



# AVG Internet Security

Manuel de l'utilisateur

**Révision du document AVG.04 (09/02/2016)**

Copyright AVG Technologies CZ, s.r.o. Tous droits réservés.  
Toutes les autres marques commerciales appartiennent à leurs détenteurs respectifs.



## Table des matières

<b>1. Introduction</b>	<b>3</b>
<b>2. Pré-requis à l'installation d'AVG</b>	<b>4</b>
2.1 Systèmes d'exploitation pris en charge	4
2.2 Configuration matérielle minimale et recommandée	4
<b>3. Processus d'installation d'AVG</b>	<b>5</b>
3.1 Bienvenue !	5
3.2 Saisissez votre numéro de licence	6
3.3 Personnalisez votre installation	8
3.4 Installation d'AVG	9
3.5 Installation terminée	10
<b>4. Opérations à effectuer après l'installation</b>	<b>11</b>
4.1 Mise à jour de la base de données virale	11
4.2 Enregistrement du produit	11
4.3 Accès à l'interface utilisateur	11
4.4 Analyse complète	11
4.5 Test Eicar	11
4.6 Configuration par défaut d'AVG	12
<b>5. Interface utilisateur AVG</b>	<b>13</b>
5.1 Ligne supérieure de navigation	14
5.2 Informations sur l'état de la sécurité	17
5.3 Présentation des composants	18
5.4 Mes applications	19
5.5 Analyse/Mise à jour des liens d'accès rapide	19
5.6 Icône de la barre d'état	20
5.7 AVG Advisor	21
5.8 AVG Accelerator	22
<b>6. Composants AVG</b>	<b>24</b>
6.1 Protection de l'ordinateur	24
6.2 Protection de la navigation Web	28
6.3 Identity Protection	29
6.4 Protection email	31
6.5 Pare-Feu	32
6.6 PC Analyzer	35
<b>7. Paramètres avancés d'AVG</b>	<b>37</b>
7.1 Affichage	37
7.2 Sons	40
7.3 Désactiver provisoirement la protection AVG	41
7.4 Protection de l'ordinateur	42



7.5 Scanner email	47
7.6 Protection de la navigation Web	62
7.7 Identity Protection	65
7.8 Analyses	66
7.9 Programmations	72
7.10 Mise à jour	80
7.11 Exceptions	84
7.12 Quarantaine	86
7.13 Auto-protection AVG	87
7.14 Préférences de confidentialité	87
7.15 Ignorer les erreurs	89
7.16 Advisor – Réseaux connus	90
<b>8. Paramètres du Pare-feu</b>	<b>91</b>
8.1 Généralités	91
8.2 Applications	93
8.3 Partage de fichiers et d'imprimantes	94
8.4 Paramètres avancés	95
8.5 Réseaux définis	96
8.6 Services système	97
8.7 Les journaux	98
<b>9. Analyse AVG</b>	<b>101</b>
9.1 Analyses prédéfinies	103
9.2 Analyse contextuelle	112
9.3 Analyse en ligne de commande	112
9.4 Programmation d'une analyse	116
9.5 Résultats des analyses	124
9.6 Détails des résultats d'analyse	125
<b>10. AVG File Shredder</b>	<b>126</b>
<b>11. Quarantaine</b>	<b>127</b>
<b>12. Historique</b>	<b>128</b>
12.1 Résultats des analyses	128
12.2 Résultats du Bouclier résident	129
12.3 Résultats d'Identity Protection	132
12.4 Résultats de la Protection email	133
12.5 Résultats du Bouclier Web	134
12.6 Journal de l'historique des évènements	136
12.7 Journal du Pare-feu	137
<b>13. Mises à jour AVG</b>	<b>139</b>
<b>14. FAQ et Assistance technique</b>	<b>140</b>



## 1. Introduction

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

**AVG Internet Security** offre plusieurs niveaux de protection pour toutes vos activités en ligne. Vous n'aurez plus à redouter l'usurpation d'identité, les virus ou les sites malveillants. La technologie AVG Protective Cloud et le réseau de protection de la communauté AVG sont inclus. Ce qui veut dire que nous collectons les informations les plus récentes et les partageons avec la communauté afin de nous assurer que chacun reçoit la meilleure protection. Cette protection en temps réel vous permet de réaliser vos opérations bancaires et vos achats Internet en toute sécurité, de partager votre vie sur les réseaux sociaux ou de naviguer et effectuer des recherches sur Internet en toute confiance.

Vous pouvez également souhaiter utiliser d'autres sources d'informations :

- **Fichier d'aide** : une section *Résolution des problèmes* est disponible directement dans le fichier d'aide inclus dans **AVG Internet Security** (*pour ouvrir le fichier d'aide, appuyez sur la touche F1 à partir de n'importe quelle boîte de dialogue de l'application*). Cette section fournit la liste des situations les plus courantes que peut rencontrer un utilisateur lorsqu'il recherche une aide professionnelle pour résoudre un problème technique. Cliquez sur la situation qui décrit le mieux votre problème afin d'obtenir des instructions détaillées sur la manière de le résoudre.
- **Site Web du Centre de support d'AVG** : Site Web du Centre de support d'AVG : vous pouvez également rechercher la solution à votre problème sur le site Web d'AVG (<http://www.avg.com/>). La section **Support** contient une présentation des groupes thématiques abordant à la fois les problèmes d'ordre commercial et technique, une section structurée de la foire aux questions et tous les contacts disponibles.
- **AVG ThreatLabs** : un site Web AVG spécifique (<http://www.avg.com/about-viruses>) est dédié aux problèmes liés aux virus et fournit un aperçu structuré des informations concernant les menaces en ligne. Vous y trouverez également des instructions sur la manière de supprimer les virus et spyware et des conseils sur la manière de rester protégé.
- **Forum de discussion** : vous pouvez également utiliser le forum de discussion des utilisateurs d'AVG à l'adresse : <http://community.avg.com/>.



## 2. Pré-requis à l'installation d'AVG

### 2.1. Systèmes d'exploitation pris en charge

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

- Windows XP Edition familiale SP3
- Windows XP Professionnel SP3
- Windows Vista (toutes éditions confondues)
- Windows 7 (toutes éditions confondues)
- Windows 8 (toutes éditions confondues)
- Windows 10 (toutes éditions confondues)

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

### 2.2. Configuration matérielle minimale et recommandée

Voici la configuration matérielle minimale pour **AVG Internet Security**:

- Processeur Intel Pentium 1,5 GHz ou plus
- 512 Mo (Windows XP) / 1 024 Mo (Windows Vista, Windows 7) de mémoire RAM
- 1,3 Go d'espace disque dur (*pour l'installation*)

Voici la configuration matérielle minimale pour **AVG Internet Security**:

- Processeur Intel Pentium 1,8 GHz ou plus
- 512 Mo (Windows XP) / 1 024 Mo (Windows Vista, Windows 7) de mémoire RAM
- 1,6 Go d'espace disque dur (*pour l'installation*)



### 3. Processus d'installation d'AVG

Pour installer **AVG Internet Security** sur l'ordinateur, vous devez posséder le fichier d'installation le plus récent. Pour être sûr d'installer la dernière version d'**AVG Internet Security**, il est recommandé de vous rendre sur le site Web d'AVG (<http://www.avg.com/>) pour télécharger le fichier d'installation. La section **Support** contient une présentation structurée des fichiers d'installation de chaque édition d'AVG. Après avoir téléchargé le fichier d'installation et l'avoir enregistré sur le disque dur, lancez la procédure d'installation, qui consiste en une séquence de boîtes de dialogue simples et faciles à comprendre. Chaque boîte de dialogue décrit brièvement ce qu'il faut faire à chaque étape du processus d'installation. Ces fenêtres sont expliquées en détail ci-dessous :

#### 3.1. Bienvenue !

Le processus d'installation commence par la boîte de dialogue **Bienvenue dans AVG Internet Security** :



#### Sélection de la langue

À ce stade, vous pouvez choisir la langue à utiliser pour le processus d'installation. Cliquez sur le menu déroulant en regard de l'option **Langue** pour afficher les langues. Choisissez-en une. Le processus d'installation se poursuivra dans cette langue. L'application sera installée dans la langue choisie, mais aussi en anglais, dont l'installation est automatique.

#### Contrat de licence utilisateur final et politique de confidentialité

Avant de poursuivre le processus d'installation, nous vous recommandons de prendre connaissance du **Contrat de licence utilisateur final** et de la **Politique de confidentialité**. Ces deux documents sont accessibles via les liens actifs dans la partie inférieure de la boîte de dialogue. Cliquez sur l'un des hyperliens pour ouvrir une nouvelle boîte de dialogue ou une nouvelle fenêtre de navigateur fournissant le texte complet du



document correspondant. Lisez attentivement ces documents, car ceux-ci ont une valeur légale contraignante. En cliquant sur le bouton **Continuer**, vous confirmez accepter ces documents.

### Continuer l'installation

Pour poursuivre l'installation, cliquez sur le bouton **Continuer**. Vous serez invité à saisir votre numéro de licence, puis le processus d'installation s'exécutera en mode totalement automatique. Il est recommandé à la plupart des utilisateurs d'utiliser cette option standard pour l'installation de **AVG Internet Security** avec tous les paramètres prédéfinis par le fournisseur du programme. Cette configuration allie un maximum de sécurité et une utilisation optimale des ressources. Par la suite, vous aurez toujours la possibilité de modifier la configuration directement dans l'application.

Vous pouvez également choisir l'option **Installation personnalisée**, disponible sous forme d'hyperlien sous le bouton **Continuer**. L'installation personnalisée est exclusivement réservée aux utilisateurs expérimentés qui ont une raison valable d'installer l'application selon des paramètres non standard. Cela leur permet d'adapter le programme à une configuration système spécifique. Si vous choisissez ce mode d'installation, après avoir saisi votre numéro de licence, vous serez redirigé vers la boîte de dialogue [Personnalisez votre installation](#), où vous pourrez régler vos paramètres.

### 3.2. Saisissez votre numéro de licence

Dans la boîte de dialogue **Saisissez votre numéro de licence**, saisissez votre numéro de licence (*mieux encore, utilisez la méthode copier-coller*) dans le champ prévu à cet effet afin de l'activer :

The image shows a dark-themed dialog box with the AVG logo in the top left corner. The title bar reads "Saisissez votre numéro de licence". Below the title is a white text input field. To the right of the input field is a blue link that says "Où puis-je le trouver?". At the bottom left, there is a small text area that says "Vous n'avez pas de licence ? Essayez AVG Internet Security gratuitement pendant 30 jours!". At the bottom right, there is a green-outlined button labeled "Continuer".

### Où trouver mon numéro de licence ?

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



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

### Comment utiliser la méthode copier-coller

La méthode **copier-coller** permet d'entrer le numéro de licence du produit **AVG Internet Security** sans faire d'erreurs. Pour ce faire, procédez comme suit :

- Ouvrez l'email contenant votre numéro de licence.
- Cliquez sur le premier caractère du numéro de licence et faites glisser la souris tout en maintenant le bouton appuyé jusqu'au dernier caractère, puis relâchez le bouton. Le numéro devrait être sélectionné (il apparaît sur fond bleu).
- Maintenez la touche **Ctrl** enfoncée, puis appuyez sur la touche **C**. Cette action copie le numéro.
- Cliquez avec le bouton gauche pour positionner le curseur à l'endroit où vous souhaitez copier le numéro, c'est-à-dire, dans la zone de texte de la boîte de dialogue **Saisissez votre numéro de licence**.
- Maintenez la touche **Ctrl** enfoncée, puis appuyez sur la touche **V**. Le numéro est collé à l'emplacement choisi.

### Continuer l'installation

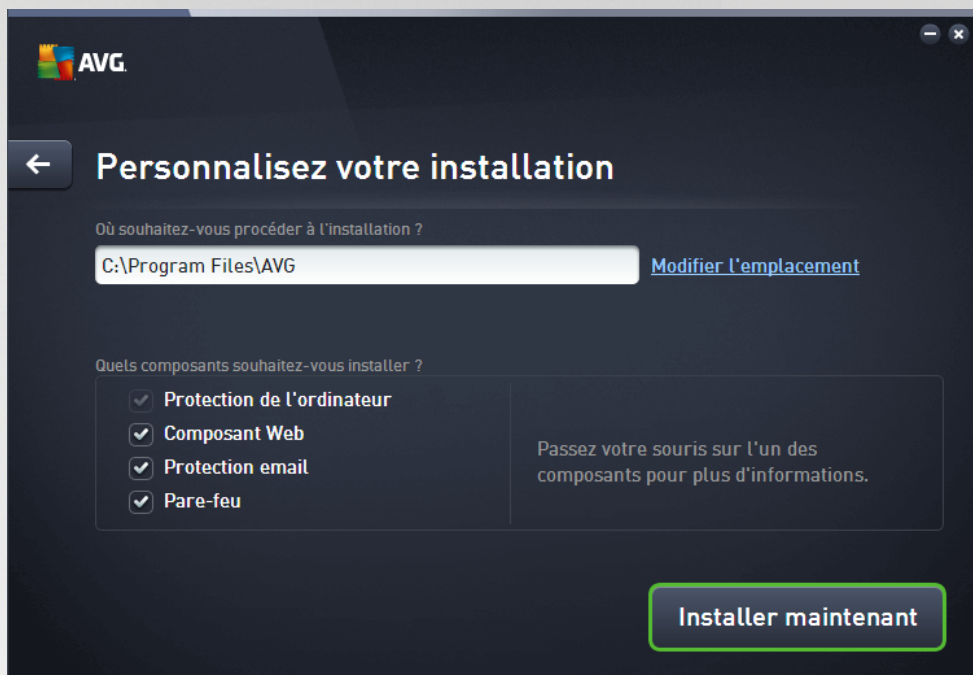
Dans la partie inférieure de la boîte de dialogue, vous trouverez le bouton **Installer maintenant**. Le bouton est activé lorsque vous renseignez votre numéro de licence. Une fois activé, cliquez sur le bouton pour lancer le processus d'installation. Si vous ne disposez pas d'un numéro de licence valide, vous pouvez installer **AVG AntiVirus Free Edition**, la version gratuite de l'application. Malheureusement, la version gratuite ne prend pas en charge toutes les fonctionnalités disponibles dans la version professionnelle complète. Nous vous invitons par conséquent à consulter le site Web d'AVG (<http://www.avg.com/>) pour de plus amples informations sur l'achat de produits AVG et les mises à niveau disponibles.





### 3.3. Personnalisez votre installation

La boîte de dialogue **Personnalisez votre installation** permet de configurer des paramètres d'installation détaillés :




#### Où souhaitez-vous procéder à l'installation ?

Spécifiez ici l'endroit où vous souhaitez installer l'application. L'adresse dans la zone de texte indique l'emplacement suggéré dans votre dossier Program Files. Si vous décidez de sélectionner un emplacement différent, cliquez sur le lien **Modifier l'emplacement** pour ouvrir une nouvelle fenêtre contenant l'arborescence de votre disque. Accédez ensuite à l'emplacement souhaité, puis confirmez.

#### Quels composants souhaitez-vous installer ?

Cette section présente tous les composants pouvant être installés. Si les paramètres par défaut ne vous satisfont pas, vous pouvez supprimer certains composants. Néanmoins, vous pouvez uniquement choisir des composants inclus dans AVG Internet Security ! La seule exception est le composant **Protection de l'ordinateur**, qui ne peut être exclu de l'installation. Lorsque vous mettez en surbrillance un élément de cette section, une brève description du composant correspondant s'affiche à droite. Pour plus d'informations sur le rôle de chacun des composants, consultez le chapitre [Présentation des composants](#) de cette documentation.

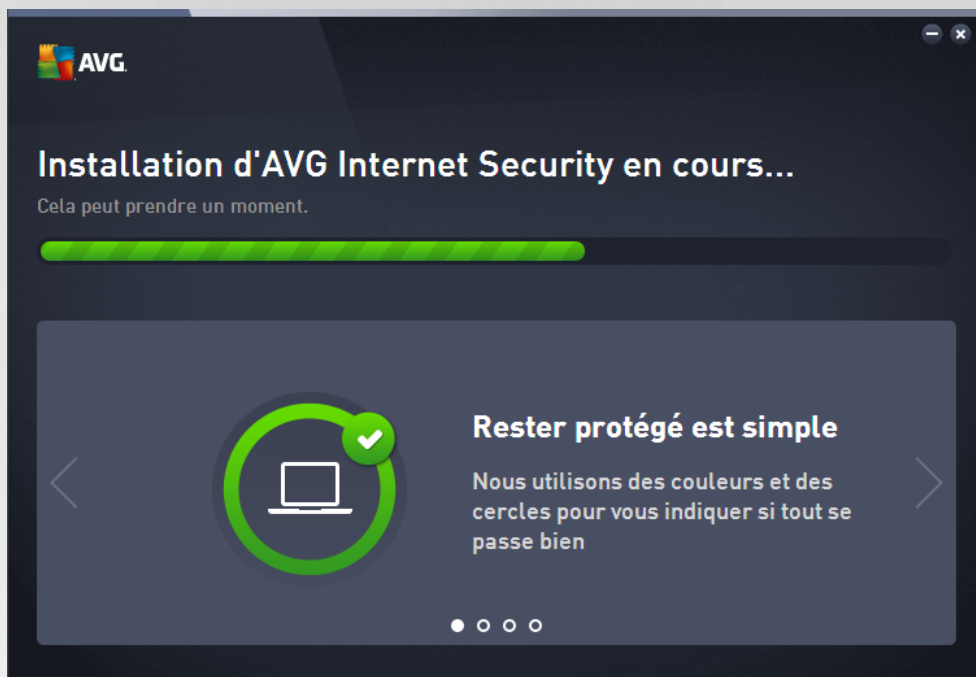
#### Continuer l'installation

Pour poursuivre l'installation, cliquez sur le bouton **Installer maintenant**. Dans le cas où vous auriez besoin de modifier ou de vérifier vos paramètres de langue, vous pouvez également revenir à la boîte de dialogue précédente en cliquant sur le bouton fléché  situé dans la partie supérieure de cette boîte de dialogue.



### 3.4. Installation d'AVG

En confirmant le lancement de l'installation dans la boîte de dialogue précédente, le processus d'installation s'exécute en mode entièrement automatique et ne requiert aucune intervention de votre part :

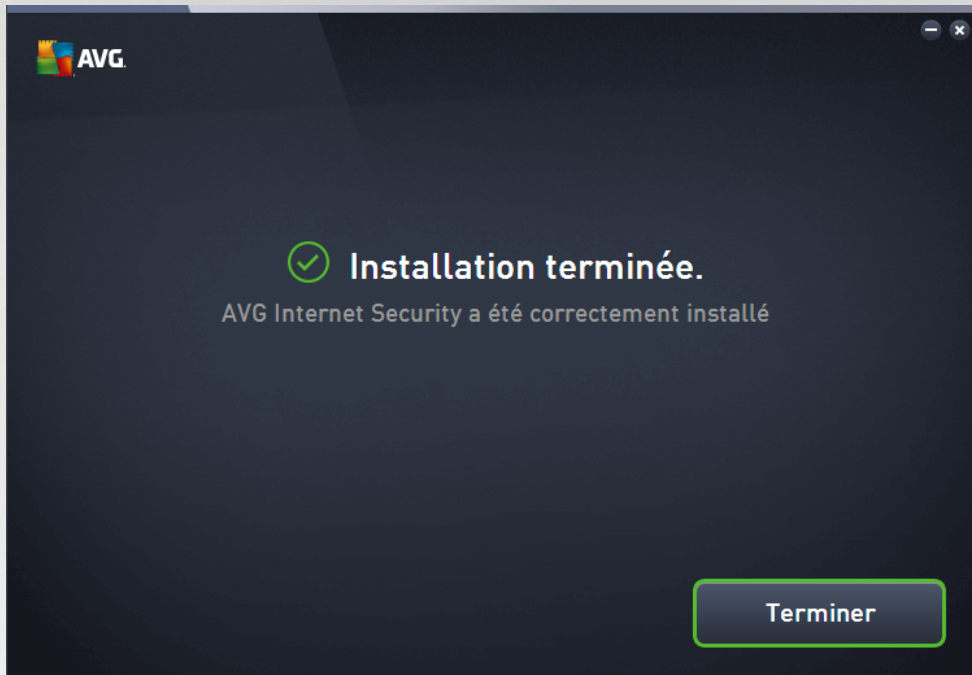


Une fois le processus d'installation terminé, vous serez automatiquement redirigé vers la boîte de dialogue suivante.



### 3.5. Installation terminée

La boîte de dialogue **Installation terminée** confirme que le programme AVG Internet Security est bien installé et configuré :



Cliquez sur le bouton **Terminer** pour finaliser le processus d'installation.



## 4. Opérations à effectuer après l'installation

### 4.1. Mise à jour de la base de données virale

Notez qu'une fois installé (après le redémarrage de l'ordinateur, si nécessaire), **AVG Internet Security** met automatiquement à jour sa base de données virale et tous les composants afin qu'ils soient entièrement opérationnels, ce qui peut prendre quelques minutes. Au cours du processus de mise à jour, vous recevrez une notification à ce sujet via les informations de la boîte de dialogue principale. Veuillez attendre un moment pour terminer le processus de mise à jour, **AVG Internet Security** sera alors complètement mis à jour et prêt à vous protéger.

### 4.2. Enregistrement du produit

Une fois l'installation d'**AVG Internet Security** terminée, enregistrez votre produit en ligne sur le site Web d'AVG (<http://www.avg.com>). A l'issue de l'enregistrement, vous bénéficierez pleinement des avantages associés à votre compte utilisateur AVG et accéderez à la lettre d'informations d'AVG ainsi qu'aux autres services réservés exclusivement aux utilisateurs enregistrés. Le moyen le plus simple d'enregistrer le produit consiste à le faire directement dans l'interface d'utilisateur d'**AVG Internet Security**. Dans le menu principal, sélectionnez [Options / Enregistrer maintenant](#) dans la ligne supérieure de navigation. La page d'**enregistrement** du site Web d'AVG (<http://www.avg.com>) s'ouvre. Suivez l'instruction fournie dans cette page.

### 4.3. Accès à l'interface utilisateur

La [boîte de dialogue principale d'AVG](#) est accessible de plusieurs façons :

- en double-cliquant sur l'icône de la [barre d'état système](#) AVG Internet Security ;
- en double-cliquant sur l'icône AVG Protection sur le bureau ;
- à partir du menu *Démarrer / Tous les programmes / AVG / AVG Protection*.

### 4.4. Analyse complète

Le risque de contamination de l'ordinateur par un virus avant l'installation d'**AVG Internet Security** 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. La première analyse peut prendre un peu de temps (*environ une heure*), mais il est recommandé de la lancer pour vous assurer que votre ordinateur n'a pas été compromis par une menace. Pour obtenir des instructions sur l'exécution d'une [Analyse complète](#), consultez le chapitre [Analyse AVG](#).

### 4.5. Test Eicar

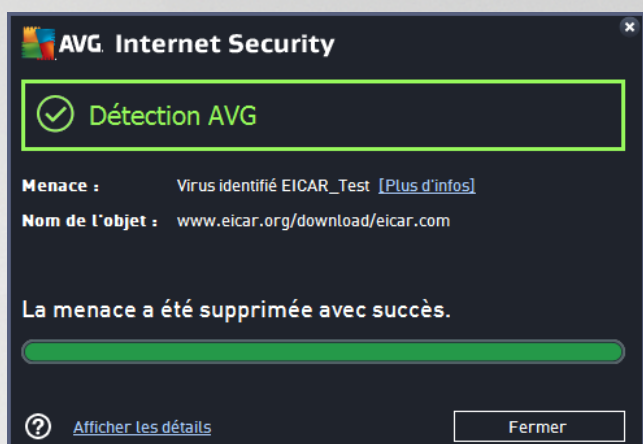
Pour confirmer que l'installation d'**AVG Internet Security** est correcte, effectuez un test EICAR.

Cette méthode standard et parfaitement sûre sert à tester le fonctionnement de l'antivirus 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](http://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, **AVG Internet Security** réagit en émettant un avertissement. Ce message du Bouclier Web indique qu'AVG est installé correctement sur votre ordinateur.



*Si AVG n'identifie pas le fichier test Eicar comme un virus, il est recommandé de vérifier de nouveau la configuration du programme.*

#### 4.6. Configuration par défaut d'AVG

La configuration par défaut (c'est-à-dire la manière dont l'application est paramétrée à l'issue de l'installation) d'**AVG Internet Security** 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.** Si vous voulez modifier la configuration d'AVG pour mieux l'adapter à vos besoins, accédez aux [paramètres avancés d'AVG](#) : sélectionnez l'élément du menu principal *Options / Paramètres avancés* et modifiez la configuration AVG dans la boîte de dialogue [Paramètres avancés d'AVG](#) qui s'affiche.



## 5. Interface utilisateur AVG

AVG Internet Security s'ouvre dans la fenêtre principale :



La fenêtre principale comprend plusieurs parties :

- **La ligne supérieure de navigation** se compose de quatre liens actifs (*AVG*, *Rapports*, *Support*, *Options*) alignés dans la partie supérieure de la fenêtre principale. [Détails >>](#)
- **La section Informations sur l'état de la sécurité** donne des informations sur l'état actuel d'**AVG Internet Security**. [Détails >>](#)
- La Présentation des composants installés se trouve dans une bande horizontale située au centre de la fenêtre principale. Les composants s'affichent sous forme de blocs vert clair et portent leur icône respective qui indique leur état actuel. [Détails >>](#)
- **Au centre de la partie inférieure de la fenêtre principale, la bande Mes applications** répertorie graphiquement les applications complémentaires déjà installées d'**AVG Internet Security**, ou dont l'installation sur votre ordinateur est recommandée. [Détails >>](#)
- Δεσ **liens d'accès rapide Analyse / Réparation / Mise à jour** sont situés dans la ligne de blocs inférieure de la fenêtre principale. Ces boutons permettent un accès immédiat aux fonctions les plus couramment utilisées et les plus importantes d'AVG. [Détails >>](#)

En dehors de la fenêtre principale d'**AVG Internet Security**, une commande supplémentaire vous permet d'accéder à l'application :

- **L'icône de la barre d'état système** est située dans le coin inférieur droit de l'écran (*sur la barre d'état système*), et indique l'état actuel d'**AVG Internet Security**. [Détails >>](#)



## 5.1. Ligne supérieure de navigation

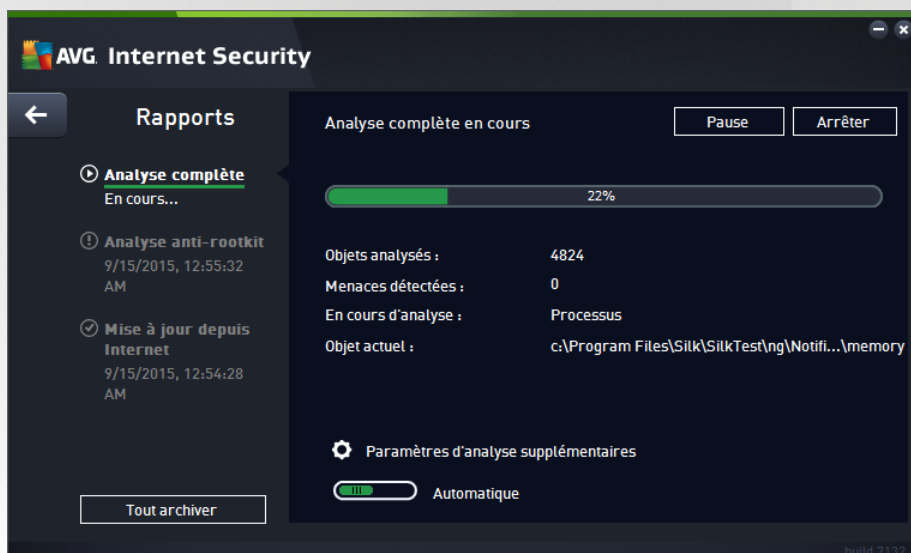
La *ligne supérieure de navigation* se compose de plusieurs liens actifs alignés dans la partie supérieure de la fenêtre principale. La navigation s'effectue par le biais des boutons suivants :

### 5.1.1. Rejoignez-nous sur Facebook

Cliquez sur le lien pour vous connecter à la [communauté AVG sur Facebook](#) et connaître les dernières informations sur AVG, les actualités, conseils et astuces qui vous permettront de toujours bénéficier d'une protection maximale sur Internet.

### 5.1.2. Rapports

Ouvre une nouvelle boîte de dialogue **Rapports** qui contient tous les rapports pertinents générés à partir d'analyses et de mises à jour lancées précédemment. Si une analyse ou une mise à jour est en cours d'exécution, un cercle en rotation s'affiche en regard de **Rapports** dans la ligne supérieure de navigation de l'[interface utilisateur principale](#). Cliquez sur ce cercle pour afficher la progression du processus :





### 5.1.3. Support

Ouvre une nouvelle boîte de dialogue composée de quatre onglets contenant toutes les informations utiles à propos du produit **AVG Internet Security** :



- **Support et licence** : cet onglet fournit des informations sur le nom du produit, le numéro de licence et la date d'expiration. Dans la partie inférieure de la boîte de dialogue, vous trouverez également des informations claires sur les personnes à contacter en cas de problème technique. Les liens actifs et boutons suivants sont disponibles dans cet onglet :
  - **Activer/Réactiver** : ouvre la nouvelle boîte de dialogue d'**activation du logiciel AVG**. Saisissez votre numéro de licence dans le champ prévu à cet effet, à la place de la référence d'achat (*utilisée pour l'installation du produit AVG Internet Security*) ou du numéro de licence actuel (*si vous installez une mise à niveau du produit AVG, par exemple*).
  - **Copier dans le Presse-papiers** : lien permettant de copier le numéro de licence, puis de le coller dans le champ correspondant. Cela vous permet d'éviter des erreurs de saisie.
  - **Renouveler maintenant** : nous vous recommandons de renouveler votre licence **AVG Internet Security** en temps utile, au moins un mois avant l'expiration de votre licence actuelle. Vous serez informé dès que la date d'expiration de cette dernière sera proche. Cliquez sur ce lien pour accéder au site Web d'AVG (<http://www.avg.com/>) et obtenir des informations détaillées sur l'état de votre licence, sa date d'expiration et l'offre de renouvellement/mise à niveau.
- L'onglet **Produit** fournit des données techniques importantes concernant le produit **AVG Internet Security**, les composants installés, la protection des emails ainsi que des informations sur le système.
- L'onglet **Programme** contient des informations techniques détaillées sur l'application **AVG Internet Security** installée, comme le numéro de version du produit principal et la liste des numéros de version de tous les produits correspondants (*par ex., Zen, PC TuneUp, etc.*). Enfin, cet onglet présente tous les composants installés, ainsi que des informations de sécurité spécifiques (*numéros de versions de la base de données virale, Link Scanner et Anti-Spam*).





- L'onglet **Contrat de licence** contient le texte intégral du contrat de licence qui vous lie à AVG Technologies.

#### 5.1.4. Options

La maintenance d'**AVG Internet Security** est accessible à partir des **options**. Cliquez sur la flèche pour ouvrir le menu déroulant.

- [Analyse de l'ordinateur](#) : lance une analyse complète de l'ordinateur.
- [Analyser le dossier sélectionné...](#) : ouvre l'interface d'analyse d'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. Cliquez sur cette option pour ouvrir une nouvelle fenêtre contenant l'arborescence de votre disque. Sélectionnez le fichier souhaité et confirmez le lancement de l'analyse.
- [Mise à jour](#) : lance automatiquement le processus de mise à jour d'**AVG Internet Security**.
- [Mise à jour depuis le répertoire...](#) : effectue la mise à jour à l'aide de fichiers 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.
- [Quarantaine](#) : ouvre l'interface à l'espace de quarantaine, Quarantaine, où AVG supprime toutes les infections détectées. 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
- [Historique](#) : offre des options de sous-menu supplémentaires et spécifiques :
  - [Résultats d'analyse](#) : affiche une boîte de dialogue contenant les résultats d'analyse.
  - [Résultats du Bouclier résident](#) : ouvre une boîte de dialogue contenant la liste des menaces détectées par le Bouclier résident.
  - [Résultats d'Identity Protection](#) : ouvre une boîte de dialogue contenant la liste des menaces détectées par [Identity Protection](#).
  - [Résultats de la Protection email](#) : ouvre une boîte de dialogue contenant la liste des pièces jointes détectées comme dangereuses par le composant Protection email.
  - [Résultats du Bouclier Web](#) : ouvre une boîte de dialogue contenant la liste des menaces détectées par le Bouclier Web.
  - [Journal de l'historique des événements](#) : ouvre l'interface de l'historique des événements présentant toutes les actions consignées du programme **AVG Internet Security**.
  - [Journal du Pare-feu](#) : ouvre une boîte de dialogue contenant la liste détaillée des actions du Pare-feu.



