique*** - la configuration sera détectée automatiquement à partir du serveur proxy

9.16.2. Numérotation

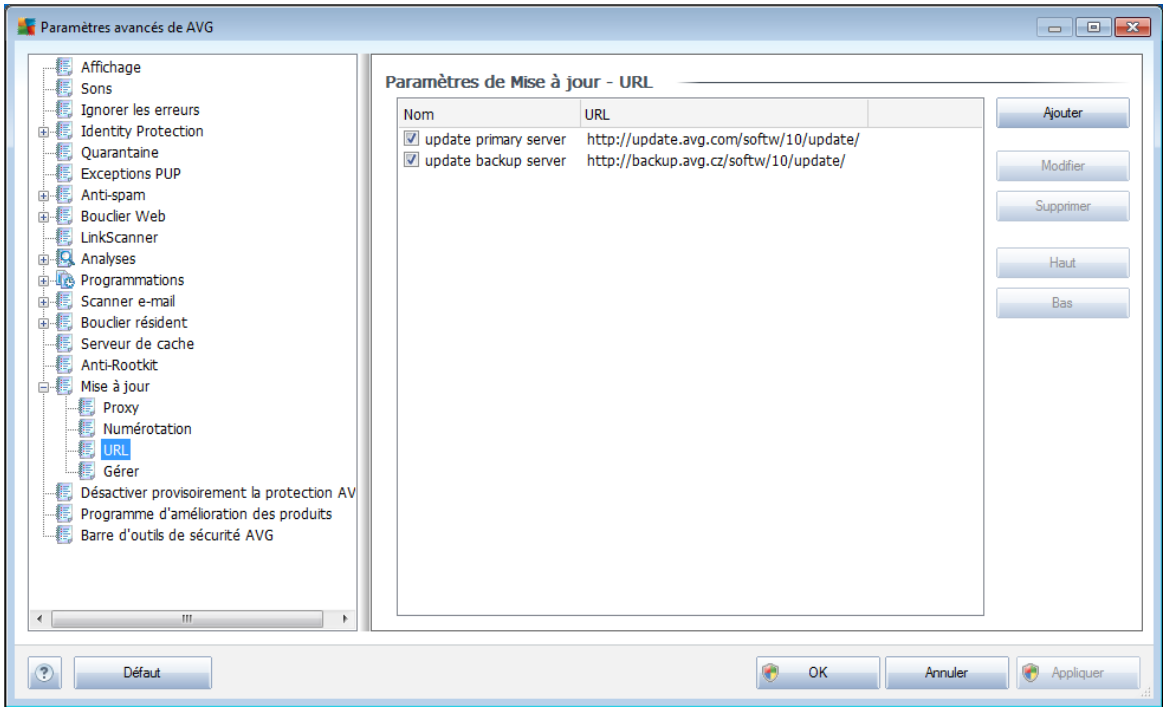


Tous les paramètres facultatifs de la boîte de dialogue ***Paramètres de mise à jour -***

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***).

9.16.3. URL

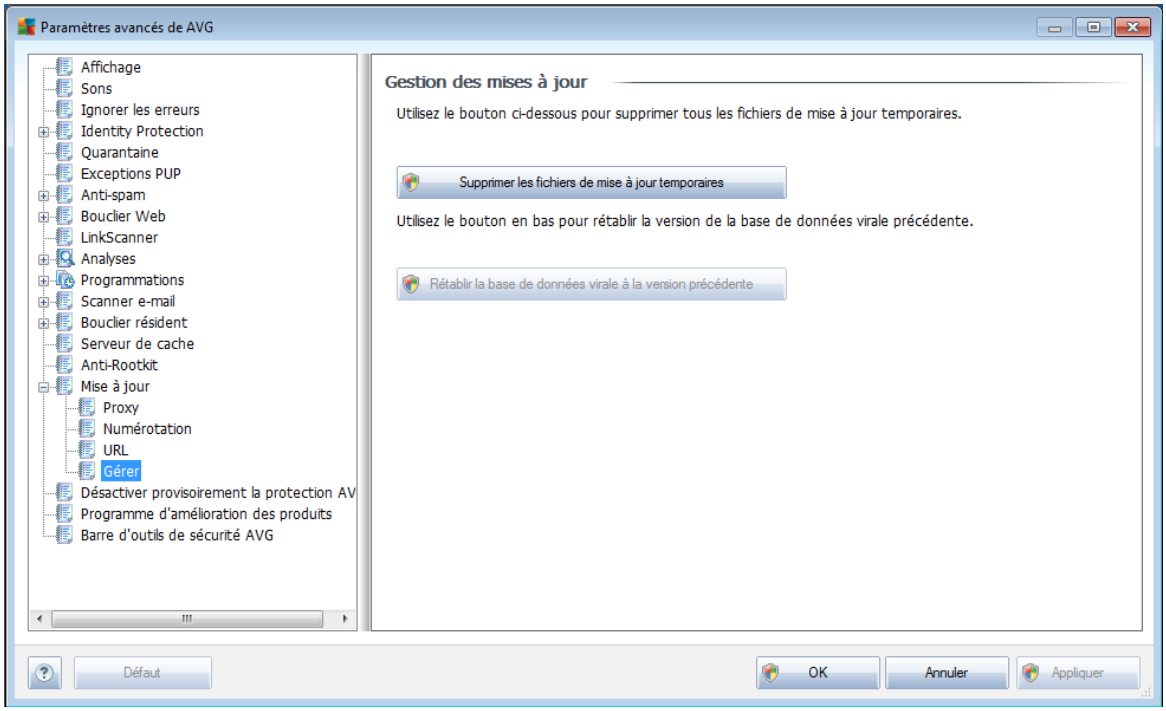


La boîte de dialogue ***URL*** contient une liste d'adresses Internet à partir desquelles il est possible de télécharger les fichiers de mise à jour. Vous pouvez redéfinir le contenu de cette liste à l'aide des boutons de fonction suivants :

- ***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

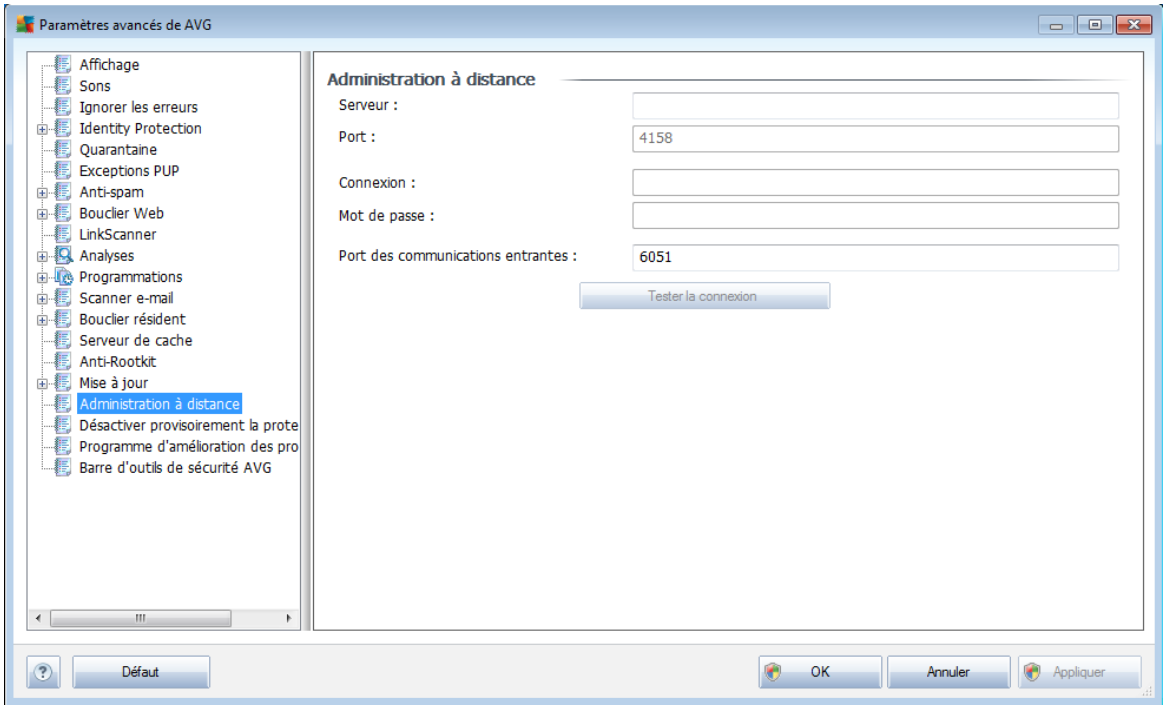
9.16.4. Gestion

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*)

9.17. 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 :

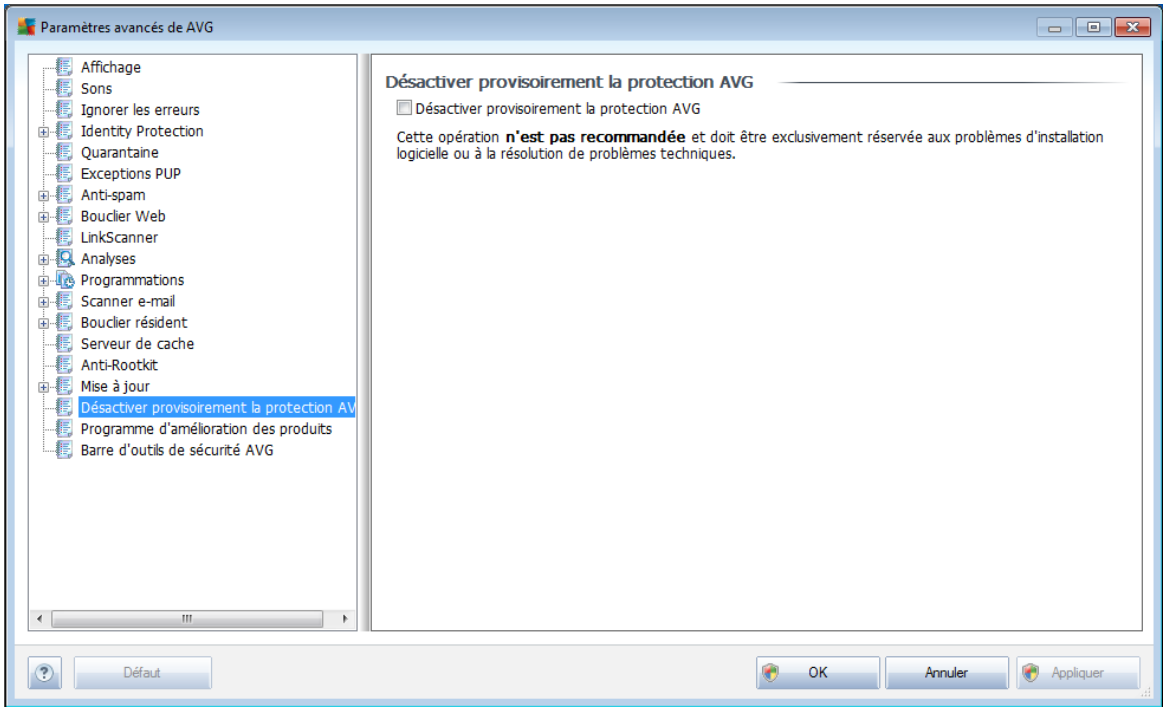
- ***Serveur*** - nom du serveur (ou adresse IP) sur lequel AVG Admin Server est installé
- ***Port*** - indiquez le numéro du port sur lequel le client AVG communique avec AVG Admin Server (*le numéro de port 4158 est utilisé par défaut - si vous voulez l'utiliser, il est inutile de le spécifier de 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,*

consultez la documentation relative à AVG SMB Edition.

9.18. Désactiver provisoirement la protection AVG



Dans la boîte de dialogue ***Désactiver provisoirement la protection AVG***, vous avez la possibilité de désactiver entièrement la protection offerte par le programme **AVG Internet Security 2011**.

Rappelez-vous que vous ne devez utiliser cette option qu'en cas d'absolue nécessité !

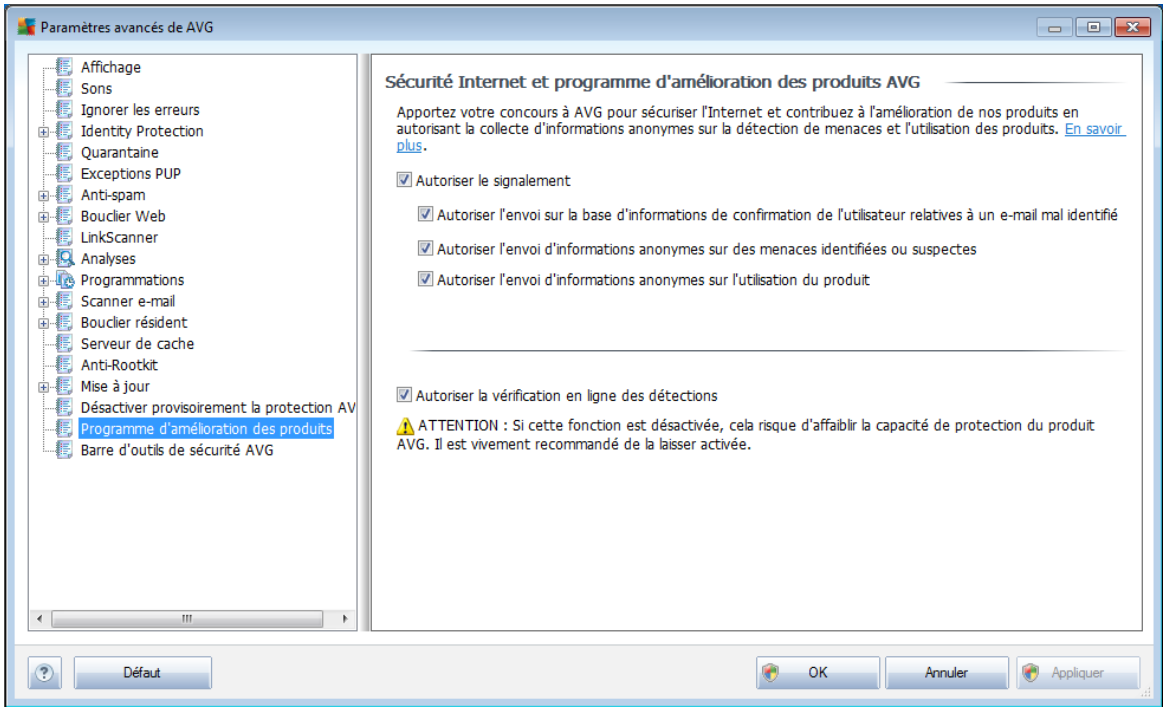
Dans la plupart des cas, il ***est déconseillé*** de désactiver AVG avant d'installer un nouveau logiciel ou pilote, même si l'assistant d'installation ou le logiciel vous suggère d'arrêter d'abord tous les programmes et applications s'exécutant sur le système afin d'empêcher les interruptions inopinées lors du processus d'installation. En cas de problème au cours de l'installation, essayez de désactiver en premier lieu le composant ***Bouclier résident***. Si vous avez momentanément désactivé la protection AVG, veillez à la réactiver dès que vous avez terminé. Si vous êtes connecté à Internet ou à un réseau alors que l'antivirus est désactivé, l'ordinateur est particulièrement vulnérable.

9.19. Programme d'amélioration des produits

La boîte de dialogue ***Sécurité Internet et programme d'amélioration des produits AVG*** vous invite à contribuer à l'amélioration des produits AVG et à une plus grande sécurité sur Internet. Cochez l'option ***Autoriser le signalement*** pour transmettre les menaces détectées à AVG. Ainsi, nous pourrons recueillir les dernières informations sur les nouvelles menaces signalées par les internautes du monde entier et, en retour,

fournir à tous une meilleure protection en ligne.

La création de rapports est assurée automatiquement. Il n'en résulte aucune gêne pour les utilisateurs. Notez par ailleurs qu'aucune donnée personnelle n'est incluse dans ces rapports. L'envoi de rapports sur les menaces détectées est facultatif, mais nous vous serions gré d'activer également cette option. Elle nous permet d'améliorer votre protection et celle des autres utilisateurs de produits AVG.



De nos jours, les simples virus représentent une infime partie des menaces. Les auteurs de codes malveillants et de sites Web piégés sont à la pointe de l'innovation et de nouveaux types de menaces ne cessent de voir le jour principalement sur Internet. Voici les plus courants :

- ***Un virus est un code malveillant qui se copie et se propage en passant souvent inaperçu jusqu'à ce qu'il ait accomplit son action.*** Certains virus constituent une menace non négligeable : ils suppriment ou modifient intentionnellement des fichiers sur leur passage. D'autres ont une action relativement moins nocive comme jouer un air de musique. Toutefois, tous les virus sont dangereux en raison de leur capacité de multiplication et de propagation, qui leur permet d'occuper intégralement l'espace mémoire d'un ordinateur en quelques instants et de provoquer une défaillance générale du système.

- ***Le ver***, une sous-catégorie de virus, se distingue des virus types en ceci qu'il n'a pas besoin d'un objet porteur et peut s'envoyer lui-même vers d'autres ordinateurs, généralement dans un mail. Il en résulte souvent une surcharge des serveurs de messagerie et des systèmes réseau.

- ***Un spyware*** se définit généralement comme une catégorie de malwares (*logiciels malveillants comportant des virus*) qui comprend des programmes (généralement des chevaux de Troie), conçus pour subtiliser des informations personnelles, des mots de passe, des numéros de carte de crédit ; ou pour infiltrer des ordinateurs et permettre aux intrus d'en prendre le contrôle à distance sans l'autorisation et à l'insu de leur propriétaire.

- Λεσ ***programmes potentiellement dangereux*** forment un catégorie de codes espions qui ne sont pas nécessairement dangereux. Un adware est un exemple spécifique de programme potentiellement dangereux. Ce logiciel est spécifiquement conçu pour diffuser des publicités, généralement dans des fenêtres contextuelles intempestives, mais non malveillantes.

- Παρ αιλλευρσ, λεσ ***tracking cookies*** peuvent être considérés comme en faisant partie car ces petits fichiers, stockés dans le navigateur Web et envoyés automatiquement au site Web "parent" lors de votre visite suivante, peuvent contenir des données comme votre historique de navigation et d'autres informations comparables.

- ***Un exploit*** est un programme malveillant qui exploite une faille du système d'exploitation, du navigateur Internet ou d'un autre programme essentiel.

- Υνε οπ∫ρατιον δε ***phishing*** consiste à tenter d'acquérir des informations confidentielles en se faisant passer pour une société connue et fiable. En règle générale, les victimes potentielles sont harcelées par des messages leur demandant de mettre à jour leurs coordonnées bancaires. Pour ce faire, elles sont invitées à suivre un lien qui les mène jusqu'à un site bancaire fictif.

- ***Le canular (hoax) est un mail envoyé en masse contenant des informations dangereuses, alarmistes ou simplement dénuées d'intérêt.*** La plupart de ces menaces utilisent des mails de type canular pour se propager.

- Λεσ ***sites Web malveillants*** opèrent en installant des programmes malveillants sur votre ordinateur. Les sites piratés font de même, à ceci près que ce sont des sites Web légitimes qui ont été contaminés par des visiteurs.

Pour vous protéger de tous ces différents types de menaces, AVG vous propose les composants spécialisés suivants :

- ***Anti-Virus*** pour protéger votre ordinateur des virus,

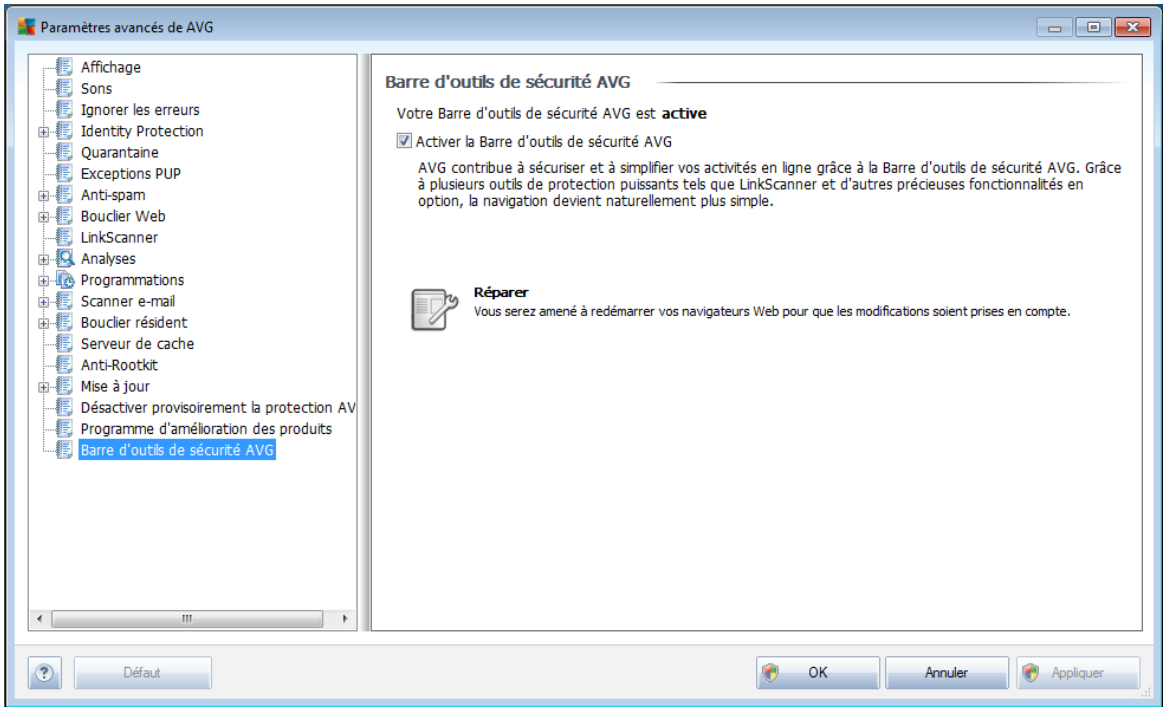
- ***Anti-Spyware*** pour protéger votre ordinateur des spywares,

- ***Bouclier Web*** pour protéger votre ordinateur des virus et des spywares durant la navigation sur Internet,

- ***LinkScanner*** pour protéger l'ordinateur contres les autres menaces en ligne mentionnées dans cette rubrique.

9.20. Barre d'outils de sécurité AVG

La ***Barre d'outils de sécurité AVG*** est un nouvel outil qui fonctionne en association avec le composant ***LinkScanner***. La ***barre d'outils de sécurité AVG*** permet également de contrôler les fonctions du composant ***LinkScanner*** et de corriger le comportement de ce dernier. Si vous installez cette barre d'outils lors de l'installation du produit **AVG Internet Security 2011**, elle est automatiquement ajoutée à votre navigateur Web (*Internet Explorer 6.0 ou version supérieure et Mozilla Firefox 3.0 ou version supérieure*). Les autres navigateurs Internet ne sont pas encore pris en charge.



Au sein de la boîte de dialogue ***Barre d'outils de sécurité AVG***, vous pouvez activer ou désactiver intégralement le composant ***Barre d'outils de sécurité AVG*** dans les paramètres avancés de l'application au moyen de l'option ***Activer la Barre d'outils de sécurité AVG***.

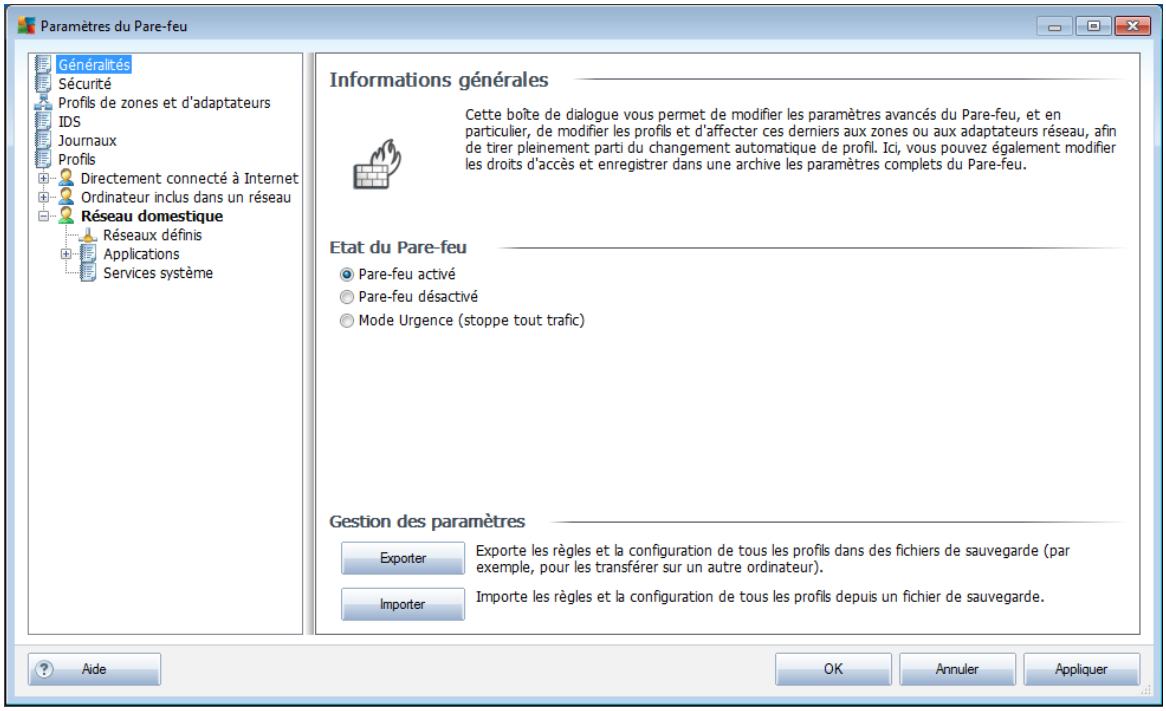
Le bouton ***Réparer*** active totalement tous les éléments de la ***barre d'outils*** (*en rétablissant les paramètres par défaut*) et s'assure que celle-ci*** fonctionne parfaitement dans tous les navigateurs Internet pris en charge. Si vous avez précédemment désactivé la ***barre d'outils de sécurité AVG***, à partir de cette boîte de dialogue ou directement à partir de votre navigateur Internet, cliquez sur ce bouton pour activer le composant.

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

La boîte de dialogue ***Informations générales*** comprend deux sections :



Etat du Pare-feu

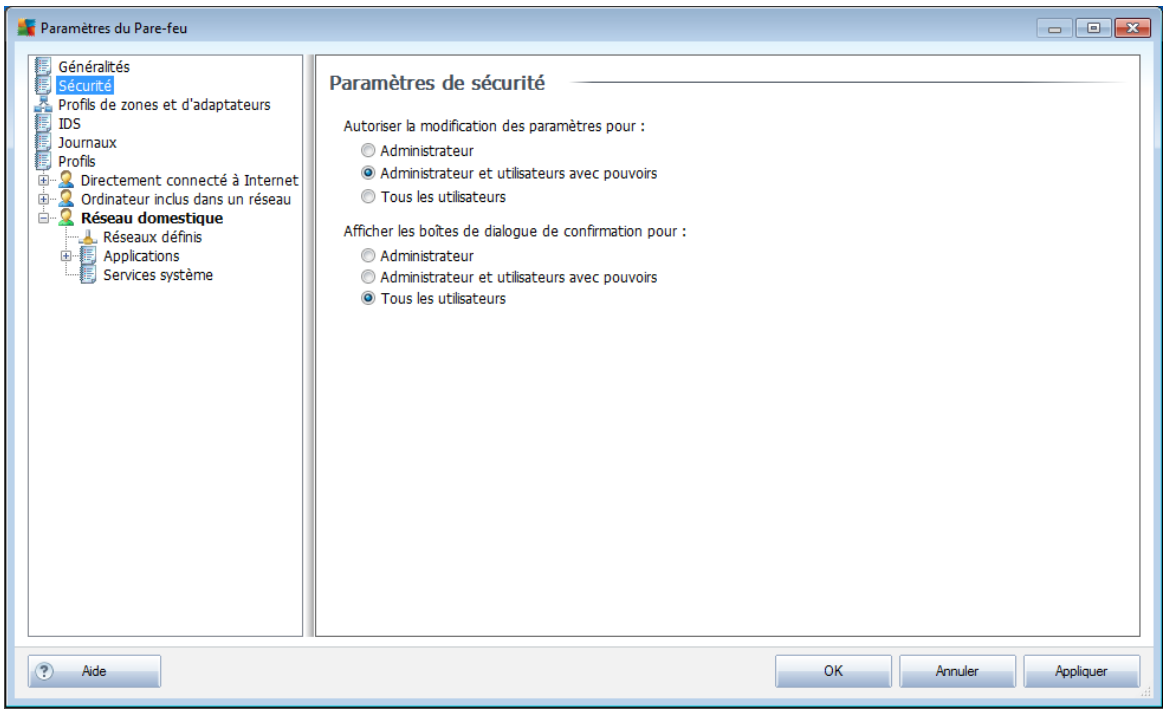
Dans cette section, vous pouvez modifier l'état du ***Pare-feu*** à votre gré :

- ***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

Gestion des paramètres

Dans la section ***Gestion des paramètres***, 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

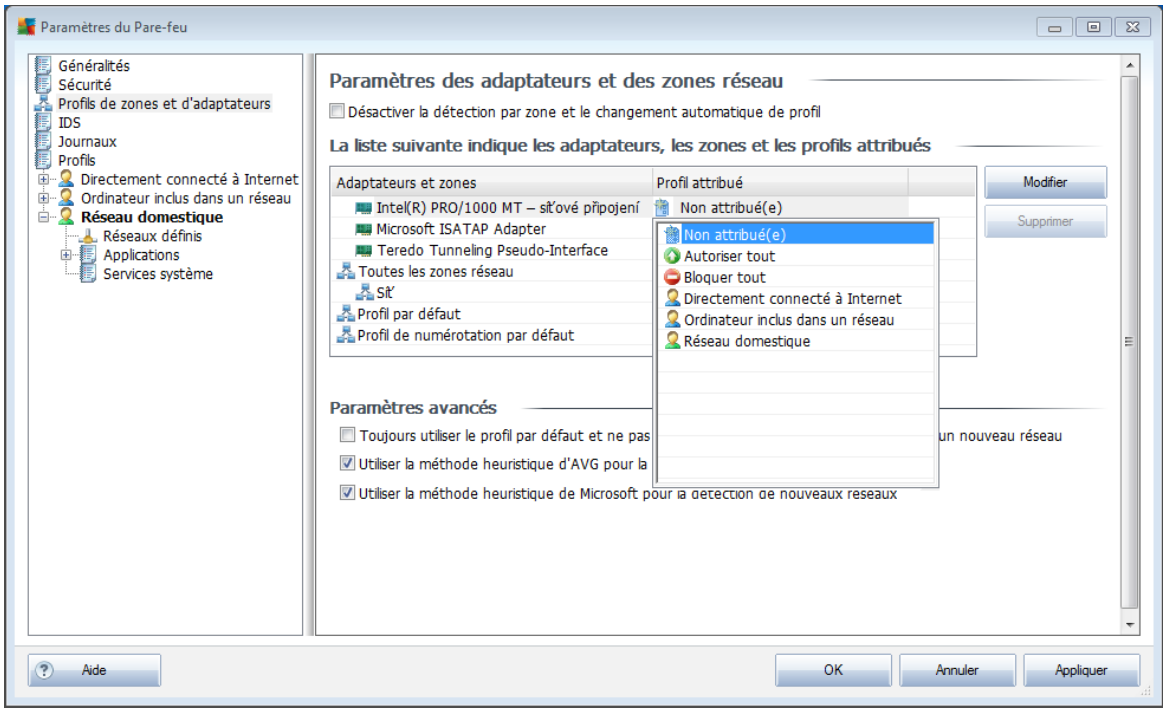
définis.

- ***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 voulez pas définir de profils, le profil courant sera utilisé. 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

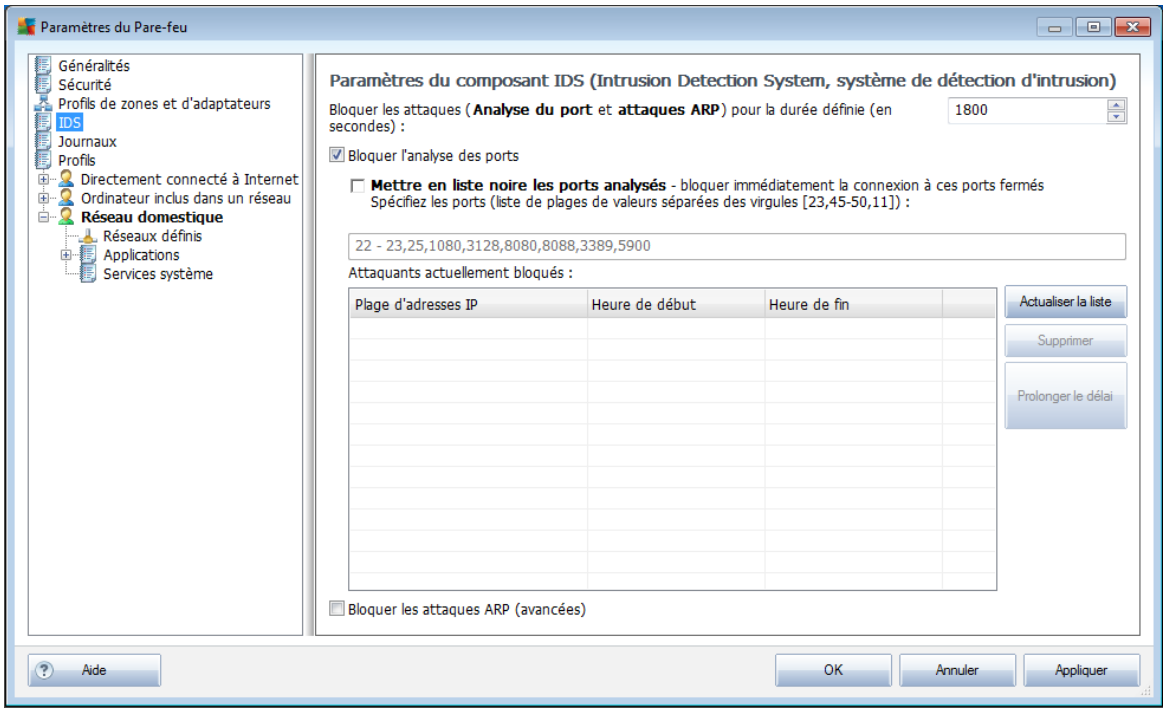
- ***Toujours utiliser le profil par défaut et ne pas afficher la boîte de dialogue de détection d'un nouveau réseau*** : quand l'ordinateur se connecte à un nouveau réseau, le ***pare-feu*** le signale et affiche une boîte de dialogue dans laquelle vous pouvez définir un type de connexion réseau et lui affecter un .***Profil de pare-feu***. Si vous ne souhaitez pas voir cette boîte de dialogue s'afficher, cochez cette case.