- **Paramètres avancés** : ouvre la boîte de dialogue Paramètres avancés d'AVG qui permet de modifier la configuration d'**AVG Internet Security**. En règle générale, 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 boîte de dialogue autonome permettant de définir la configuration avancée du composant Pare-feu.
- **Sommaire** : ouvre les fichiers d'aide du programme AVG.
- **Obtenir de l'assistance** : ouvre la [boîte de dialogue du support](#) contenant tous les contacts accessibles et les informations de support.
- **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 sur le site Web d'AVG (<http://www.avg.com/>), où vous pouvez consulter des informations détaillées sur le virus identifié.
- **Activer/Réactiver** : ouvre la boîte de dialogue d'activation comportant le numéro de licence que vous avez saisi au cours du processus d'installation. Dans cette boîte de dialogue, vous pouvez remplacer le numéro de licence de vente (*avec lequel vous avez installé AVG*) ou votre ancien numéro (*si vous installez une mise à niveau du produit AVG, par exemple*). Remarque : si vous utilisez une version d'évaluation d'**AVG Internet Security**, les deux dernières options sont remplacées par **Acheter** et **Activer**, ce qui vous permet de vous procurer de suite la version complète du programme. Si le programme **AVG Internet Security** est installé avec une référence d'achat, vous avez alors le choix entre les options **Enregistrer** et **Activer** :
- **Enregistrer maintenant / MyAccount** : renvoie à la page d'enregistrement du site Web d'AVG (<http://www.avg.com/>). Complétez le formulaire d'enregistrement ; seuls les clients ayant dûment enregistré leur produit AVG peuvent bénéficier de l'assistance technique gratuite.
- **A propos d'AVG** : ouvre une nouvelle boîte de dialogue avec quatre onglets qui contiennent des données sur la licence achetée, les services de support auxquels elle donne accès, ses conditions d'utilisation et des informations sur le produit et le programme. (*Il est possible d'ouvrir cette boîte de dialogue en cliquant sur le lien [Support](#) dans la navigation principale.*)

## 5.2. Informations sur l'état de la sécurité

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



- L'icône verte indique que le programme **AVG Internet Security est complètement opérationnel**. Votre système est totalement protégé et à jour ; tous les composants installés fonctionnent convenablement.



- L'icône jaune 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 dans le programme **AVG Internet Security** ; vous avez sans doute choisi de désactiver certains composants. Vous êtes toujours protégé ! Certains paramètres d'un composant réclament toutefois votre attention. Le composant dont la configuration pose problème sera indiqué par une bande d'avertissement orange dans [l'interface utilisateur principale](#).



L'icône jaune s'affiche également si vous décidez, pour une raison quelconque, d'ignorer les erreurs d'un composant. L'option **Ignorer les erreurs** est accessible dans la section [Paramètres avancés / Ignorer les erreurs](#). Sélectionnez cette option pour indiquer que vous avez constaté que le composant comporte une erreur, mais que vous souhaitez conserver la configuration d'**AVG Internet Security** en l'état et ne plus être informé de l'erreur par l'icône de la barre d'état. Vous pouvez être amené à utiliser cette option dans certaines situations, mais il est vivement conseillé de désactiver l'option **Ignorer les erreurs**, dès que possible.

L'icône jaune peut également s'afficher si **AVG Internet Security** nécessite un redémarrage de votre ordinateur (**Redémarrage nécessaire**). Tenez compte de cet avertissement et redémarrez votre ordinateur.



- L'icône orange indique que l'état **AVG Internet Security est critique**. Un ou plusieurs composants ne fonctionnent pas correctement et **AVG Internet Security** 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 Internet Security n'est pas configuré de manière optimale, un nouveau bouton, Corriger (ou Tout corriger si le problème implique plusieurs composants), apparaît près des informations relatives à l'état de la sécurité. Cliquez sur ce bouton pour lancer le processus automatique de vérification et de configuration du programme. C'est un moyen simple d'optimiser les performances d'AVG Internet Security et d'établir un niveau de sécurité maximal !**

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. À défaut, vous risquez de mettre en péril la sécurité de votre système.

**Remarque : vous pouvez à tout moment obtenir des informations sur l'état du programme AVG Internet Security en consultant [l'icône de la barre d'état système](#).**

### 5.3. Présentation des composants

La **Présentation des composants installés** se trouve dans une bande horizontale située au centre de la [fenêtre principale](#). Les composants s'affichent sous forme de blocs vert clair et portent leur icône respective. Chaque bloc affiche des informations au sujet de l'état actuel de la protection. Si le composant est configuré correctement et complètement opérationnel, les informations apparaissent en lettres vertes. Si le composant est arrêté ou dans un état d'erreur, ou si sa fonctionnalité est limitée, un texte d'avertissement en lettres orange s'affiche. **Il est vivement recommandé d'examiner les paramètres de chaque composant.**

Passez la souris sur le composant pour afficher un texte court en bas de la [fenêtre principale](#). Ce texte fournit des informations essentielles sur la fonctionnalité du composant. Il vous informe également de l'état actuel du composant et précise si l'un des services associés n'est pas configuré correctement.

#### Liste des composants installés

Dans **AVG Internet Security**, la section **Panneau de présentation des composants** contient des renseignements sur les composants suivants :

- **Ordinateur** : ce composant couvre deux services : **AntiVirus Shield** détecte les virus, spyware, vers, chevaux de Troie, fichiers exécutables ou bibliothèques indésirables sur votre système tout en vous protégeant des adwares malveillants. **Anti-Rootkit** recherche les rootkits dangereux qui se cachent



dans les applications, les lecteurs ou les bibliothèques. [Détails >>](#)

- **Navigation Web** : vous protège des attaques lorsque vous effectuez des recherches ou naviguez sur Internet. [Détails >>](#)
- **Identité** : Le composant exécute le service **Identity Shield** qui protège en permanence vos ressources numériques contre les menaces connues ou non qui existent sur Internet. [Détails >>](#)
- **Emails** : analyse vos messages entrants pour y détecter les messages indésirables et bloquer les virus, les attaques par phishing ou d'autres menaces. [Détails >>](#)
- **Firewall** : contrôle toutes les communications sur chaque port réseau, vous protège des attaques malveillantes et bloque toutes les tentatives d'intrusion. [Détails >>](#)

### Actions accessibles

- **Cliquer sur l'icône d'un composant** permet de le mettre en surbrillance dans la vue générale des composants. Par ailleurs, la description de la fonctionnalité de base du composant est s'affiche en bas de l'[interface utilisateur](#).
- **Cliquer une fois sur l'icône d'un composant** a pour effet d'ouvrir la propre interface du composant présentant son état actuel, des données relatives à sa configuration et des statistiques.

## 5.4. Mes applications

Dans le champ **Mes applications** (*ligne de blocs verts sous le jeu de composants*), vous trouverez la liste des applications AVG supplémentaires installées ou qu'il est recommandé d'installer sur votre ordinateur. Les blocs s'affichent de manière standard et peuvent représenter l'une des applications suivantes :

- **Protection des appareils mobiles** est une application qui protège votre téléphone portable contre les virus et les logiciels malveillants. Elle permet également de suivre à distance votre smartphone en cas de perte ou d'oubli.
- **L'application PC TuneUp** est un outil avancé d'analyse approfondie et de correction du système permettant d'améliorer la vitesse et la performance globale de votre ordinateur.

Pour de plus amples informations sur l'une des applications répertoriées dans **Mes applications**, cliquez sur le bloc correspondant. Vous serez redirigé vers la page Web d'AVG dédiée, à partir de laquelle vous pouvez télécharger le composant.

## 5.5. Analyse/Mise à jour des liens d'accès rapide

Les **Liens d'accès rapide** se trouvent dans la ligne de boutons inférieure de l'[interface utilisateur](#) d'**AVG Internet Security**. Ces liens permettent d'accéder instantanément aux fonctions de l'application les plus importantes et les plus utilisées, comme l'analyse et la mise à jour. Ils sont disponibles dans chaque boîte de dialogue de l'interface utilisateur :

- **Analyser maintenant** : ce bouton comprend deux sections. Suivez le lien **Analyser maintenant** pour lancer immédiatement l'[analyse complète](#) et observer la progression et les résultats de l'opération dans la fenêtre [Rapports](#) ouverte. Le bouton **Options** ouvre la boîte de dialogue des **Options d'analyse** dans laquelle vous pouvez [gérer les analyses planifiées](#) et modifier les paramètres de







[l'Analyse complète](#) ou de [l'Analyse des fichiers ou des dossiers spécifiques](#). (Pour en savoir plus, consultez le chapitre [Analyse AVG](#))

- **+ de performances** : ce bouton vous permet d'accéder au service [PC Analyzer](#), un outil avancé d'analyse approfondie et de correction du système, permettant d'améliorer la vitesse et les performances globales de votre ordinateur.
- **Mettre à jour** : cliquez sur ce bouton pour lancer la mise à jour immédiate du produit. Vous serez prévenu des résultats de la mise à jour dans la boîte de dialogue contextuelle, affichée au-dessus de l'icône AVG dans la barre d'état système. (Pour en savoir plus, consultez le chapitre [Mises à jour AVG](#)).

## 5.6. Icône de la barre d'état

L'**icône de la barre d'état d'AVG** (dans la barre des tâches Windows, coin inférieur droit de l'écran) indique l'état actuel d'**AVG Internet Security**. Elle est toujours visible dans la barre d'état, que [l'interface utilisateur d'AVG Internet Security](#) soit ouverte ou fermée :

### Affichage de l'icône de barre d'état d'AVG

-  En couleur pleine, sans éléments additionnels, l'icône indique que tous les composants d'**AVG Internet Security** sont actifs et pleinement opérationnels. Toutefois, l'icône peut prendre cette apparence alors qu'un des composants n'est pas pleinement opérationnel, parce que l'utilisateur a choisi d'en [ignorer l'état](#). (En confirmant ce choix, vous indiquez que vous savez que le [composant comporte une erreur](#), mais que, pour une raison ou une autre, vous ne voulez ni la corriger ni en être averti.)
-  Un point d'exclamation sur l'icône indique qu'un composant (voire plusieurs) [comporte une erreur](#). Prêtez attention à ce type d'avertissement à chaque fois et tentez de corriger le problème de configuration incorrecte d'un composant. Pour modifier la configuration du composant, double-cliquez sur l'icône de la barre d'état afin d'ouvrir [l'interface utilisateur de l'application](#). Pour identifier les composants [comportant une erreur](#), consultez la section [Informations sur l'état de la sécurité](#).
-  L'icône de la barre d'état peut également comporter un rayon lumineux clignotant en rotation. Ce type d'image signale qu'un processus de mise à jour est en cours.
-  En revanche, une flèche sur l'icône signifie que des analyses **AVG Internet Security** sont en cours.

### Informations de l'icône de barre d'état d'AVG

L'**icône de la barre d'état AVG** fournit également des informations sur les activités actuelles du programme **AVG Internet Security** et sur les changements éventuels d'état du programme (par exemple le lancement automatique d'une analyse programmée ou mise à jour, un changement de profil ou de l'état d'un composant, une erreur, etc.) par la fenêtre contextuelle qui s'affiche depuis l'icône de la barre d'état.



### Actions exécutables via l'icône de barre d'état d'AVG

L'**icône de la barre d'état d'AVG** peut également servir de lien d'accès rapide à l'[interface utilisateur](#) d'**AVG Internet Security**. Pour cela, il suffit de double-cliquer dessus. Lorsque vous cliquez avec le bouton droit sur l'icône, un menu contextuel affiche les options suivantes :

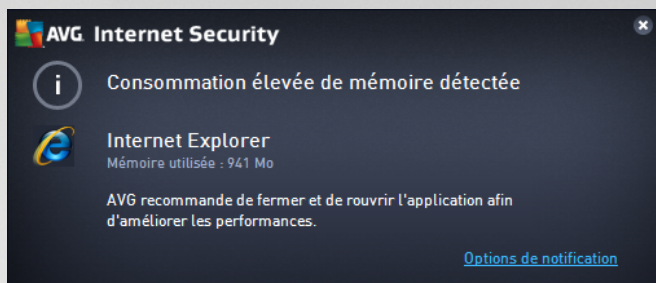
- **Ouvrir AVG** : cliquez pour ouvrir l'[interface utilisateur](#) d'**AVG Internet Security**.
- **Désactiver provisoirement la protection AVG** : permet de désactiver entièrement la protection offerte par le programme **AVG Internet Security**. Rappelez-vous que vous ne devez utiliser cette option qu'en cas d'absolue nécessité ! Dans la plupart des cas, il n'est pas nécessaire de désactiver **AVG Internet Security** avant d'installer un nouveau logiciel ou pilote, même si l'assistant d'installation ou le logiciel vous indique d'arrêter tous les programmes et applications s'exécutant sur le système et qui pourraient créer des interruptions inopinées lors du processus d'installation. Si vous êtes amené à désactiver provisoirement **AVG Internet Security**, vous devez le réactiver dès la fin de vos opérations. Si vous êtes connecté à Internet ou à un réseau alors que l'antivirus est désactivé, l'ordinateur est particulièrement vulnérable.
- **Analyse** : ouvre le menu contextuel des [analyses prédéfinies](#) ([Analyse complète](#) et [Analyse zones sélectionnées](#)) et permet de sélectionner et de lancer immédiatement l'analyse souhaitée.
- **Pare-Feu** : cliquez ici pour ouvrir le menu contextuel permettant un accès rapide à tous les [modes disponibles pour le Pare-feu](#). Sélectionnez un mode dans le menu et cliquez pour confirmer la modification du mode de pare-feu actuellement configuré.
- **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. Vous avez le choix entre les actions suivantes : *Définir la priorité pour toutes les analyses*, *Suspendre toutes les analyses* ou *Arrêter toutes les analyses*.
- **Corriger les performances** : cliquez pour lancer le composant [PC Analyzer](#).
- **Se connecter à AVG MyAccount** : ouvre la page d'accueil MyAccount dans laquelle vous pouvez gérer vos produits, acheter des solutions de protection supplémentaires, télécharger des fichiers d'installation, vérifier vos commandes et factures et mettre à jour vos informations personnelles.
- **Mise à jour** : lance une [mise à jour](#) immédiate.
- **Aide** : ouvre le fichier d'aide en première page.

## 5.7. AVG Advisor

**AVG Advisor** a été conçu pour détecter les problèmes susceptibles de ralentir votre ordinateur ou de le mettre en péril. Il recommande également une action permettant de remédier à la situation. Si vous sentez un ralentissement soudain de votre ordinateur (*navigation sur Internet, performances globales*), il n'est pas toujours évident d'en détecter la cause, ni de savoir comment résoudre le problème. C'est à cette étape qu'**AVG Advisor** intervient : Il affiche une notification dans la barre d'état du système, qui vous informe de l'origine probable du problème et propose des solutions pour le résoudre. **AVG Advisor** contrôle en permanence tous les processus s'exécutant sur votre ordinateur afin de détecter les éventuels problèmes et propose des conseils sur la manière d'éviter le problème.



**AVG Advisor** s'affiche sous la forme d'une fenêtre contextuelle au-dessus de la barre d'état système :



**AVG Advisor** surveille spécifiquement les éléments suivants :

- **L'état de tous les navigateurs Web actuellement ouverts.** Les navigateurs Web peuvent saturer la mémoire, en particulier lors de l'ouverture simultanée de multiples onglets ou fenêtres. Ils peuvent également consommer trop de ressources systèmes et donc ralentir votre ordinateur. En pareil cas, il est en général utile de redémarrer le navigateur.
- **Connexions poste à poste en cours d'exécution.** Suite à l'utilisation du protocole P2P pour le partage de fichiers, la connexion peut parfois rester active, exploitant une grande quantité de votre bande passante. La vitesse de la navigation sur Internet peut s'en ressentir.
- **Un réseau inconnu avec un nom familier.** Cela ne s'applique généralement qu'aux utilisateurs se connectant à divers réseaux, notamment à l'aide d'ordinateurs portables. Si un nouveau réseau inconnu porte le même nom qu'un réseau connu et fréquemment utilisé (*comme Maison ou MonWifi*), il peut y avoir confusion et vous pouvez vous connecter par accident à un réseau totalement inconnu et présentant des risques potentiels. **AVG Advisor** permet d'éviter cette situation en vous avertissant lorsque le nom connu correspond en fait à un nouveau réseau. Bien sûr, si vous décidez que le réseau inconnu est sécurisé, vous pouvez l'enregistrer dans une liste **AVG Advisor** de réseaux connus afin qu'il ne soit plus signalé à l'avenir.

Dans de tels cas de figure, **AVG Advisor** vous signale le problème qui risque de se produire et indique le nom et l'icône du processus ou de l'application à l'origine du conflit. **AVG Advisor** vous suggère également les mesures à prendre pour éviter ce problème.

### **Navigateurs pris en charge**

Cette fonction est compatible avec les navigateurs Web suivants : Internet Explorer, Chrome, Firefox, Opera, Safari.

## **5.8. AVG Accelerator**

**AVG Accelerator** permet une lecture vidéo en ligne plus fluide et facilite les téléchargements supplémentaires. Lorsque le processus d'accélération vidéo est en cours, une fenêtre contextuelle de la barre d'état vous en informe.



**AVG Internet Security** ✕

**i** Vrouuuuum !  
Nous accélérons votre flux vidéo.

[Options de notification](#)





## 6. Composants AVG

### 6.1. Protection de l'ordinateur


Le composant **Ordinateur** fournit deux services de sécurité principaux : **AntiVirus** et **Coffre-fort de données**.

- **AntiVirus** est un moteur d'analyse qui protège tous les fichiers, les zones système de l'ordinateur et les supports amovibles (*disque flash etc.*) et recherche les virus connus. Tout virus détecté sera bloqué, puis supprimé ou placé en [Quarantaine](#). Ce processus passe inaperçu, car la protection résidente s'exécute "en arrière-plan". AntiVirus a également recours à la méthode heuristique en utilisant les caractéristiques des virus pour analyser les fichiers. En d'autres termes, le service AntiVirus est en mesure de filtrer un virus inconnu si ce nouveau virus porte certaines caractéristiques de virus existants. **AVG Internet Security** est également en mesure d'analyser et de détecter des exécutables ou bibliothèques DLL qui peuvent se révéler dangereux pour le système (*divers types de spyware, adware etc.*). Par ailleurs, AntiVirus analyse la base de registre de votre système afin de rechercher toute entrée suspecte et les fichiers Internet temporaires. Il vous permet de traiter les éléments à risque de la même manière que les infections.
- **Un Coffre-fort de données** vous permet de créer des coffres-forts de données virtuels pour stocker des données importantes ou sensibles. Le contenu d'un Coffre-fort de données est chiffré et protégé par un mot de passe de votre choix. Ainsi, personne ne peut y accéder sans autorisation.




#### Commandes de la boîte de dialogue


Pour basculer d'une section à l'autre de la boîte de dialogue, il vous suffit de cliquer n'importe où dans le panneau du service correspondant. Le panneau s'affiche alors en surbrillance dans une couleur bleu plus clair. Dans chaque section de la boîte de dialogue, vous trouverez les commandes suivantes. Leur fonctionnalité est la même, quel que soit le service auquel elles appartiennent (*AntiVirus ou Coffre-fort de données*) :

 **Activé/Désactivé** : ce bouton ressemble à un feu tricolore et possède d'ailleurs une fonction



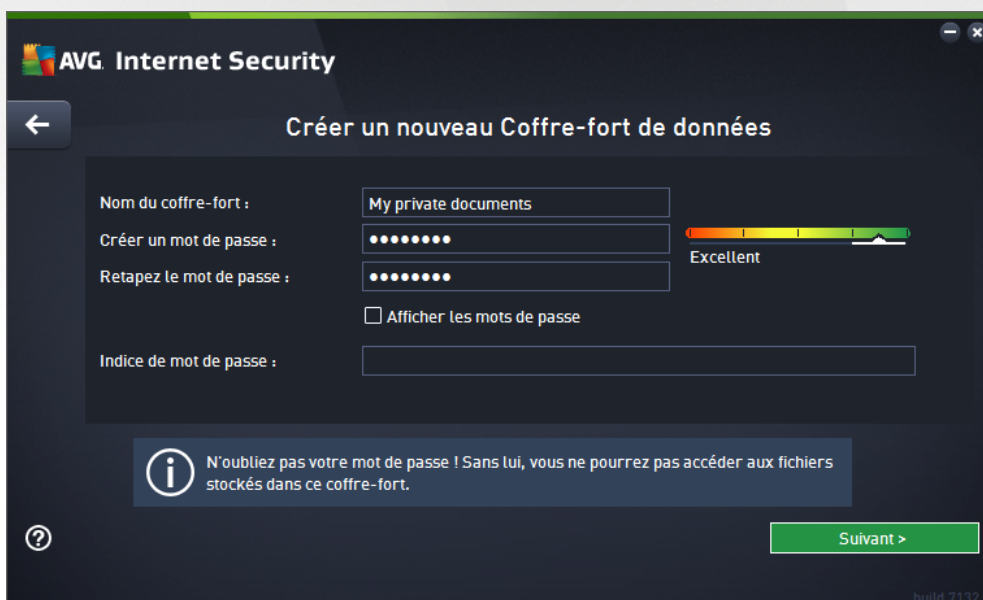
similaire. Cliquez dessus pour basculer d'une position à l'autre. La couleur verte signifie **Activé** et indique que le service AntiVirus est actif et complètement opérationnel. La couleur rouge signifie que ce service est **désactivé**. À moins que vous n'ayez une très bonne raison de désactiver ce service, nous vous conseillons vivement de conserver les paramètres par défaut pour toute la configuration de sécurité. Les paramètres par défaut garantissent une performance optimale de l'application et une sécurité maximale. Si, pour une raison ou une autre, vous devez désactiver ce service, vous serez averti du risque éventuel auquel vous vous exposez par un signe d'**avertissement** rouge, et, pendant ce temps, vos informations ne seront pas totalement protégées. **Veillez à réactiver ce service aussitôt que possible.**

 **Paramètres** : cliquez sur ce bouton pour être redirigé vers les [paramètres avancés](#) de l'interface. Dans la boîte de dialogue qui s'ouvre, vous pourrez configurer le service sélectionné, à savoir [AntiVirus](#). L'interface des paramètres avancés permet de modifier toute la configuration d'un service de sécurité au sein d'**AVG Internet Security**. Cette opération est réservée aux utilisateurs expérimentés.

 **Flèche** : utilisez la flèche verte située dans la partie supérieure gauche de la section de la boîte de dialogue pour retourner à l'[interface utilisateur principale](#) qui répertorie les composants.

### Comment créer votre coffre-fort de données

Dans la section **Coffre-fort de données** de la boîte de dialogue **Protection de l'ordinateur**, vous trouverez le bouton **Créer votre coffre-fort**. Cliquez sur le bouton pour ouvrir une nouvelle boîte de dialogue du même nom dans laquelle vous pouvez spécifier les paramètres de votre coffre-fort. Renseignez toutes les informations nécessaires et suivez les instructions de l'application.



Commencez par spécifier le nom de votre coffre-fort, puis créez un mot de passe fort :

- **Nom du coffre-fort** : pour créer un nouveau coffre-fort, vous devez d'abord choisir un nom approprié pour le reconnaître. Si vous partagez l'ordinateur avec d'autres membres de la famille, vous pouvez vouloir inclure votre nom ainsi que d'autres indications concernant le contenu du coffre-fort, par exemple *Emails de papa*.



- **Créer mot de passe / Retaper le mot de passe** : créez un mot de passe pour votre coffre-fort de données et saisissez-le dans les champs de texte respectifs. L'indicateur graphique situé à droite vous indiquera si votre mot de passe est faible (*relativement facile à pirater avec des logiciels spéciaux*) ou fort. Nous vous recommandons de choisir un mot de passe qui soit au moins de force moyenne. Vous pouvez renforcer la sécurité de votre mot de passe en utilisant des lettres majuscules, des chiffres, des nombres et d'autres caractères tels que des points ou des tirets. Pour être sûr que le mot de passe que vous saisissez est correct, activez la case **Afficher les mots de passe** (*assurez-vous que personne ne voit votre écran*).
- **Indice de mot de passe** : nous vous recommandons vivement de créer un indice de mot de passe qui vous permettra de vous souvenir de votre mot de passe, en cas d'oubli. Notez qu'un Coffre-fort de données permet de conserver vos fichiers en toute sécurité : l'accès n'est possible qu'en possédant le mot de passe ; il n'existe pas d'alternative. Si vous oubliez votre mot de passe, vous ne pourrez plus accéder à votre coffre-fort de données !

Lorsque vous avez renseigné toutes les données requises dans les champs de texte, cliquez sur **Suivant** pour poursuivre vers l'étape suivante :



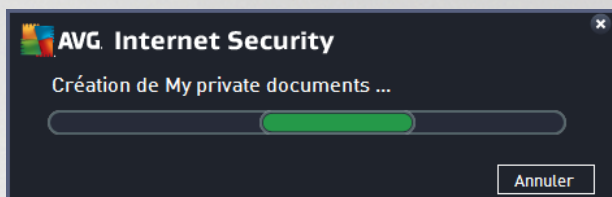
Cette boîte de dialogue fournit les options de configuration suivantes :

- **Emplacement** indique où le coffre-fort de données sera physiquement situé. Recherchez un emplacement approprié sur votre disque dur ou conservez l'emplacement prédéfini, qui est votre dossier *Documents*. Veuillez noter qu'une fois qu'un coffre-fort est créé, vous ne pouvez pas modifier son emplacement.
- **Taille** : vous pouvez prédéfinir la taille de votre coffre-fort de données, ce qui allouera l'espace nécessaire sur le disque. Cette valeur ne doit pas être trop petite (*pas assez d'espace pour vos besoins*), ni trop grande (*utilisation inutile d'un espace disque trop important*). Si vous savez déjà ce que vous souhaitez mettre dans le coffre-fort de données, vous pouvez placer tous les fichiers dans un dossier et utiliser le lien **Sélectionnez un dossier** pour calculer automatiquement la taille totale. Vous pourrez modifier ultérieurement cette taille en fonction de vos besoins.
- **Accès** : les cases à cocher de cette section vous permettent de créer des raccourcis pratiques vers votre coffre-fort de données.



### Comment utiliser votre coffre-fort de données

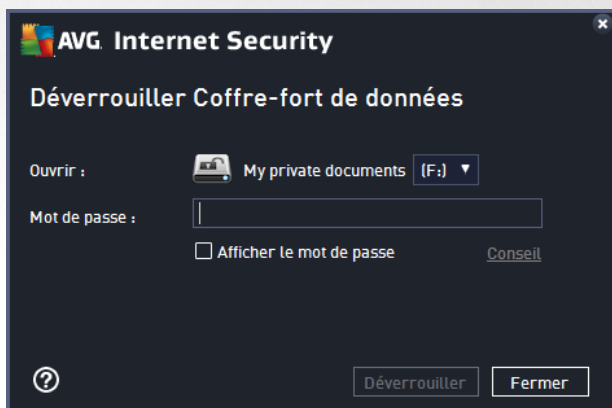
Une fois les paramètres sélectionnés, cliquez sur le bouton **Créer un coffre-fort**. Une nouvelle boîte de dialogue **Votre coffre-fort de données est maintenant prêt** s'affiche pour vous indiquer que vous pouvez désormais déposer des fichiers dans votre coffre-fort. À chaque tentative d'accès au coffre-fort, vous serez invité à le déverrouiller à l'aide du mot de passe que vous avez défini au préalable :



Pour utiliser votre coffre-fort de données, vous devez tout d'abord l'ouvrir. Pour ce faire, cliquez sur le bouton **Ouvrir maintenant**. À l'ouverture, le coffre-fort de données s'affiche en tant que nouveau disque virtuel sur votre ordinateur. Attribuez-lui la lettre de votre choix dans le menu déroulant (*vous pourrez choisir uniquement à partir des disques disponibles à ce moment-là*). En principe, vous n'êtes pas autorisé à choisir C (*attribuée en général à votre disque dur*), A (*lecteur de disquettes*) ou D (*lecteur de DVD*). Veuillez noter que vous pouvez choisir une autre lettre de disque disponible à chaque fois que vous déverrouillez un coffre-fort de données.

### Comment déverrouiller votre coffre-fort de données

Lors de la prochaine tentative d'accès au coffre-fort, vous serez invité à le déverrouiller à l'aide du mot de passe que vous avez défini au préalable :



Dans le champ, saisissez votre mot de passe pour vous autoriser vous-même, puis cliquez sur le bouton **Déverrouiller**. Si vous avez du mal à vous rappeler votre mot de passe, cliquez sur **Indice** pour afficher l'indice du mot de passe que vous avez défini lors de la création du coffre-fort de données. Le nouveau coffre-fort de données s'affichera dans l'aperçu de vos coffres-forts de données en tant que DÉVERROUILLÉ et vous pourrez ajouter/supprimer des fichiers selon vos besoins.



## 6.2. Protection de la navigation Web

La **protection de la navigation Web** se divise en deux services : **LinkScanner Surf-Shield** et **Bouclier Web**:

- **LinkScanner Surf-Shield** 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. **LinkScanner Surf-Shield n'est pas conçu pour la protection des plateformes serveur !**
- 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. 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. **Le Bouclier Web AVG n'est pas conçu pour la protection des plateformes serveur !**





### Commandes de la boîte de dialogue


Pour basculer d'une section à l'autre de la boîte de dialogue, il vous suffit de cliquer n'importe où dans le panneau du service correspondant. Le panneau s'affiche alors en surbrillance dans une couleur bleu plus clair. Dans chaque section de la boîte de dialogue, vous trouverez les commandes suivantes. Leur fonctionnalité est



la même, quel que soit le service auquel elles appartiennent (*LinkScanner Surf-Shield* ou *Bouclier Web*) :

 **Activé/Désactivé** : ce bouton ressemble à un feu tricolore et possède d'ailleurs une fonction similaire. Cliquez dessus pour basculer d'une position à l'autre. La couleur verte signifie **Activé** et indique que le service LinkScanner Surf-Shield ou Bouclier Web est actif et complètement opérationnel. La couleur rouge signifie que ce service est **désactivé**. À moins que vous n'ayez une très bonne raison de désactiver ce service, nous vous conseillons vivement de conserver les paramètres par défaut pour toute la configuration de sécurité. Les paramètres par défaut garantissent une performance optimale de l'application et une sécurité maximale. Si, pour une raison ou une autre, vous devez désactiver ce service, vous serez averti du risque éventuel auquel vous vous exposez par un signe d'**avertissement** rouge, et, pendant ce temps, vos informations ne seront pas totalement protégées. **Veillez à réactiver ce service aussitôt que possible.**

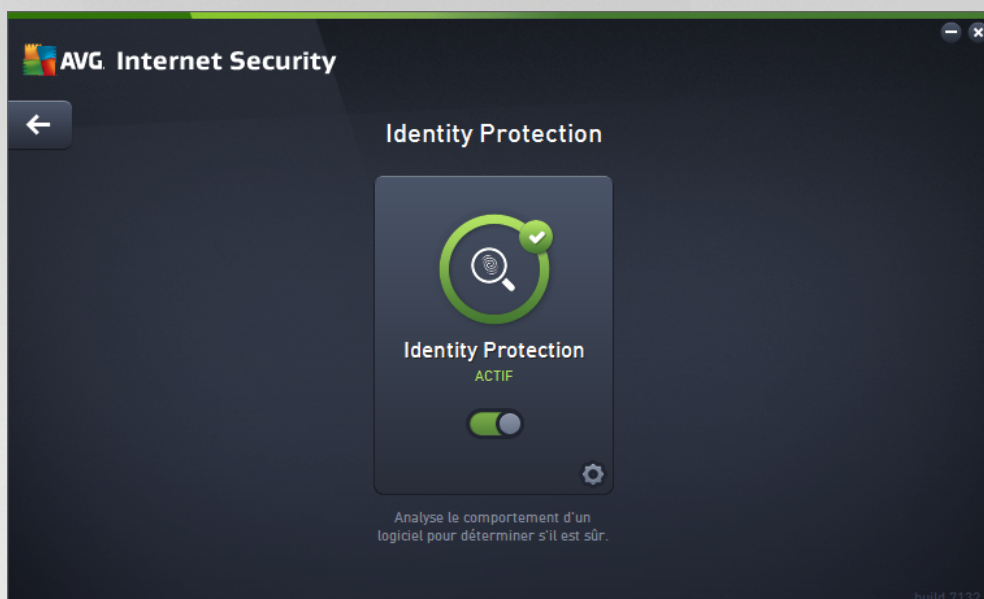
 **Paramètres** : cliquez sur ce bouton pour être redirigé vers les [paramètres avancés](#) de l'interface. Dans la boîte de dialogue qui s'ouvre, vous pourrez configurer le service sélectionné, soit [LinkScanner Surf-Shield](#) ou [Bouclier Web](#). L'interface des paramètres avancés permet de modifier toute la configuration d'un service de sécurité au sein d'**AVG Internet Security**. Cette opération est réservée aux utilisateurs expérimentés.

 **Flèche** : utilisez la flèche verte située dans la partie supérieure gauche de la section de la boîte de dialogue pour retourner à l'[interface utilisateur principale](#) qui répertorie les composants.

### 6.3. Identity Protection


Le **composant** Identity Protection exécute le service **Identity Shield** qui protège en permanence vos ressources numériques contre les menaces connues ou non qui existent sur Internet:


- **Identity Protection** est un service anti-malware qui vous protège contre tout type de programmes malveillants (*spyware, 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. Identity Protection est une application conçue pour empêcher les usurpateurs d'identité de voler vos mots de passe, coordonnées bancaires, numéros de carte de crédit et autres ressources numériques personnelles au moyen de toutes sortes de logiciels malveillants (*malware*) qui prennent pour cible votre ordinateur. Il vérifie que tous les programmes exécutés sur votre ordinateur ou sur le réseau partagé fonctionnent correctement. Identity Protection détecte et bloque de façon permanente les comportements suspects et protège votre ordinateur contre tous les nouveaux contenus malveillants. Identity Protection assure la protection en temps réel de votre ordinateur contre les menaces nouvelles et inconnues. Il contrôle l'ensemble des processus (*processus cachés y compris*) et plus de 285 comportements différents afin de déterminer si une activité malveillante est en cours sur votre système. Ainsi, il peut identifier des menaces non décrites dans la base de données virale. Lorsqu'un code inconnu s'introduit dans votre ordinateur, il est automatiquement analysé afin de vérifier s'il a un comportement malveillant, puis suivi. S'il s'avère que le fichier est malveillant, Identity Protection place le code en [Quarantaine](#) et annule les modifications apportées au système (*injections de code, modifications de registre, ouverture de ports etc.*). Vous n'avez pas besoin d'exécuter une analyse pour vous protéger. Cette technologie est proactive. Elle ne nécessite que de rares mises à jour et est toujours en mode de surveillance.