- Utiliser la méthode heuristique d'AVG pour la détection de nouveaux réseaux : permet de collecter des informations sur un réseau récemment détecté grâce à son propre mécanisme.

- ***Utiliser la méthode heuristique de Microsoft pour la détection de nouveaux réseaux*** : permet de récupérer des informations sur un réseau récemment détecté par le service Windows (*cette option est disponible pour Windows Vista ou versions ultérieures*).

10.4. IDS

Le composant ***Intrusion Detection System*** (système de détection d'intrusion) est une fonctionnalité d'analyse des comportements spécialement conçue pour identifier et bloquer les tentatives de communication suspectes sur des ports spécifiques de votre ordinateur. Vous pouvez configurer les paramètres d'IDS dans l'interface suivante :



La boîte de dialogue ***Paramètres du composant IDS (Intrusion Detection System,***

système de détection d'intrusion) présente les options de configuration suivantes :

- Λεοπτιον ***Bloquer les attaques pour la durée définie*** - permet de définir le temps (en secondes) durant lequel un port doit être bloqué, chaque fois qu'une tentative de communication suspecte y est détectée. Par défaut, ce laps de temps est fixé à 1 800 secondes (*30 minutes*).

- ***Bloquer l'analyse des ports*** – cochez cette case pour bloquer les tentatives de communication entrante sur tous les ports TCP et UDP. Pour ce type de connexion, cinq tentatives sont autorisées, et la sixième est bloquée.

    - ***Mettre en liste noire les ports analysés*** – cochez cette case pour bloquer immédiatement toute tentative de communication sur les ports indiqués dans la zone de texte ci-dessous. Les ports individuels ou les plages de ports doivent être séparés par des virgules. Une liste prédéfinie de ports recommandés est disponible, si vous souhaitez utiliser cette fonctionnalité.

    - ***La section attaquants actuellement bloquées*** - cette section répertorie les tentatives communication bloquées par le ***Pare-feu***. L'historique complet des tentatives bloquées peut être consulté dans la boîte de dialogue ***Journaux***, onglet *Journaux d'analyse des ports*).

- ***Bloquer les attaques ARP*** permet d'activer le blocage de certains types de tentatives de communication au sein d'un réseau local, signalées par le composant ***IDS*** comme étant potentiellement dangereuses. Le délai fixé dans la zone ***Bloquer les attaques pour la durée définie prend alors effet.*** Nous recommandons l'utilisation de cette fonctionnalité uniquement aux utilisateurs expérimentés, maîtrisant le type et le niveau de risque de leur réseau local.

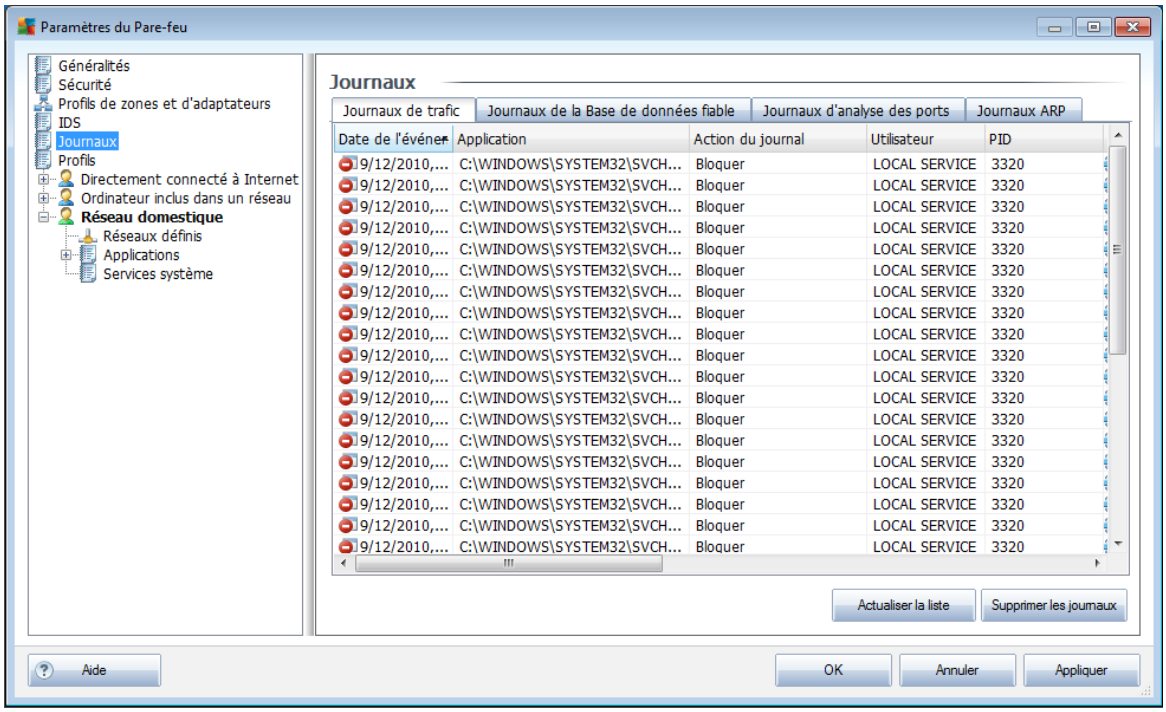
Boutons de commande

- ***Actualiser la liste*** - cliquez sur le bouton pour mettre à jour la liste (*pour inclure toute tentative bloquée récemment*)

- ***Supprimer*** - cliquez sur ce bouton pour annuler le blocage sélectionné

- ***Prolonger le délai*** - cette option permet de prolonger la période pendant laquelle une tentative donnée est bloquée. Une nouvelle boîte de dialogue avec des options supplémentaires s'ouvre afin de vous permettre de définir une heure et une date spécifiques ou une durée illimitée.

10.5. 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.*) sur quatre 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, lorsque 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.
- ***Journaux d'analyse des ports*** - fournit de toutes les activités ***Intrusion Detection System*** .

- ***Journaux ARP*** - enregistrement d'informations relatives au blocage de certains types de tentatives de communication au sein d'un réseau local (option *Bloquer les attaques ARP*) détectées par le système ***Intrusion Detection System*** comme présentant un risque potentiel.

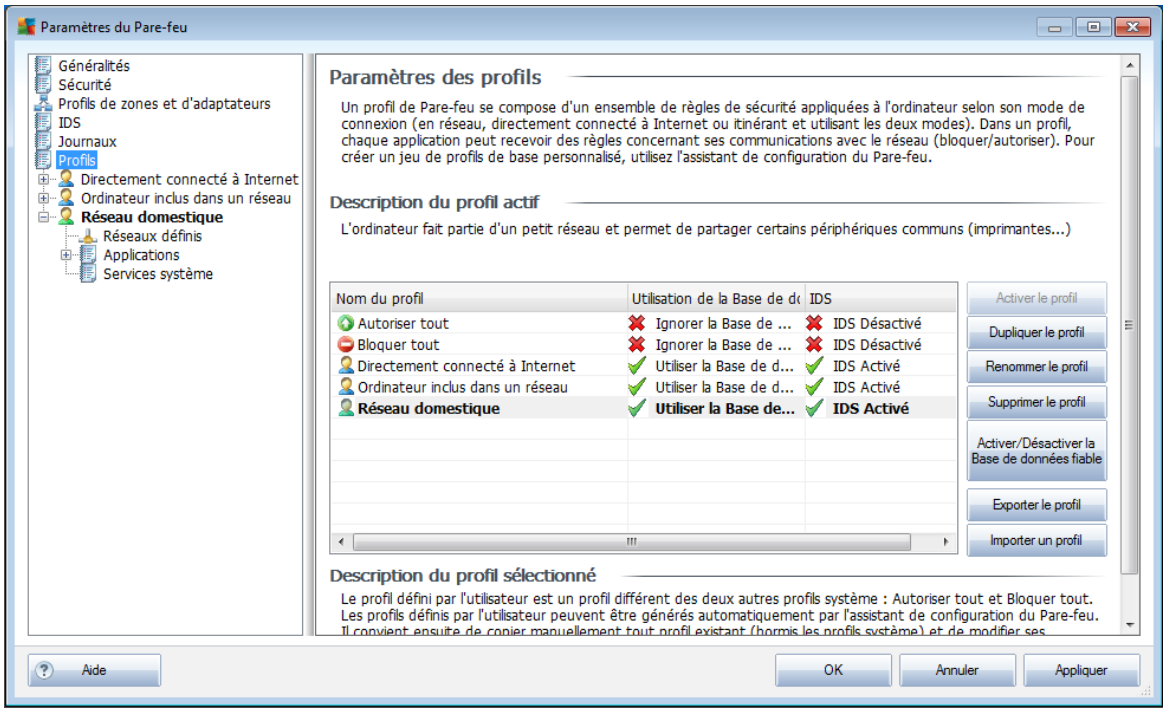
Boutons de commande

- ***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 supprimer toutes les entrées du tableau.

10.6. Profils

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



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

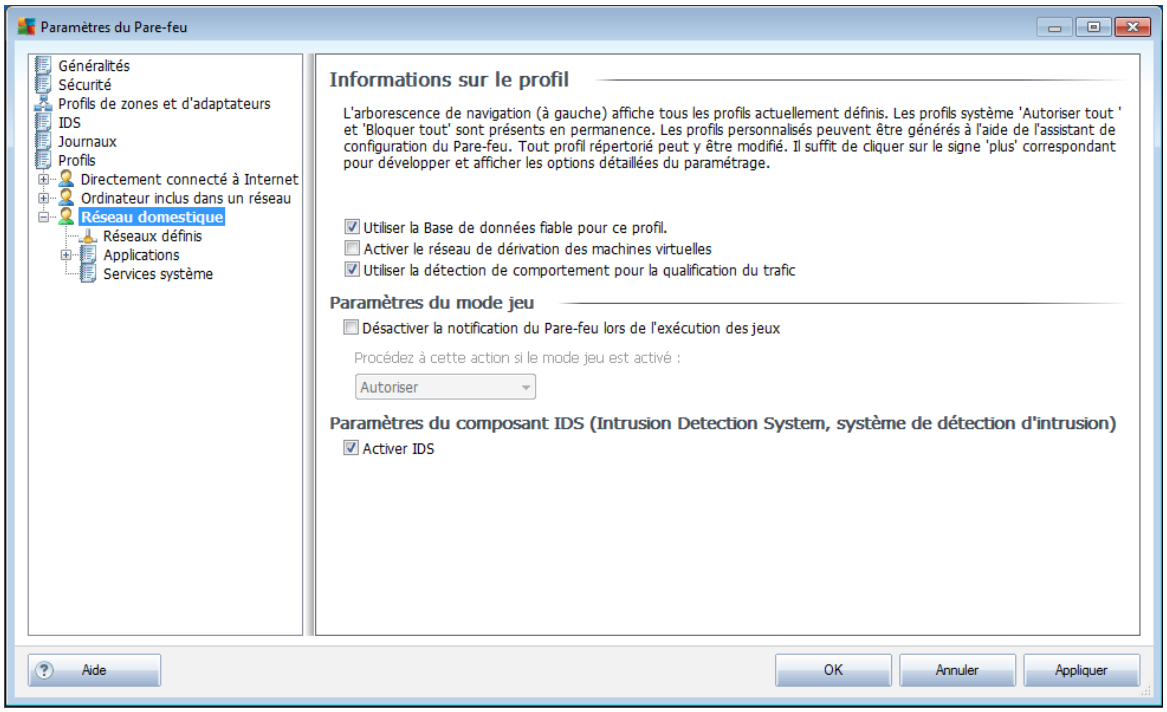
- ***Activer le profil*** - ce bouton définit le profil sélectionné comme étant actif. La configuration de ce profil sera alors utilisée par le ***Pare-feu*** pour contrôler le trafic réseau

- ***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

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*) :

10.6.1. 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 pour ce profil*** - (*option activée par défaut*) cochez cette option pour activer la *base de données fiable* (*, c'est-à-dire la base de données interne de collecte d'informations AVG relatives aux applications fiables et certifiées communiquant 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 des machines virtuelles*** - (*paramètre désactivé par défaut*), cochez cette case pour permettre aux machines virtuelles VMware de se connecter directement au 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 ***Identity Protection*** lors de l'évaluation d'une application. ***Identity Protection*** signale si l'application se comporte de manière suspecte ou si elle est fiable et peut être autorisée dans le cadre des communications 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 mode plein écran (*généralement des jeux, mais aussi toute autre application exécutée en plein écran comme les présentations PowerPoint*). Cependant, ces messages d'informations peuvent interférer avec l'application en cours.

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.

En mode jeu, toutes les tâches programmées (*analyses, mises à jour*) sont reportées jusqu'à la fermeture de l'application.

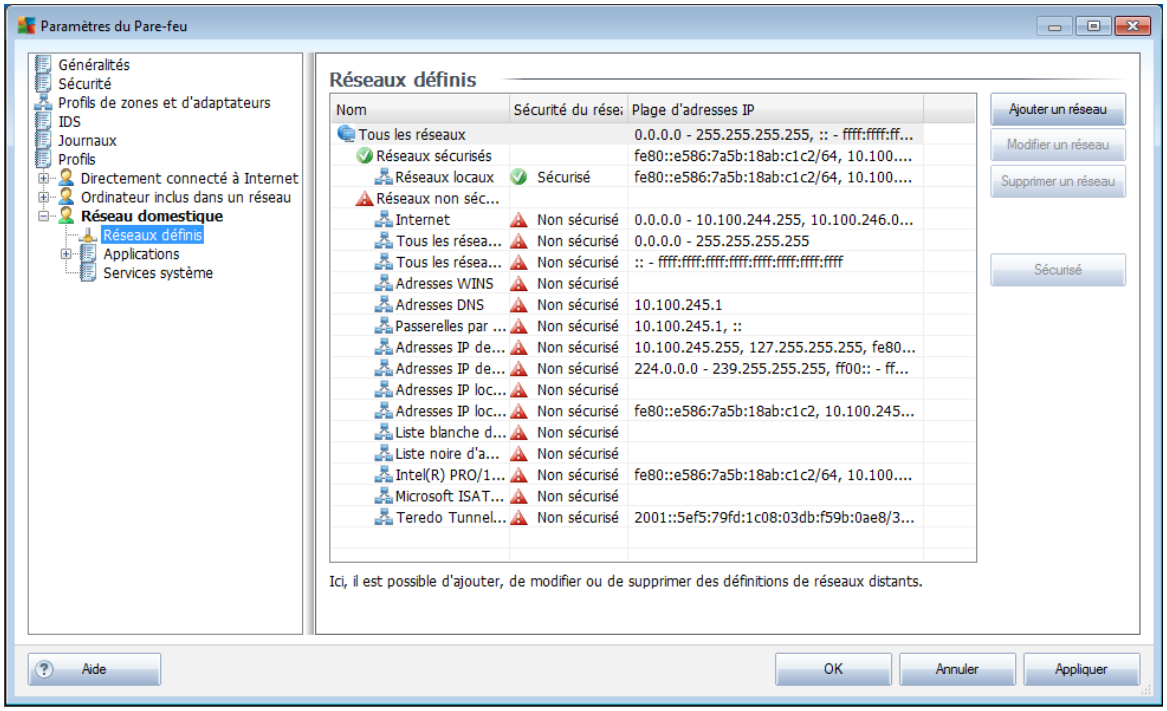
Paramètres du composant IDS (Intrusion Detection System, système de détection d'intrusion)

Cochez la case ***Activer IDS*** pour activer une fonction d'analyse comportementale spécialisée conçue pour identifier et bloquer toute communication suspecte sur

certains ports de l'ordinateur (*pour en savoir plus à ce sujet, consultez le chapitre consacré au système de détection d'intrusion de cette documentation*).

10.6.2. Réseaux définis

La boîte de dialogue ***Réseaux définis*** dresse la liste de tous les réseaux auxquels est relié l'ordinateur.

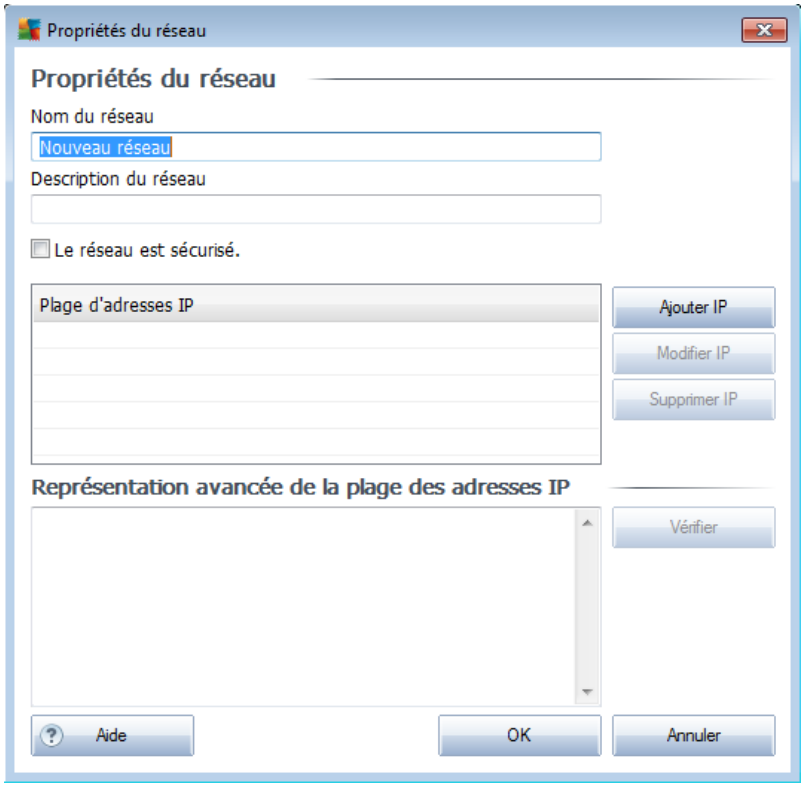


Les informations suivantes sont fournies pour chaque réseau détecté :

- ***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.

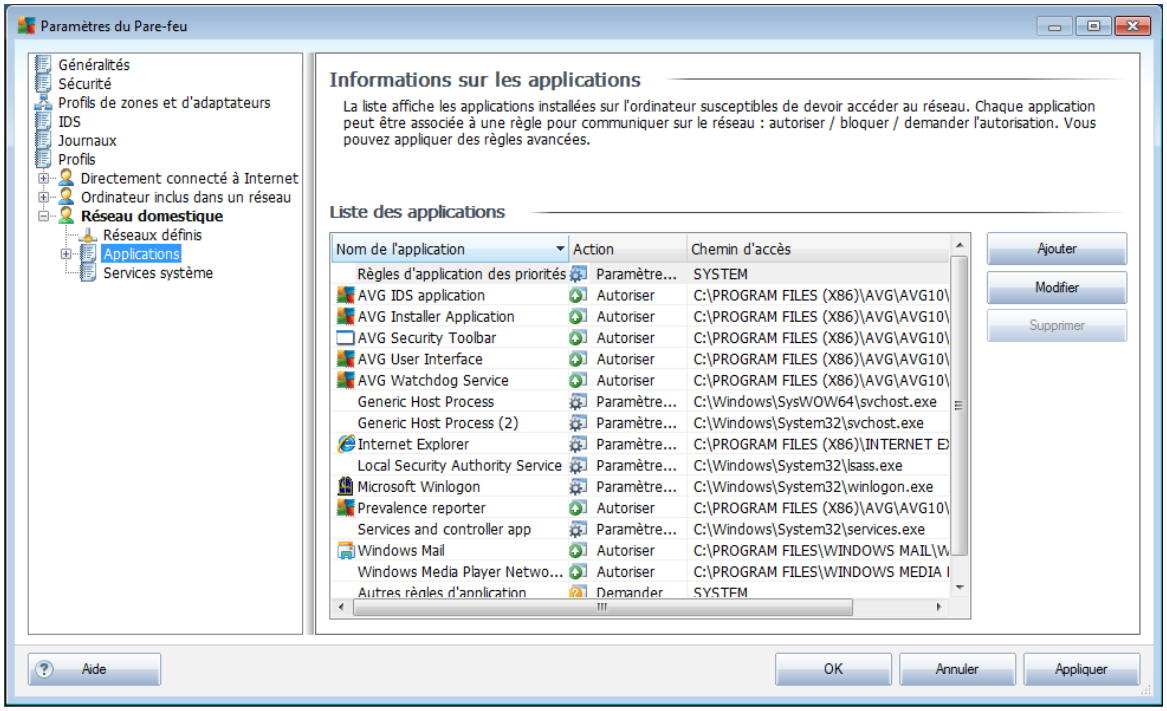
- ***Modifier un réseau*** - ouvre la boîte de dialogue ***Propriétés du réseau*** (*voir ci-dessus*) dans laquelle vous pouvez modifier les paramètres d'un réseau déjà défini (*la boîte de dialogue est identique à la boîte de dialogue d'insertion d'un nouveau réseau, décrite au paragraphe précédent*)

- ***Supprimer un réseau*** - ce bouton retire la référence du réseau sélectionné de la liste des réseaux

- ***Le réseau est sécurisé*** - par défaut, tous les réseaux sont considérés comme non sécurisés. Déclarez un réseau comme sécurisé seulement si vous êtes

certain qu'il est fiable (*et inversement, si le réseau est jugé sécurisé, le bouton qui s'affiche est Marqué comme non sécurisé*).

10.6.3. Applications



La boîte de dialogue d'information ***Applications***indique toutes les applications installées qui pourraient être amenées à communiquer sur le réseau et les icônes affectées à l'action assignée :

- - Autoriser les communications pour tous les réseaux
- - Autoriser les communications uniquement pour les réseaux définis comme Sécurisé
- - Bloquer les communications
- - Afficher la boîte de dialogue appelant une décision de l'utilisateur (*l'utilisateur devra décider s'il autorise ou bloque la communication lorsque l'application tente de se connecter au réseau*)
- - Définition des paramètres avancés

Les applications figurant dans la liste sont celles qui ont été détectées sur l'ordinateur (*et leurs actions respectives*).

Remarque : notez que seules les applications déjà installées ont pu être détectées. Par conséquent, si vous installez une nouvelle application après la recherche, vous aurez à définir des règles de pare-feu associées. Par défaut,

lorsque la nouvelle application tente de se connecter sur le réseau pour la première fois, le pare-feu crée automatiquement une règle en fonction de la base de données fiable ou vous invite à autoriser ou à bloquer les communications. Dans ce dernier cas, vous pouvez configurer votre réponse comme règle permanente (qui sera alors répertoriée dans cette boîte de dialogue).

Pour toute nouvelle application, vous pouvez aussi définir une règle immédiatement dans cette boîte de dialogue : cliquez simplement sur ***Ajouter*** et fournissez les détails nécessaires sur l'application.

Outre les applications, la liste contient aussi deux fonctions particulières :

- ***Règles d'application des priorités*** (*en haut de la liste*) sont des règles préférentielles, qui sont toujours appliquées avant toute autre règle de n'importe quelle application.
- ***Autres règles d'applications*** (*au bas de la liste*) sont utilisées en dernière instance lorsque aucune règle d'application spécifique ne s'applique (par exemple, pour une application inconnue et non définie).

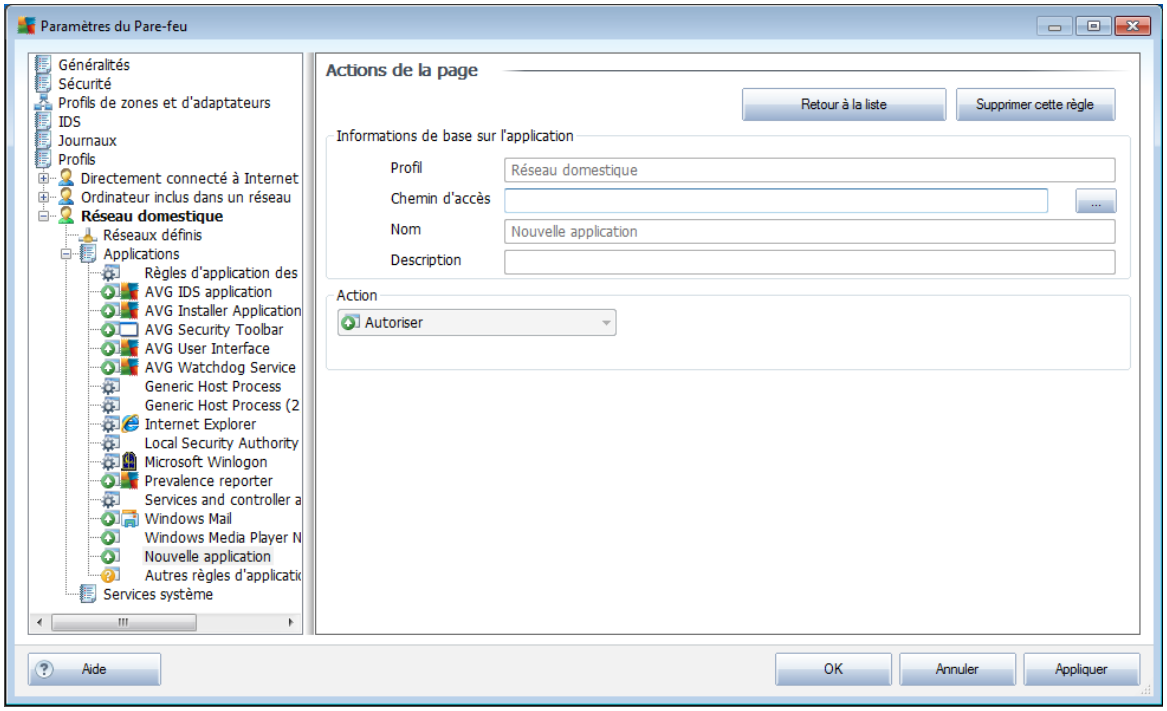
Ces fonctions ont des options de paramétrage différentes de celles des applications courantes et ne s'adressent qu'à des utilisateurs expérimentés. Nous vous conseillons vivement de ne modifier ces paramètres !

Boutons de commande

La liste peut être modifiée à l'aide des boutons suivants :

- ***Ajouter*** - ouvre une boîte de dialogue ***Actions de la page*** vide visant à définir de nouvelles règles d'application
- ***Modifier*** - ouvre la même boîte de dialogue ***Actions de la page*** renseignée selon les données fournies lors de la modification d'un ensemble de règles d'une application
- ***Supprimer*** - retire l'application sélectionnée de la liste

Cette boîte de dialogue vous permet de définir précisément les paramètres des applications:



Actions de la page

- Λε βουτον ***Retour à la liste*** affiche la présentation de l'ensemble des règles d'application définies.
- Λε βουτον ***Supprimer cette règle*** efface la règle d'application actuellement affichée. Notez que cette action ne peut pas être annulée !

Informations de base sur l'application

Dans cette section, vous devez indiquer le ***nom*** de l'application et donner éventuellement une ***description*** *(commentaire bref pour votre usage personnel*). Dans le champ ***Chemin***, entrez le chemin d'accès complet à l'application (*le fichier exécutable*) sur le disque. Vous pouvez aussi identifier l'application facilement dans l'arborescence en cliquant sur le bouton "***...***".

Action sur l'application

***Dans le menu déroulant, sélectionnez la règle de pare-feu de l'application, c'est-à-dire précisez l'action qu'effectue le pare-feu lorsque l'application tente de se

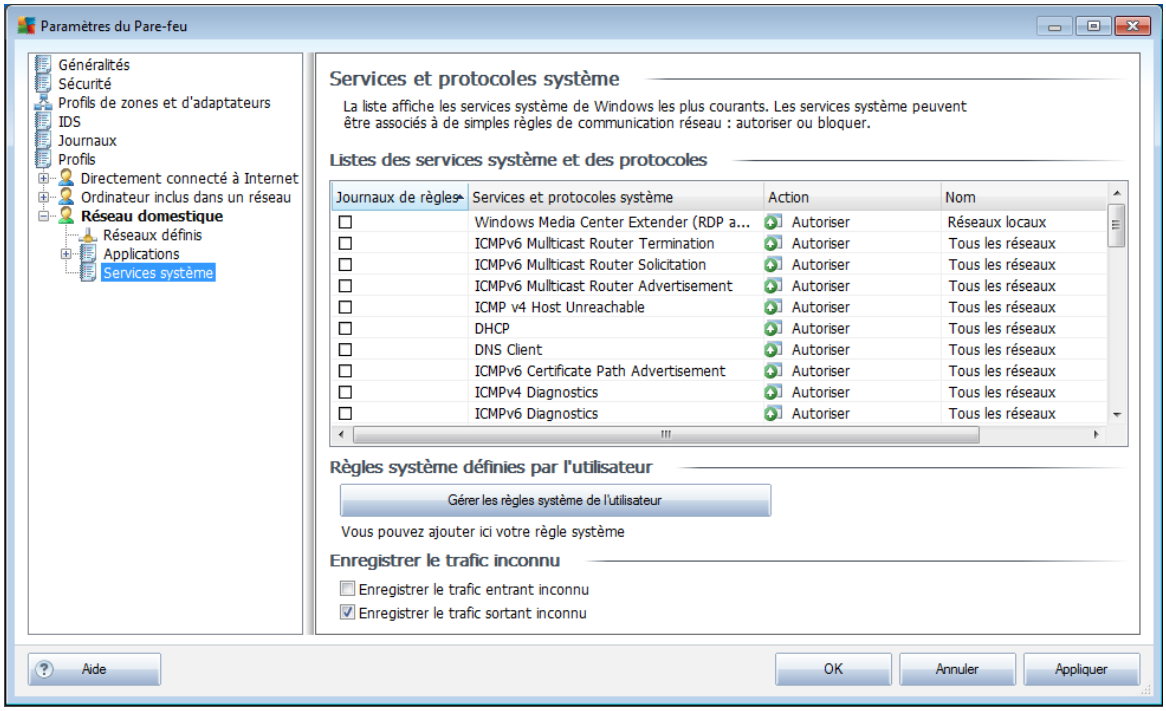
connecter au réseau). ***

- - ***Autoriser tout*** permet à l'application de communiquer sur tous les réseaux définis et avec les adaptateurs sans limitations.
- - ***Autoriser la connexion sécurisée*** permet à l'application de communiquer uniquement sur les réseaux définis comme fiables (sécurisés).
- - ***Bloquer*** interdit automatiquement la communication : l'application n'est autorisée à se connecter à aucun réseau.
- - ***Demander*** ouvre une boîte de dialogue où vous pouvez choisir de bloquer ou d'autoriser la tentative de communication en cours.
- - ***Paramètres avancés*** affiche des options de configuration supplémentaires dans la partie inférieure de la boîte de dialogue dans la section ***Règles détaillées de l'application***. Les règles détaillées sont appliquées en fonction de leur rang dans la liste. Le classement se modifie à l'aide des fonctions ***Haut*** et ***Bas.*** Après avoir cliqué sur une règle donnée de la liste, la présentation de ses détails s'affichent dans la partie inférieure de la boîte de dialogue. Il est possible de modifier une valeur soulignée de couleur bleue en cliquant dans la boîte de dialogue correspondante. Pour supprimer la règle en surbrillance, cliquez simplement sur ***Supprimer***. Pour définir une nouvelle règle, utilisez le bouton ***Ajouter*** pour ouvrir la boîte de dialogue de ***modification des détails de la règle*** qui permet de spécifier tous les détails nécessaires.

10.6.4. Services système

Seuls les utilisateurs expérimentés devraient apporter des modifications dans la boîte de dialogue Services et protocoles système !

La boîte de dialogue ***Services et protocoles système*** répertorie tous les services système et les protocoles standard qui pourraient être amenés à communiquer sur le réseau.



Listes des services système et des protocoles

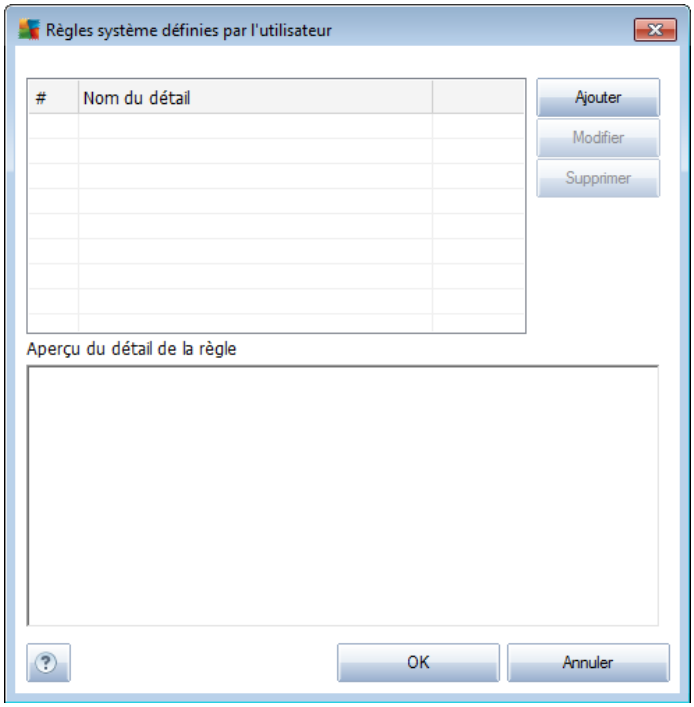
Le tableau comporte les colonnes suivantes :

- ***Journaux de règles*** - cette case permet d'activer l'enregistrement de l'application de chaque règle dans les journaux.
- ***Services et protocoles système*** - cette colonne affiche le nom du service système correspondant.
- ***Action*** - cette colonne affiche une icône pour l'action associée :
  - Autoriser les communications pour tous les réseaux
  - Autoriser les communications uniquement pour les réseaux définis comme Sécurisé
  - Bloquer les communications
- ***Réseaux*** - cette colonne indique le réseau spécifique auquel la règle s'applique.