### Commandes de la boîte de dialogue

Dans la boîte de dialogue, vous trouverez les commandes suivantes :

 **Activé/Désactivé** : ce bouton ressemble à un feu tricolore et possède d'ailleurs une fonction similaire. Cliquez dessus pour basculer d'une position à l'autre. La couleur verte signifie **Activé** et indique que ce service de sécurité est actif et complètement opérationnel. La couleur rouge signifie que ce service est **désactivé**. À moins que vous n'ayez une très bonne raison de désactiver ce service, nous vous conseillons vivement de conserver les paramètres par défaut pour toute la configuration de sécurité. Les paramètres par défaut garantissent une performance optimale de l'application et une sécurité maximale. Si, pour une raison ou une autre, vous devez désactiver ce service, vous serez averti du risque éventuel auquel vous vous exposez par un signe d'**avertissement** rouge, et, pendant ce temps, vos informations ne seront pas totalement protégées. **Veillez à réactiver ce service aussitôt que possible.**

 **Paramètres** : cliquez sur ce bouton pour être redirigé vers l'interface des [paramètres avancés](#). Dans la boîte de dialogue qui s'ouvre, vous pourrez configurer le service sélectionné, par exemple [Identity Protection](#). L'interface des paramètres avancés permet de modifier toute la configuration d'un service de sécurité au sein d'**AVG Internet Security**. Cette opération est réservée aux utilisateurs expérimentés.

 **Flèche** : utilisez la flèche verte située dans la partie supérieure gauche de la section de la boîte de dialogue pour retourner à l'[interface utilisateur principale](#) qui répertorie les composants.

Malheureusement, le service Identity Alert n'est pas inclus dans **AVG Internet Security**. Si vous voulez utiliser ce type de protection, cliquez sur le bouton **Mettre à jour pour activer** et vous serez redirigé vers la page Web depuis laquelle vous pouvez acquérir la licence d'Identity Alert.

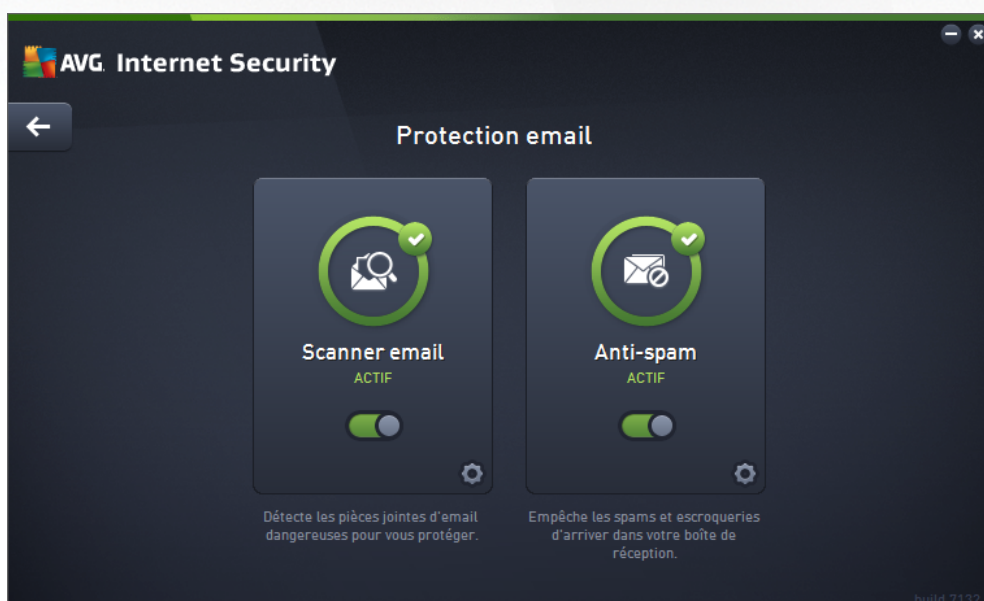
*Notez que même pour les versions AVG Premium Security, le service Identity Alert est uniquement disponible dans les régions suivantes : États-Unis, Royaume-Uni, Canada et Irlande.*



## 6.4. Protection email

Le composant **Protection email** comporte les deux services de sécurité suivants : **Scanner email** et **Anti-Spam** (le service Anti-Spam n'est accessible qu'avec les éditions Internet/Premium Security).

- **Scanner email** : 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 email, par exemple*) dans des formulaires en ligne, ces usagers contribuent à augmenter les risques d'attaque par email. Les sociétés utilisent généralement des comptes de messagerie à usage professionnel et appliquent des filtres anti-spam et autres moyens pour réduire ce risque. Le composant Protection email assure l'analyse de chaque email envoyé ou reçu. Lorsqu'un virus est détecté dans un message, il est immédiatement mis en [Quarantaine](#). Le composant permet également de filtrer les pièces jointes et d'ajouter un texte de certification aux messages dépourvus d'infection. **Scanner email n'est pas conçu pour les plateformes serveur !**
- **Anti-Spam** vérifie tous les emails entrants et marque les courriers indésirables comme « spam ». *Ce terme 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.* Le composant Anti-Spam est capable de modifier l'objet du message (*identifié comme du spam*) en ajoutant une chaîne spéciale. Il est ensuite très facile de filtrer vos messages dans votre client de messagerie. Le composant 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 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 votre [liste noire](#) (*pour systématiquement les considérer comme du spam*).










## Commandes de la boîte de dialogue

Pour basculer d'une section à l'autre de la boîte de dialogue, il vous suffit de cliquer n'importe où dans le panneau du service correspondant. Le panneau s'affiche alors en surbrillance dans une couleur bleu plus clair. Dans chaque section de la boîte de dialogue, vous trouverez les commandes suivantes. Leur fonctionnalité est la même, quel que soit le service auquel elles appartiennent (*Scanner email* ou *Anti-Spam*) :

 **Activé/Désactivé** : ce bouton ressemble à un feu tricolore et possède d'ailleurs une fonction similaire. Cliquez dessus pour basculer d'une position à l'autre. La couleur verte signifie **Activé** et indique que ce service de sécurité est actif et complètement opérationnel. La couleur rouge signifie que ce service est **désactivé**. À moins que vous n'ayez une très bonne raison de désactiver ce service, nous vous conseillons vivement de conserver les paramètres par défaut pour toute la configuration de sécurité. Les paramètres par défaut garantissent une performance optimale de l'application et une sécurité maximale. Si, pour une raison ou une autre, vous devez désactiver ce service, vous serez averti du risque éventuel auquel vous vous exposez par un signe d'**avertissement** rouge, et, pendant ce temps, vos informations ne seront pas totalement protégées. **Veillez à réactiver ce service aussitôt que possible.**

 **Paramètres** : cliquez sur ce bouton pour être redirigé vers les [paramètres avancés](#) de l'interface. Dans la boîte de dialogue qui s'ouvre, vous pourrez configurer le service sélectionné, soit [Scanner email](#) ou [Anti-Spam](#). L'interface des paramètres avancés permet de modifier toute la configuration d'un service de sécurité au sein d'**AVG Internet Security**. Cette opération est réservée aux utilisateurs expérimentés.

 **Flèche** : utilisez la flèche verte située dans la partie supérieure gauche de la section de la boîte de dialogue pour retourner à l'[interface utilisateur principale](#) qui répertorie les composants.

## 6.5. 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 des 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 et 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 par Internet ou le 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.

Dans **AVG Internet Security**, le **Pare-feu** contrôle tout le trafic passant par chaque port réseau 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, il 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.



## Le Pare-feu AVG n'est pas conçu pour protéger les plateformes serveur !

**Recommandation** : en règle générale, il est déconseillé d'utiliser plusieurs pare-feux 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 afin d'éviter des conflits entre AVG et ces programmes, ainsi que d'autres problèmes.



**Remarque** : après l'installation d'AVG Internet Security, le composant pare-feu peut nécessiter un redémarrage de l'ordinateur. Dans ce cas, une boîte de dialogue s'affiche pour vous en informer. Elle comporte le bouton **Redémarrer maintenant**. Le composant pare-feu est complètement activé une fois que l'ordinateur a été redémarré. De plus, la possibilité de saisie dans la boîte de dialogue est désactivée. Veuillez suivre les instructions et redémarrer votre ordinateur dès que possible !

## Modes Pare-feu disponibles

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 mode particulier. En d'autres termes, un mode Pare-feu est une configuration spécifique du composant Pare-feu. Vous pouvez utiliser plusieurs configurations prédéfinies de ce type.

- **Automatique** : ce mode Pare-feu gère tout le trafic réseau automatiquement. Vous n'aurez aucune décision à prendre. Le Pare-feu autorisera la connexion des applications connues et créera une règle permettant à chacune d'entre elles de se connecter ultérieurement. Pour les autres applications, le Pare-feu décidera si la connexion doit être autorisée ou bloquée en fonction de leur comportement. Aucune règle ne sera créée pour ces applications, qui seront contrôlées à chaque fois qu'elles tenteront de se connecter. Le mode Automatique est recommandé pour la majorité des utilisateurs, car il s'effectue discrètement.
- **Interactif** : ce mode est utile si vous souhaitez contrôler intégralement le trafic entre le réseau et votre ordinateur. Le Pare-feu contrôle le trafic et vous informe à chaque tentative de communication ou de transfert de données, vous laissant le choix d'autoriser ou de bloquer cette opération au moment



opportun. Réservé aux utilisateurs expérimentés.

- **Bloquer l'accès à Internet** : la connexion Internet est totalement bloquée, vous ne pouvez pas accéder à Internet et aucune personne externe n'a accès à votre ordinateur. Ce mode est réservé pour des périodes courtes et spécifiques.
- **Désactiver la protection du pare-feu (non recommandé)** : la désactivation du Pare-feu autorise la communication totale entre le réseau et votre ordinateur. Par conséquent, votre ordinateur est exposé aux attaques des pirates. Veuillez réfléchir attentivement avant d'utiliser cette option.

Notez qu'il existe également un mode automatique spécifique au sein du Pare-feu. Ce mode est toujours activé et protège votre ordinateur lorsque le composant [Ordinateur](#) ou [Identité](#) est désactivé. Dans un tel cas de figure, il autorise uniquement les applications connues et parfaitement sûres. Vous devrez choisir vous-même si les autres applications peuvent être ou non autorisées. Grâce à cette protection silencieuse, votre ordinateur reste à l'abri des attaques, même lorsque ces composants de protection sont désactivés.

**Il est fortement recommandé de ne jamais désactiver le pare-feu ! Néanmoins, si le besoin se présente et qu'il est primordial que vous désactiviez le composant Pare-feu, vous pouvez le faire en sélectionnant le mode Désactiver la protection pare-feu à partir de la liste des modes de pare-feu située au-dessus.**

## Commandes de la boîte de dialogue

Cette boîte de dialogue fournit une vue générale des informations de base sur l'état du composant Pare-feu :

- **Mode Pare-feu** : donne des informations sur le mode de pare-feu actuellement sélectionné. A l'aide du bouton **Modifier** situé en regard de ces informations, basculez dans l'interface des paramètres du [Pare-feu](#) pour passer à un autre mode (*pour obtenir une description des profils de Pare-feu et suivre les recommandations à ce sujet, reportez-vous au paragraphe précédent*).
- **Partage de fichiers et d'imprimantes** : indique l'état actuel de la disponibilité du partage de fichiers et d'imprimantes (*dans les deux directions*). Partager des fichiers et des imprimantes signifie partager tous les fichiers ou dossiers que vous signalez comme étant « Partagés » dans Windows, les unités de disque, les imprimantes, les scanners et autres appareils de ce type. Le partage de ces éléments n'est souhaitable qu'à l'intérieur d'un réseau que vous jugez sécurisé (*chez vous, au bureau ou à l'école, par exemple*). Toutefois, si vous êtes connecté à un réseau public (*WiFi d'un aéroport ou cybercafé, par exemple*), il est préférable de ne rien partager.
- **Connecté à** : fournit des informations sur le nom du réseau auquel vous êtes actuellement connecté. Sous Windows XP, le nom du réseau correspond à l'appellation que vous avez choisie pour ce réseau spécifique au moment de la connexion initiale. A partir de Windows Vista, le nom de réseau est automatiquement issu du Centre Réseau et partage.
- **Rétablir par défaut** : cliquez sur ce bouton pour remplacer la configuration actuelle du Pare-feu et rétablir la configuration par défaut selon la détection automatique.

Cette boîte de dialogue contient les commandes graphiques suivantes :



**Paramètres** : cliquez sur ce bouton pour ouvrir un menu contextuel comportant deux options :

- **Paramètres avancés** : cette option vous redirige vers [l'interface des paramètres du Pare-feu](#) afin



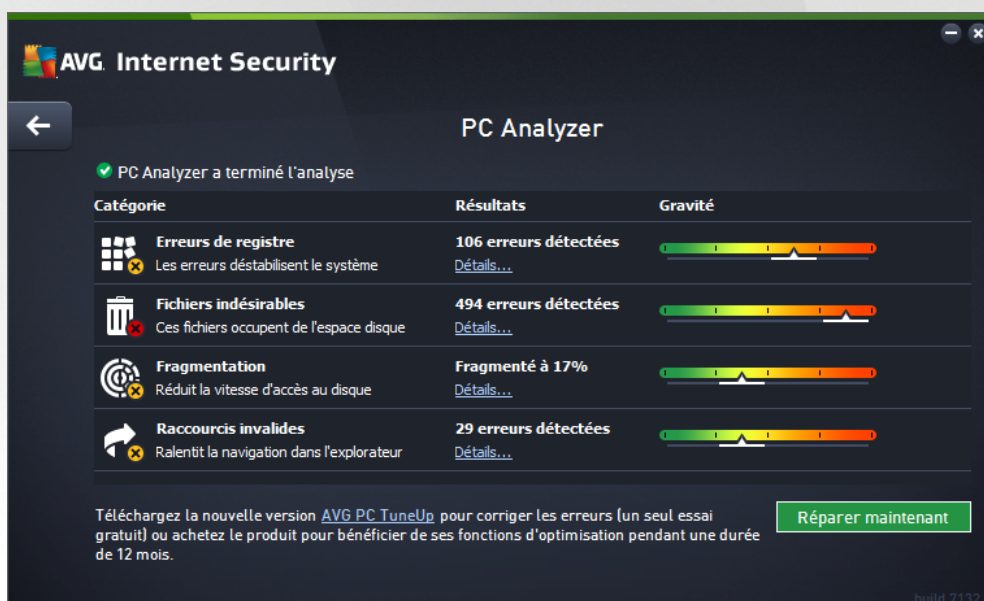
de modifier toute la configuration du Pare-feu. Néanmoins, il est vivement conseillé de ne pas modifier la configuration si vous n'êtes pas un utilisateur expérimenté !

- o **Supprimer la protection du Pare-feu** : en sélectionnant cette option, vous allez désinstaller le composant Pare-feu, ce qui risque d'affaiblir votre protection. Si vous souhaitez malgré tout supprimer le composant Pare-feu, confirmez votre choix et le composant sera complètement désinstallé.

← **Flèche** : utilisez la flèche verte située dans la partie supérieure gauche de la section de la boîte de dialogue pour retourner à l'[interface utilisateur principale](#) qui répertorie les composants.

## 6.6. PC Analyzer

Le composant **PC Analyzer** est un outil avancé d'analyse approfondie et de correction du système, permettant d'améliorer la vitesse et les performances globales de votre ordinateur. Il se lance via le bouton **+ de performances** situé dans la [boîte de dialogue interface utilisateur principale](#) ou via la même option listée dans le menu contextuel de l'[icône AVG de la barre d'état](#). Vous serez en mesure de suivre la progression de l'analyse et d'examiner ses résultats dans le graphique qui apparaîtra :



Il est possible d'analyser les catégories suivantes : erreurs de registre, fichiers indésirables, fragmentation et raccourcis endommagés.

- **Erreurs du registre** indique le nombre d'erreurs dans le Registre de Windows susceptibles de ralentir l'ordinateur ou de provoquer l'apparition de messages d'erreur.
- **Fichiers indésirables** indique le nombre de fichiers qui utilisent de l'espace disque et dont vous pouvez sans doute vous passer. Généralement, il s'agit de nombreux types de fichiers temporaires et de 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 en différents endroits du disque physique.



- **Raccourcis endommagés** indique les raccourcis qui ne fonctionnent plus, mènent à des emplacements inexistantes etc.

Les résultats indiquent le nombre et le type de défaillances système détectées en fonction de chaque catégorie évaluée. Les résultats d'analyse se présentent également sous la forme d'un graphique (axe de la colonne **Gravité**).

### Boutons de commande

- **Arrêter l'analyse** (à l'écran alors que l'analyse est en cours) : ce bouton permet d'arrêter l'analyse de votre ordinateur.
- **Réparer maintenant** (à l'écran une fois que l'analyse est terminée) : malheureusement, la fonction du PC Analyzer dans **AVG Internet Security** est limitée à l'analyse actuelle du statut de votre PC. AVG fournit toutefois un outil avancé d'analyse approfondie et de correction du système, permettant d'améliorer la vitesse et les performances globales de votre ordinateur. Cliquez sur le bouton pour être redirigé vers le Site Web dédié et obtenir plus d'informations.

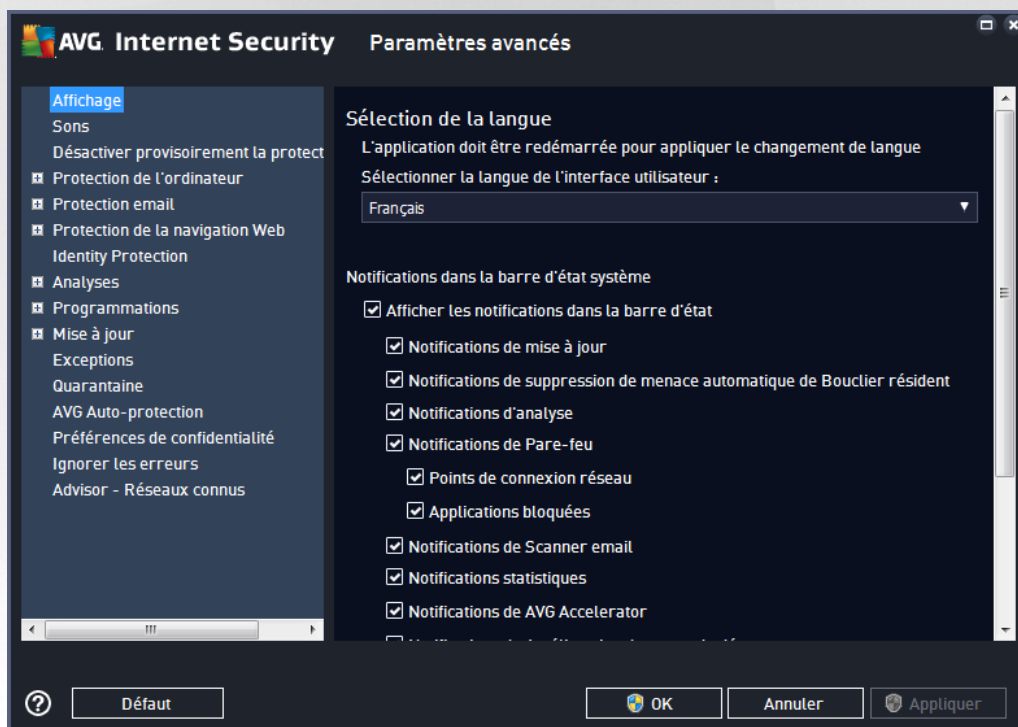


## 7. Paramètres avancés d'AVG

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

### 7.1. Affichage

Le premier élément de l'arborescence de navigation, **Affichage**, porte sur les paramètres généraux de l'**AVG Internet Security** [interface utilisateur](#) et fournit quelques options essentielles du comportement de l'application :



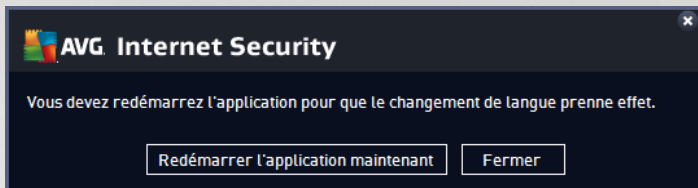
#### Sélection de la langue

Dans la section **Sélection de la langue**, vous pouvez sélectionner la langue de votre choix depuis le menu déroulant. La langue sélectionnée sera valable pour tous les composants de l'[interface utilisateur](#) d'**AVG Internet Security**. Le menu déroulant ne propose que les langues que vous avez sélectionnées au cours du processus d'installation en plus de l'anglais (*l'anglais étant toujours installé par défaut*). Pour terminer le passage d'**AVG Internet Security** vers une autre langue, il faut redémarrer l'application. Pour ce faire, procédez comme suit :

- Dans le menu déroulant, sélectionnez la langue dans laquelle vous voulez utiliser l'application
- Confirmez votre sélection en appuyant sur le bouton **Appliquer** (angle inférieur droit de la boîte de dialogue)



- Appuyez sur le bouton **OK** pour confirmer
- Une nouvelle boîte de dialogue vous informe que pour modifier la langue de l'application, vous devez redémarrer **AVG Internet Security**
- Appuyez sur le bouton **Redémarrer AVG maintenant** pour confirmer le redémarrage du programme, puis patientez jusqu'à ce que le changement de langue soit effectif :



### Notifications de la barre d'état

Dans cette section, vous pouvez supprimer l'affichage de notifications dans la barre d'état indiquant l'état de l'application **AVG Internet Security**. Par défaut, l'affichage des notifications dans la barre d'état est autorisé. Il est vivement recommandé de conserver cette configuration. Les notifications système fournissent des informations sur le lancement de l'analyse ou du processus de mise à jour, et sur la modification de l'état d'un composant **AVG Internet Security**. Il est vivement conseillé de lire attentivement ces notifications.

Cependant, si pour une raison quelconque vous préférez ne pas recevoir ce type d'information ou si vous ne voulez recevoir que certaines notifications (*liées à un composant AVG Internet Security spécifique*), vous pouvez définir et préciser vos préférences en activant ou en désactivant les options suivantes :

- **Afficher les notifications dans la barre d'état** (*option activée par défaut*) : toutes les notifications s'affichent par défaut. Décochez cette option pour désactiver complètement l'affichage de toutes les notifications dans la barre d'état. Lorsqu'elle est active, vous pouvez sélectionner les notifications qui doivent s'afficher :
  - **Notifications de mise à jour** (*option activée par défaut*) : indiquez si les informations concernant le lancement, la progression et la finalisation du processus de mise à jour d'**AVG Internet Security** doivent être affichées.
  - **Notifications de suppression automatique des menaces du Bouclier résident** (*option activée par défaut*) : indiquez si les informations sur les processus d'enregistrement, de copie et d'ouverture de fichier doivent être affichées ou supprimées (*cette configuration apparaît uniquement si l'option Réparer automatiquement du Bouclier résident est activée*).
  - **Notifications d'analyse** (*option activée par défaut*) : indiquez si les informations sur le lancement automatique de l'analyse programmée, sa progression et ses résultats doivent être affichées.
  - **Notifications du Pare-feu** (*option activée par défaut*) : indiquez si les informations concernant les processus et l'état du Pare-feu doivent être affichées (par exemple, les avertissements sur l'activation/la désactivation d'un composant, les éventuels goulets d'étranglement, etc.). Deux autres options spécifiques sont disponibles dans cet élément (*pour une description détaillée de ces options, consultez le chapitre [Pare-feu](#) de ce document*):
    - **Points de connexion réseau** (*désactivé par défaut*) : lors de la connexion à un réseau, le



Pare-feu indique s'il connaît le réseau et comment le partage de fichiers et d'imprimantes sera défini.

- **Applications bloquées** (*activé par défaut*) : lorsqu'une application inconnue ou suspecte tente de se connecter à un réseau, le Pare-feu bloque la tentative et affiche une notification. Cela permet de vous tenir informé ; nous vous recommandons donc de toujours laisser cette fonction activée.

- **Notifications du [Scanner email](#)** (*option activée par défaut*) : indiquez si les informations sur l'analyse de tous les messages entrants et sortants doivent être affichées.
- **Informations statistiques** (*option activée par défaut*) : laissez la case cochée pour permettre l'affichage régulier d'informations statistiques dans la barre des tâches.
- **Notifications d'AVG Accelerator** (*option activée par défaut*) : indiquez si les informations sur les activités d'**AVG Accelerator** doivent être affichées. Le service **AVG Accelerator** permet d'obtenir une lecture vidéo en ligne plus fluide et facilite les téléchargements supplémentaires.
- **Notifications d'amélioration du temps de démarrage** (*option désactivée par défaut*) : indiquez si vous souhaitez être informé de l'accélération du temps de démarrage de votre ordinateur.
- **Notifications d'AVG Advisor** (*option activée par défaut*) : indiquez si les informations sur les activités d' [AVG Advisor](#) doivent être affichées dans le panneau contextuel de la barre d'état système.

## Mode jeu

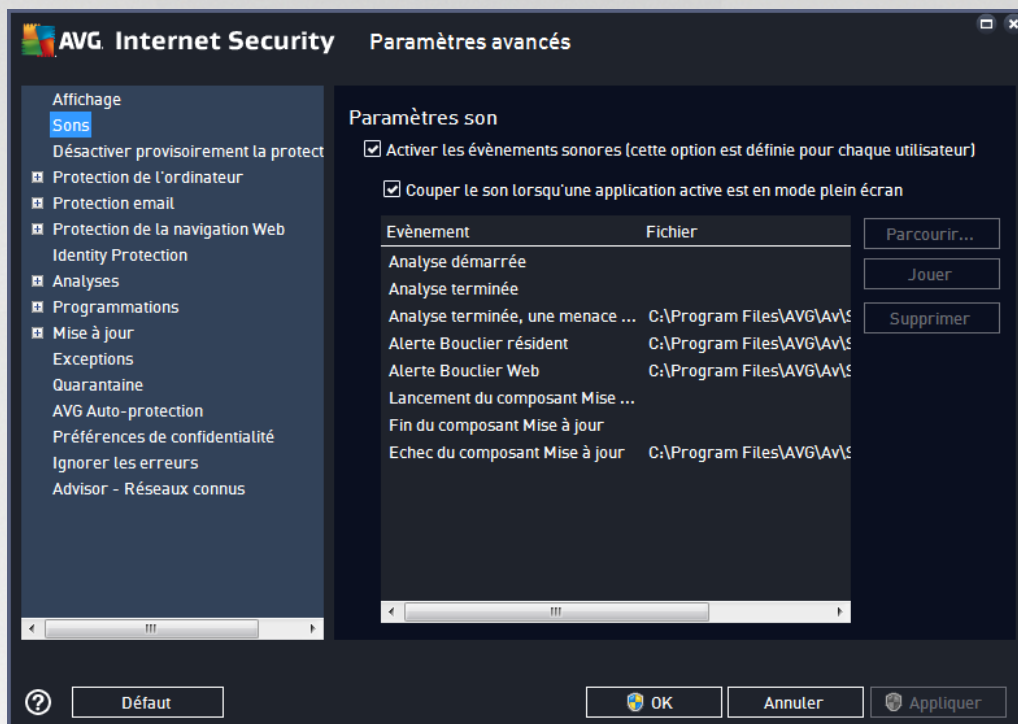
Cette fonction est conçue pour des applications plein écran pour lesquelles les bulles d'informations AVG (*qui s'affichent après le démarrage d'une analyse programmée*) seraient perturbantes (*risque de réduction de la fenêtre de l'application ou de corruption des images*). Pour éviter ce type de problème, il est recommandé de cocher la case **Activer le mode jeu lorsqu'une application est exécutée en mode plein écran** (*paramètre par défaut*).





## 7.2. Sons

La boîte de dialogue **Paramètres de son** vous permet d'indiquer si vous souhaitez ou non qu'une notification sonore vous signale certaines actions d'**AVG Internet Security**.



Ces paramètres concernent uniquement l'utilisateur actuel. Autrement dit, chaque utilisateur de l'ordinateur peut définir ses propres paramètres audio. Pour autoriser les notifications sonores, cochez l'option **Activer les événements sonores** (option activée par défaut) pour activer la liste d'actions correspondantes. Vous pouvez également activer l'option **Couper le son lorsqu'une application active est en mode plein écran** afin de supprimer les notifications sonores susceptibles de vous déranger (voir aussi la section [Mode jeu du chapitre Paramètres avancés/Affichage](#) de ce document).

### Boutons de commande

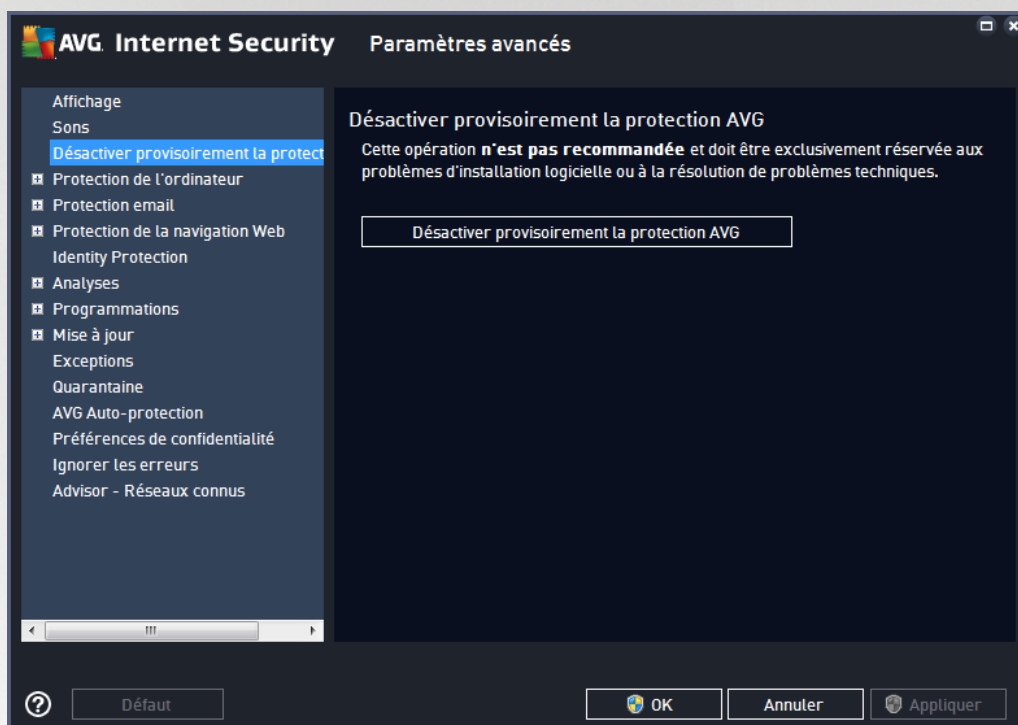
- **Parcourir...** : après avoir sélectionné un évènement dans la liste, cliquez sur le bouton **Parcourir** pour rechercher dans votre disque le fichier audio à lui associer. (Notez que seuls les sons \*.wav sont pris en charge pour l'instant !)
- **Jouer** : pour écouter le son sélectionné, mettez en surbrillance l'évènement dans la liste, puis cliquez sur le bouton **Jouer**.
- **Supprimer** : cliquez sur ce bouton pour supprimer le son associé à un évènement.



### 7.3. 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**.

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



Dans la plupart des cas, il n'est **pas nécessaire** de désactiver **AVG Internet Security** avant d'installer un nouveau logiciel ou pilote, même si l'assistant d'installation ou le logiciel vous indique d'arrêter tous les programmes et applications s'exécutant sur le système et qui pourraient créer des interruptions inopinées lors du processus d'installation. En cas de problème durant l'installation, tentez de [désactiver la protection résidente](#) (dans la boîte de dialogue liée, commencez par désélectionner **Activer Bouclier résident**). Si vous êtes amené à désactiver provisoirement **AVG Internet Security**, vous devez le réactiver dès la fin de vos opérations. Si vous êtes connecté à Internet ou à un réseau alors que l'antivirus est désactivé, l'ordinateur est particulièrement vulnérable.



## Désactivation de la protection AVG

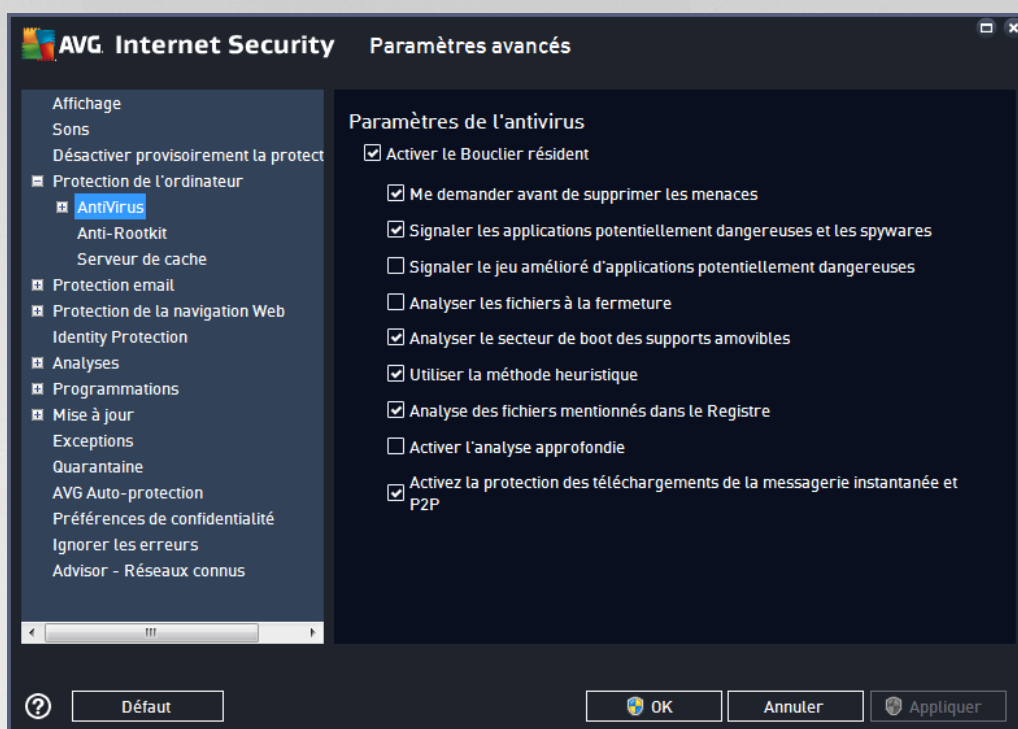
Cochez la case **Désactiver provisoirement la protection AVG**, puis cliquez sur **Appliquer** pour confirmer votre choix. Dans la nouvelle boîte de dialogue **Désactiver provisoirement la protection AVG**, indiquez la durée de la désactivation d'**AVG Internet Security**. Par défaut, la protection est désactivée pendant 10 minutes, ce qui vous laisse suffisamment de temps pour effectuer les manipulations courantes (l'installation d'un nouveau logiciel, par exemple). Vous pouvez opter pour un délai plus long, mais cette option est déconseillée lorsqu'elle n'est pas absolument nécessaire. A la fin de la durée spécifiée, tous les composants désactivés sont automatiquement réactivés. Au maximum, la protection AVG peut être désactivée jusqu'au redémarrage de l'ordinateur. Il est également possible de désactiver le composant **Pare-feu** dans la boîte de dialogue **Désactiver provisoirement la protection AVG**. Pour ce faire, cochez la case en regard de **Désactiver la protection du Pare-feu**.



## 7.4. Protection de l'ordinateur

### 7.4.1. AntiVirus

Les composants **AntiVirus** et **Bouclier résident** protègent en permanence votre ordinateur de tous les types de virus, spyware et malware connus (*y compris des programmes malveillants dits dormants ou inactifs, c'est-à-dire téléchargés mais pas encore actifs*).



Dans la boîte de dialogue **Paramètres du Bouclier résident**, il est possible d'activer ou de désactiver la protection résidente en cochant ou en désélectionnant la case **Activer le Bouclier résident** (cette option est activée par défaut). En outre, vous pouvez sélectionner les options de protection résidente à activer :

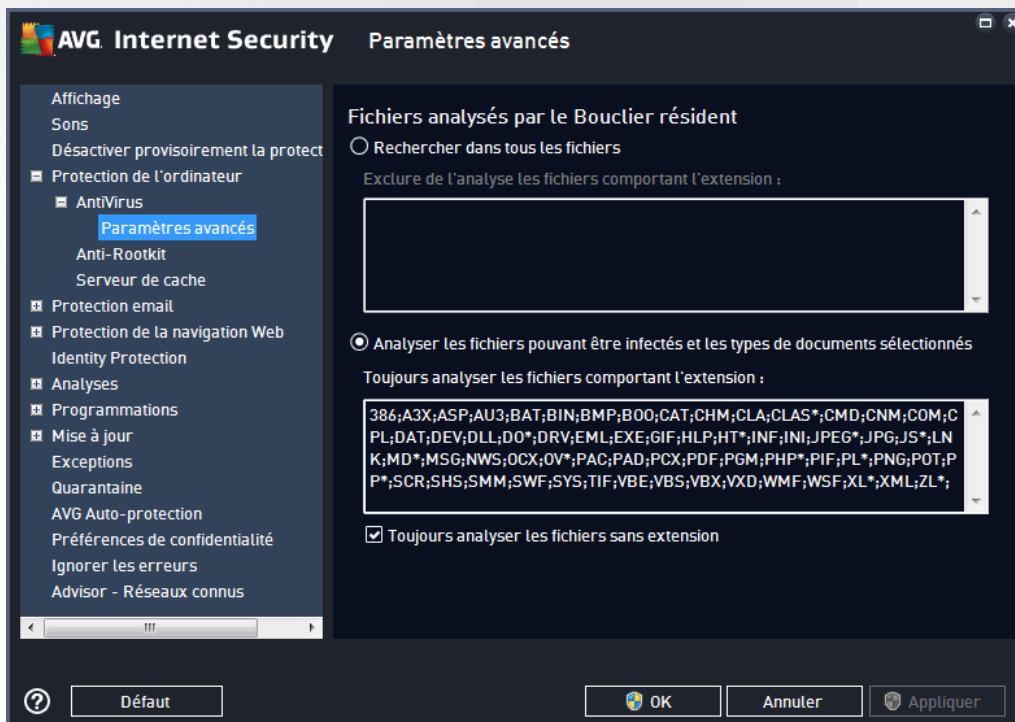
- **Me demander avant de supprimer les menaces** (option activée par défaut) : cochez cette case pour vous assurer que le Bouclier résident n'exécutera aucune action automatiquement. Il affichera plutôt une boîte de dialogue décrivant la menace identifiée, qui vous permettra de décider de l'action à effectuer. Si vous ne cochez pas la case, **AVG Internet Security** réparera automatiquement l'infection et, si cette opération n'est pas possible, l'objet sera mis en [Quarantaine](#).
- **Signaler les programmes potentiellement dangereux et les spyware** (option activée par défaut) : cochez cette case pour activer la recherche de spyware et de virus. Les spyware désignent une catégorie de programmes malveillants : 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 ordinateur.
- **Signaler le jeu amélioré de programmes potentiellement dangereux** (option désactivée par défaut) : l'indication permet de détecter les jeux étendus de spyware 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 utilisés à des fins malveillantes. Il s'agit d'une mesure supplémentaire visant à améliorer la sécurité de votre ordinateur. 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 ou 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) : cochez cette



option pour analyser la présence de menaces dans les secteurs d'amorçage des disques amovibles, des disques durs externes et des disques flash USB.

- **Utiliser la méthode heuristique** (option activée par défaut) : l'analyse heuristique sert de moyen de détection (émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel).
- **Analyse des 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 prochain démarrage de l'ordinateur.
- **Activer l'analyse approfondie** (option désactivée par défaut) : dans certaines situations (cas d'extrême 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.
- **Activer la protection de la Messagerie Instantanée et des téléchargements P2P** (option activée par défaut) : cochez cette case pour vérifier que la communication via la messagerie instantanée (par exemple AIM, Yahoo!, ICQ, Skype, MSN Messenger, ...) et les données téléchargées grâce aux réseaux de poste à poste (réseaux permettant des connexions directes entre les clients, sans passer par un serveur, qui sont potentiellement dangereux et principalement utilisés pour partager des fichiers de musique) ne contiennent aucun virus.

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) :



Cochez la case correspondante pour décider si vous voulez **Rechercher dans tous les fichiers** ou **Analyser**

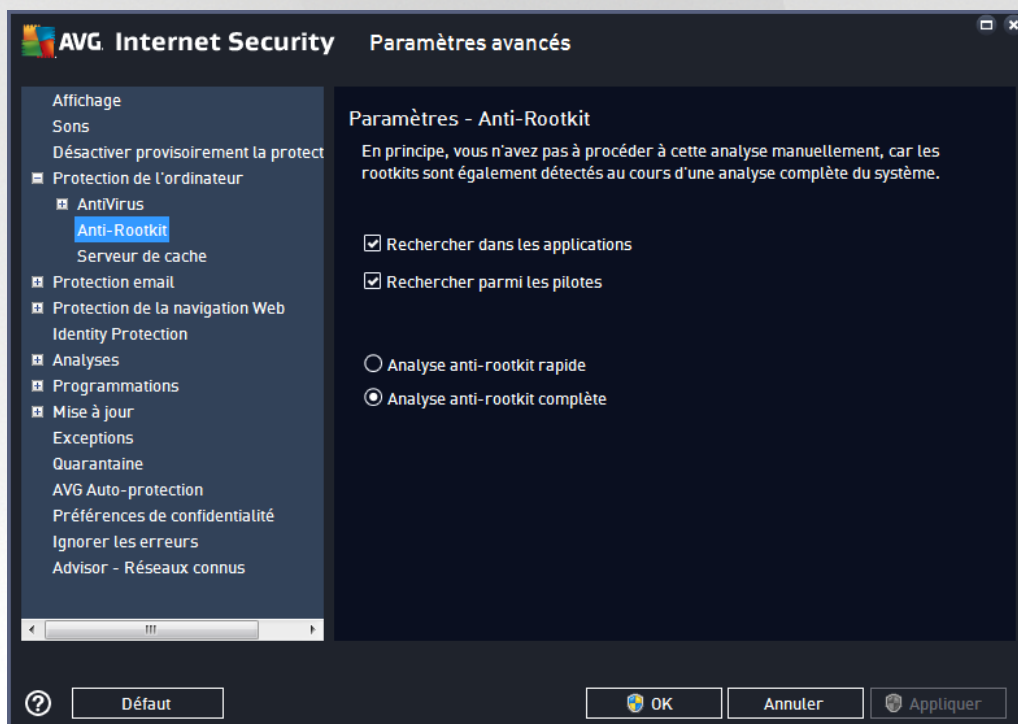


**les fichiers pouvant être infectés et les types de documents sélectionnés.** Pour accélérer le processus d'analyse tout en bénéficiant d'un niveau maximal de protection, il est recommandé de conserver les paramètres par défaut. De cette façon, seuls les fichiers susceptibles d'être infectés seront analysés. Dans la section correspondante de la boîte de dialogue, vous pourrez également modifier la liste d'extensions répertoriant les fichiers inclus dans l'analyse.

Cochez la case **Toujours analyser les fichiers sans extension** (activée par défaut) pour vous assurer que les fichiers sans extension, et dont le format est inconnu, sont également analysés par le Bouclier résident. Nous vous recommandons de garder activée cette fonction, car les fichiers dépourvus d'extension sont suspects.

### 7.4.2. Anti-Rootkit

Dans la boîte de dialogue **Paramètres Anti-Rootkit**, vous pouvez modifier la configuration du service **Anti-Rootkit** et certains paramètres de l'analyse anti-rootkit. L'analyse anti-rootkit est un processus par défaut inclus dans l'[Analyse complète de l'ordinateur](#) :



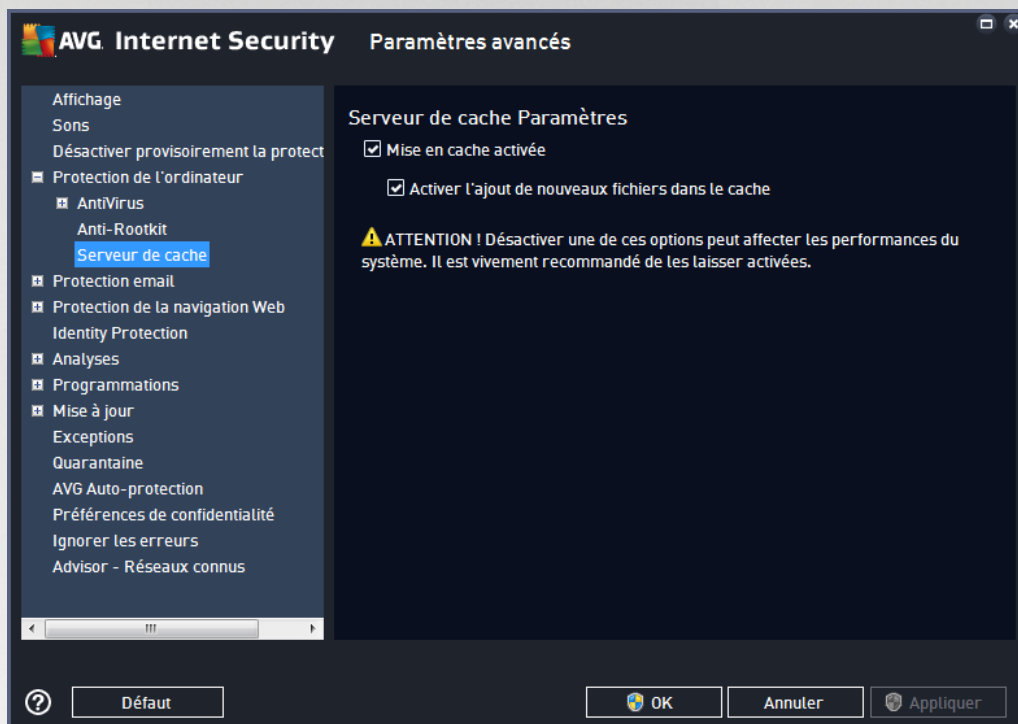
**Rechercher dans les applications** et **Rechercher parmi les pilotes** vous permettent de préciser en détail les éléments à inclure dans l'analyse anti-rootkit. Ces paramètres sont destinés à des utilisateurs expérimentés ; nous vous recommandons de conserver toutes les options actives. Vous pouvez 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 généralement*)
- **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*)



### 7.4.3. Serveur de cache

La **boîte de dialogue Paramètres du serveur de cache** porte sur le processus de serveur de cache qui est conçu pour accélérer tous les types d'analyse par **AVG Internet Security** :



Le serveur de cache recueille et conserve les informations relatives aux fichiers fiables (*un fichier est considéré comme fiable s'il comporte une signature numérique provenant d'une source fiable*). Par la suite, ces fichiers sont automatiquement considérés comme étant fiables et ne sont pas analysés de nouveau ; ils sont donc ignorés lors des analyses.

La boîte de dialogue **Paramètres du serveur de cache** comporte les options de configuration suivantes :

- **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. Veuillez noter que l'analyse risque de durer plus longtemps et que les performances de l'ordinateur risquent d'en être diminuées étant donné que chaque fichier en cours d'utilisation fera d'abord l'objet d'une analyse antivirus et anti-spyware.
- **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.

**A moins que vous n'ayez une très bonne raison de désactiver le serveur de cache, nous vous conseillons fortement de conserver les paramètres par défaut et de laisser les deux options activées ! Si vous ne le faites pas, vous risqueriez de subir une baisse de la vitesse et des performances du système.**

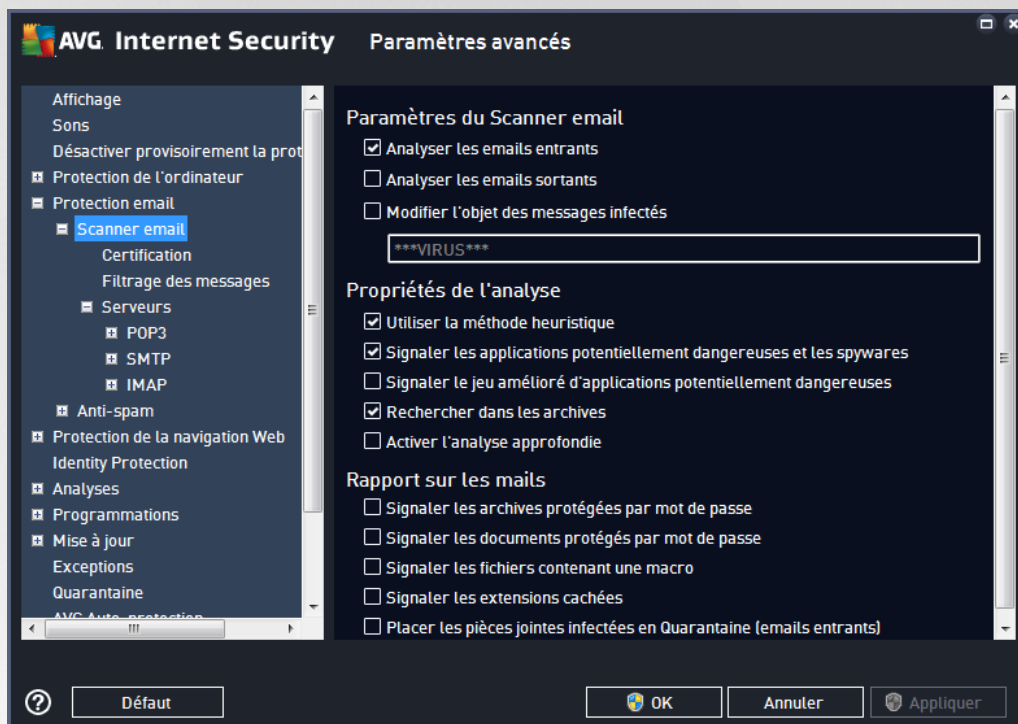


## 7.5. Scanner email

Dans cette section, vous pouvez modifier de manière approfondie la configuration des composants [Scanner email](#) et [Anti-Spam](#) :

### 7.5.1. Scanner email

La boîte de dialogue **Scanner email** comporte trois sections :



### Analyse des emails

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

- **Analyser le courrier entrant** (*option activée par défaut*) : cette option permet d'activer ou de désactiver l'analyse des emails 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 emails envoyés par votre compte
- **Modifier l'objet des messages infectés** (*option désactivée par défaut*) : si vous voulez être averti du fait que le message analysé a été détecté en tant que message infecté, cochez cette case et indiquez le texte à afficher dans le champ prévu à cet effet. Ce texte sera alors inséré dans le champ "Objet" pour chaque email infecté détecté 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 emails. 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 spyware** (*option activée par défaut*) : cochez cette case pour activer la recherche de spyware et de virus. Les spyware désignent une catégorie de programmes malveillants : 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 ordinateur.
- **Signaler le jeu amélioré de programmes potentiellement dangereux** (*option désactivée par défaut*) : l'indication permet de détecter les jeux étendus de spyware 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 utilisés 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 certaines situations (*par exemple, en cas de suspicion de présence d'un virus ou d'une attaque 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

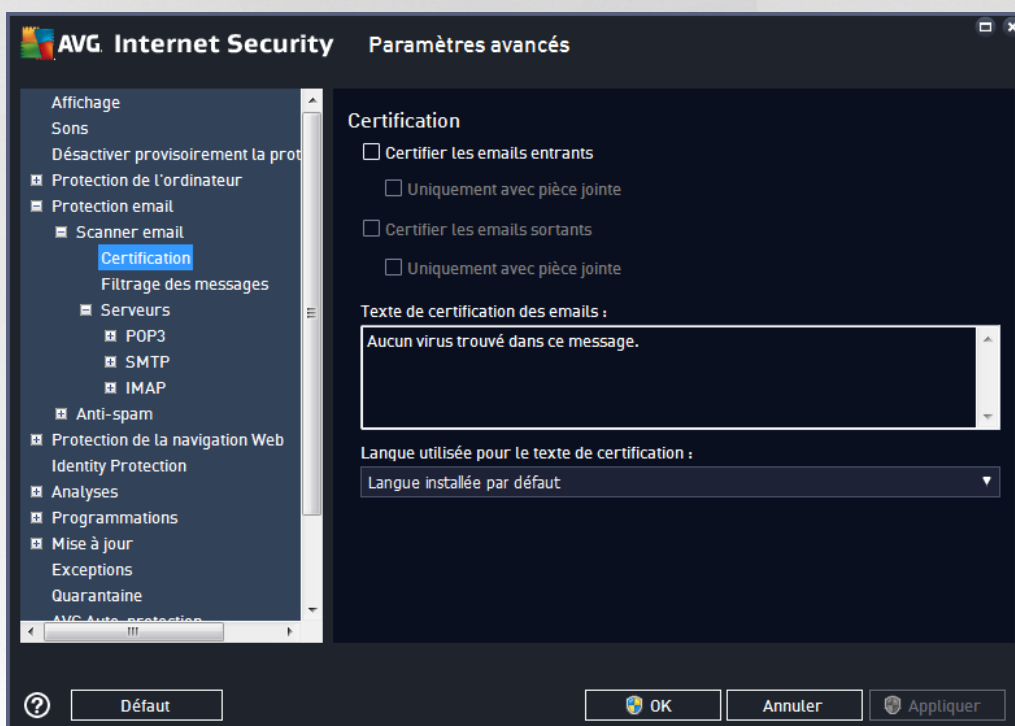
Dans cette section, vous pouvez définir des rapports supplémentaires sur les fichiers potentiellement dangereux ou suspects. Veuillez noter qu'aucun avertissement ne sera affiché, seul un texte de certification sera ajouté à la fin du message et tous les rapports associés seront recensés dans la boîte de dialogue [Détection du Scanner email](#).

- **Signaler les archives protégées par mot de passe** : les archives (*ZIP, RAR etc.*) protégées par mot de passe ne peuvent pas faire l'objet d'une analyse virale. Cochez cette option pour les signaler comme étant potentiellement dangereuses.
- **Signaler les documents protégés par mot de passe** : documents qui sont protégés par mot de passe et qui, à ce titre, ne peuvent pas faire l'objet d'une recherche virale. Cochez cette option 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*). À ce titre, une macro peut contenir des instructions potentiellement dangereuses. Vous pouvez cocher la case pour vous assurer que les fichiers contenant des macros seront signalés comme étant suspects.
- **Signaler les extensions cachées** : les extensions masquées peuvent afficher un fichier exécutable suspect comme "objet.txt.exe" sous la forme d'un fichier texte inoffensif de type "objet.txt". Cochez cette option pour signaler ces fichiers comme étant potentiellement dangereux.



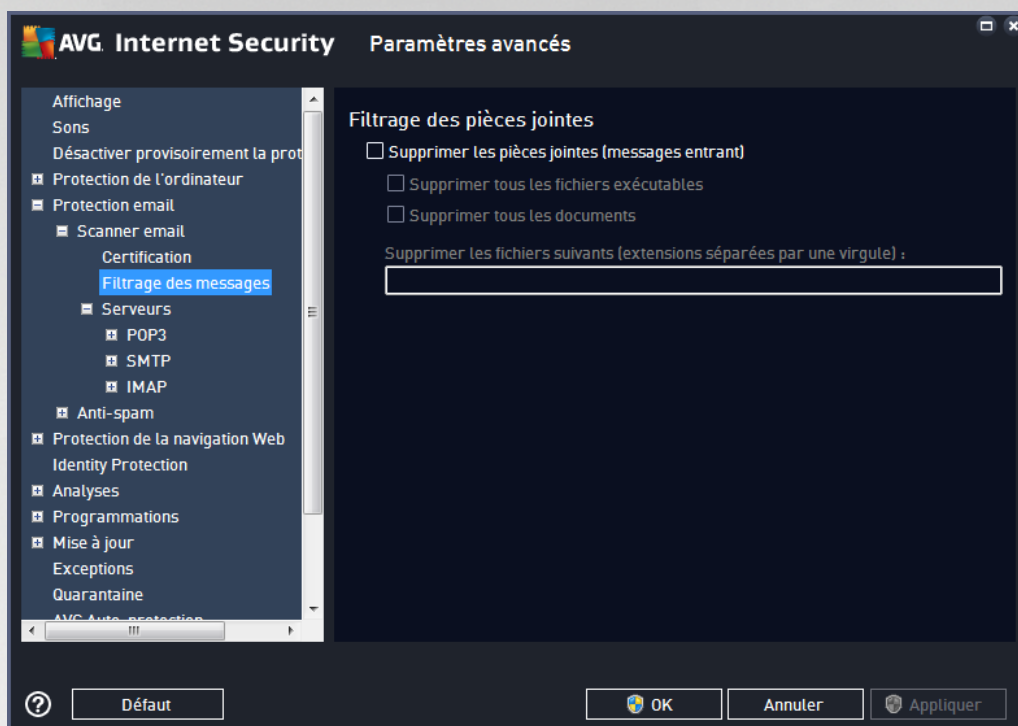
- **Placer les pièces jointes infectées en Quarantaine** : indiquez si vous voulez être averti par email lorsque l'analyse d'un email révèle la présence d'une archive protégée par mot de passe, d'un document protégé par mot de passe, d'une macro contenant un fichier et/ou d'un fichier dont l'extension est masquée. En l'occurrence, définissez si l'objet détecté doit être placé en [Quarantaine](#).

Dans la boîte de dialogue **Certification**, vous pouvez cocher des cases spécifiques pour décider si vous voulez certifier vos messages entrants (**Certifier les messages entrants**) et/ou vos messages sortants (**Certifier les messages sortants**). Pour chacune de ces options, vous pouvez en outre définir le paramètre **Avec pièces jointes uniquement** afin que la certification ne concerne que les emails comportant une pièce jointe :



Par défaut, le texte de certification consiste en un message simple indiquant qu'*Aucun virus n'a été détecté dans ce message*. Cependant, il est possible de développer ou de modifier cette information en fonction de vos besoins : rédigez le texte de certification de votre choix dans le champ **Texte de certification des messages électroniques**. Dans la section **Langue utilisée pour le texte de certification des messages électroniques**, vous pouvez en outre définir la langue dans laquelle la partie automatiquement générée de la certification (*Aucun virus n'a été détecté dans ce message*) doit être affichée.

**Remarque** : souvenez-vous que seul le texte par défaut sera affiché dans la langue choisie, mais votre texte personnalisé ne sera pas traduit automatiquement !



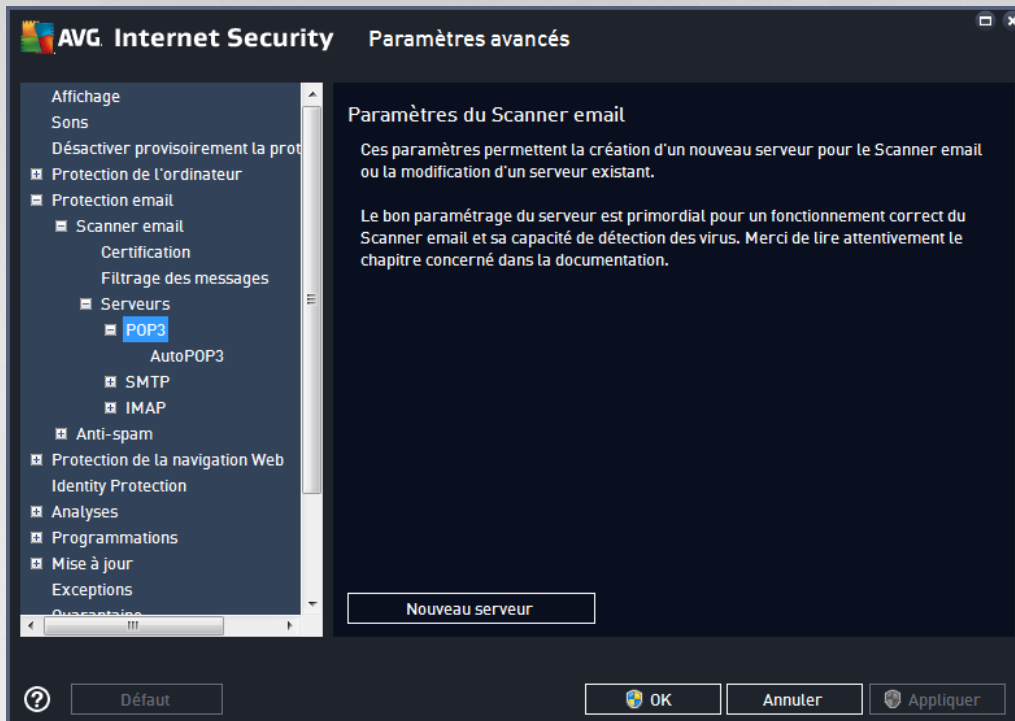
La boîte de dialogue **Filtrage des pièces jointes** est destinée à vous aider à définir les paramètres de l'analyse des pièces jointes aux emails. Par défaut, l'option **Supprimer les pièces jointes** est désactivée. Si vous décidez de l'activer, toutes les pièces jointes signalées comme infectées ou 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

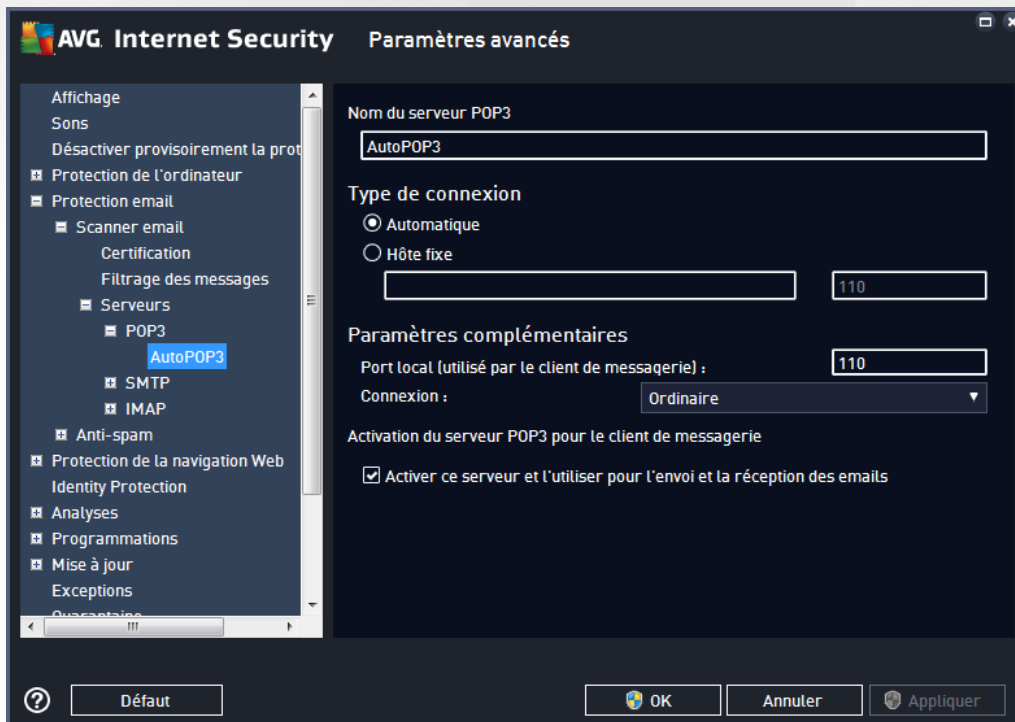
La section **Serveurs** permet de modifier les paramètres des serveurs du [Scanner email](#).

- [Serveur POP3](#)
- [Serveur SMTP](#)
- [Serveur IMAP](#)

De même, vous pouvez définir de nouveaux serveurs pour le courrier entrant ou sortant à l'aide du bouton **Ajouter un nouveau serveur**.



Dans cette boîte de dialogue, vous pouvez configurer un nouveau serveur [Scanner email](#) à l'aide du protocole POP3 pour les messages entrants :

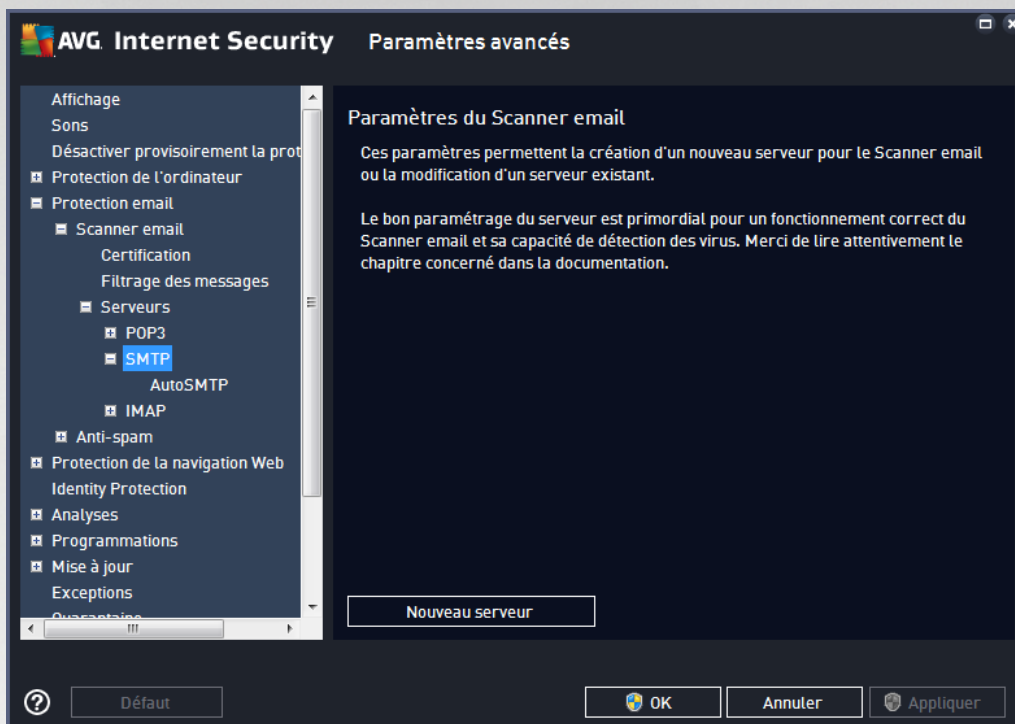


- **Nom du serveur POP3** : dans ce champ, vous pouvez spécifier le nom des serveurs récemment

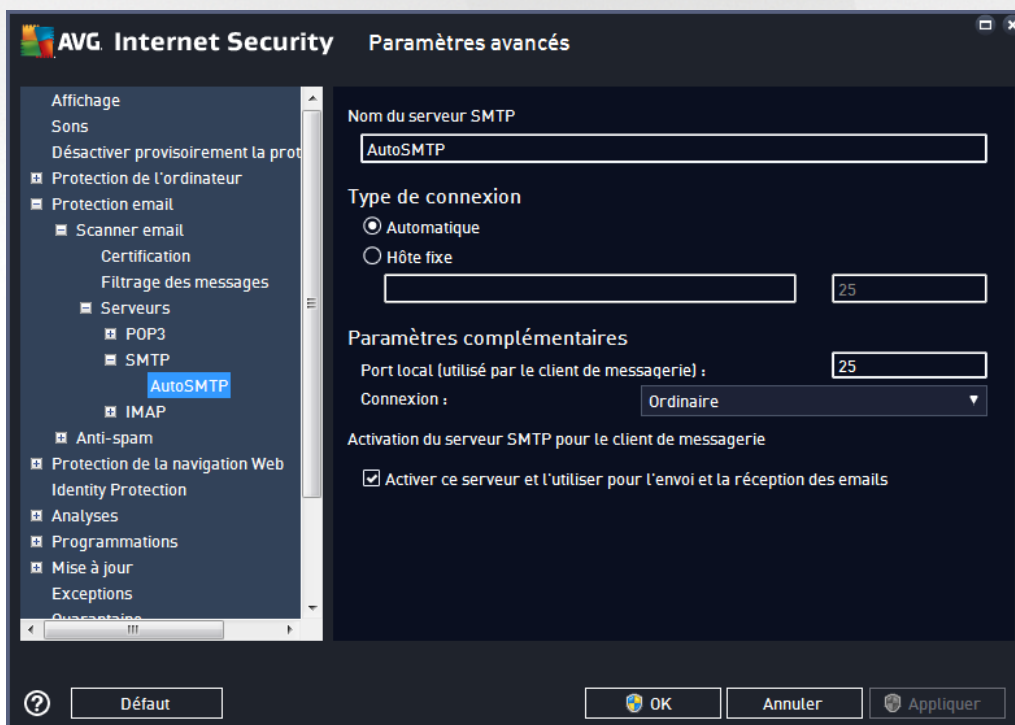


ajoutés (pour ajouter un serveur POP3, cliquez avec le bouton droit sur l'option POP3 du menu de navigation gauche).