Pour modifier les paramètres d'un élément figurant dans la liste (*y compris les actions assignées*), cliquez avec le bouton droit de la souris sur l'élément, puis sélectionnez ***Modifier***.***Toutefois, la modification d'une règle système ne doit être effectuée que par des utilisateurs expérimentés. Il est fortement recommandé de ne pas modifier la règle système.***

Règles système définies par l'utilisateur

Pour ouvrir une nouvelle boîte de dialogue permettant de définir votre propre règle du service système (*voir illustration ci-dessous*), cliquez sur le bouton ***Gérer les règles système de l'utilisateur***. La partie supérieure de la boîte de dialogue ***Règles système définies par l'utilisateur*** présente tous les détails de la règle système actuellement modifiée, la partie inférieure porte sur le détail sélectionné. Les règles système définies par l'utilisateur peuvent être modifiées, ajoutées ou supprimées à l'aide du bouton prévu à cet effet. En revanche, seule la modification est autorisée pour les détails des règles définies par l'éditeur:



Attention : *notez que ces paramètres avancés s'adressent essentiellement aux administrateurs réseau qui maîtrisent parfaitement le processus de configuration du Pare-feu. Si vous ne connaissez pas les types de protocoles de communication, les numéros de port réseau, les définitions d'adresse IP, etc., ne modifiez pas ces paramètres. S'il est nécessaire de modifier la configuration, consultez l'aide pour obtenir des informations détaillées.*

Enregistrer le trafic inconnu

- ***Enregistrer le trafic entrant inconnu*** *(option désactivée par défaut)* – cochez cette case pour consigner dans les journaux chaque tentative de connexion à votre ordinateur provenant d'un élément extérieur inconnu.

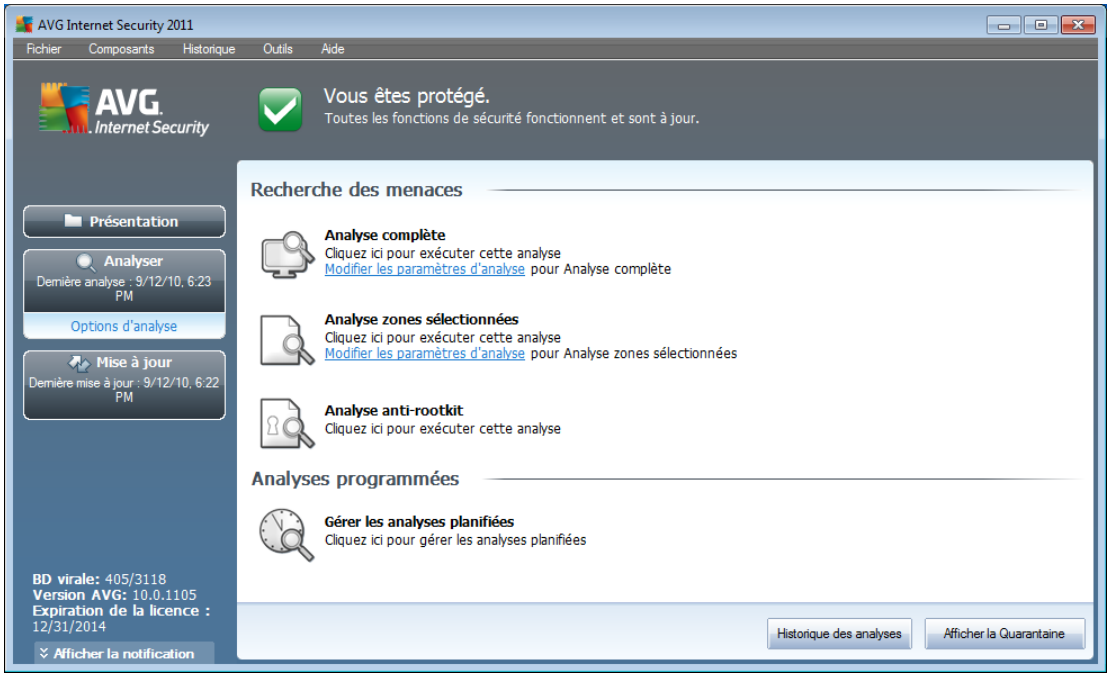
- ***Enregistrer le trafic entrant inconnu*** *(option désactivée par défaut)* – cochez cette case pour consigner dans les journaux chaque tentative de

connexion à votre ordinateur provenant d'un élément extérieur inconnu.

11. Analyse AVG

L'analyse est au cœur de la fonctionnalité du programme **AVG Internet Security 2011** . 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 via ***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 des analyses*** 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

Parmi les principales fonctions d'**AVG Internet Security 2011**, citons 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.

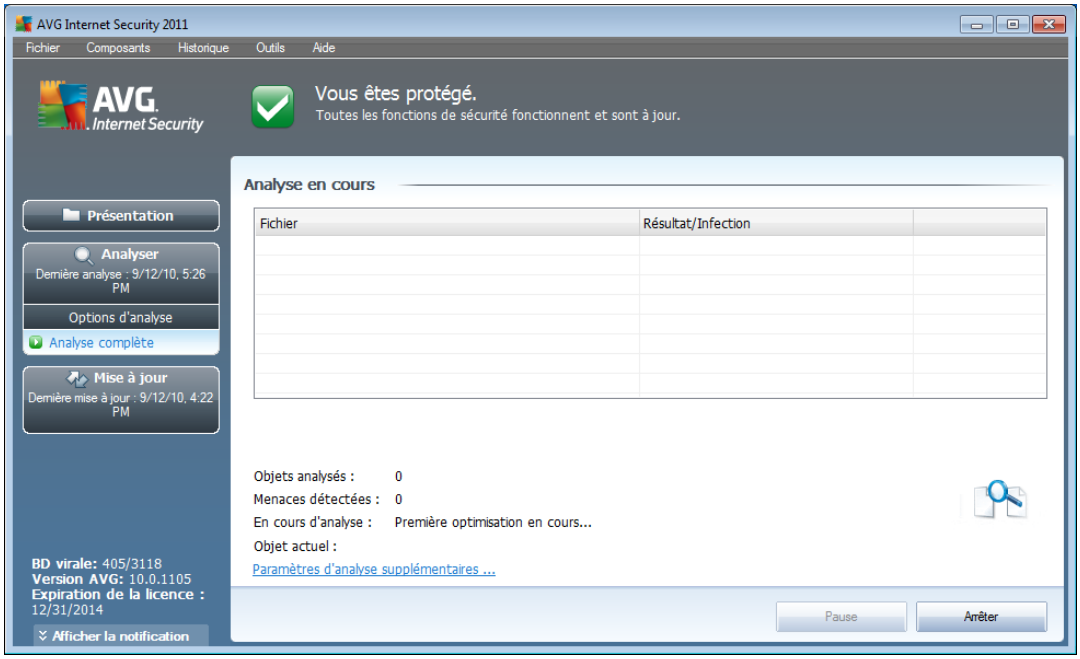
Dans **AVG Internet Security 2011**, vous trouverez les types d'analyses prédéfinies par l'éditeur du logiciel :

11.2.1. Analyse complète

L'***analyse complète*** vérifie 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 confinant dans la zone de ***quarantaine***. L'analyse de l'ordinateur doit être exécutée sur un poste de travail au moins une fois par semaine.

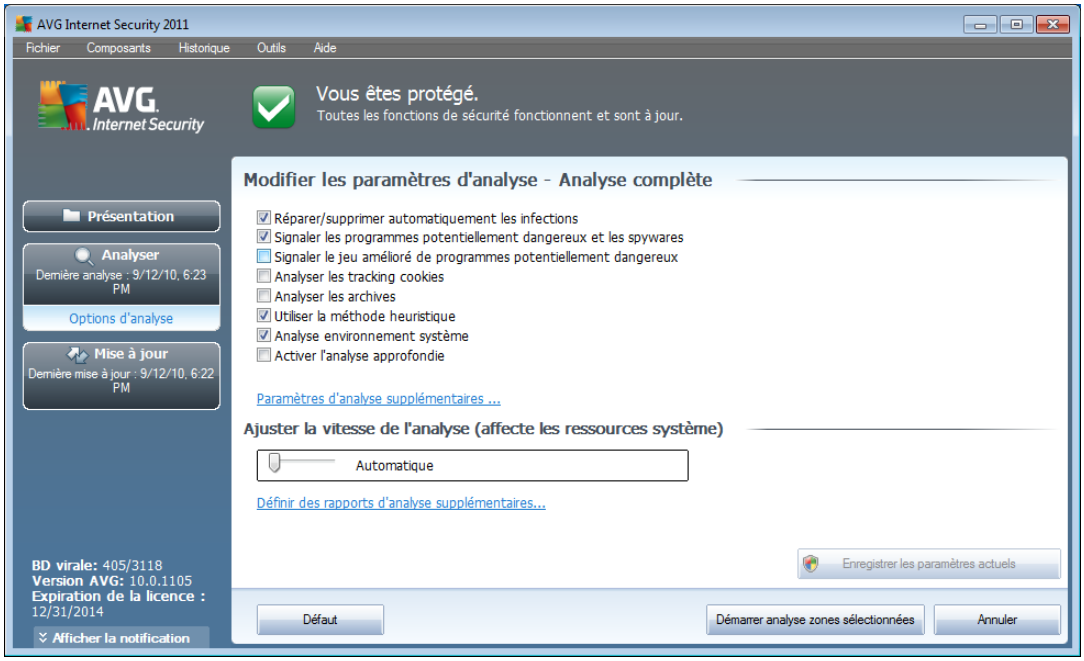
Lancement de l'analyse

L'***analyse complète***peut être lancée directement de 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

Vous avez la possibilité d'ajuster les paramètres prédéfinis par défaut de l'option ***Analyse complète***. Cliquez sur le lien ***Modifier les paramètres d'analyse*** pour ouvrir la boîte de dialogue ***Modifier les paramètres d'analyse de l'analyse complète*** *(accessible par l'interface d'analyse en activant le lien Modifier les paramètres d'analyse du module 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 :

    - ***Réparer/supprimer automatiquement les infections*** (*option activée par défaut*) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement dans la mesure du possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en ***quarantaine***.

    - ***Signaler les programmes potentiellement dangereux et les spywares*** (*option activée par défaut*) : cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

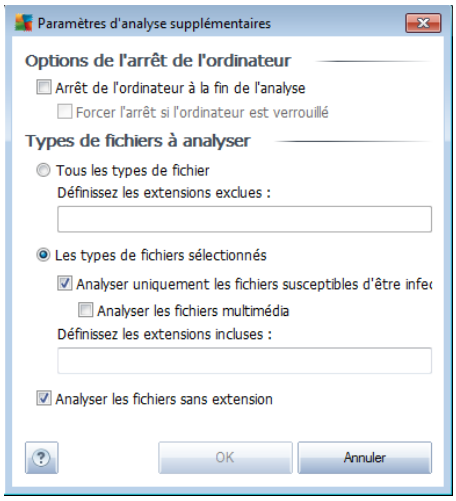
    - ***Signaler le jeu amélioré de programmes potentiellement dangereux*** - *(option désactivée par défaut*) : permet de détecter le jeu étendu des spywares qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

    - ***Analyser les tracking cookies*** (*option désactivée 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 leur panier d'achat électronique).

- ***Analyser les archives*** (*option désactivée par défaut*) : ce paramètre indique que l'analyse examine 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.
- ***Analyse environnement système*** (*option activée par défaut*) : l'analyse vérifie les fichiers système de l'ordinateur.
- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*suspicion d'une infection de l'ordinateur*), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

- ***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. Si l'option ***Arrêt de l'ordinateur à la fin de l'analyse*** est activée, l'option ***Forcer l'arrêt si l'ordinateur est verrouillé*** devient disponible et 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

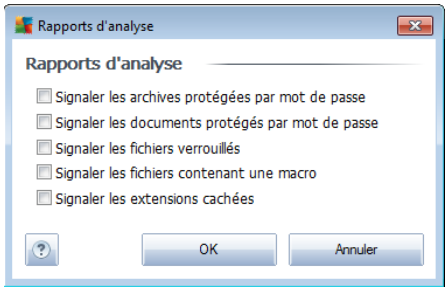
exclure de l'analyse en répertoriant les extensions de fichiers (séparées par des virgules) à ne pas analyser ; ou les;

- ***Les types de fichiers 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 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 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*** - 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.

- ***Ajuster la vitesse de l'analyse*** - le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, elle est fixée au niveau moyen qui optimise 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 lorsque vous quittez temporairement votre poste de travail*).

- ***Définir des rapports d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Rapports d'analyse***, dans laquelle 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* ***Analyse AVG / 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

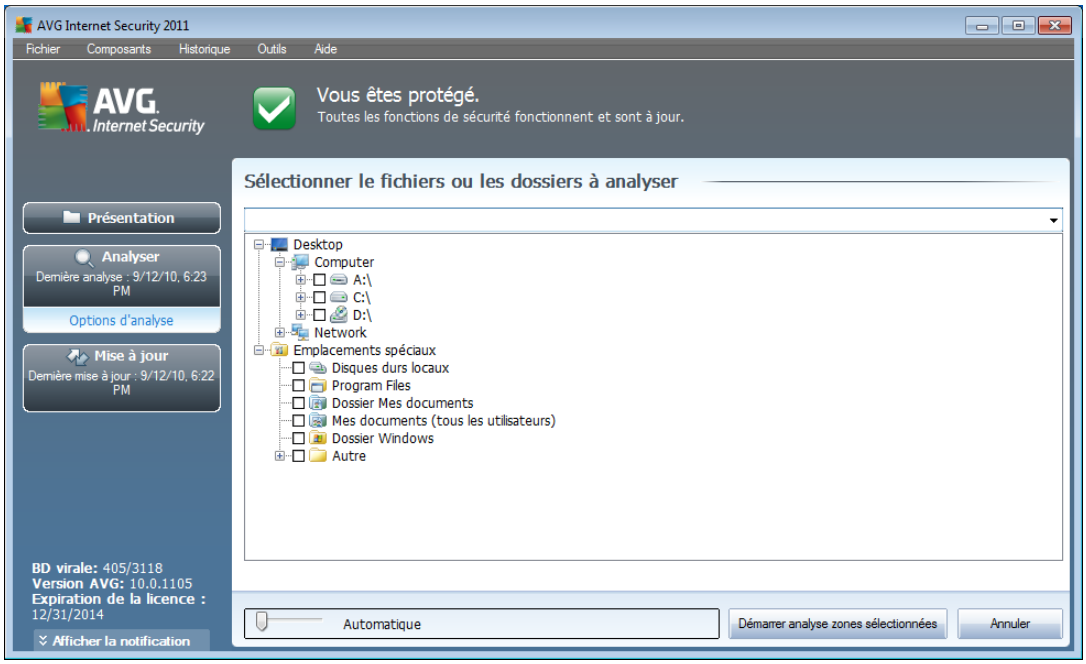
Analyse zones sélectionnées - analyse seulement les zones de l'ordinateur que vous avez sélectionnées en vue d'une analyse (*dossiers, disque durs, disquettes, CD, etc.)*). Le déroulement de l'analyse en cas de détection virale, ainsi que la solution appliquée, est le même que pour une analyse complète 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 correspondante. 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.

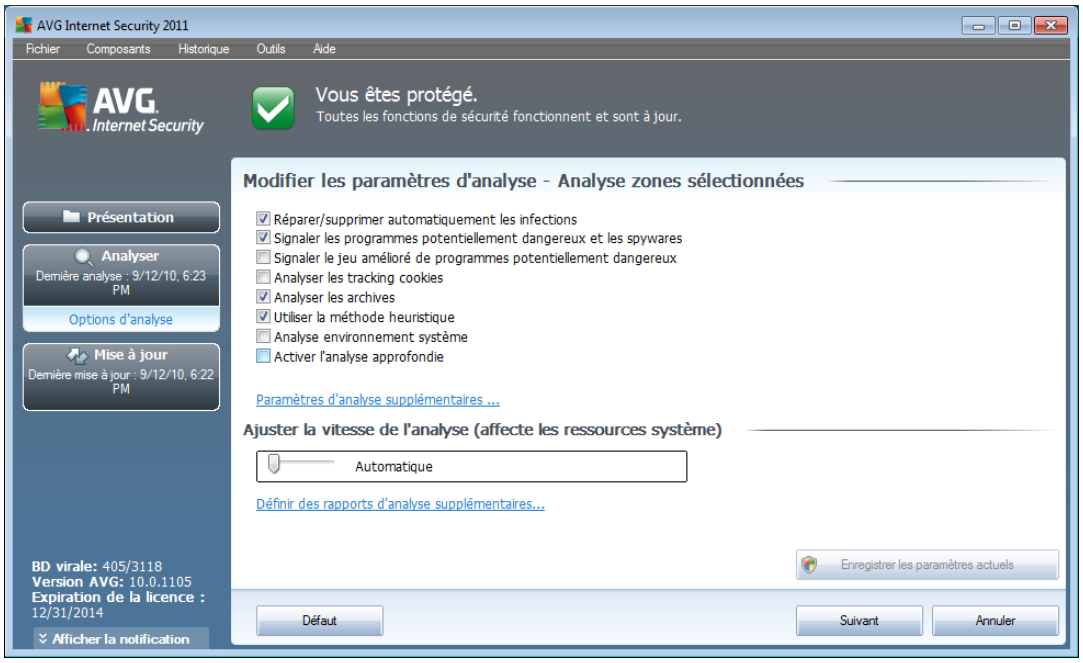
Il est aussi possible d'analyser un dossier spécifique et d'exclure tous ses sous-dossiers du processus. Pour ce faire, il suffit d'insérer le signe moins "**-**" avant le chemin d'accès généré automatiquement (*voir la capture d'écran*). Pour exclure un dossier complet de l'analyse, utilisez le paramètre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

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



Modification de la configuration de l'analyse

Vous pouvez modifier les paramètres prédéfinis par défaut de l'option ***Analyser des fichiers ou des dossiers spécifiques***. Activez le lien ***Modifier les paramètres d'analyse*** pour accéder à la boîte de dialogue ***Modifier les paramètres d'analyse - Analyse de fichiers ou dossiers spécifiques***. ***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 :

    - ***Réparer/supprimer automatiquement les infections*** (*option activée par défaut*) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement dans la mesure du possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en ***quarantaine***.

    - ***Signaler les programmes potentiellement dangereux et les spywares*** (*option activée par défaut*) : cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

    - ***Signaler le jeu amélioré de programmes potentiellement dangereux*** - *(option désactivée par défaut)* : permet de détecter le jeu étendu des spywares qui ne posent aucun problème et sont sans danger dès lors

qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

- ***Analyser les tracking cookies*** (*option désactivée 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 leur panier d'achat électronique*).

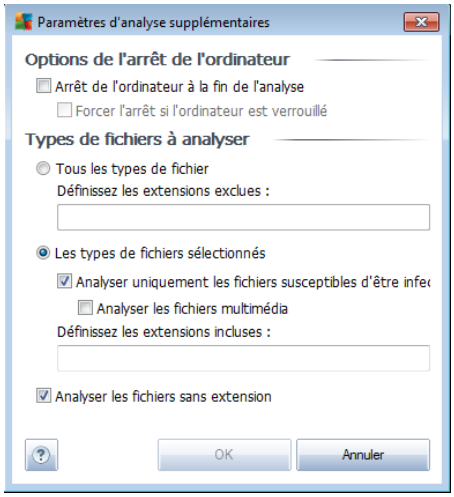
- ***Analyser les archives*** (*option désactivée par défaut*) : ce paramètre indique que l'analyse examine tous les fichiers même ceux stockés dans des d'archives (archives ZIP, RAR, par exemple).

- ***Utiliser la méthode heuristique*** (*option désactivée 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.

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

- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*suspicion d'une infection de l'ordinateur*), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même, s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

- ***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. Si l'option ***Arrêt de l'ordinateur à la fin de l'analyse*** est activée, l'option ***Forcer l'arrêt si l'ordinateur est verrouillé*** devient disponible et permet d'arrêter l'ordinateur même s'il est verrouillé.

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

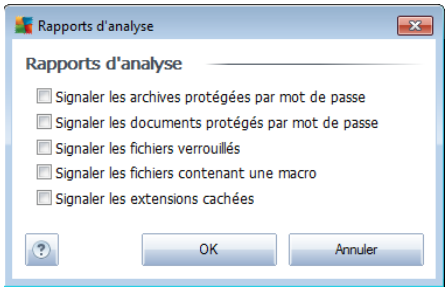
  - ***Tous les types de fichier*** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers (séparées par des virgules) à ne pas analyser ; ou les

  - ***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'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 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 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*** - 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 lorsque 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 :



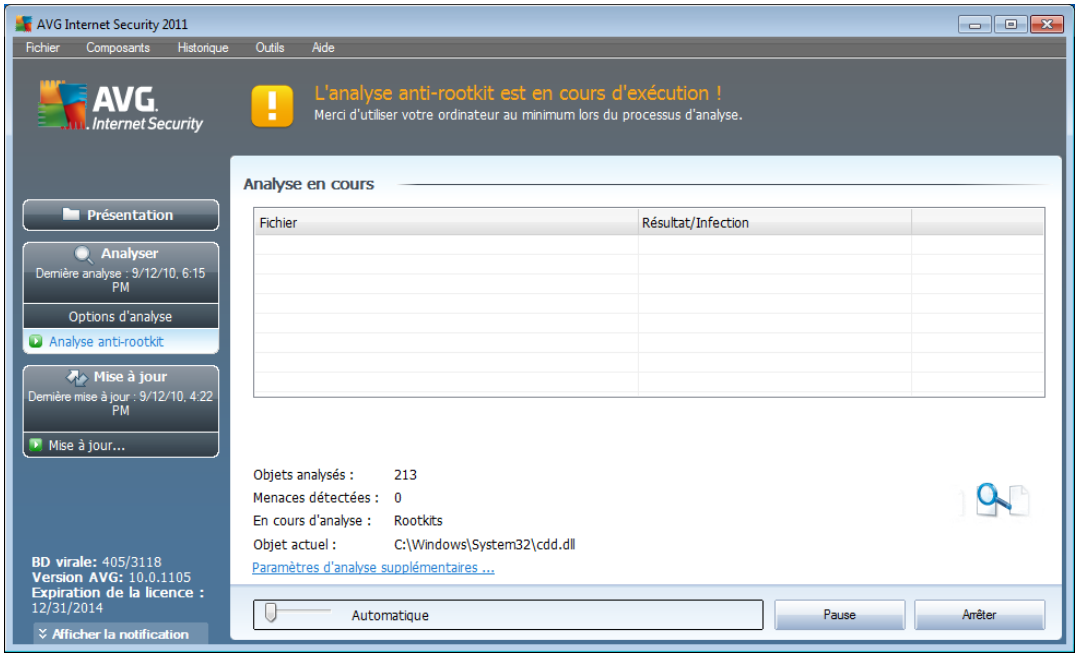
Avertissement : *ces paramètres d'analyse sont identiques à ceux d'une nouvelle analyse, comme indiqué dans le chapitre* ***Analyse AVG / Programmation de l'analyse / Comment faire l'analyse****. Si vous décidez de modifier la configuration* ***Analyse zones sélectionnées*** *par défaut, vous pouvez 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 fichiers ou dossiers spécifiques).*

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 exécutée 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.

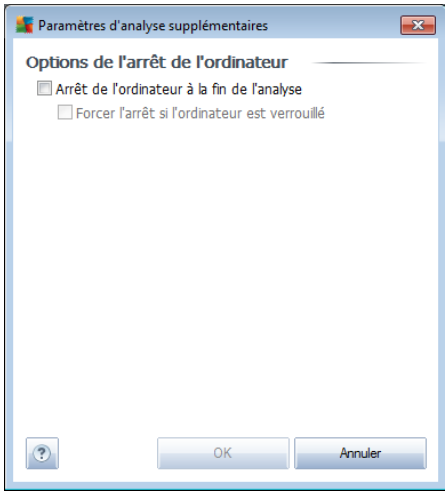


Modification de la configuration de l'analyse

L'analyse anti-rootkit est toujours exécutée 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, la configuration suivante est disponible, mais uniquement lorsqu'une analyse est en cours :

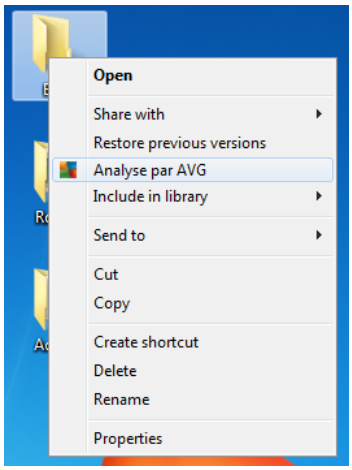
- ***Analyse automatique*** - le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, le niveau de priorité attribué est moyen (*Analyse automatique*), qui applique le meilleur compromis entre le processus d'analyse et l'utilisation des ressources système. Vous pouvez aussi 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 lorsque 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 exécutées sur l'ensemble ou des zones sélectionnées de l'ordinateur, **AVG Internet Security 2011** offre la possibilité d'examiner 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 Internet Security 2011**, 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 en 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 un point-virgule, par exemple : ***avgscanx /scan=C:\;D:***

Paramètres d'analyse

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 démarrez l'ordinateur en mode sans échec, 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 n'est accessible qu'en mode sans échec, 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 de l'ordinateur
- ***/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

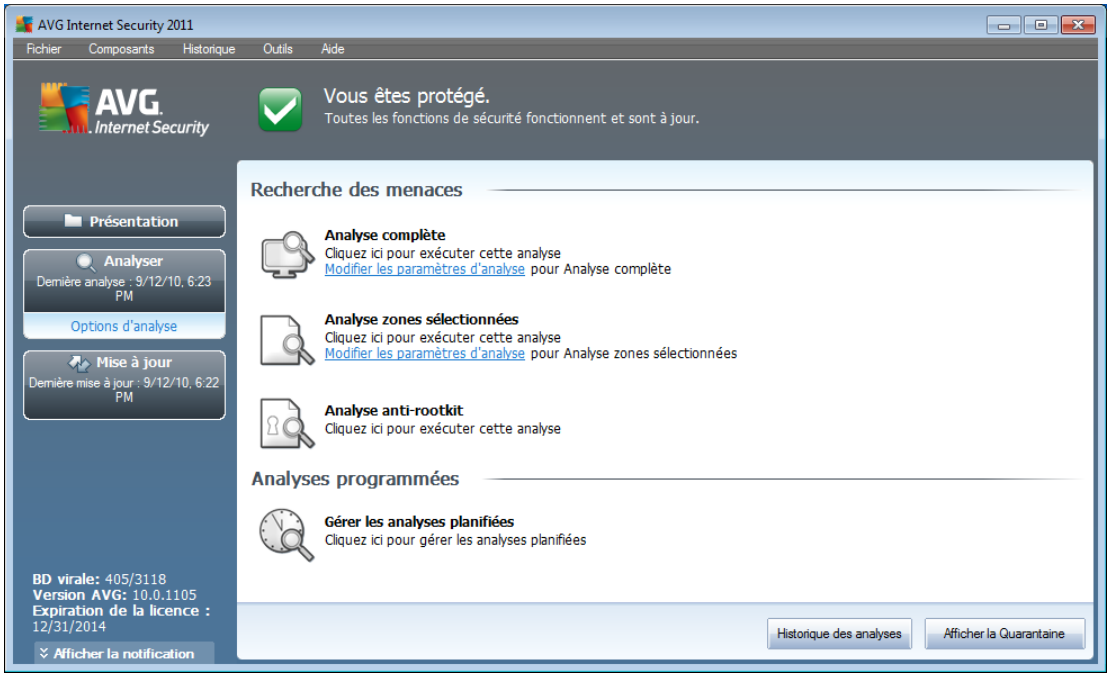
- ***/PROC*** Analyser les processus actifs
- ***/PUP*** Signaler les "programmes potentiellement dangereux"
- ***/REG*** Analyser la base de registre
- ***/COO*** Analyser les cookies
- ***/?*** Affichage de l'aide sur un sujet
- ***/HELP*** Affichage de la rubrique d'aide en rapport avec l'élément actuellement sélectionné ou affiché
- ***/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
- ***/ARCBOMBSW*** Signaler les fichiers archives compressées à plusieurs reprises

11.5. Programmation de l'analyse

Avec **AVG Internet Security 2011**, vous pouvez effectuer une analyse à la demande (par exemple, lorsque vous soupçonnez qu'un virus s'est infiltré dans l'ordinateur) ou selon un programme prévu. 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.

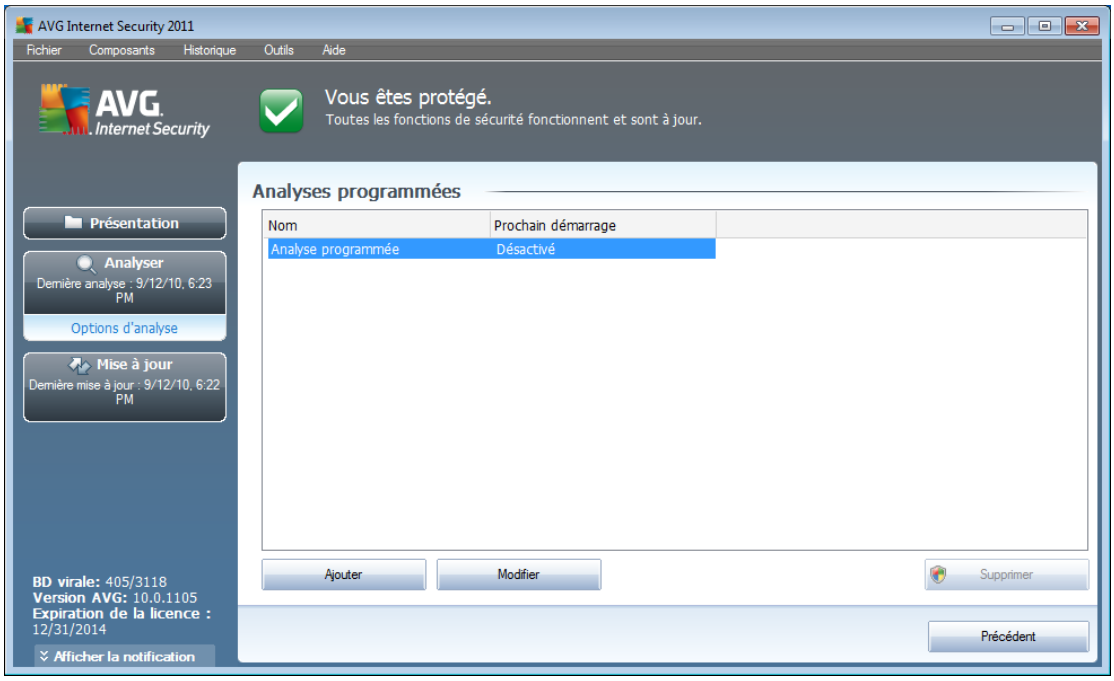
Il est possible d'effectuer une***analyse complète*** régulièrement, c'est-à-dire une fois par semaine au moins. Si possible, faites aussi une analyse complète l'ordinateur une fois par jour, comme configuré par défaut dans la programmation de l'analyse. Si l'ordinateur est toujours sous tension, vous 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 programmées actuellement :



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.

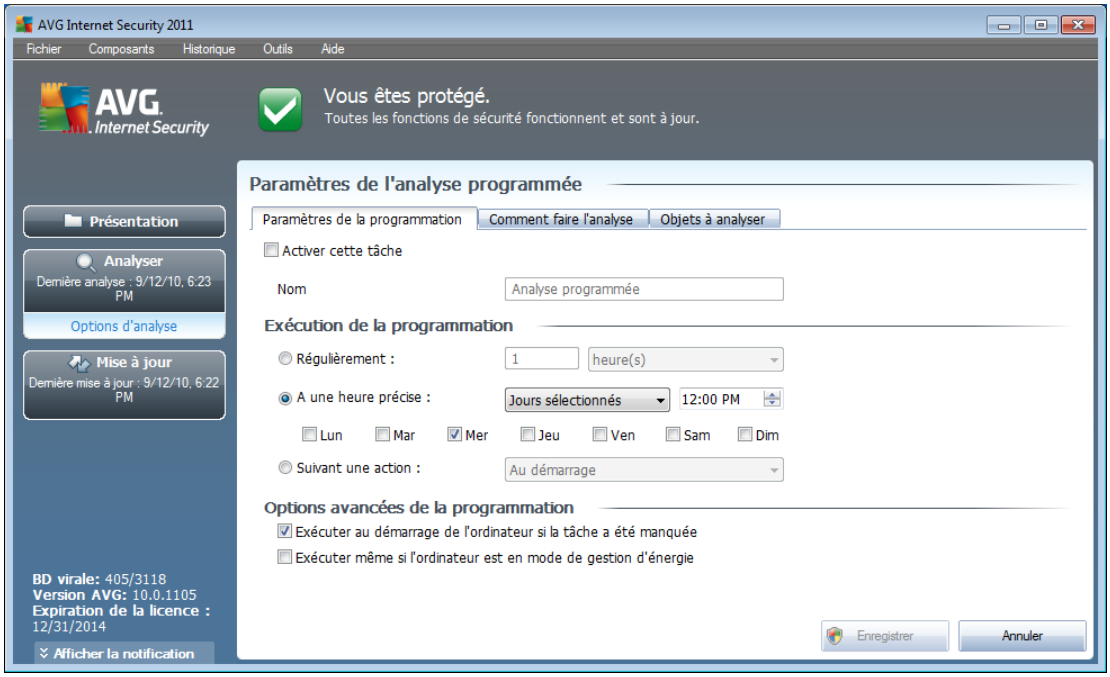
- ***Modifier*** - ce bouton n'est actif que si vous avez déjà sélectionné une analyse existante dans la liste des analyses programmées. Dans ce cas, le bouton est accessible ; il suffit de cliquer dessus pour accéder à la boîte de dialogue ***Paramètres de l'analyse programmée***, onglet ***Paramètres 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 analyse programmée*** *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 à l'ouverture de la boîte de dialogue*), ***et*** et ***Objets à analyser***.



Dans l'onglet ***Paramètres de la programmation***, vous pouvez cocher/désélectionner la case ***Activer cette tâche*** pour désactiver temporairement l'analyse programmée et le 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 en regard 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 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 d'indiquer 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.