- **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 du 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 110.
- **Paramètres complémentaires** : spécifie des paramètres plus détaillés :
  - **Port local** : indique le port sur lequel transitent les communications provenant de l'application de messagerie. Dans votre programme de messagerie, vous devez alors indiquer que ce port fait office de port de communication 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 risque d'être contrôlées ou surveillées par une tierce partie. Cette fonction n'est disponible que si le serveur de messagerie de destination est compatible.
- **Activation du serveur POP3 pour le client de messagerie** : cochez/décochez cette case pour activer ou désactiver le serveur POP3 spécifié



Dans cette boîte de dialogue, vous pouvez configurer un nouveau serveur [Scanner email](#) à l'aide du protocole SMTP pour les messages sortants :

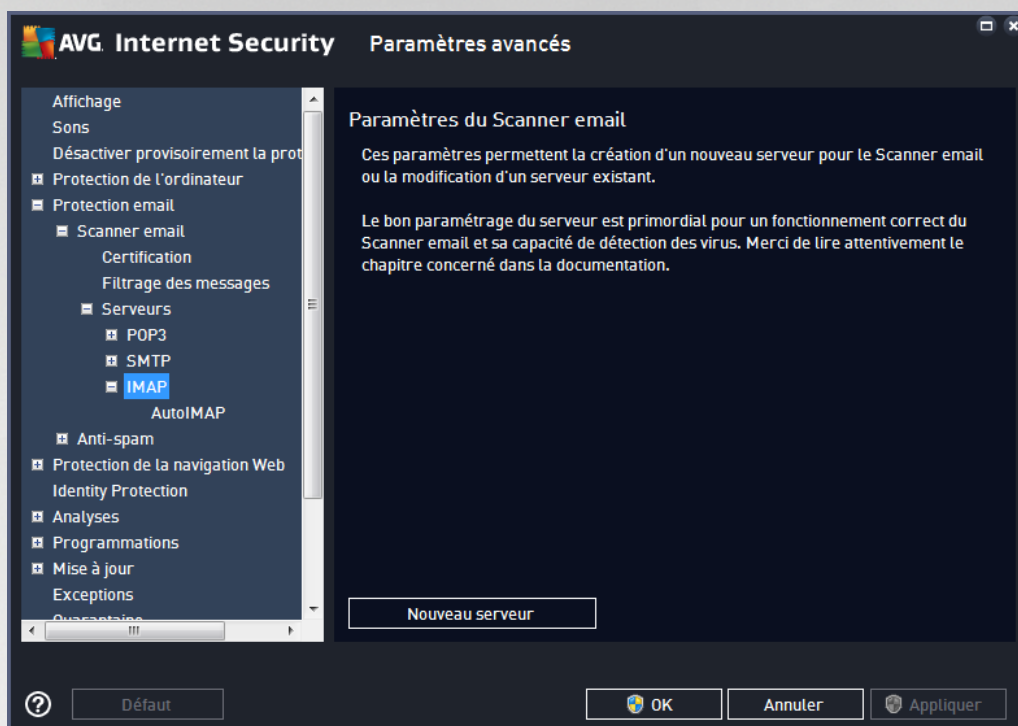


- **Nom du serveur SMTP** : dans ce champ, vous pouvez spécifier le nom des serveurs récemment

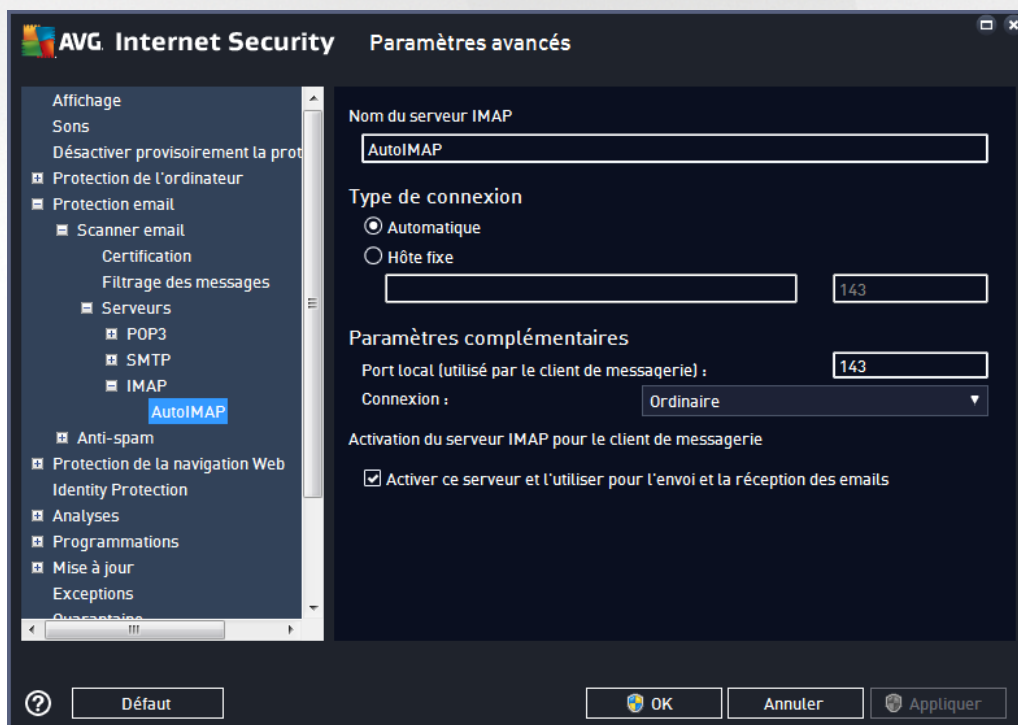


ajoutés (pour ajouter un serveur SMTP, cliquez avec le bouton droit sur l'option SMTP du menu de navigation gauche). Dans le cas d'un serveur créé automatiquement (serveur « AutoSMTP »), ce champ est désactivé.

- **Type de connexion** : définit la méthode de sélection du serveur de messagerie pour les emails 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 du serveur de messagerie. En guise de nom, vous pouvez utiliser un nom de domaine (*smtp.acme.com, par exemple*) ainsi qu'une adresse IP (*123.45.67.89, par exemple*). Si le serveur de messagerie fait appel à un port non standard, il est possible de saisir ce port à la suite du nom du serveur en séparant ces éléments par le signe deux-points (*smtp.acme.com:8200, par exemple*). Le port standard des communications SMTP est le port 25.
- **Paramètres complémentaires** : spécifie des paramètres plus détaillés :
  - **Port local** : indique le port sur lequel transitent les communications provenant de l'application de messagerie. Dans votre programme de messagerie, vous devez alors indiquer que ce port fait office de port de communication SMTP.
  - **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 est disponible seulement si le serveur de messagerie de destination est compatible.
- **Activation du serveur SMTP pour le client de messagerie** : cochez/décochez cette case pour activer ou désactiver le serveur SMTP spécifié ci-dessus



Dans cette boîte de dialogue, vous pouvez configurer un nouveau serveur [Scanner email](#) 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

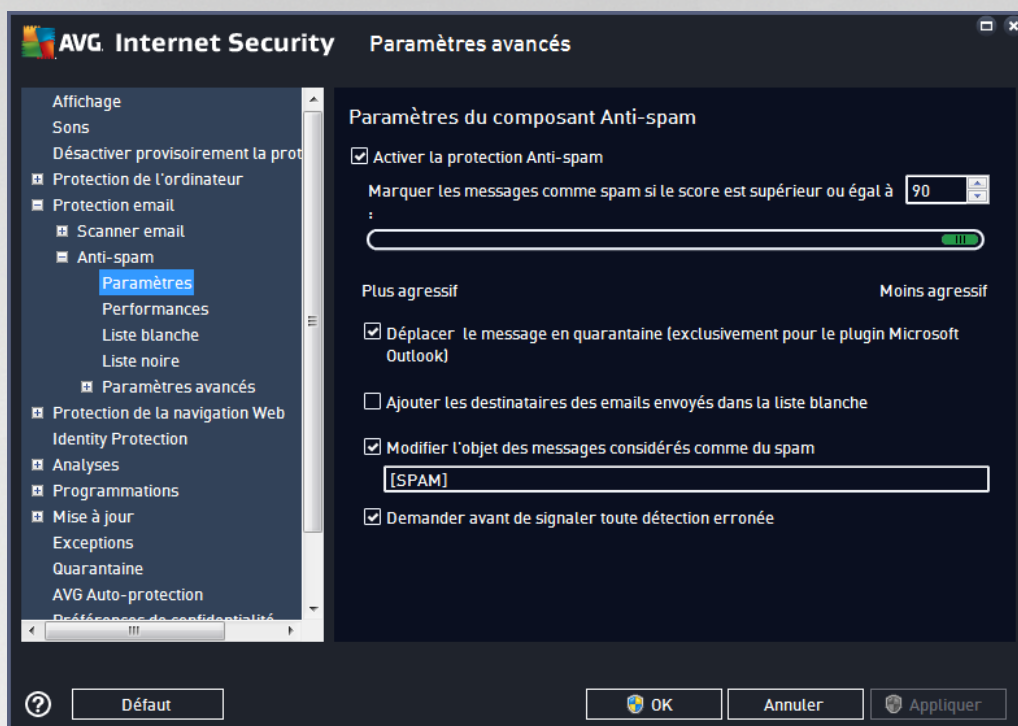




ajoutés (pour ajouter un serveur IMAP, cliquez avec le bouton droit sur l'option IMAP du menu de navigation gauche).

- **Type de connexion** : définit la méthode de sélection du serveur de messagerie pour les emails 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 du serveur de messagerie. En guise de nom, vous pouvez utiliser un nom de domaine (*smtp.acme.com, par exemple*) ainsi qu'une adresse IP (*123.45.67.89, par exemple*). Si le serveur de messagerie fait appel à un port non standard, il est possible de saisir ce port à la suite du nom du serveur en séparant ces éléments par le signe deux-points (*imap.acme.com:8200, par exemple*). Le port standard des communications IMAP est le port 143.
- **Paramètres complémentaires** : spécifie des paramètres plus détaillés :
  - **Port local utilisé** : indique le port sur lequel doivent transiter les communications provenant de l'application de messagerie. Vous devez alors indiquer, dans votre programme de messagerie, que ce port est utilisé 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 risquer d'être analysées ou contrôlées par une tierce partie. Cette fonction est disponible seulement si le serveur de messagerie de destination est compatible.
- **Activation du serveur IMAP pour le client de messagerie** : cochez/décochez cette case pour activer ou désactiver le serveur IMAP spécifié ci-dessus

## 7.5.2. Anti-Spam



Dans la boîte de dialogue **Paramètres anti-spam**, désélectionnez la case **Activer la protection anti-spam** pour autoriser/interdire l'analyse anti-spam dans les communications par email. 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 étant des spams si le résultat est supérieur à**, saisissez la valeur ou faites glisser le curseur vers la gauche ou vers la droite.

La plage des valeurs est comprise entre 50 et 90. Voici l'effet obtenu selon le score que vous définissez :

- **Valeur 80-90** : les messages électroniques 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 anti-spam**, vous pouvez aussi définir la façon dont les messages indésirables doivent être traités :

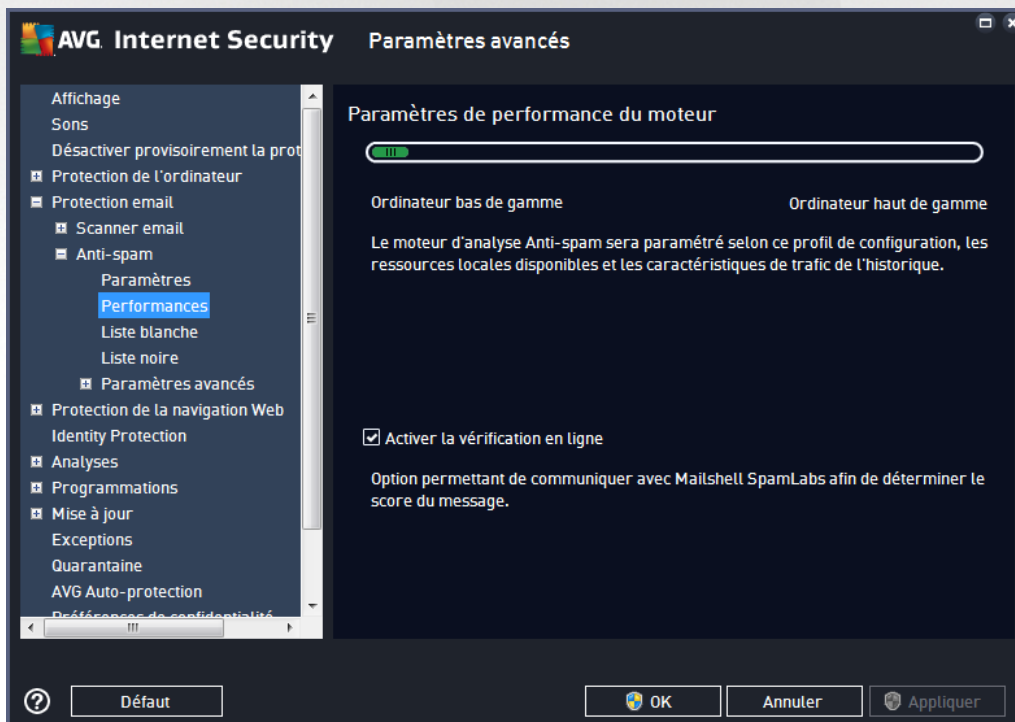
- **Déplacer le message dans le répertoire des indésirables** (*uniquement pour le plugin Microsoft*)



Outlook) : cochez cette case pour que tous les messages détectés comme du courrier indésirable soient automatiquement transférés dans le dossier des messages indésirables de votre client de messagerie Microsoft Outlook. Cette fonction n'est actuellement pas prise en charge par d'autres clients de messagerie.

- **Ajouter les destinataires des messages envoyés dans 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 de messagerie peuvent être transmis.
- **Modifier l'objet des messages considérés comme du spam** : cochez cette case pour que tous les messages détectés comme du spam soient signalés à l'aide d'un mot ou d'un caractère particulier dans l'objet du message. Le texte souhaité doit être saisi dans la zone de texte activée.
- **Demander avant de signaler toute détection erronée** : option activée si, au cours de l'installation, vous avez accepté de participer au projet relatif aux [préférences de la confidentialité](#). En pareil cas, vous avez autorisé le signalement des menaces détectées à AVG. Ce rapport est automatique. 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.

La boîte de dialogue **Paramètres de performance du moteur** (associée à l'élément **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 du mode **Ordinateur bas de gamme** au mode **Ordinateur haut de gamme**.

- **Ordinateur bas de gamme** : aucune règle n'est utilisée pendant le processus d'analyse visant à



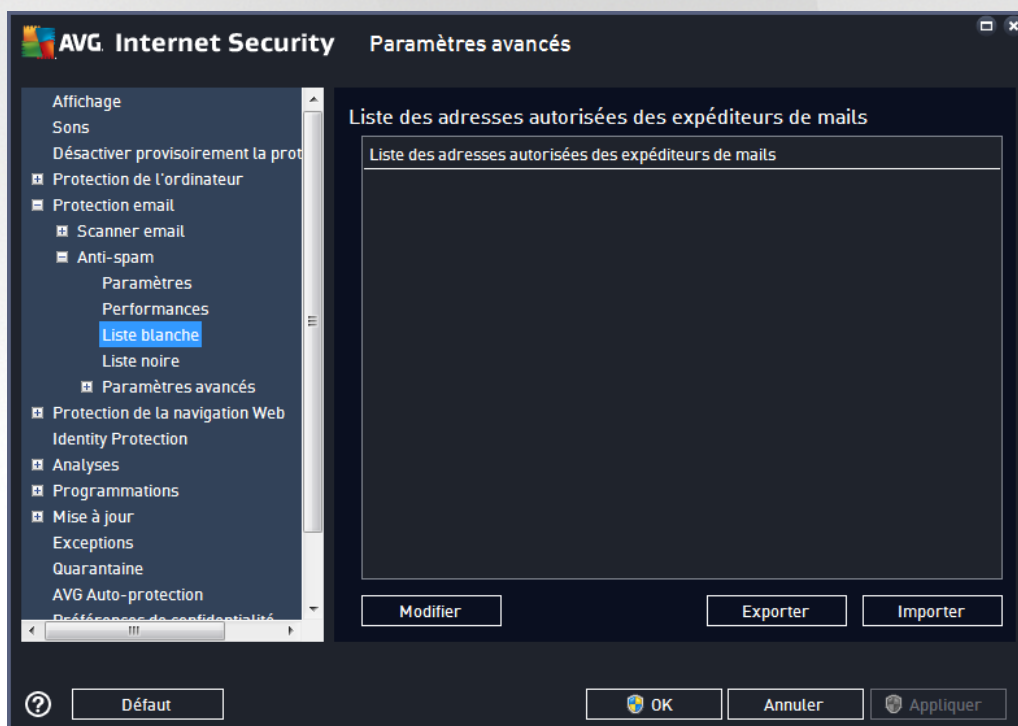
identifier le spam. Seules les données de formation servent à l'identification du spam. Ce mode ne convient pas pour une utilisation standard, sauf si votre ordinateur est peu véloce.

- **Ordinateur haut de gamme** : ce mode exige une quantité de mémoire importante. Durant 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.**

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.

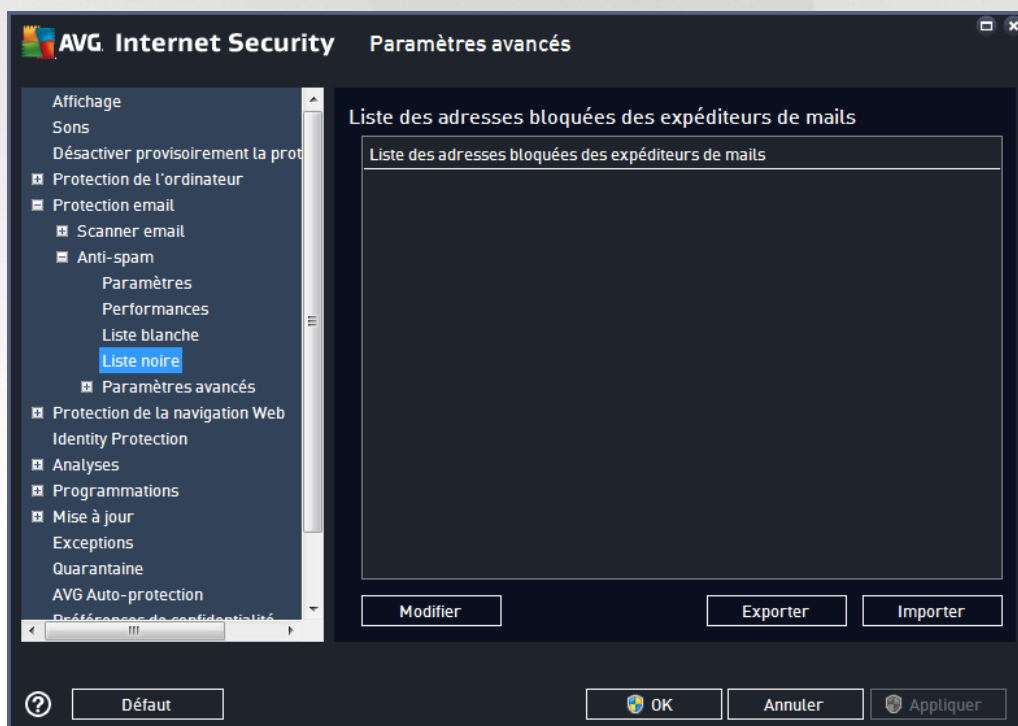


## Boutons de commande

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. Le contenu du fichier doit inclure un seul élément par ligne (*adresse, nom de domaine*).

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 identifiés 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.



## Boutons de commande

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.

***La catégorie Paramètres avancés contient les options de configuration détaillées de la fonction Anti-Spam. Ces paramètres sont destinés uniquement 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.***

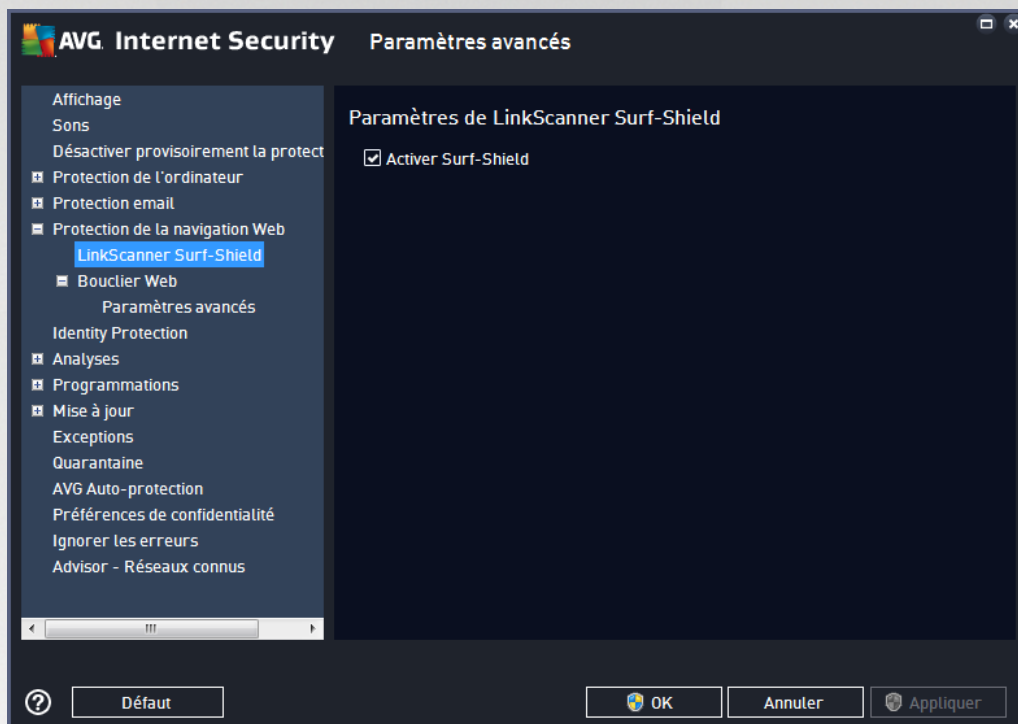
Si vous pensez devoir modifier la configuration Anti-Spam à un niveau très avancé, conformez-vous aux instructions fournies dans l'interface utilisateur. Généralement, vous trouverez dans chaque boîte de dialogue une seule fonction spécifique que vous pouvez ajuster. Sa description figure toujours dans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

- **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



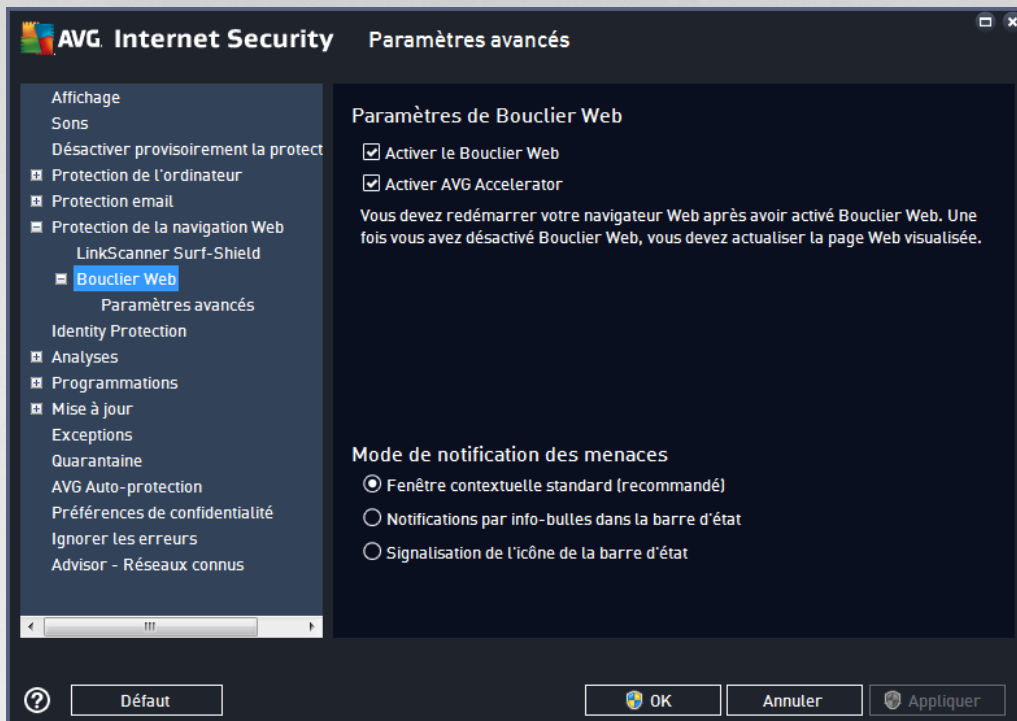
## 7.6. Protection de la navigation Web

La boîte de dialogue des **paramètres de LinkScanner** permet d'activer ou de désactiver les fonctions suivantes :



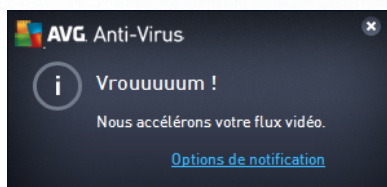
- **Activer Surf-Shield** (option activée par défaut) : protection active (*en temps réel*) contre les sites hébergeant des exploits, lorsque vous y accédez. Les connexions à des sites malveillants et leur contenu piégé sont bloqués au moment où l'utilisateur demande à y accéder via un navigateur Web (ou toute autre application qui utilise le protocole HTTP).

### 7.6.1. Bouclier Web



La boîte de dialogue **Bouclier Web** comporte les options suivantes :

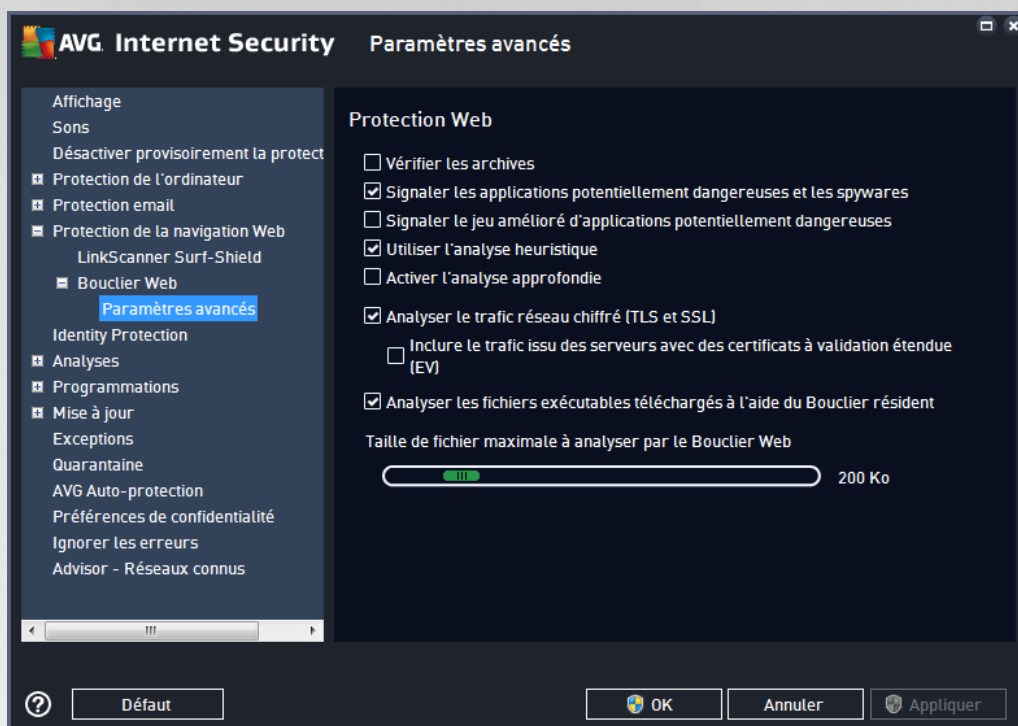
- **Activer le Bouclier Web** (*option activée par défaut*) : active/désactive l'ensemble du service **Bouclier Web**. Pour accéder à d'autres paramètres avancés du **Bouclier Web**, ouvrez la boîte de dialogue suivante intitulée [Protection Web](#).
- **Activer AVG Accelerator** (*option activée par défaut*) : active/désactive le service AVG Accelerator. AVG Accelerator permet une lecture vidéo en ligne plus fluide et facilite les téléchargements supplémentaires. Lorsque le processus d'accélération vidéo est en cours, une fenêtre contextuelle de la barre d'état vous en informe.



#### 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.





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 :

- **Vérifier les archives** (option désactivée par défaut) : analyse le contenu des éventuelles archives contenues dans la page Web à afficher.
- **Signaler les programmes potentiellement dangereux et les spyware** (option activée par défaut) : cochez cette case pour activer la recherche des spyware et des virus. Les spyware désignent une catégorie de programmes malveillants : 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 ordinateur.
- **Signaler le jeu amélioré d'applications potentiellement dangereuses** : (option désactivée par défaut) : l'indication permet de détecter les jeux étendus de spyware 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 utilisés 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 la méthode 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 qui analyseront jusqu'aux zones de l'ordinateur les moins susceptibles



d'être infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

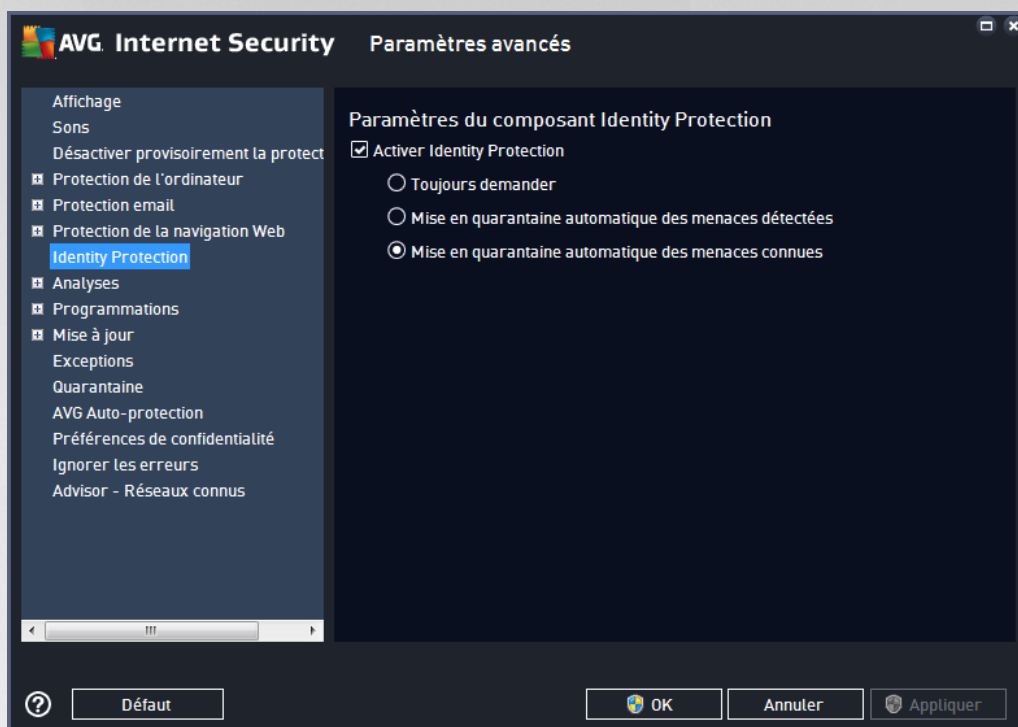
- **Analyser les trafics réseau cryptés (TLS et SSL) (option activé par défaut)** : activer cette option permet à AVG d'analyser toutes les communications réseau cryptées, c'est-à-dire les connexions sur les protocoles de sécurité (SSL et TLS, sa version la plus récente). Cette méthode s'applique aux sites Web qui utilisent HTTPS et aux connexions des clients de messagerie qui utilisent TLS/SSL. Le trafic sécurisé est déchiffré, fait l'objet de recherches de malware, puis est à nouveau chiffré pour être distribué sans risque à votre ordinateur. Dans cette option, vous pouvez décider d'**Inclure le trafic à partir des serveurs possédant des certificats à validation étendue (VE)** et d'analyser également les communications réseau cryptées à partir des serveurs certifiés par un certificat à validation étendue. L'émission de ce type de certificat requiert une validation étendue par l'autorité de certification. Les sites Web exécutés à l'aide de ce certificat sont donc beaucoup plus fiables (*moins susceptibles de distribuer des malware*). Vous pouvez donc décider de ne pas analyser le trafic provenant des serveurs bénéficiant d'une certification à validation étendue, ce qui rendra la communication chiffrée relativement plus rapide.
- **Analyser les fichiers exécutables téléchargés à l'aide du Bouclier résident (option activée par défaut)** : Analyser les fichiers exécutables (*dont les extensions type sont : .exe, .bat ou .com*) une fois leur téléchargement terminé. Le bouclier résident analyse les fichiers avant le téléchargement pour s'assurer qu'aucun fichier malveillant n'accède à votre ordinateur. Toutefois, cette analyse est limitée par la **Taille maximale des fichiers à analyser** : cf. l'élément suivant de cette boîte de dialogue. Les fichiers volumineux sont par conséquent analysés secteur par secteur, c'est également le cas pour la plupart des fichiers exécutables. Les fichiers exécutables peuvent réaliser différentes opérations sur votre ordinateur, il est donc essentiel qu'ils soient sûrs à 100 %. Cette vérification est possible uniquement en analysant le fichier secteur par secteur avant de le télécharger et une nouvelle fois lorsque le téléchargement est terminé. Nous vous recommandons de laisser cette option cochée. Si vous la désactivez, vous pouvez tout de même être sûr qu'AVG détectera tout code malveillant. Mais généralement, cette option ne permettra pas d'évaluer un fichier exécutable dans son ensemble et risque de générer de fausses détections.