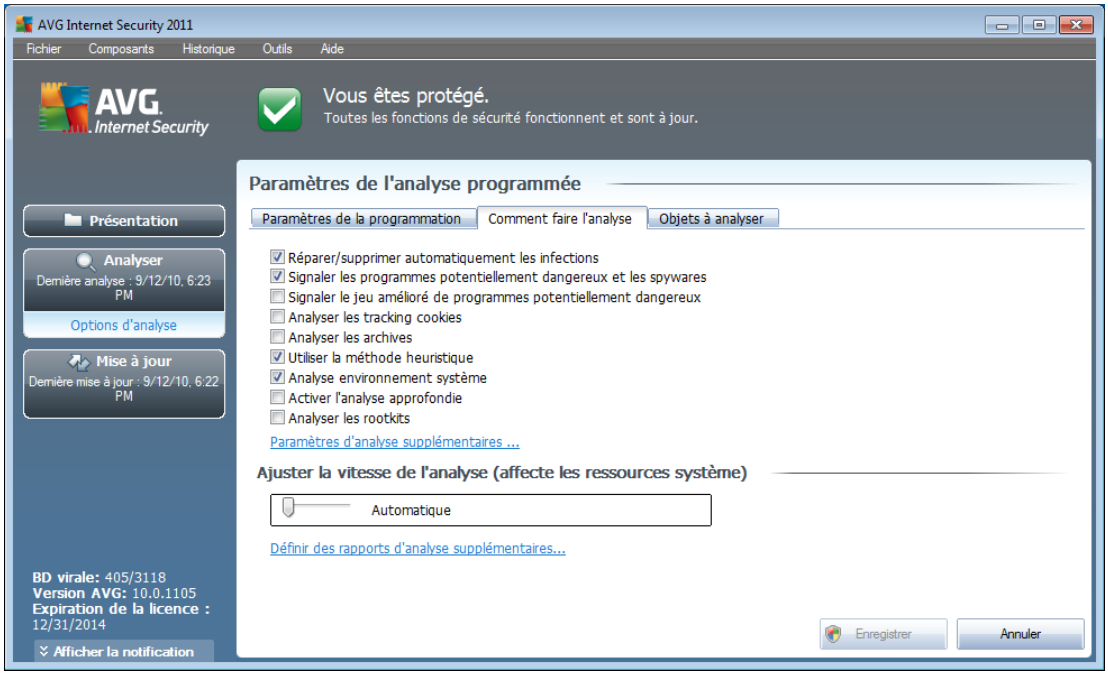
Boutons de commande de la boîte de dialogue Paramètres de l'analyse programmée

Deux boutons de commande figurent sur les trois onglets de la boîte de dialogue ***Paramètres de l'analyse programmée*** (***Paramètres de la programmation***, ***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.

11.5.2. Comment faire l'analyse



Dans l'onglet ***Comment faire l'analyse***, vous trouverez la liste des 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 dans la mesure du 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. L'action recommandée consiste à confiner le fichier infecté en ***quarantaine***.

- ***Signaler les programmes potentiellement dangereux et les spywares*** (*activé par défaut*) : cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** *(option désactivée par défaut*) : permet de détecter le jeu étendu des spywares*** qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

- ***Analyser les tracking cookies*** (*option désactivée par défaut*) : ce paramètre du composant ***Anti-Spyware*** indique que les cookies devront 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 leur panier d'achat électronique*).

- ***Analyser les archives*** (*option désactivée 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.

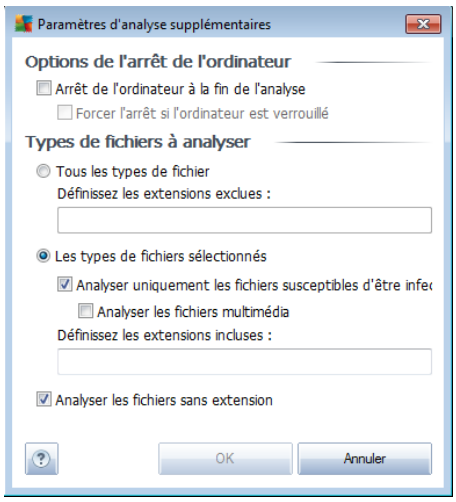
- ***Analyse environnement système*** (*option activée par défaut*) : l'analyse vérifie les fichiers système de l'ordinateur.

- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*suspicion d'une infection de l'ordinateur*), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

- ***Analyser les rootkits*** (*option désactivée par défaut*) : 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. Si l'option ***Arrêt de l'ordinateur à la fin de l'analyse*** est activée, l'option ***Forcer l'arrêt si l'ordinateur est verrouillé*** devient disponible et 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 les;

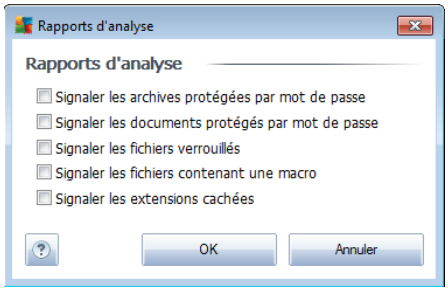
    - ***Les types de fichiers sélectionnés*** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers 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 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*** - 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.

- ***Ajuster la vitesse de l'analyse*** - le curseur vous permet de modifier la

priorité du processus d'analyse. Le niveau intermédiaire est le meilleur compromis entre vitesse d'analyse et 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 lorsque vous quittez temporairement votre poste de travail*).

- ***Définir des rapports d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Rapports d'analyse***, dans laquelle 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****.*

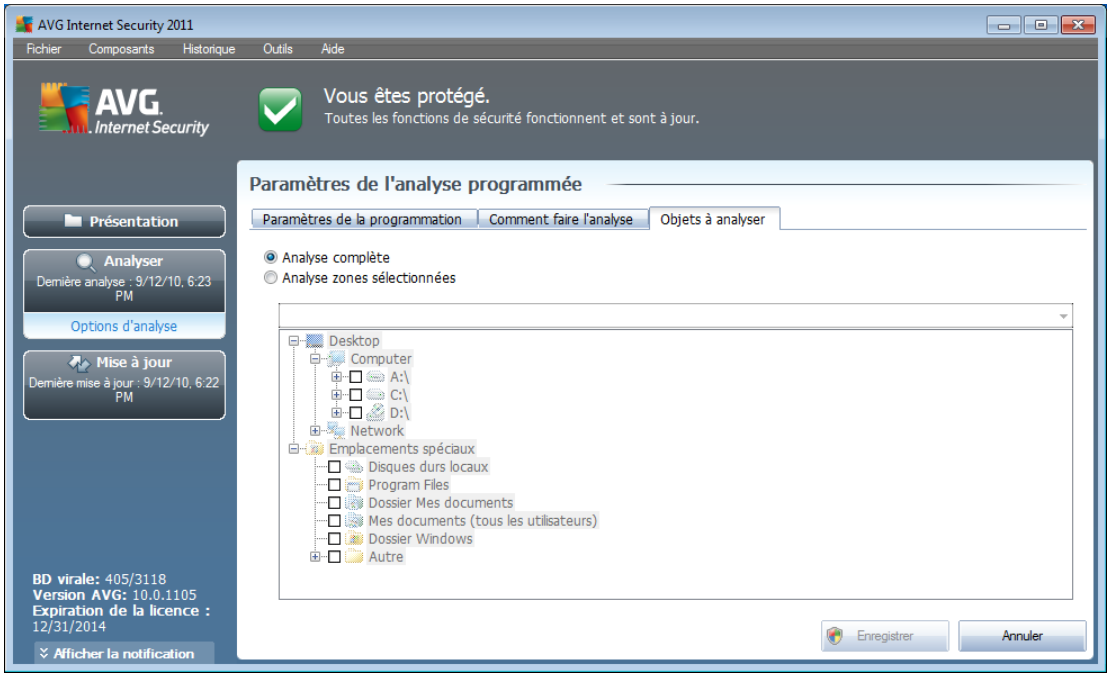
Boutons de commande

Deux boutons de commande 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 fonction :

- ***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.

11.5.3. Objets à analyser



Sous l'onglet ***Objet à analyser***, indiquez si vous voulez programmer l'analyse complète ou l'analyse des zones sélectionnées.

Si vous préférez l'analyse des zones sélectionnées, cela a pour effet d'activer, dans la partie inférieure de la boîte de dialogue, l'arborescence. Vous pouvez alors sélectionner les dossiers à analyser (*développez les catégories en cliquant sur le signe plus pour voir le dossier souhaité*). Vous pouvez sélectionner plusieurs dossiers en sélectionnant leur case respective. Les dossiers sélectionnés apparaîtront dans la zone de texte en haut de la boîte de dialogue et le menu déroulant conservera l'historique des analyses sélectionnées pour une utilisation ultérieure. *Autre solution, vous pouvez aussi saisir manuellement le chemin complet du dossier souhaité (si vous spécifiez plusieurs chemins, séparez-les par un point-virgule sans espace*).

Dans l'arborescence, vous noterez également la présence d'une entrée ***Emplacements spéciaux***. Voici la liste des emplacements qui seront analysés lorsque la case associée est cochée :

- ***Disques durs locaux*** - tous les disques durs de l'ordinateur
- ***Program Files***
    - C:\Program Files\
    - *dans la version 64 bits* C:\Program Files (x86)
- ***Dossier Mes documents***

- *Win XP :* C:\Documents and Settings\Utilisateur\Mes Documents\
- *Windows Vista/7* : C:\Utilisateurs\utilisateur\Documents\

- ***Documents partagés***
  - *Win XP* : C:\Documents and Settings\All Users\Documents\
  - *Windows Vista/7* : C:\Utilisateurs\Public\Documents\

- ***Dossier Windows*** - C:\Windows\

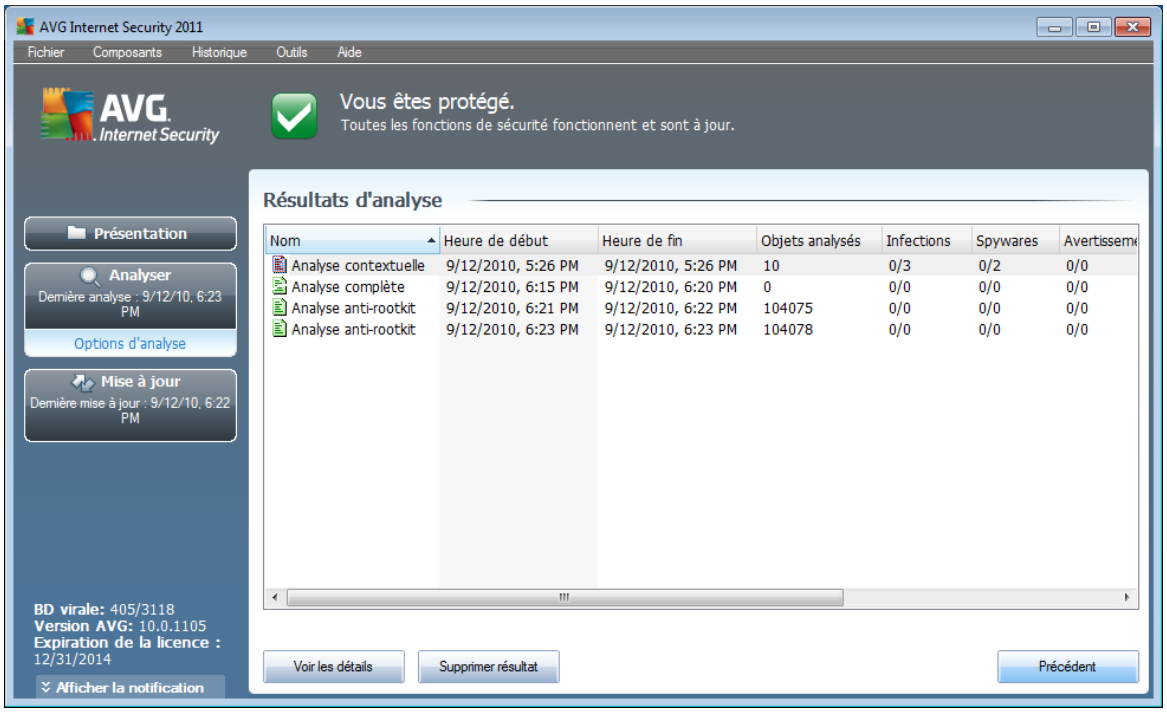
- ***Autre***
  - *Lecteur système* - le disque dur sur lequel le système d'exploitation est installé (en général, il s'agit de C:)
  - *Dossier système* - C:\Windows\System32\
  - *Dossier Fichiers temporaires* - C:\Documents and Settings\User\Local\ (*Windows XP*) ou C:\Utilisateurs\utilisateur\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Fichiers Internet temporaires* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*) ou C:\Utilisateurs\utilisateur\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

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 possèdent 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
- ***Avertissements*** - nombre d'objets suspects
- ***Rootkits*** - nombre de rootkits
- ***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*** - cliquez sur ce bouton pour ouvrir la boîte de dialogue ***Résultats des analyses*** et examiner les détails de l'analyse sélectionnée
- ***Supprimer résultat*** - cliquez sur ce bouton pour supprimer l'élément sélectionné de la présentation 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.

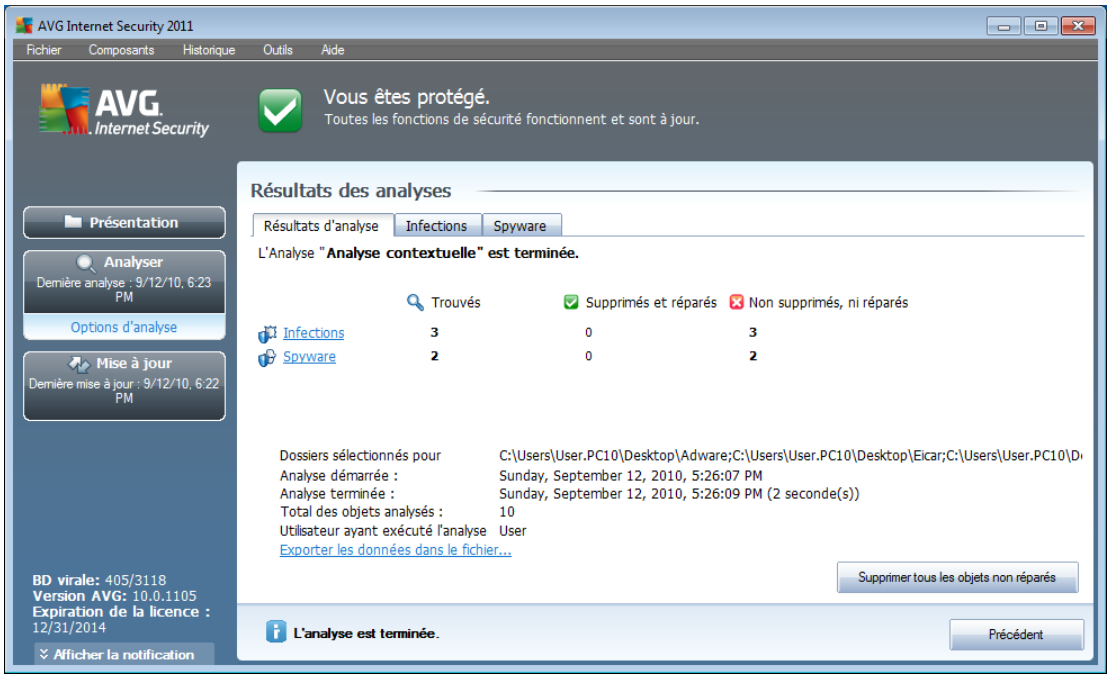
La boîte de dialogue est subdivisée en plusieurs onglets :

- ***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 si l'analyse détecte des cookies, par

exemple

- ***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. Vous trouverez également des informations sur des objets que l'analyse n'a pas réussi à traiter (comme des archives protégées par mot de passe).