Le curseur au bas de la boîte de dialogue vous permet de définir la **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 maximale du fichier 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 par le Bouclier Web, vous restez protégé : si le fichier est infecté, le **Bouclier résident** le détecte immédiatement.

## 7.7. Identity Protection

**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 (*pour une description détaillée des fonctions du composant, consultez le chapitre [Identity Protection](#)*).

La boîte de dialogue des **paramètres 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 vous le déconseillons fortement, sauf si 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** : 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](#). 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** (option activée par défaut) : laissez cette option activée si vous voulez que toutes les applications identifiées comme potentiellement malveillantes soient immédiatement et automatiquement consignées en [Quarantaine](#).

## 7.8. 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 :

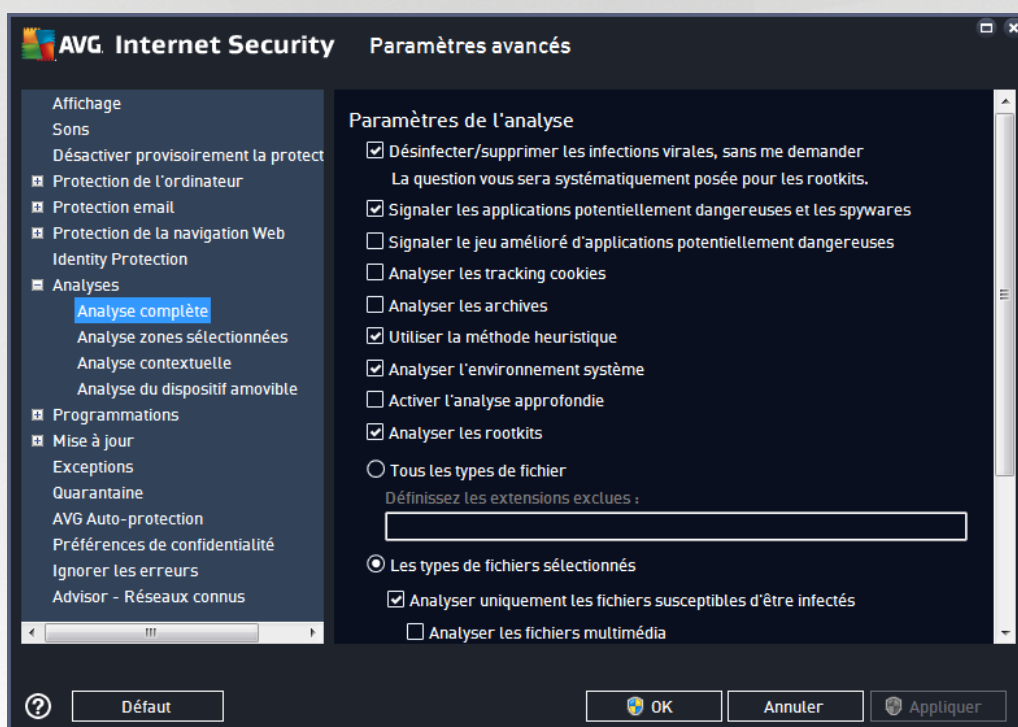
- [Analyse complète](#) : analyse standard prédéfinie appliquée à l'ensemble des fichiers contenus dans l'ordinateur
- [Analyse zones sélectionnées](#) : analyse standard prédéfinie appliquée aux zones spécifiées de l'ordinateur



- [Analyse contextuelle](#) : analyse spécifique d'un objet directement sélectionné dans l'environnement de l'Explorateur Windows
- [Analyse du dispositif amovible](#) : analyse spécifique des périphériques amovibles connectés à votre ordinateur

### 7.8.1. Analyse complète

L'option **Analyse complète** permet de modifier les paramètres d'une analyse prédéfinie par l'éditeur du logiciel, [Analyse complète](#) :



### 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 les infections sans me demander** (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 spyware** (option activée par défaut) : cochez cette case pour activer la recherche de spyware et de virus. Les spyware désignent une catégorie de programmes malveillants : 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 ordinateur.
- **Signaler le jeu amélioré de programmes potentiellement dangereux** (option désactivée par



*défaut*) : l'indication permet de détecter les jeux étendus de spyware 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 utilisés 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*) : avec ce paramètre, les cookies sont 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*) : avec ce paramètre, 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.
- **Analyser l'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 qui analyseront jusqu'aux zones de l'ordinateur les moins susceptibles d'être infectées. Gardez à l'esprit que cette méthode prend énormément de temps.
- **Analyser les rootkits** (*option activée par défaut*) : l'analyse [anti-rootkit](#) recherche les éventuels rootkits présents sur votre ordinateur, c'est-à-dire les programmes et technologies destinés à masquer 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.

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 à ne pas analyser (*séparées par des virgules*).
- **Types de fichiers sélectionnés** : vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent être infectés 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 multimédias (*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 *automatique* d'utilisation des ressources. Cette configuration permet d'accélérer l'analyse : elle réduit le temps 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 la quantité de ressources système utilisées en augmentant la durée de l'analyse.

### Définir des rapports d'analyse supplémentaires...

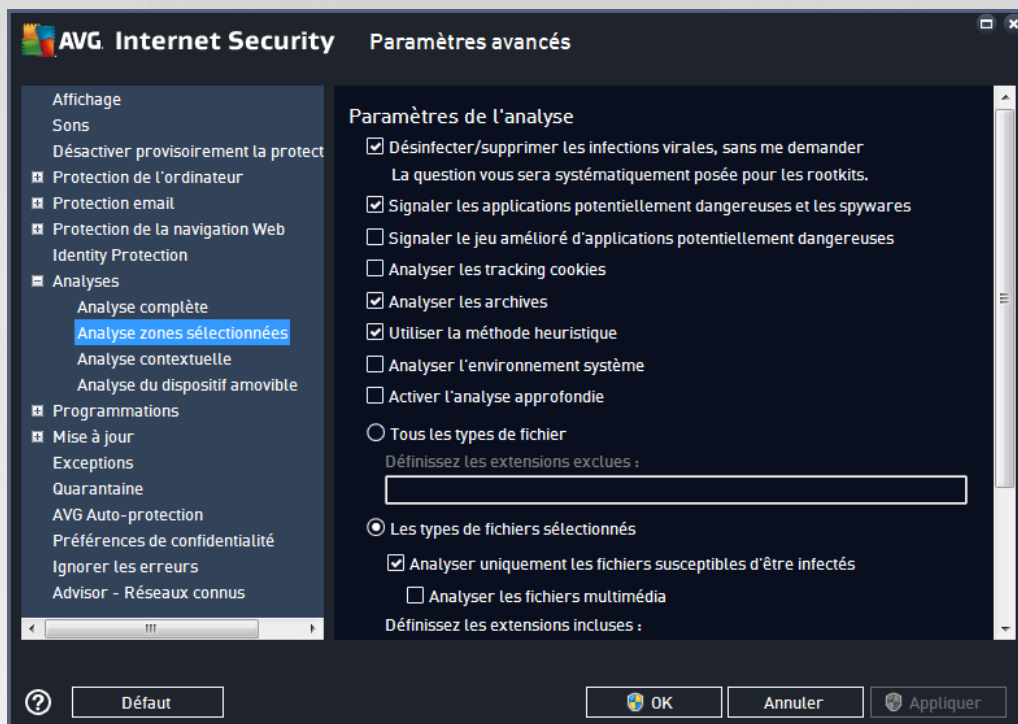
Cliquez sur **Définir des rapports d'analyse supplémentaires** Cliquez sur le lien pour ouvrir la boîte de dialogue **Rapports d'analyse** dans laquelle vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :





### 7.8.2. Analyse zones sélectionnées

L'interface d'édition de l'**Analyse zones sélectionnées** est presque identique à celle de l'[Analyse complète](#), mais les paramètres par défaut sont plus stricts en ce qui concerne l'[Analyse complète](#) :

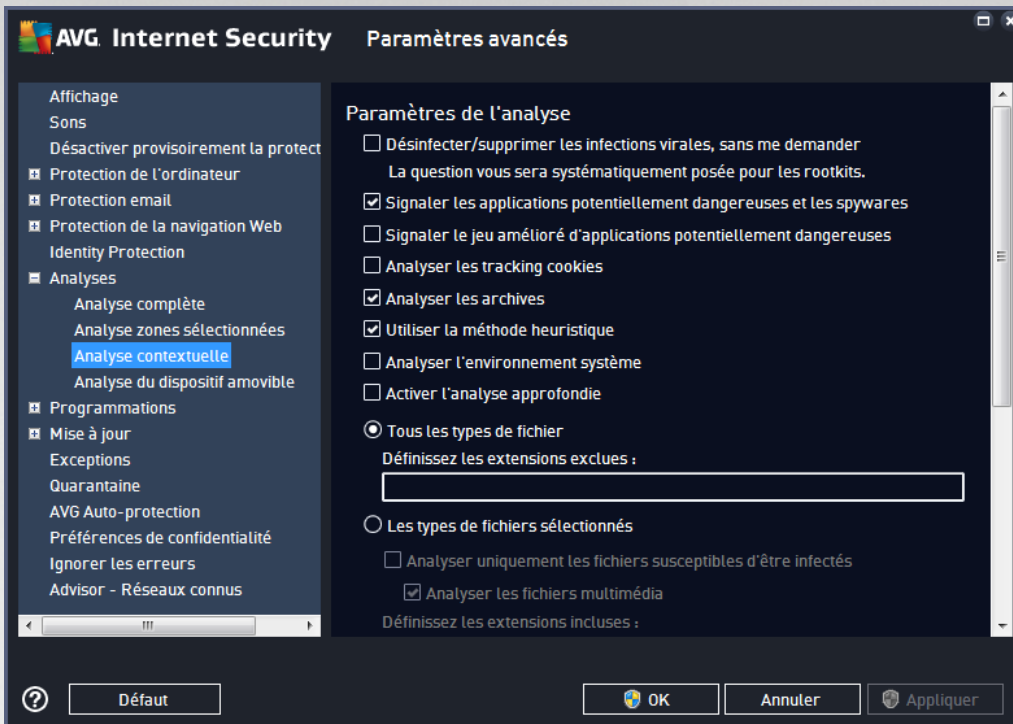


Tous les paramètres définis dans cette boîte de dialogue de configuration s'appliquent uniquement aux zones sélectionnées pour l'analyse, dans le cadre de l'option [Analyse zones sélectionnées](#).

**Remarque :** Pour obtenir la description des paramètres qui vous intéressent, consultez le chapitre [Paramètres avancés d'AVG / Analyses / Analyse complète](#).

### 7.8.3. 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](#) :



Les options d'édition sont presque identiques à celles disponibles 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](#).

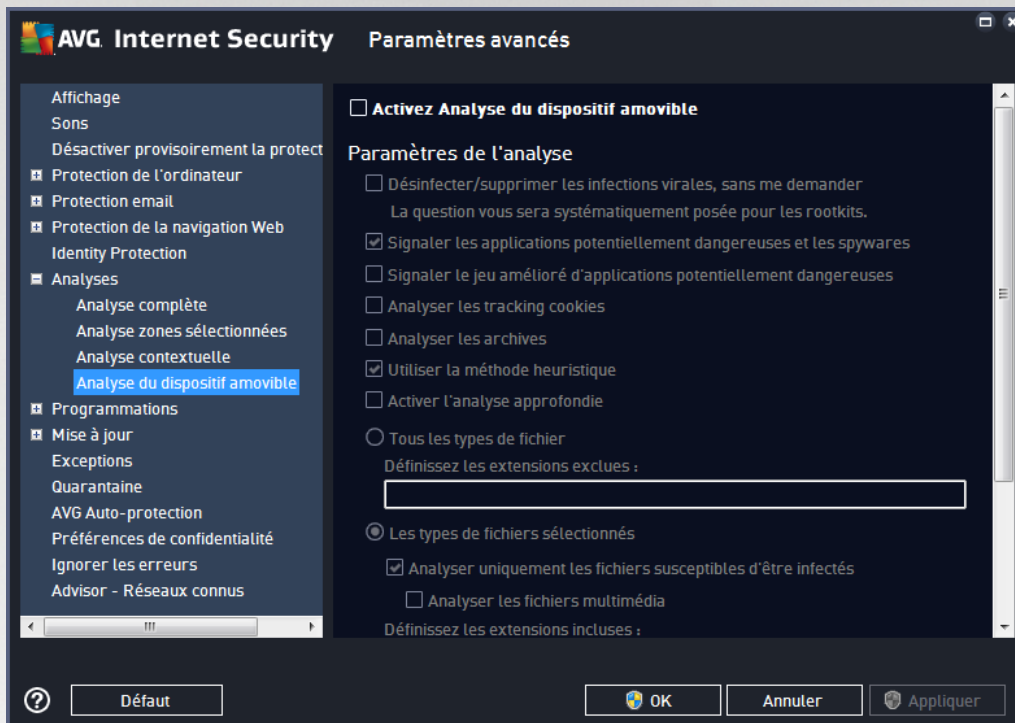
Comme la boîte de dialogue [Analyse complète](#), celle de l'**Analyse contextuelle** inclut la section **Affichage de la progression et des résultats de l'analyse**, dans laquelle vous indiquez si vous voulez que la progression de l'analyse et ses résultats soient accessibles à partir de l'interface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





#### 7.8.4. Analyse du dispositif amovible

L'interface d'édition de l'*Analyse du dispositif amovible* ressemble beaucoup à celle de l'[Analyse complète](#) :



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

**Remarque :** Pour obtenir la description des paramètres qui vous intéressent, consultez le chapitre [Paramètres avancés d'AVG / Analyses / Analyse complète](#).

#### 7.9. Programmations

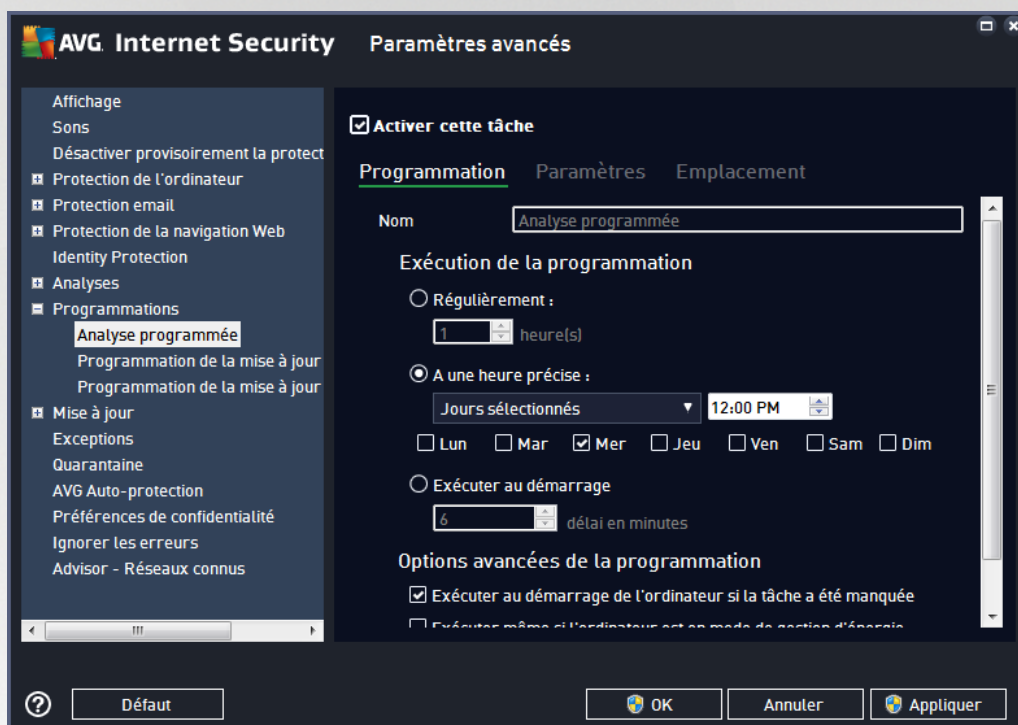
Dans l'entrée **Programmations**, vous êtes libre de modifier les paramètres par défaut des éléments suivants :

- [Analyse programmée](#)
- [Programmation de la mise à jour des définitions](#)
- Programmation de la mise à jour du programme
- [Programmation de la mise à jour de l'anti-spam](#)



### 7.9.1. Analyse programmée

Les paramètres de l'analyse programmée peuvent être modifiés (ou une nouvelle analyse peut être programmée) depuis les trois onglets : Dans chaque onglet, vous pouvez cocher/décocher la case **Activer cette tâche** pour désactiver temporairement l'analyse programmée et la réactiver au moment opportun:



La zone de texte **Nom** (désactivée pour toutes les programmations par défaut) affiche le nom 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.

**Par 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. À l'inverse, « Analyse de l'environnement système » est un nom descriptif précis. Il est également nécessaire de spécifier dans le nom de l'analyse si celle-ci porte sur l'ensemble de l'ordinateur ou une sélection de fichiers ou de dossiers. Notez que les analyses personnalisées sont toujours basées sur l'[analyse des zones sélectionnées](#).

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

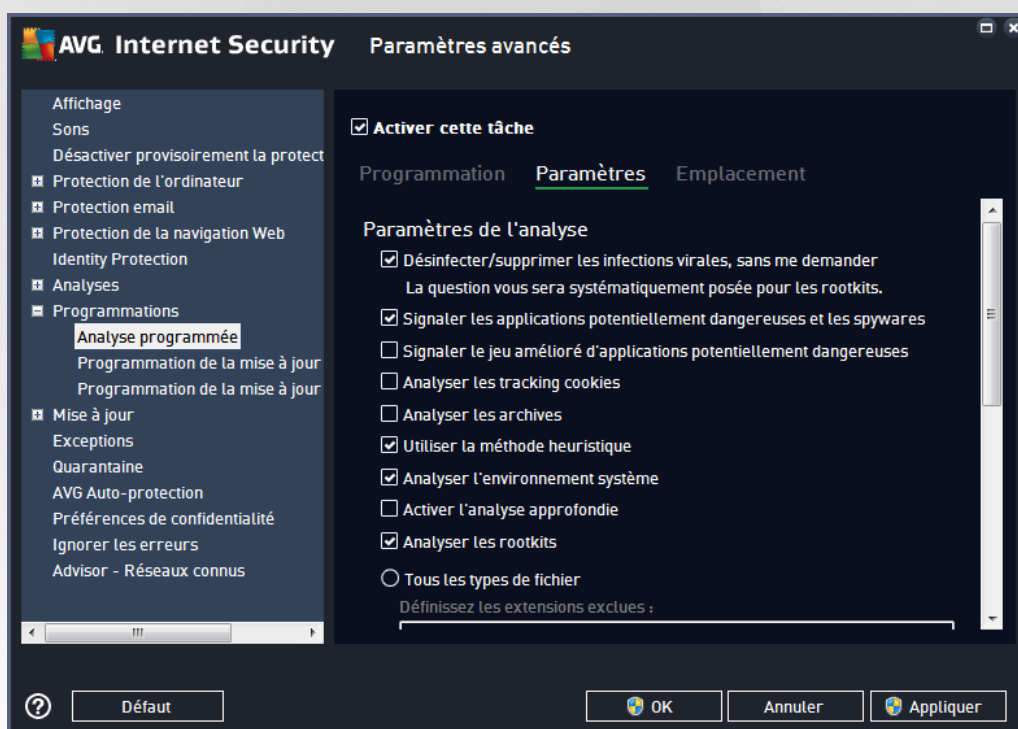
#### Exécution de la programmation

Ici, spécifiez l'intervalle entre chaque exécution de la nouvelle analyse. La périodicité de l'analyse peut être programmée à des intervalles réguliers (**Régulièrement**), à une date et une heure précises (**A une heure précise**) ou encore être associée à un événement (**Exécuter au démarrage**).



## Options avancées de la programmation

- **Exécuter au démarrage de l'ordinateur si la tâche a été manquée** : si vous programmez l'analyse pour qu'elle s'exécute à une heure spécifique, cette option garantit qu'elle sera effectuée ultérieurement, si l'ordinateur est éteint à l'heure programmée.
- **Exécuter même si l'ordinateur est en mode de gestion d'énergie** : l'analyse sera effectuée même si l'ordinateur est alimenté par batterie à l'heure programmée.



Sous l'onglet **Paramètres de 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** :

- **Désinfecter/supprimer les infections virales sans me demander** (option activée par défaut) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement, si cela est possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en [Quarantaine](#).
- **Signaler les applications potentiellement dangereuses et les spyware** (option activée par défaut) : cochez cette case pour activer la recherche de spyware et de virus. Les spyware désignent une catégorie de programmes malveillants : 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 ordinateur.
- **Signaler le jeu amélioré d'applications potentiellement dangereuses** (option désactivée par défaut) : l'indication permet de détecter les jeux étendus de spyware 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 utilisés 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*) : avec ce paramètre, les cookies sont 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, y compris ceux stockés dans des formats d'archives (archives ZIP, RAR etc.).
- **Utiliser la méthode heuristique** (*option activée par défaut*) : l'analyse heuristique (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*) est l'une des méthodes employées pour détecter des virus pendant l'analyse.
- **Analyser l'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 qui analyseront jusqu'aux zones de l'ordinateur les moins susceptibles d'être infectées. Gardez à l'esprit que cette méthode prend énormément de temps.
- **Analyser les rootkits** : (*option activée par défaut*) 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.

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 à ne pas analyser (*séparées par des virgules*).
- **Types de fichiers sélectionnés** : vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent être infectés 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 multimédias (*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

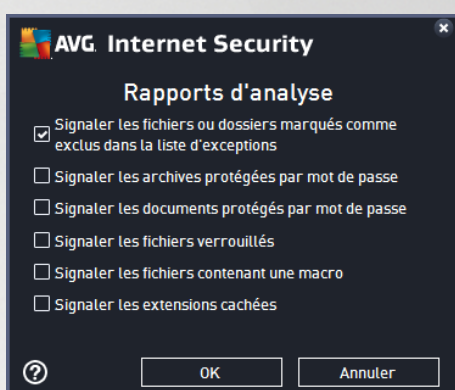
Dans cette section, il est possible de régler la vitesse d'analyse en fonction des ressources système. Par



défaut, cette option est réglée sur le niveau *automatique* d'utilisation des ressources. Cette configuration permet d'accélérer l'analyse : elle réduit le temps 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 la quantité de ressources système utilisées en augmentant la durée de l'analyse.

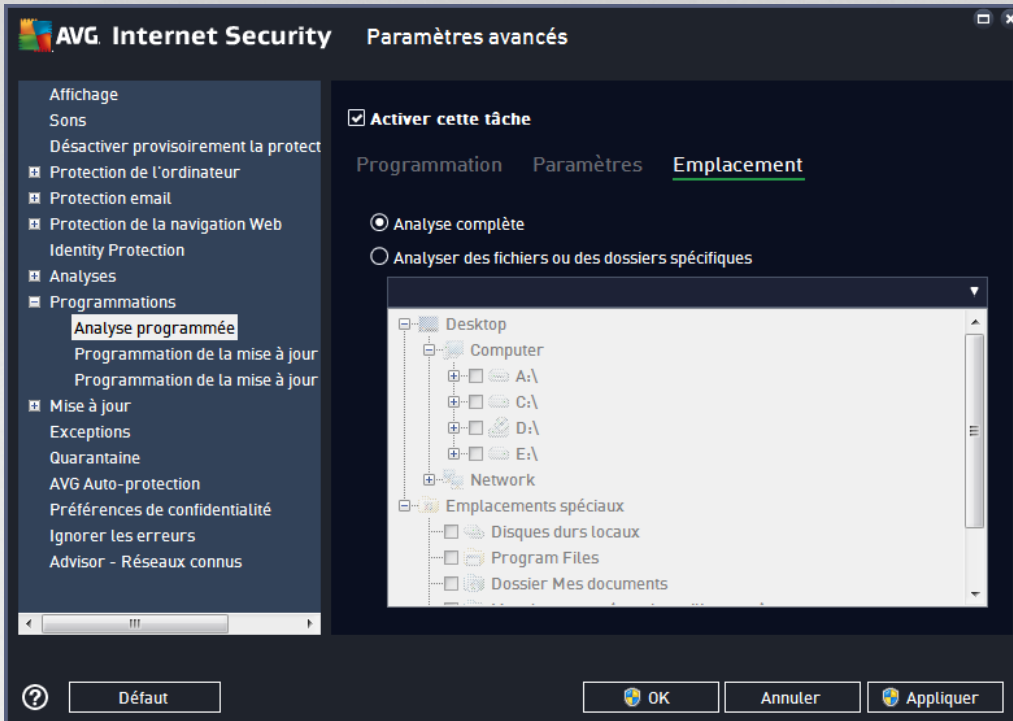
### Définir des rapports d'analyse supplémentaires

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



### Options de l'arrêt de l'ordinateur

Dans la section **Options de l'arrêt de l'ordinateur**, vous pouvez indiquer 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.

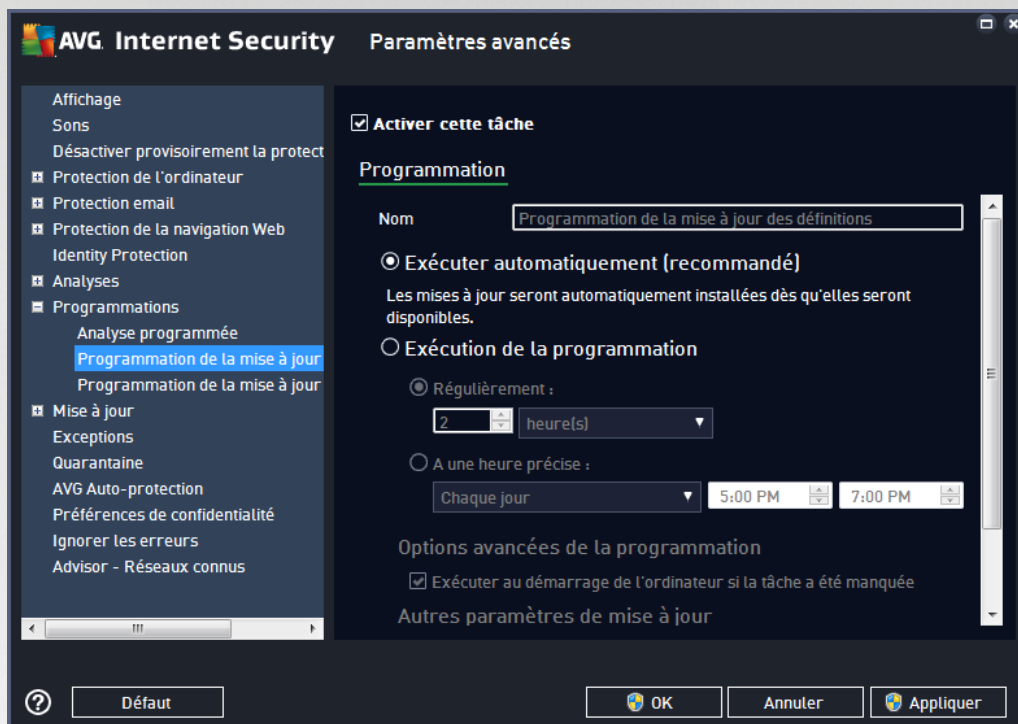


Sous l'onglet **Localisation**, indiquez si vous voulez programmer l'[analyse complète](#) ou l'[analyse des zones sélectionnées](#). Si vous optez pour la deuxième solution, la structure de l'arborescence affichée dans la partie inférieure de la boîte de dialogue devient active et permet de définir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



## 7.9.2. Programmation de la mise à jour des définitions

En cas de *nécessité absolue*, désélectionnez la case **Activer cette tâche** pour désactiver provisoirement la mise à jour programmée des définitions et la réactiver au moment opportun :



Dans la boîte de dialogue correspondante, vous spécifiez en détail les paramètres du programme de mise à jour : La zone de texte **Nom** (*désactivée pour toutes les programmations par défaut*) affiche le nom attribué à cette programmation par le fournisseur du programme.

### Exécution de la programmation

La tâche est lancée automatiquement par défaut (**s'exécute automatiquement**) dès lors qu'une nouvelle mise à jour des définitions virales est disponible. Nous vous recommandons de respecter cette configuration, à moins que vous ayez une bonne raison de ne pas le faire ! Ensuite, vous pouvez configurer manuellement le lancement de la tâche et préciser les intervalles de temps concernant le lancement des nouvelles mises à jour programmées de définitions. Il est possible de répéter l'exécution de la mise à jour après un laps de temps donné (**Régulièrement**), ou à une heure et une date précises (**A une heure précise**).

### Options avancées de la programmation

Cette section permet de définir dans quelles conditions la mise à jour de la définition 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

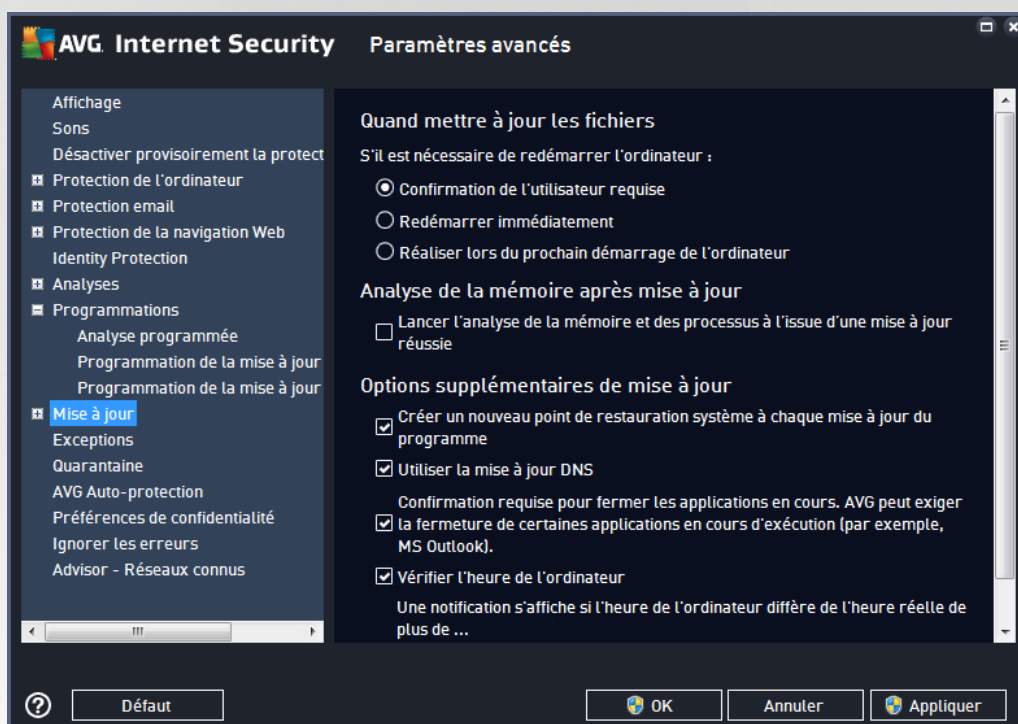
Enfin, cochez l'option **Exécuter de nouveau la mise à jour lorsque la connexion Internet sera disponible**



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 planifiée 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](#)).

### 7.9.3. Programmation de la mise à jour de l'Anti-Spam

En cas de nécessité absolue, décochez la case **Activer cette tâche** pour désactiver temporairement la mise à jour programmée du composant [Anti-Spam](#) et la réactiver au moment opportun :



Dans la boîte de dialogue correspondante, vous spécifiez en détail les paramètres du programme de mise à jour : La zone de texte **Nom** (*désactivée pour toutes les programmations par défaut*) affiche le nom 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 l'exécution 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 (**Exécuter au démarrage**).

#### 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.



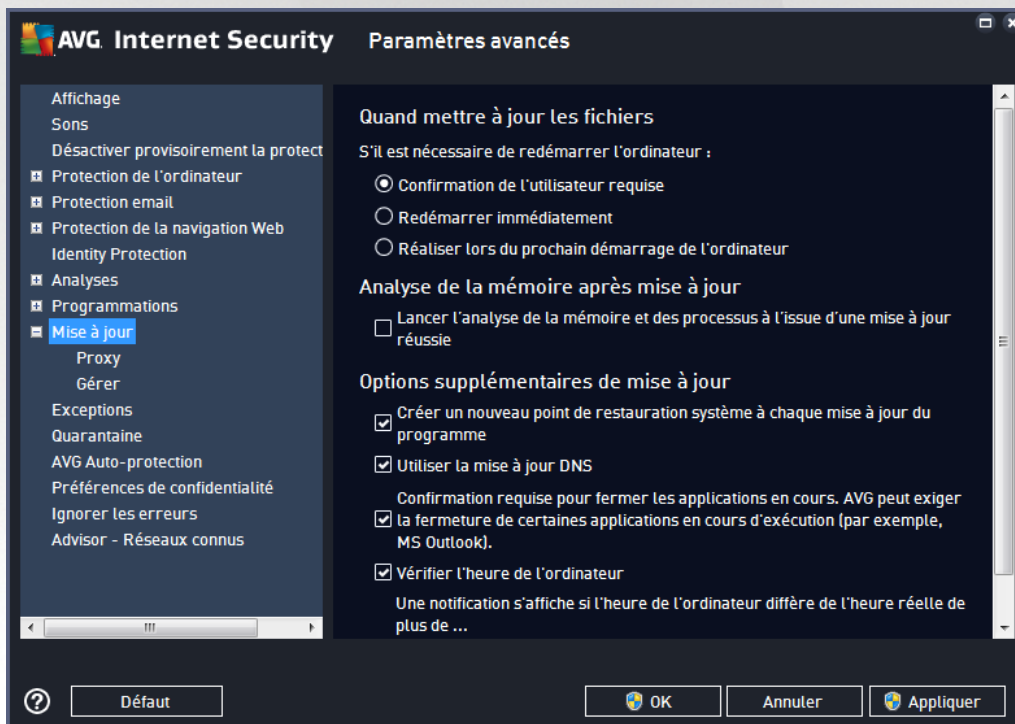


## Autres paramètres de mise à jour

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 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](#)).

## 7.10. 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 pouvez choisir une des trois solutions alternatives si le processus de mise à jour nécessite un redémarrage de l'ordinateur. Vous pouvez programmer la finalisation de la mise à jour pour le prochain redémarrage de l'ordinateur ou la lancer immédiatement :

- **Confirmation de l'utilisateur requise (par défaut)** : un message vous invite à approuver le redémarrage nécessaire pour finaliser le processus de [mise à jour](#)
- **Redémarrer immédiatement** : l'ordinateur redémarre automatiquement à l'issue du processus de [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 reportée au prochain démarrage de l'ordinateur. Souvenez-vous que cette option n'est recommandée que si vous êtes sûr de redémarrer votre ordinateur au moins une fois par jour.

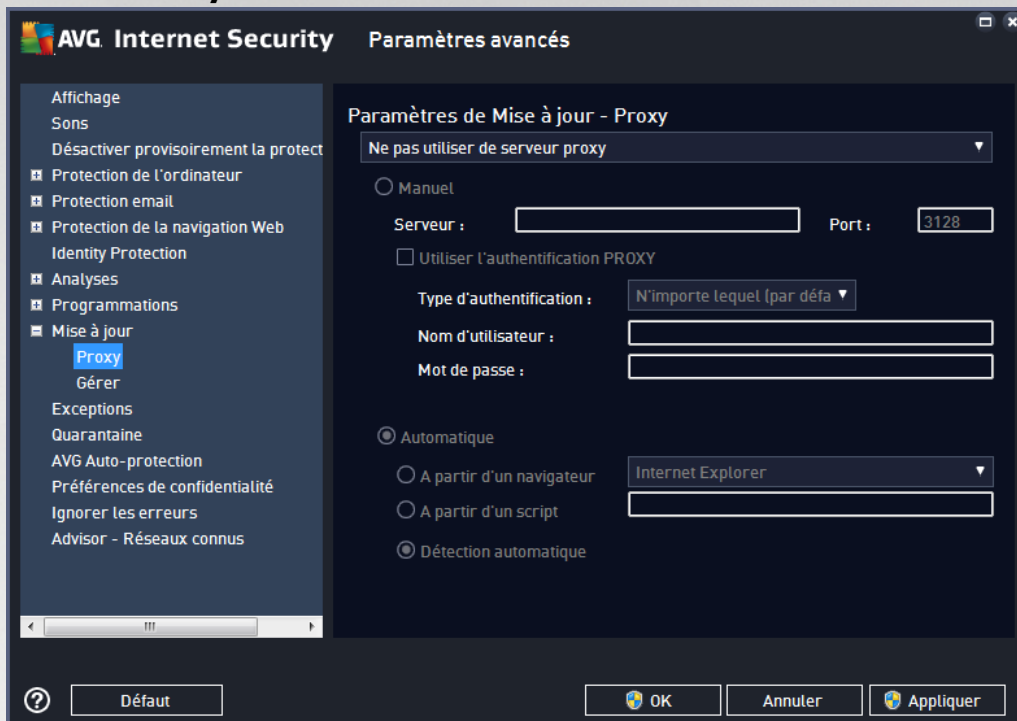
### Analyse de la mémoire après mise à jour

Cochez cette case pour indiquer que vous voulez exécuter une nouvelle analyse de la mémoire après chaque mise à jour réussie. 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 pendant chaque nouvelle mise à jour du programme** (*option activée par défaut*) : un point de restauration est créé avant le lancement de chaque mise à jour du programme AVG. En cas d'échec de la mise à jour et de blocage de votre système d'exploitation, vous avez alors la possibilité de restaurer le système d'exploitation tel qu'il était configuré à partir de ce point. Cette option est accessible via Démarrer / Tous les programmes / Accessoires / Outils système / Restauration du système, mais elle est réservée aux utilisateurs expérimentés. Laissez cette case cochée si vous voulez utiliser cette fonctionnalité.
- **Utiliser la mise à jour DNS** (*option activée par défaut*) : lorsque cette option est cochée et que la mise à jour est lancée, **AVG Internet Security** recherche les informations portant sur la base de données virale et le programme les plus récents, sur le serveur DNS. Seuls les fichiers de mise à jour indispensables requis sont téléchargés et appliqués. De cette manière, le nombre total de données est réduit au minimum et l'opération de mise à jour est plus rapide.
- **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** (*option activée par défaut*) : cochez cette case si vous voulez être informé lorsque l'écart entre l'heure de l'ordinateur et l'heure réelle est plus grand que le nombre d'heures spécifié.

### 7.10.1. 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 ou 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 :

- **Ne pas utiliser de serveur proxy** (paramètres par défaut)
- **Utiliser un proxy**
- **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 permettant d'accéder à Internet (*par défaut, il s'agit du 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.

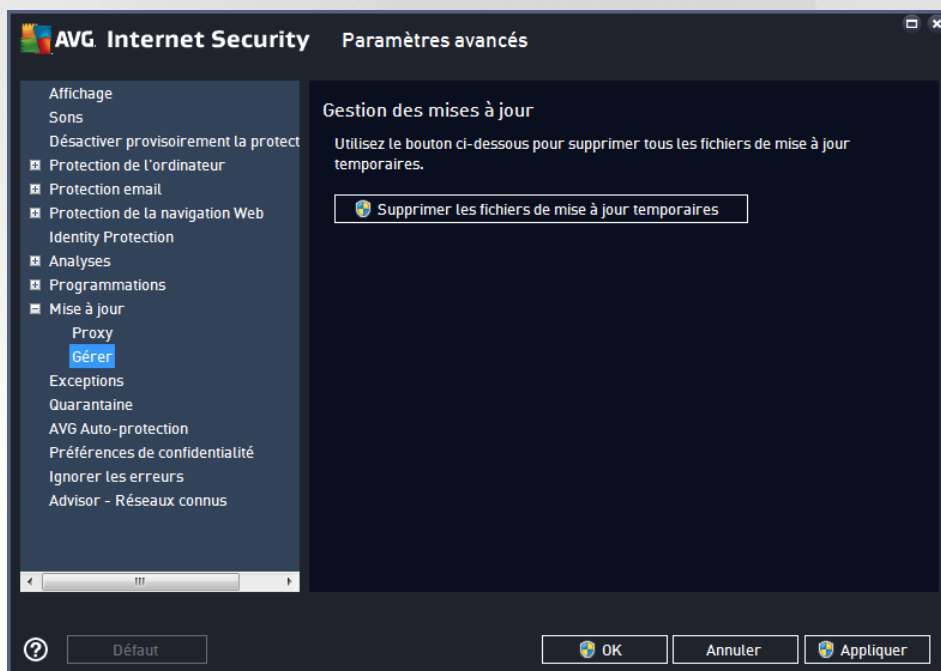
### Configuration automatique

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

### 7.10.2. Gérer

La boîte de dialogue **Gestion des mises à jour** comporte deux options accessibles via deux boutons :



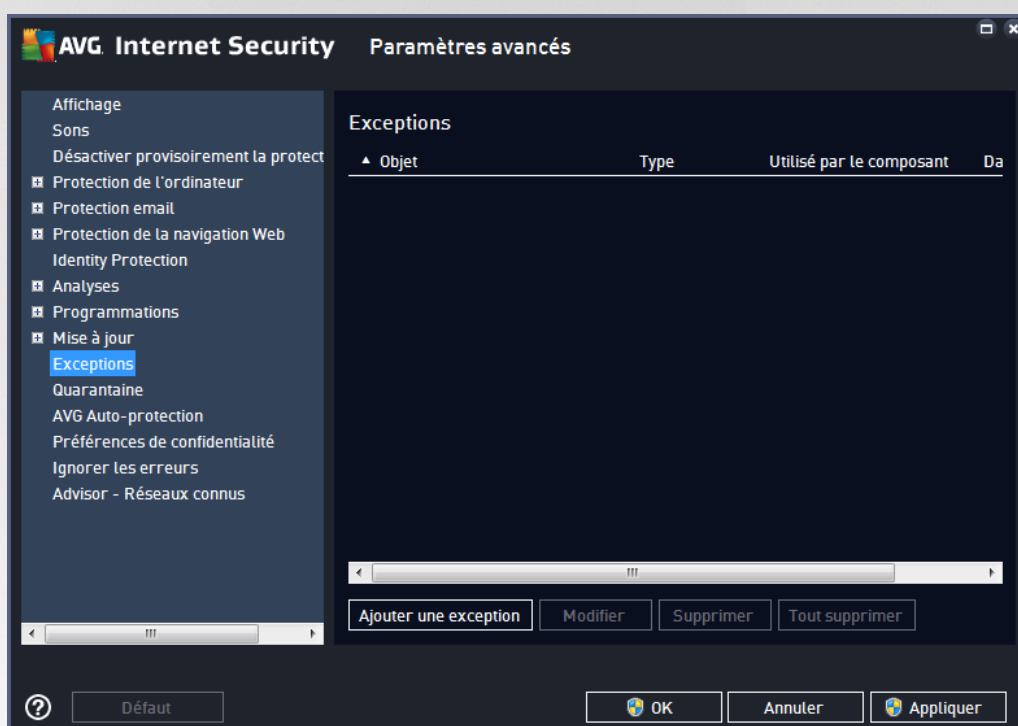
- **Supprimer les fichiers de mise à jour temporaires** : cliquez sur ce bouton pour supprimer tous les fichiers redondants de votre disque dur (par défaut, ces fichiers sont conservés pendant 30 jours)
- **Revenir à la version précédente de la base virale** : cliquez sur ce bouton pour supprimer la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



## 7.11. Exceptions

Dans la boîte de dialogue **Exceptions**, vous pouvez définir des exceptions, c'est-à-dire des éléments qui seront ignorés par **AVG Internet Security**. Vous devrez définir une exception si AVG ne cesse d'identifier un programme ou un fichier comme une menace ou de bloquer un site Web qu'il considère comme dangereux. Ajoutez ce fichier ou site Web à la liste d'exceptions et il ne sera plus détecté ou bloqué par AVG.

**Assurez-vous toujours que le fichier, programme ou site Web en question est fiable à 100 % !**



Le tableau affiché dans la boîte de dialogue dresse la liste des exceptions s'il en existe déjà. Une case à cocher figure à côté de chaque élément. Si la case est cochée, l'exception est effective. Dans le cas contraire, elle est seulement définie sans être utilisée. En cliquant sur l'en-tête de colonne, vous pouvez trier les éléments autorisés en fonction du critère correspondant.

### Boutons de commande

- **Ajouter une exception** : servez-vous de ce bouton pour ouvrir une nouvelle boîte de dialogue afin de spécifier l'élément à exclure de l'analyse AVG :

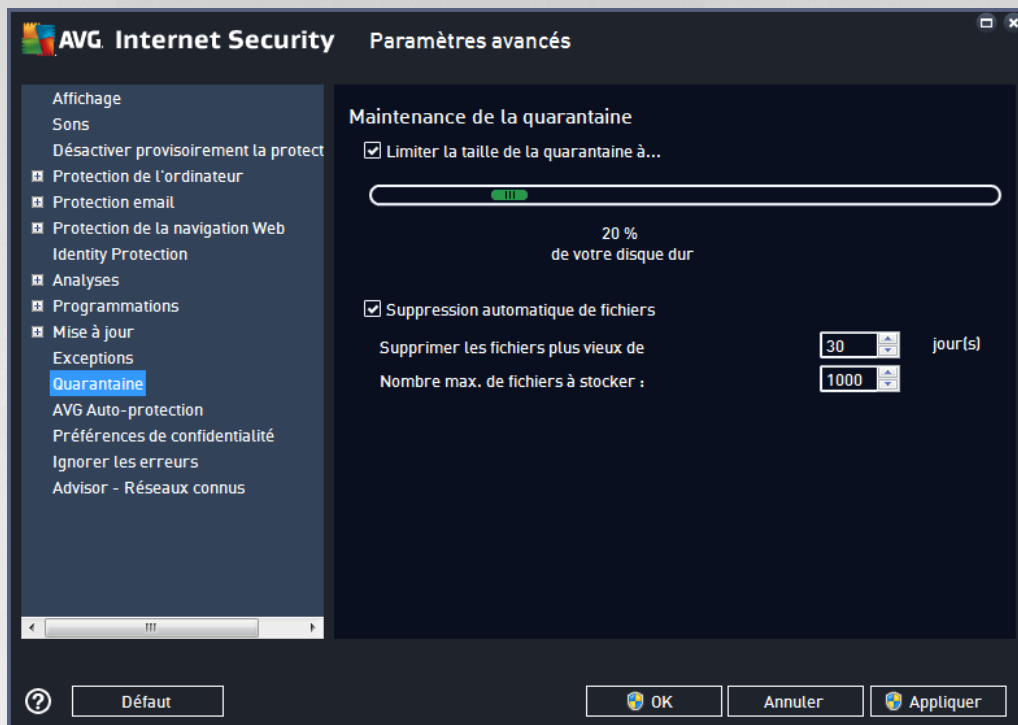


Vous serez d'abord invité à définir le type d'objet (application ou fichier, dossier, URL ou certificat par exemple). Ensuite, vous devrez parcourir le disque et définir le chemin vers cet objet ou saisir l'URL. Enfin, vous pouvez définir les fonctions AVG qui devront ignorer l'objet spécifié (*Bouclier résident, Identity Protection, Analyse*).

- **Modifier** : ce bouton est actif uniquement si des exceptions ont déjà été définies et sont répertoriées dans le tableau. Il permet alors de modifier l'exception sélectionnée et de configurer ses paramètres.
- **Supprimer** : servez-vous de ce bouton pour annuler une exception définie précédemment. Vous pouvez supprimer toutes les exceptions une par une ou mettre en surbrillance un bloc d'exceptions dans la liste et les supprimer en cliquant sur ce bouton. Après la suppression d'une exception de la liste, l'élément correspondant (fichier, dossier, URL) est de nouveau vérifié par AVG. Notez que seule l'exception est supprimée, pas le fichier ni le dossier.
- **Tout supprimer** : ce bouton permet de supprimer toutes les exceptions définies dans la liste.



## 7.12. Quarantaine

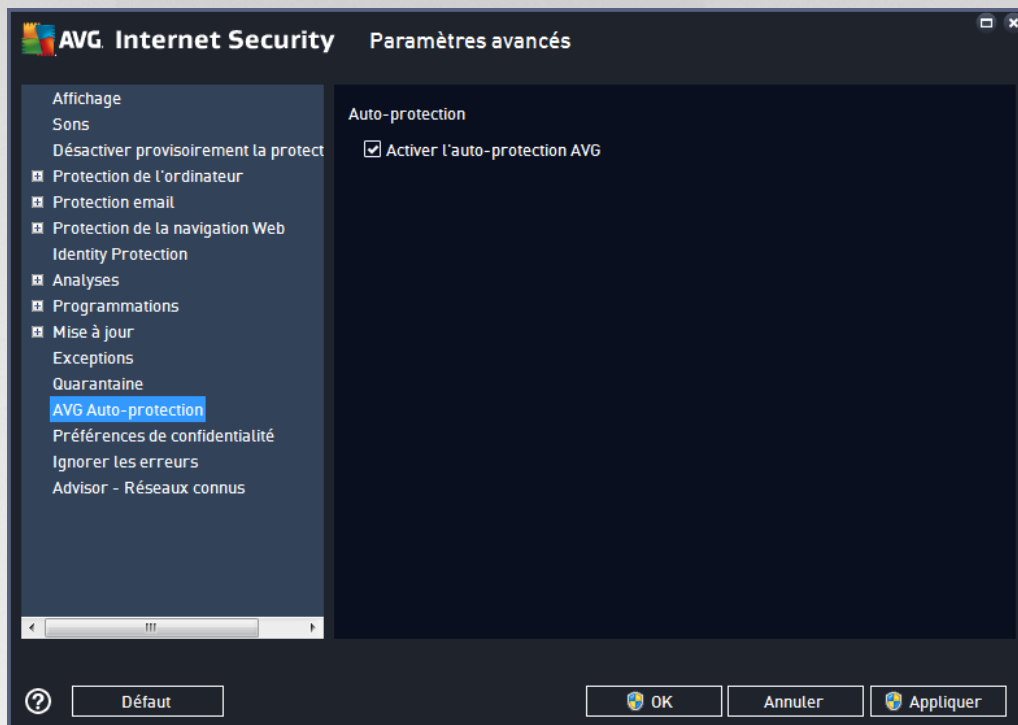


La boîte de dialogue **Maintenance de la quarantaine** permet de définir plusieurs paramètres liés à l'administration des objets stockés dans le module [Quarantaine](#) :

- **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**).



### 7.13. Auto-protection AVG



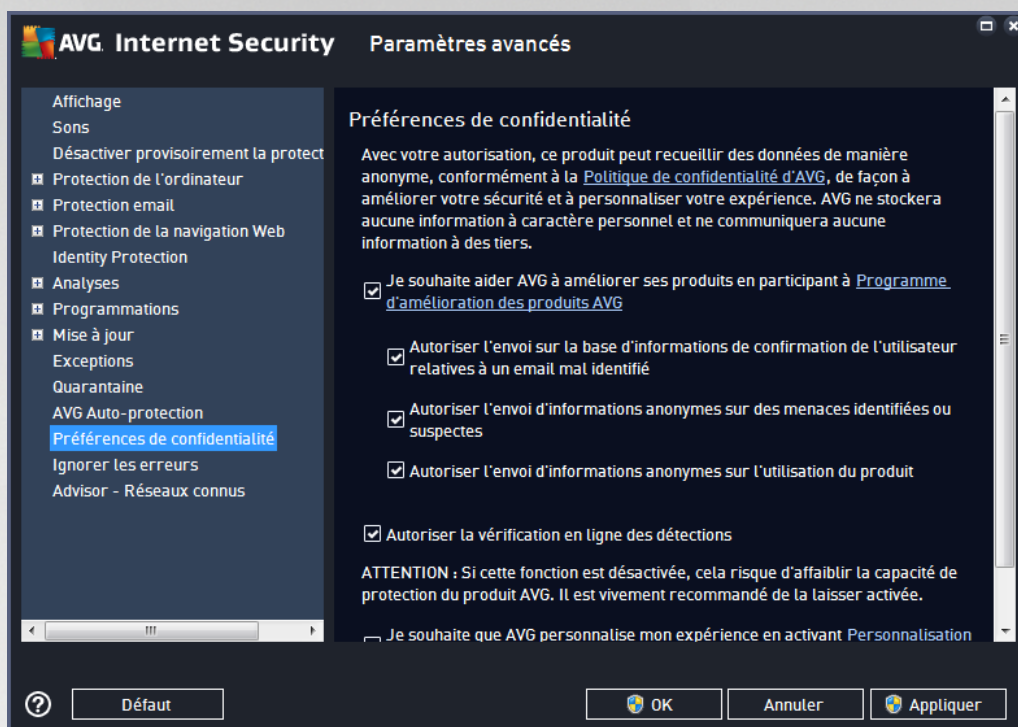
L'**Auto-protection AVG** permet à **AVG Internet Security** de protéger ses processus, fichiers, clés de registre et pilotes de toute modification ou désactivation. Ce type de protection s'avère particulièrement utile lorsque certaines menaces sophistiquées tentent de désactiver la protection antivirus pour être libre d'endommager votre ordinateur.

***Nous vous recommandons de conserver cette fonction activée !***

### 7.14. Préférences de confidentialité

La boîte de dialogue **Préférences de confidentialité** vous invite à participer à l'amélioration des produits AVG et à nous aider à optimiser le niveau général de sécurité Internet. Grâce à vos signalements, nous pourrions 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. Pour le confort des utilisateurs, les rapports sont générés automatiquement. Par ailleurs, aucune donnée personnelle n'est incluse dans ces rapports. Le signalement des menaces détectées est facultatif. Cependant, nous vous demandons de ne pas désactiver cette option. Elle nous permet d'améliorer votre protection et celle des autres utilisateurs d'AVG.





Les options de configuration suivantes sont disponibles dans la boîte de dialogue :

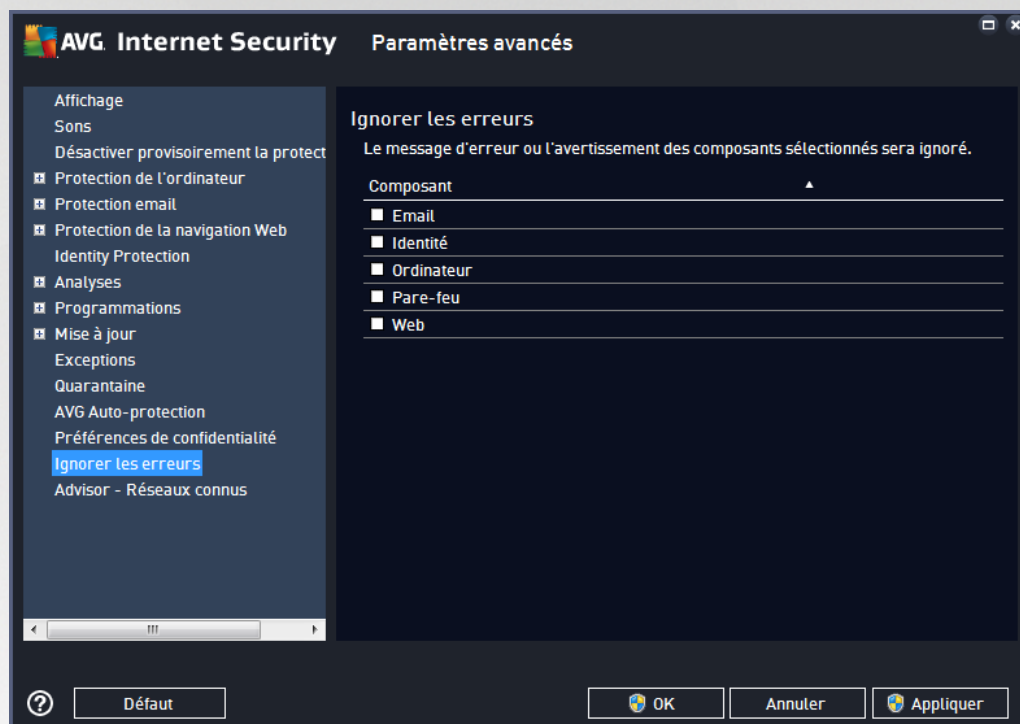
- **Autoriser le signalement (activée par défaut)** : cochez cette case si vous souhaitez nous aider à améliorer davantage **AVG Internet Security**. Ainsi, toutes les menaces seront signalées à AVG. Ce faisant, nous pourrions recueillir les dernières informations sur les nouvelles menaces signalées par les internautes du monde entier et, en retour, fournir à tous une meilleure protection en ligne. Pour le confort des utilisateurs, les rapports sont générés automatiquement. Par ailleurs, aucune donnée personnelle n'est incluse dans ces rapports.
  - **Autoriser l'envoi de données relatives à un email mal identifié avec l'accord de l'utilisateur (activée par défaut)** : envoyez des informations sur des messages identifiés, par erreur, comme spam ou sur du spam non détecté par l'Anti-Spam. Vous serez amené à confirmer l'envoi de ce genre d'informations.
  - **Autoriser l'envoi d'informations anonymes sur des menaces identifiées ou suspectes (activée par défaut)** : cette option permet d'envoyer des informations sur un code ou un type de comportement suspects ou dangereux (il peut s'agir d'un virus, d'un spyware ou d'une page Web malveillante) détectés sur l'ordinateur.
  - **Autoriser l'envoi d'informations anonymes sur l'utilisation du produit (activée par défaut)** : cette option permet d'envoyer des données statistiques sur l'utilisation de l'application, comme le nombre de détections, les analyses exécutées, les mises à jour réussies ou non, etc.
- **Autoriser la vérification en ligne des détections (activée par défaut)** : les menaces détectées seront examinées pour en exclure les faux positifs.
- **Je souhaite qu'AVG personnalise mon expérience en activant AVG Personalization (option désactivée par défaut)** : cette fonctionnalité analyse de manière anonyme le comportement des programmes et applications installés sur votre PC. En fonction de cette analyse, AVG peut vous



proposer des services ciblant directement vos besoins, afin de vous offrir un maximum de sécurité.

## 7.15. Ignorer les erreurs

Dans la boîte de dialogue *Ignorer les erreurs*, 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 [Informations sur l'état de la 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 pastel, l'icône ne peut plus signaler toute autre erreur susceptible d'apparaître par la suite.

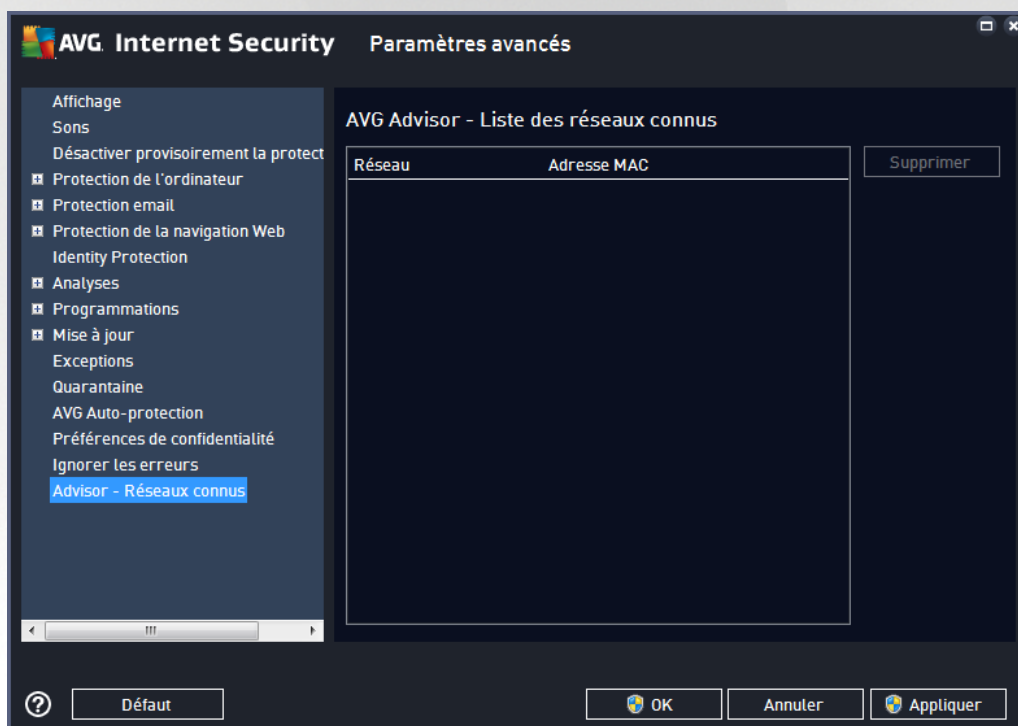
Aussi, dans la boîte de dialogue *Ignorer les erreurs*, sélectionnez les composants qui risquent de présenter une erreur (ou qui sont désactivés) dont vous voulez ignorer l'état. Cliquez sur **OK** pour confirmer.



## 7.16. Advisor – Réseaux connus

L'outil [AVG Advisor](#) comprend une fonction surveillant les réseaux auxquels vous vous connectez. Lorsqu'un nouveau réseau est disponible (*portant un nom réseau déjà utilisé, ce qui peut prêter à confusion*), il vous en informe et vous recommande de vérifier la sécurité de ce réseau. Si vous décidez que ce nouveau réseau est sécurisé, vous pouvez également l'enregistrer dans cette liste (*grâce au lien affiché dans la notification qui apparaît au-dessus de la barre d'état AVG Advisor à chaque fois qu'un réseau inconnu est détecté. Pour de plus amples informations, reportez-vous au chapitre sur [AVG Advisor](#).* [AVG Advisor](#) mémorise alors les attributs uniques de ce réseau (*en particulier l'adresse MAC*) et n'affichera plus la notification de ce réseau. Chaque réseau auquel vous vous connectez sera automatiquement considéré comme un réseau connu et ajouté à la liste. Vous pouvez supprimer des entrées individuelles en cliquant sur le bouton **Supprimer**. Le réseau correspondant sera alors à nouveau considéré comme inconnu et potentiellement non sûr.

Depuis cette boîte de dialogue, vous pouvez vérifier quels réseaux sont considérés comme des réseaux connus :



**Remarque :** la fonction AVG Advisor liée aux réseaux connus n'est pas prise en charge par les systèmes Windows XP 64 bits.



## 8. 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. La configuration du Pare-feu s'affiche dans une nouvelle fenêtre à partir de laquelle vous pouvez modifier les paramètres avancés du composant par le biais de plusieurs boîtes de dialogue de configuration. La configuration peut être affichée en mode basique ou expert. Le mode basique de configuration s'affiche à l'ouverture initiale de la fenêtre et vous permet de modifier les paramètres suivants :

- [Généralités](#)
- [Applications](#)
- [Partage de fichiers et d'imprimantes](#)

En bas de la boîte de dialogue, cliquez sur le bouton **Mode expert**. De nouveaux éléments s'affichent pour vous permettre de configurer les paramètres avancés du Pare-feu :

- [Paramètres avancés](#)
- [Réseaux définis](#)
- [Services système](#)
- [Journaux](#)

### 8.1. Généralités

La boîte de dialogue **Informations générales** fournit une vue d'ensemble de tous les modes disponibles pour le Pare-feu. Pour changer de mode Pare-feu, il vous suffit de sélectionner un autre mode dans le menu.

***Toutefois, l'éditeur du logiciel a configuré tous les composants d'AVG Internet Security de manière à optimiser les performances. Il est déconseillé de modifier la configuration par défaut du composant sans motif valable. Vous devez être un utilisateur expérimenté pour changer ces paramètres.***



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 mode particulier. En d'autres termes, un mode Pare-feu est une configuration spécifique du composant Pare-feu. Vous pouvez utiliser plusieurs configurations prédéfinies de ce type.

- **Automatique** : ce mode Pare-feu gère tout le trafic réseau automatiquement. Vous n'aurez aucune décision à prendre. Le Pare-feu autorisera la connexion des applications connues et créera une règle permettant à chacune d'entre elles de se connecter ultérieurement. Pour les autres applications, le Pare-feu décidera si la connexion doit être autorisée ou bloquée en fonction de leur comportement. Aucune règle ne sera créée pour ces applications, qui seront contrôlées à chaque fois qu'elles tenteront de se connecter. **Le mode Automatique est recommandé pour la majorité des utilisateurs, car il s'effectue discrètement.**
- **Interactif** : ce mode est utile si vous souhaitez contrôler intégralement le trafic entre le réseau et votre ordinateur. Le Pare-feu contrôle le trafic et vous informe à chaque tentative de communication ou de transfert de données, vous laissant le choix d'autoriser ou de bloquer cette opération au moment opportun. Réservé aux utilisateurs expérimentés.
- **Bloquer l'accès à Internet** : la connexion Internet est totalement bloquée ; vous ne pouvez pas accéder à Internet et aucune personne externe n'a accès à votre ordinateur. Ce mode est réservé pour des périodes courtes et spécifiques.
- **Désactiver la protection du pare-feu** : la désactivation du Pare-feu autorise la communication totale entre le réseau et votre ordinateur. Par conséquent, votre ordinateur est exposé aux attaques des pirates. Veuillez réfléchir attentivement avant d'utiliser cette option.

Notez qu'il existe également un mode automatique spécifique au sein du Pare-feu. Ce mode est toujours activé et protège votre ordinateur lorsque le composant [Ordinateur](#) ou [Identité](#) est désactivé. Dans un tel cas de figure, il autorise uniquement les applications connues et parfaitement sûres. Vous devrez choisir vous-même si les autres applications peuvent être ou non autorisées. Grâce à cette protection silencieuse, votre ordinateur reste à l'abri des attaques, même lorsque ces composants de protection sont désactivés.