11.7.1. Onglet Résultats d'analyse



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

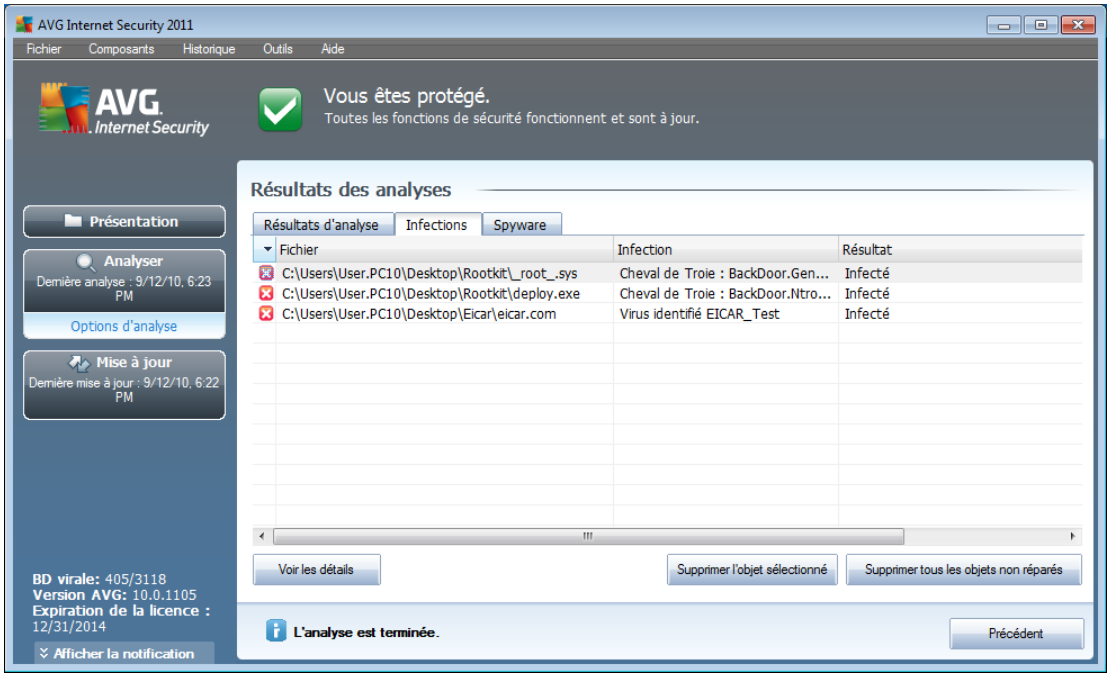
- les infections / spywares détectés
- les infections / spywares supprimés
- le nombre d'infections / de spywares qui n'ont pu être supprimés ou réparés

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 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*

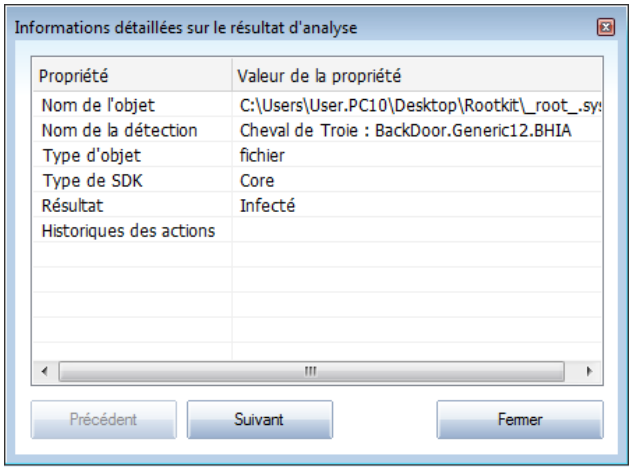
*dans la boîte de dialogue **Exceptions PUP** des paramètres avancés*)

- ***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
- ***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 des ***informations détaillées sur l'objet*** :

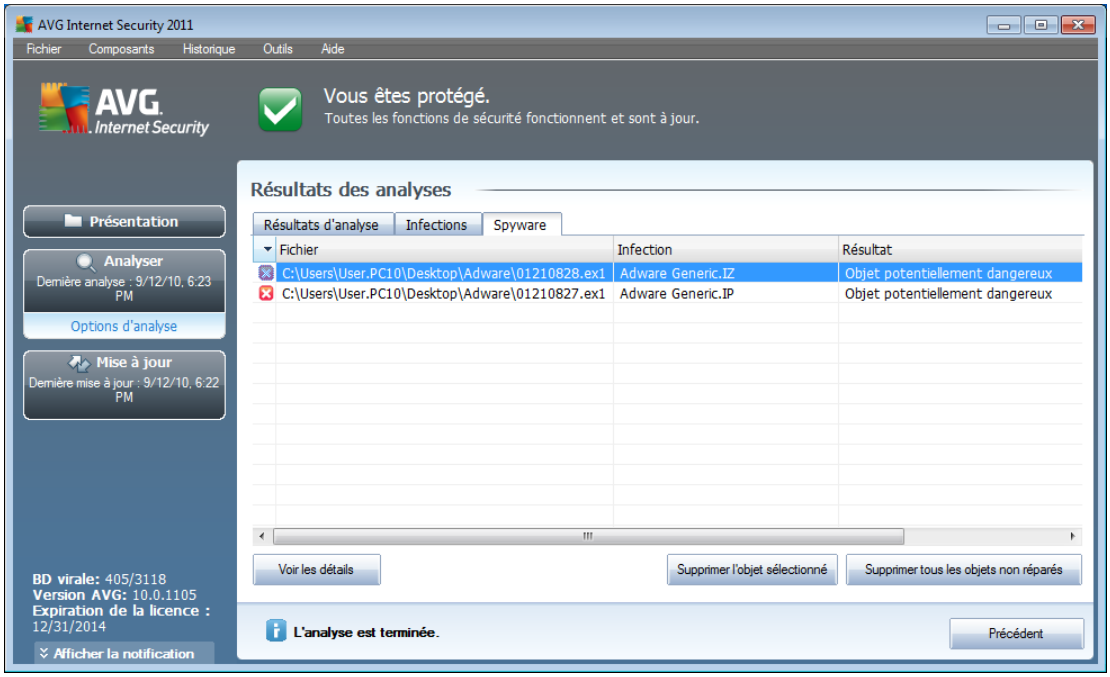


  Dans cette boîte de dialogue, vous trouverez des informations détaillées sur l'objet infectieux détecté (*ex : nom et emplacement de l'objet infecté, type d'objet, type SDK, résultat de la détection et historique des actions liées à l'objet détecté*). Les boutons ***Précédent*** et ***Suivant*** vous donnent accès aux informations sur des résultats spécifiques. Le bouton ***Fermer*** permet de quitter la boîte de dialogue.

- ***Supprimer l'objet sélectionné*** - servez-vous de ce bouton pour mettre les objets trouvés en ***quarantaine***
- ***Supprimer tous les objets non réparés*** - 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 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 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*

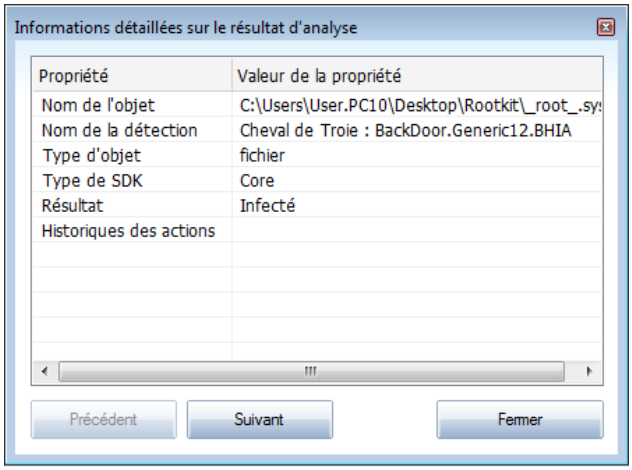
*dans la boîte de dialogue **Exceptions PUP** des paramètres avancés*)

- ***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
- ***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 des ***informations détaillées sur l'objet*** :



  Dans cette boîte de dialogue, vous trouverez des informations détaillées sur l'objet infectieux détecté (*ex : nom et emplacement de l'objet infecté, type d'objet, type SDK, résultat de la détection et historique des actions liées à l'objet détecté*). 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 l'objet sélectionné*** - servez-vous de ce bouton pour mettre les objets trouvés en ***quarantaine***
- ***Supprimer tous les objets non réparés*** - 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. Se 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***.

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 dupant ou en contournant les 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***.

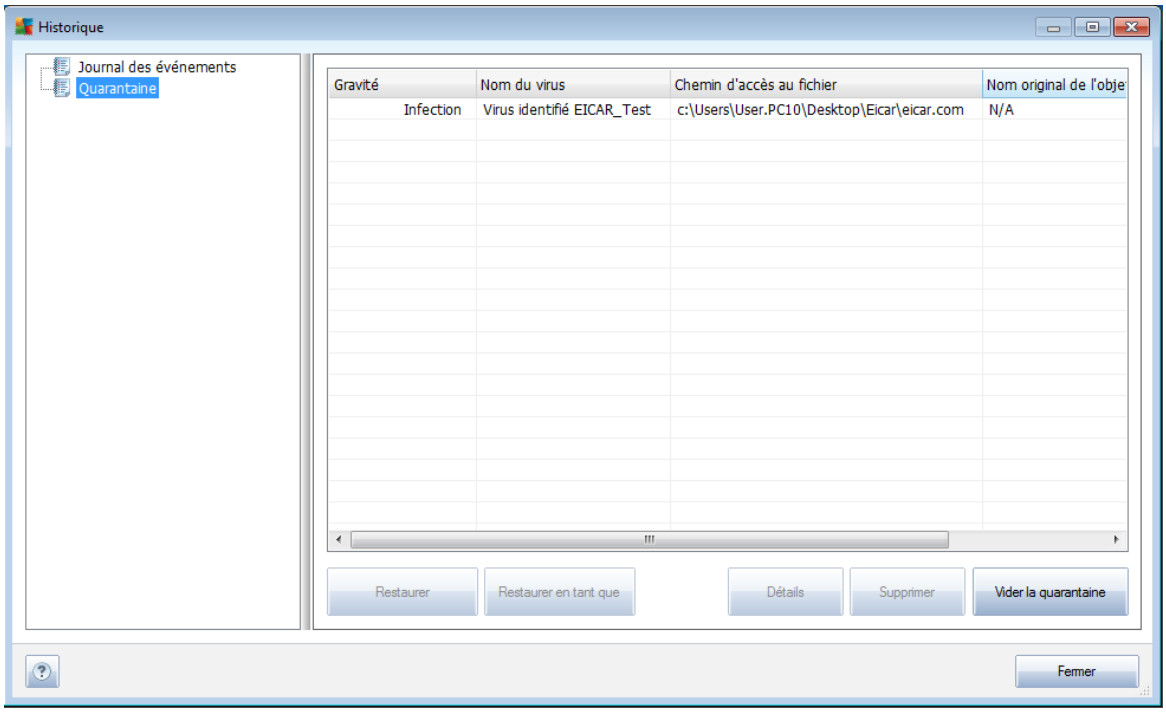
11.7.6. Onglet Informations

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 par le biais d'un ***avertissement*** ou d'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*** - Semblable 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 ce 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 afin de se dissimuler au système.
- ***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. Le principal objet de la ***quarantaine*** consiste à conserver en lieu sûr et durant un laps de temps défini, tout fichier supprimé lors de l'analyse au cas où vous auriez besoin de ces fichiers ultérieurement. Si l'absence du fichier entraîne des problèmes, envoyez-nous le fichier pour analyse ou restaurez-le à son emplacement d'origine.

L'interface ***Quarantaine*** s'affiche dans une fenêtre différente et présente des informations générales sur les objets infectés et déplacés en quarantaine :

- ***Gravité*** - si vous choisissez d'installer le composant ***Identity Protection*** dans **AVG Internet Security 2011**, les objets trouvés sont classés (indication visuelle) selon une échelle à quatre niveaux allant de sécurisé (■□□□) jusqu'à très dangereux (■■■■). Vous avez également accès à des informations sur le type d'infection (*en fonction de leur niveau d'infection ; tous les objets reportés sont infectés ou le sont potentiellement*)

- ***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***

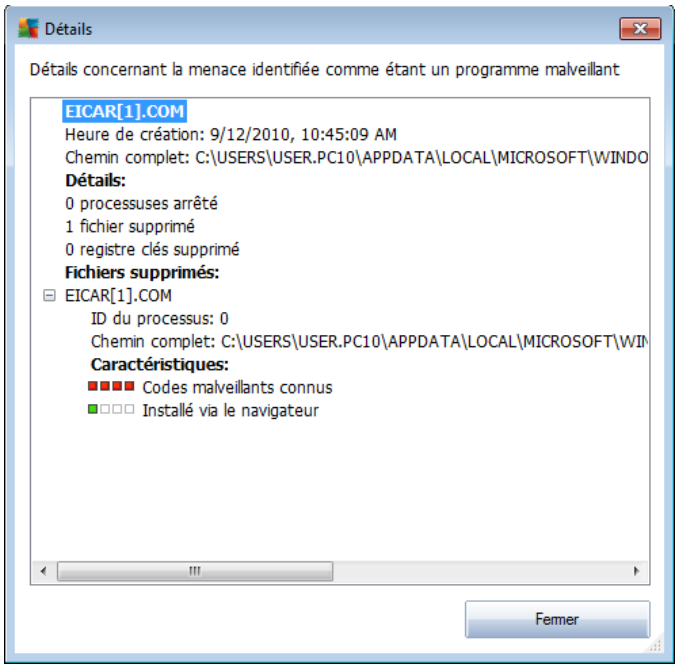
Boutons de commande

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.

- ***Détails*** – ce bouton s'applique seulement aux menaces détectées par ***Identity Protection***. Après avoir activé le bouton, une présentation synthétique des détails des menaces s'affiche (*fichiers/processus affectés, caractéristiques du processus, etc.*). Notez que pour tous les éléments détectés autrement que par IDP, ce bouton est grisé et inactif.



- ***Supprimer*** - supprime définitivement le fichier infecté de la ***Quarantaine***

- ***Vider la quarantaine*** - Vider intégralement le contenu de la***Quarantaine***.

Lorsque vous supprimez des fichiers de la ***quarantaine, ils sont définitivement effacés du disque dur (***ils ne sont pas mis dans la Corbeille*).*

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. De cette manière, vous êtes sûr que le programme **AVG Internet Security 2011** reste à jour 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.

Remarque : *si une mise à jour planifiée du programme coïncide avec une analyse programmée, le processus de mise à jour a priorité sur l'analyse qui est interrompue.*

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. Lorsque aucune mise à jour n'est disponible, le processus n'a pas lieu.

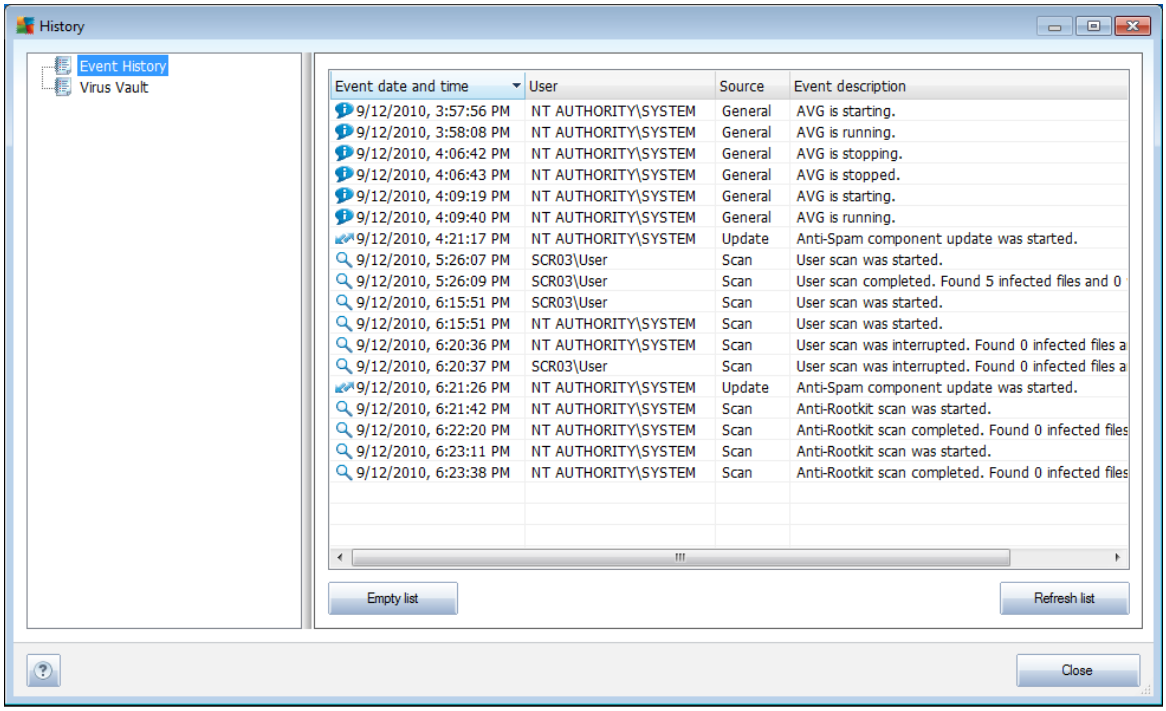
12.3. Processus de mise à jour

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. Au cours du processus de mise à jour, l'interface ***de mise à jour*** s'affiche. Elle permet d'observer le déroulement de la procédure sous forme graphique et présente des données statistiques pertinentes (*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 accessible via Démarrer / Tous les programmes / Accessoires / Outils système / Restauration du système. Seuls les utilisateurs expérimentés devraient effectuer des changements à ce niveau !*

13. Journal des évènements



La boîte de dialogue ***Journal de l'historique des évènements*** est accessible par la barre de menus, menu ***Historique, puis Journal de l'historique des évènements*** . Dans cette boîte de dialogue, vous trouverez un résumé des évènements les plus importants survenus pendant l'exécution du programme **.** La commande ***Journal de l'historique des évènements*** enregistre les types d'évènements 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 évènements importants

Pour chaque évènement, les informations suivantes s'affichent :

- ***Date et heure de l'évènement*** donne la date et l'heure exactes de l'évènement
- ***Utilisateur*** indique qui a démarré l'évènement
- ***Source*** indique le composant source ou une autre partie du système AVG qui a déclenché l'évènement

- ***Description de l'évènement*** donne un bref résumé de ce qui s'est réellement passé

Boutons de commande

- ***Vider la liste*** - supprime toutes les entrées de la liste d'évènements
- ***Actualiser la liste*** - met à jour toutes les entrées de la liste d'évènements

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***.