## 8.2. Applications

La boîte de dialogue **Application** répertorie toutes les applications qui ont tenté de communiquer sur le réseau jusqu'à présent et les icônes affectées à l'action assignée :



Les applications figurant dans la **Liste des applications** sont celles qui ont été détectées sur l'ordinateur (et leurs actions respectives). Les types d'action suivants peuvent être utilisés :

-  : autoriser les communications pour tous les réseaux
-  : bloquer les communications
-  : définition des paramètres avancés

**Notez que seules les applications déjà installées ont pu être détectées. Par défaut, lorsque la nouvelle application tente de se connecter au 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 la communication. 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 » lorsqu'aucune règle d'application spécifique ne s'applique (par exemple, pour une application inconnue et non définie). Sélectionnez l'action à déclencher lorsqu'une telle application tente de communiquer sur le réseau : Bloquer (la communication sera toujours bloquée) ; Autoriser (la communication sera autorisée sur n'importe quel réseau) ; Demander (chaque fois que l'application tente de communiquer sur le réseau, vous serez invité à indiquer si cette communication doit être autorisée ou bloquée). **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 pas modifier ces paramètres !**

### Boutons de commande

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

- **Ajouter** : ouvre une boîte de dialogue vide pour définir de nouvelles règles d'application.
- **Modifier** : ouvre la même boîte de dialogue 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.

## 8.3. Partage de fichiers et d'imprimantes

Partager des fichiers et des imprimantes signifie partager tous les fichiers ou dossiers que vous signalez comme étant « Partagés » dans Windows, les unités de disque, les imprimantes, les scanners et autres appareils de ce type. Le partage de ces éléments n'est souhaitable qu'à l'intérieur d'un réseau que vous jugez sécurisé (*chez vous, au bureau ou à l'école, par exemple*). Toutefois, si vous êtes connecté à un réseau public (*WiFi d'un aéroport ou cybercafé, par exemple*), il est préférable de ne rien partager. Le Pare-feu AVG peut bloquer ou autoriser facilement le partage et vous permettre d'enregistrer votre choix pour les réseaux auxquels vous avez déjà accédé.

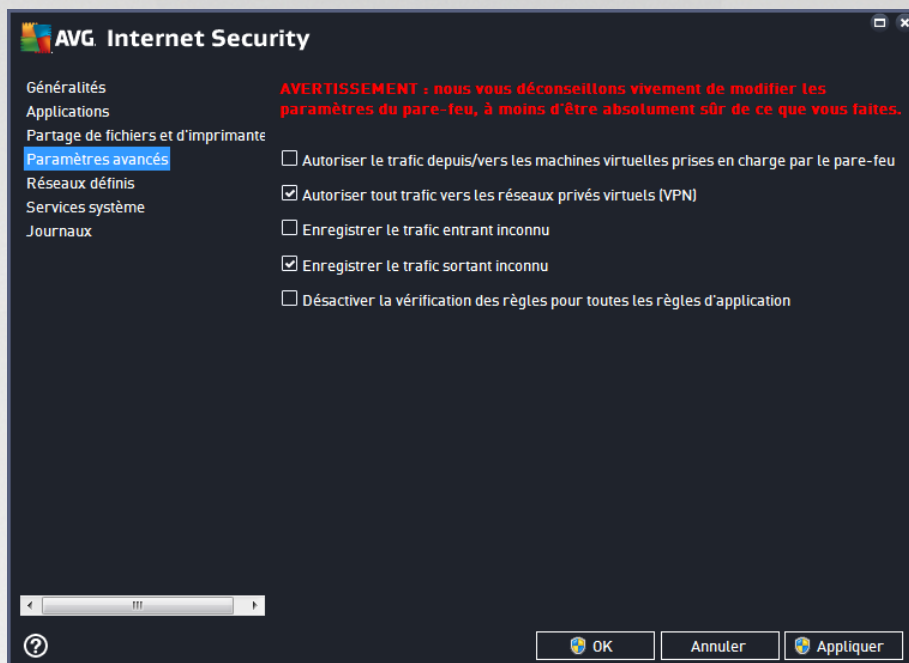


Dans la boîte de dialogue **Partage de fichiers et d'imprimantes**, vous pouvez modifier la configuration du partage des fichiers et des imprimantes actuellement connectés au réseau. Sous Windows XP, le nom du réseau correspond à l'appellation que vous avez choisie pour ce réseau spécifique au moment de la connexion initiale. A partir de Windows Vista, le nom de réseau est automatiquement issu du Centre Réseau et partage.



## 8.4. Paramètres avancés

**Vous devez être un utilisateur expérimenté pour apporter des modifications dans la boîte de dialogue Paramètres avancés.**



La boîte de dialogue **Paramètres avancés** vous permet d'activer ou non les paramètres de Pare-feu suivants :

- **Autoriser le trafic depuis/vers les machines virtuelles prises en charge par le pare-feu** : prise en charge de la connexion réseau pour les machines virtuelles comme VMware.
- **Autoriser tout trafic vers les réseaux privés virtuels (VPN)** : prise en charge des connexions VPN (aux ordinateurs distants)..
- **Enregistrer le trafic entrant/sortant inconnu** : toute tentative de communication (entrée ou sortie) par des applications inconnues est enregistrée dans le [journal du Pare-feu](#).
- **Désactiver la vérification de toutes les règles d'application** : le pare-feu surveille en permanence les fichiers couverts par chaque règle d'application. Lorsqu'une modification est apportée au fichier binaire, le pare-feu tente une fois de plus de confirmer la légitimité de l'application par des moyens classiques, à savoir en vérifiant son certificat, en recherchant dans la [base de données des applications fiables](#), etc. Si l'application ne peut être considérée comme sécurisée, le pare-feu menacera davantage l'application en fonction du [mode sélectionné](#) :
  - si le pare-feu fonctionne en [mode Automatique](#), l'application sera autorisée par défaut ;
  - si le pare-feu est en [mode Interactif](#), l'application sera bloquée et une boîte de dialogue s'affichera, demandant à l'utilisateur de décider comment traiter l'application.

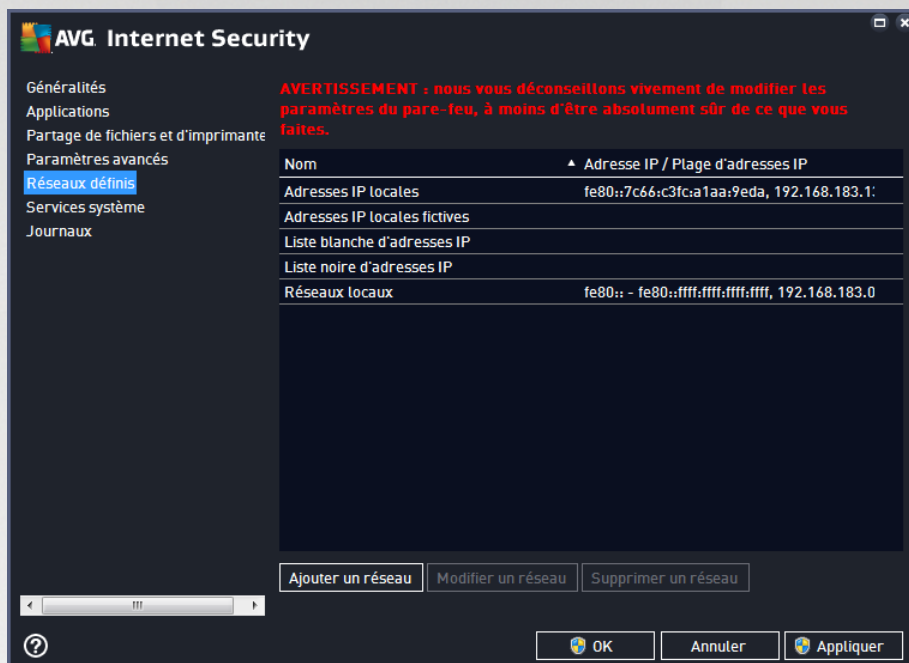
Naturellement, il est possible de sélectionner la procédure souhaitée séparément pour chaque application dans la boîte de dialogue [Applications](#).





## 8.5. Réseaux définis

**Seuls les utilisateurs expérimentés doivent apporter des modifications dans la boîte de dialogue Réseaux définis.**

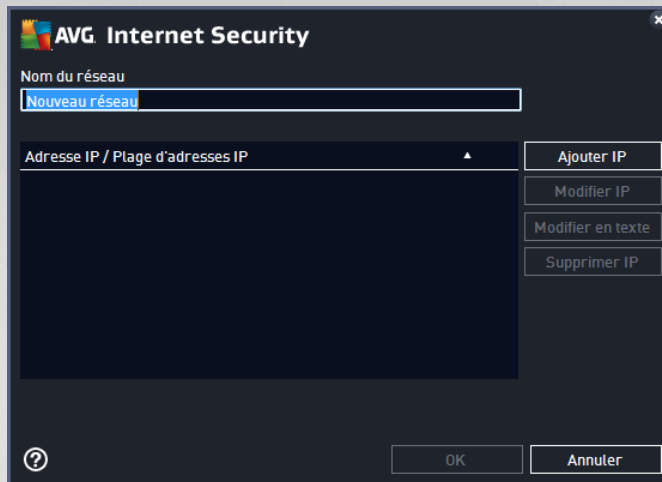


La boîte de dialogue **Réseaux définis** dresse la liste de tous les réseaux auxquels est relié l'ordinateur. La liste fournit les informations suivantes sur chaque réseau détecté :

- **Réseaux** : fournit la liste des réseaux auxquels l'ordinateur est relié.
- **Plage d'adresses IP** : chaque réseau est automatiquement détecté et spécifié sous la forme d'une plage d'adresses IP.

### Boutons de commande

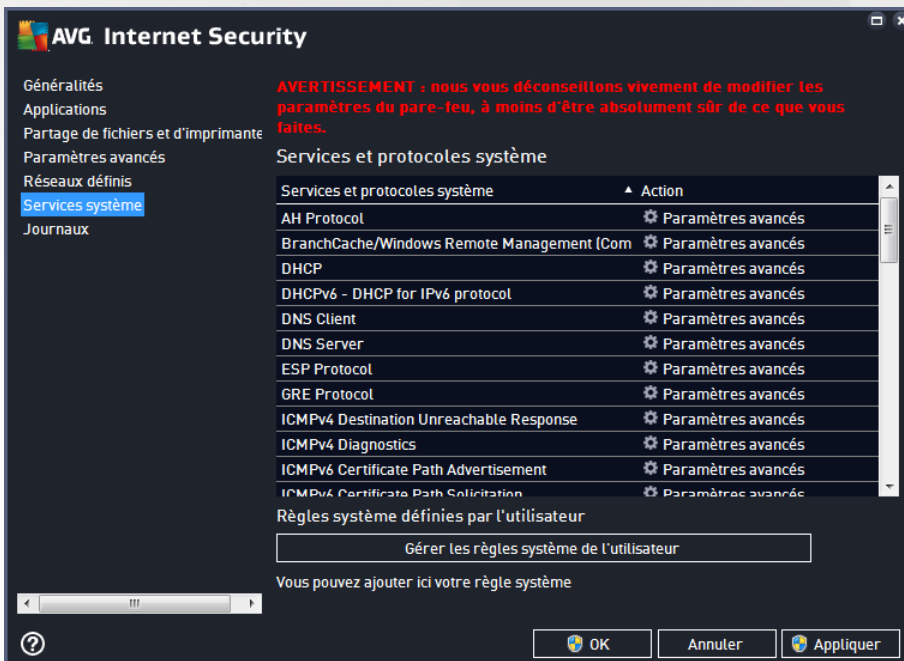
- **Ajouter un réseau** : ouvre une nouvelle boîte de dialogue dans laquelle vous pouvez modifier les paramètres du réseau qui vient d'être défini, par exemple, son **nom** et sa **plage d'adresses IP** :



- **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 (cette 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 au réseau sélectionné de la liste des réseaux.

## 8.6. Services système

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



La boîte de dialogue répertorie tous les services système et les protocoles standard qui pourraient être amenés à communiquer sur le réseau. Le tableau comporte les colonnes suivantes :

- **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
  - Bloquer les communications

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**. **Il est vivement conseillé de ne pas modifier la règle système et de ne réserver cette tâche qu'à des utilisateurs expérimentés.**

### 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 même boîte de dialogue s'affiche si vous décidez de modifier la configuration d'un élément de la liste des protocoles et services système existants. La partie supérieure de la boîte de dialogue présente tous les détails de la règle système en cours de modification et la partie inférieure affiche le détail sélectionné. Les détails des règles peuvent être modifiés, ajoutés ou supprimés à l'aide du bouton prévu à cet effet.



**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.**

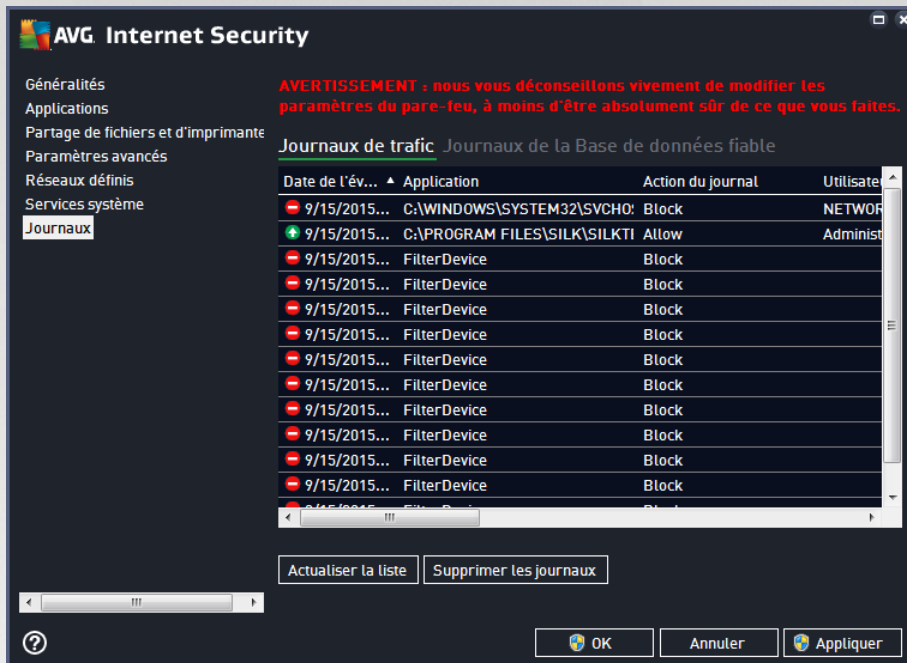
## 8.7. Les journaux

**Seuls les utilisateurs expérimentés doivent apporter des modifications dans la boîte de dialogue Journaux.**

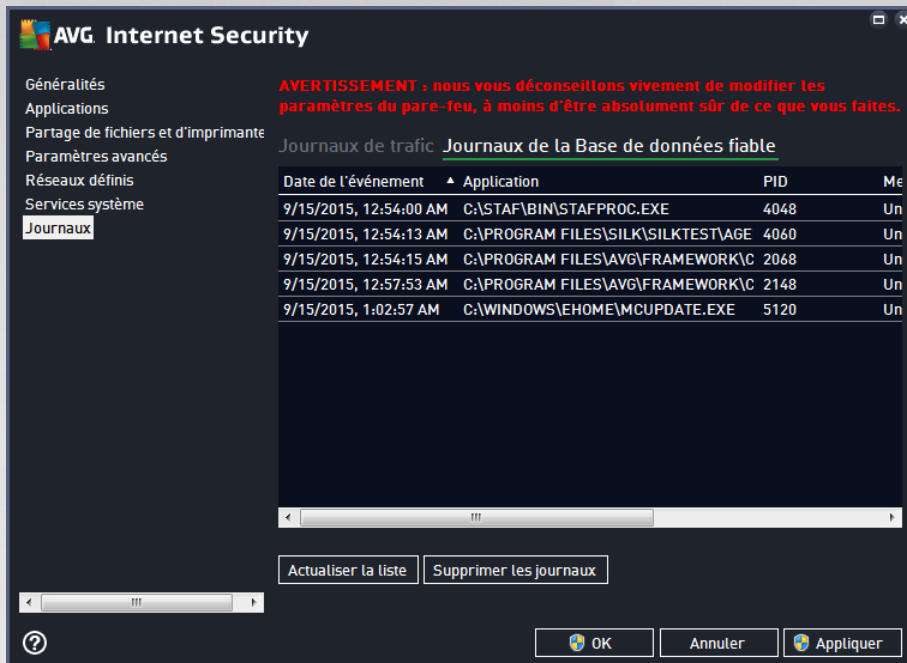
La boîte de dialogue **Journaux** permet de passer en revue l'ensemble des actions et des événements du Pare-feu qui ont été enregistrés ainsi que la description détaillée des paramètres associés sur deux onglets :



- **Journaux de trafic** : cet onglet fournit des informations sur les activités de toutes les applications qui ont essayé de se connecter au réseau. Pour chaque activité, vous pouvez connaître la date de l'événement, le nom de l'application, l'action du journal correspondante, le nom d'utilisateur, le PID, la direction du trafic, le type de protocole, les numéros des ports locaux et distants, etc.



- **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.



### 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.
- **Supprimer les journaux** : ce bouton supprime toutes les entrées du tableau.



## 9. Analyse AVG

Par défaut, **AVG Internet Security** n'exécute aucune analyse, car après l'analyse l'initiale (*que vous serez invité à lancer*), vous devriez être parfaitement protégé par les composants résidents d'**AVG Internet Security** qui restent toujours sur leur garde et ne laissent aucun code malveillant pénétrer dans l'ordinateur. Bien entendu, vous pouvez [programmer une analyse](#) à intervalle régulier ou exécuter manuellement une analyse à la demande quand bon vous semble.

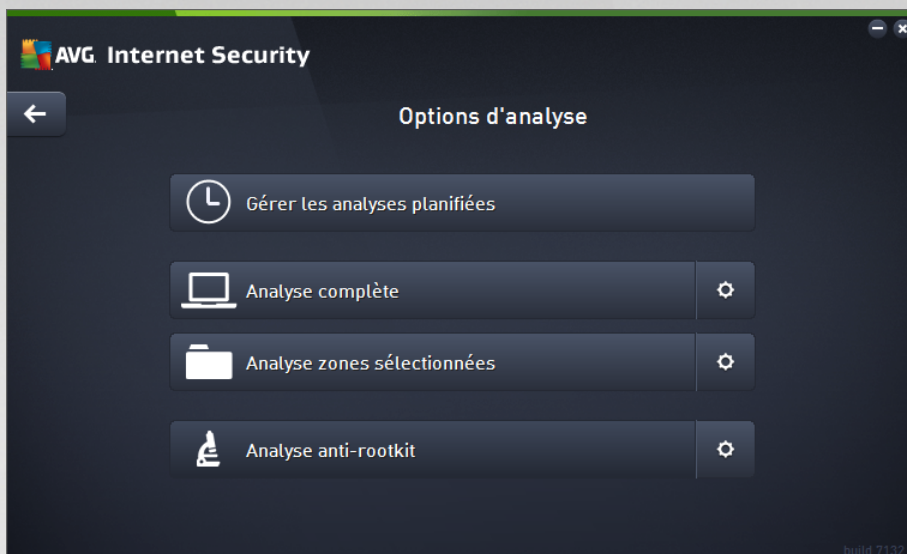
L'interface d'analyse AVG est accessible depuis l'[interface utilisateur principale](#) via le bouton subdivisé en deux

sections : 

- **Analyser maintenant** : appuyez sur le bouton pour lancer immédiatement l'[Analyse complète](#) et observer la progression et les résultats de l'opération dans la fenêtre [Rapports](#) qui s'ouvre immédiatement :



- **Options** : ce bouton (*qui s'affiche sous la forme de trois lignes horizontales dans un champ vert*) ouvre la boîte de dialogue des **Options d'analyse** dans laquelle vous pouvez [gérer les analyses planifiées](#) et modifier les paramètres de l'[Analyse complète](#) ou de l'[Analyse des fichiers ou des dossiers spécifiques](#).



La boîte de dialogue **Options d'analyse** est divisée en trois sections dédiées à la configuration de l'analyse.

- **Gérer les analyses planifiées** : ouvre une nouvelle [boîte de dialogue contenant toutes les programmations d'analyse](#). Avant de définir vos propres analyses, vous ne verrez dans le tableau qu'une seule analyse programmée, prédéfinie par l'éditeur du logiciel. Cette analyse est désactivée par défaut. Pour l'activer, cliquez avec le bouton droit de la souris et choisissez l'option *Activer la tâche* dans le menu contextuel. Une fois l'analyse programmée activée, vous pouvez [modifier sa configuration](#) à l'aide du bouton *Modifier la programmation de l'analyse*. Vous pouvez également cliquer sur le bouton *Ajouter une programmation d'analyse* pour créer votre propre programmation d'analyse.
- **Analyse complète / Paramètres** : ce bouton comprend deux sections. Cliquez sur *Analyse complète* pour lancer immédiatement l'analyse complète de l'ordinateur (*pour plus de détails sur cette analyse, veuillez vous reporter au chapitre correspondant intitulé [Analyses prédéfinies / Analyse complète](#)*). En cliquant sur *Paramètres*, vous accédez à la [boîte de dialogue de configuration de l'analyse complète de l'ordinateur](#).
- **Analyse des fichiers ou des dossiers spécifiques / Paramètres** : ce bouton comprend également deux sections. Cliquez sur *Analyse zones sélectionnées* pour lancer immédiatement l'analyse des zones de l'ordinateur que vous avez sélectionnées (*pour plus de détails sur cette analyse, veuillez vous reporter au chapitre correspondant intitulé [Analyses prédéfinies / Analyse zones sélectionnées](#)*). En cliquant sur *Paramètres*, vous accédez à la [boîte de dialogue de configuration de l'analyse des fichiers et dossiers sélectionnés](#).
- **Analyse de l'ordinateur à la recherche de rootkits / Paramètres** : la section de gauche du bouton libellé *Analyse de l'ordinateur à la recherche de rootkits* lance immédiatement l'analyse anti-rootkit (*pour plus de détails sur l'analyse anti-rootkit, reportez-vous au chapitre respectif intitulé [Analyses prédéfinies / Analyse de l'ordinateur à la recherche de rootkits](#)*). En cliquant sur *Paramètres*, vous accédez à la [boîte de dialogue de configuration de l'analyse anti-rootkit](#).



## 9.1. Analyses prédéfinies

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

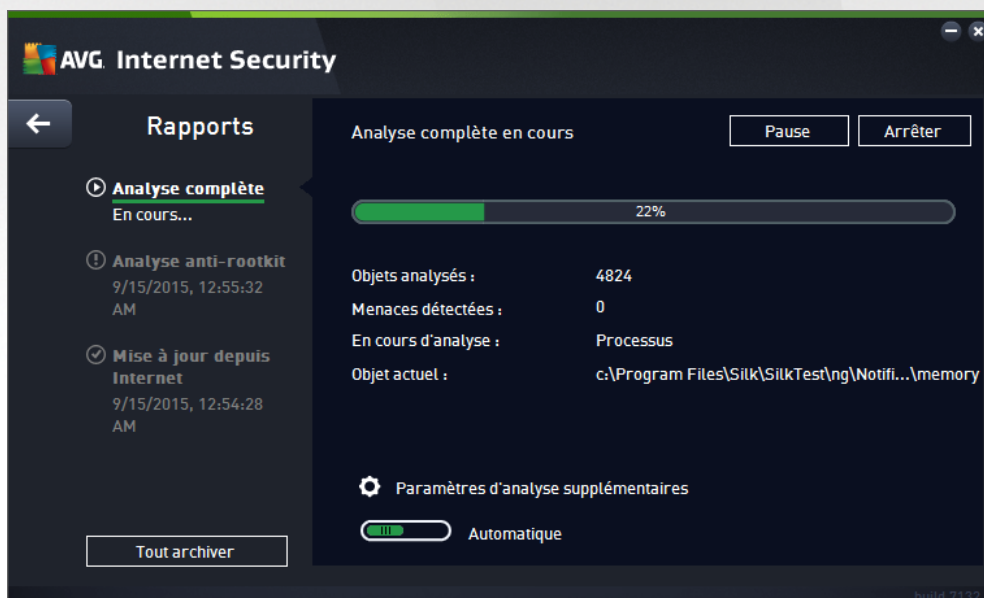
Dans **AVG Internet Security**, plusieurs types d'analyse prédéfinies par l'éditeur du logiciel sont disponibles :

### 9.1.1. 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 tous les disques durs de l'ordinateur, détecte et répare tous les virus trouvés ou retire l'infection en la confinant dans la zone de [Quarantaine](#). L'analyse complète doit être exécutée sur un ordinateur au moins une fois par semaine.

#### Lancement de l'analyse

L'**Analyse complète** peut être lancée directement depuis l'[interface utilisateur principale](#) en cliquant sur le bouton **Analyser**. 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 de **progression de l'analyse complète** (voir *capture d'écran*), vous pouvez vérifier la progression du processus d'analyse et les résultats obtenus. L'analyse peut être interrompue provisoirement (**Interrompre**) ou annulée (**Arrêter**) si nécessaire.



#### Modification de la configuration de l'analyse

Vous pouvez modifier la configuration de l'**Analyse complète** dans la **boîte de dialogue** Analyse complète - Paramètres (accessible par le biais du lien Paramètres associé à Analyse complète dans la boîte de dialogue [Options d'analyse](#)). **Il est recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité.**





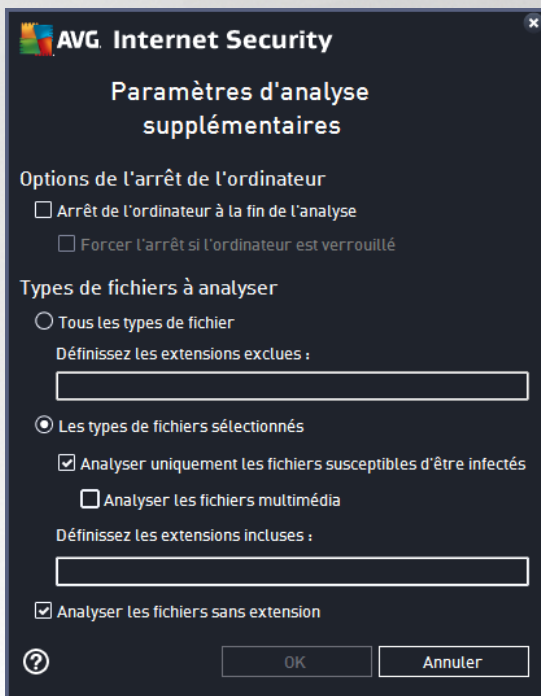
Dans la liste des paramètres d'analyse, vous pouvez activer/désactiver des paramètres spécifiques en fonction de vos besoins :

- **Réparer/supprimer les infections sans me demander** (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 spyware** (option activée par défaut) : cochez cette case pour activer la recherche de spyware et de virus. Les spyware désignent une catégorie de programmes malveillants : 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 ordinateur.
- **Signaler le jeu amélioré de programmes potentiellement dangereux** (option désactivée par défaut) : l'indication permet de détecter les jeux étendus de spyware 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 utilisés 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) : avec ce paramètre, les cookies sont 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).
- **Rechercher dans les archives** (option désactivée par défaut) : avec ce paramètre, 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 qui analyseront jusqu'aux zones de l'ordinateur les moins susceptibles d'être infectées. Gardez à l'esprit que cette méthode prend énormément de temps.
- **Analyser les rootkits** (option activée par défaut) : ajoute l'analyse anti-rootkit à l'analyse complète de l'ordinateur. L'[analyse Anti-rootkit](#) peut aussi être lancée séparément.
- **Paramètres d'analyse supplémentaires** : ce lien ouvre une nouvelle boîte de dialogue Paramètres d'analyse supplémentaires permettant de spécifier les paramètres suivants :



- **Options d'arrêt de l'ordinateur** : indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. 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.
- **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 à ne pas analyser (séparées par des virgules) ;
  - **Types de fichiers sélectionnés** : vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent être infectés 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 multimédias (*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, cette option est réglée sur le niveau *automatique* d'utilisation des ressources. 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 signaler :



**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.

### 9.1.2. Analyse des fichiers ou dossiers sélectionnés

**Analyse zones sélectionnées** : analyse uniquement les zones de l'ordinateur que vous avez sélectionnées (*dossiers, disques 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 la boîte de dialogue [Options d'analyse](#) en cliquant sur le bouton **Analyse zones sélectionnées**. 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 le champ situé dans la partie supérieure de cette boîte de dialogue. Il est également 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**

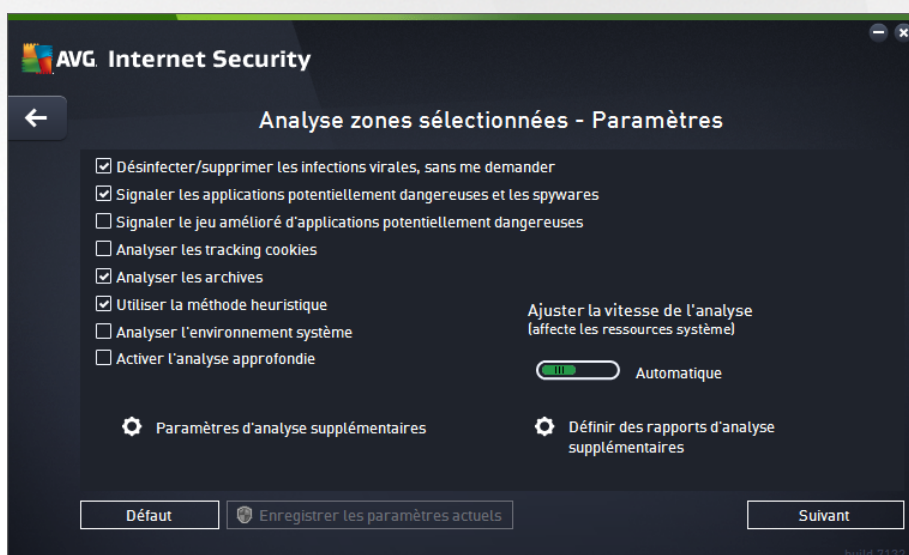


*l'analyse* ; le processus est fondamentalement identique à celui de l'[analyse complète](#) de l'ordinateur.



### Modification de la configuration de l'analyse

Vous pouvez modifier la configuration de l'**Analyse zones sélectionnées** dans la boîte de dialogue **Analyse zones sélectionnées - Paramètres** (accessible par le biais du lien Paramètres associé à Analyse zones sélectionnées dans la boîte de dialogue [Options d'analyse](#)). **Il est recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité.**



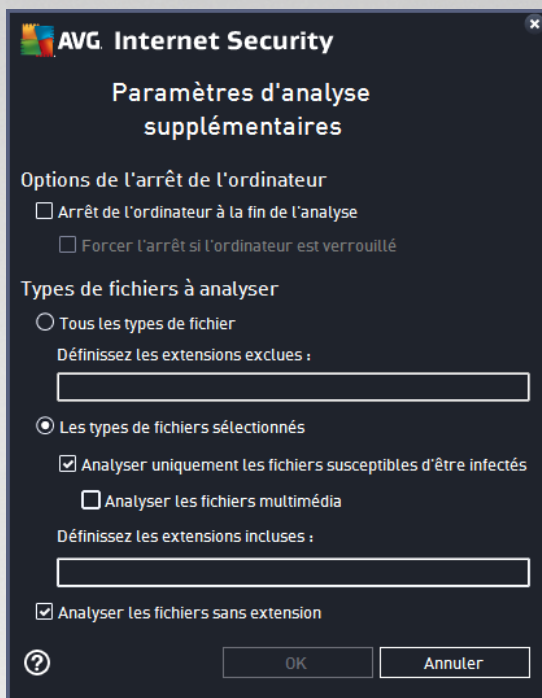
Dans la liste des paramètres d'analyse, vous pouvez activer/désactiver des paramètres spécifiques en fonction de vos besoins :

- **Désinfecter/supprimer les infections virales sans me demander** (option activée par défaut) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement, si cela est possible.



S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en [Quarantaine](#).

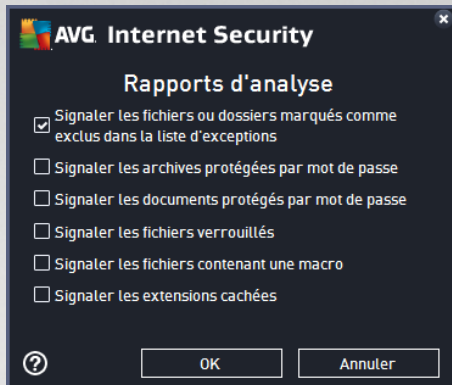
- **Signaler les applications potentiellement dangereuses et les spyware** (option activée par défaut) : cochez cette case pour activer la recherche de spyware et de virus. Les spyware désignent une catégorie de programmes malveillants : même s'ils représentent généralement un risque pour la sécurité, 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 ordinateur.
- **Signaler le jeu amélioré d'applications potentiellement dangereuses** (option désactivée par défaut) : l'indication permet de détecter les jeux étendus de spyware 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 utilisés 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 activée par défaut) : Avec ce paramètre, les cookies sont 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 rootkits** (option activée par défaut) : Ce paramètre indique que l'analyse doit examiner tous les fichiers stockés dans des archives ZIP, RAR etc.
- **Utiliser la méthode heuristique** (option activée par défaut) : L'analyse heuristique (émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel) est l'une des méthodes employées pour détecter des virus pendant l'analyse.
- **Analyser l'environnement système** (option désactivée par défaut) : L'analyse vérifiera également 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 qui analyseront jusqu'aux zones de l'ordinateur les moins susceptibles d'être 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 d'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.
- **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 à ne pas analyser (séparées par des virgules).
  - **Types de fichiers sélectionnés** : vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent être infectés 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 multimédias (*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, cette option est réglée sur le niveau *automatique* d'utilisation des ressources. 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](#)).

### 9.1.3. Analyse de l'ordinateur à la recherche de rootkits

**Analyse de l'ordinateur à la recherche de rootkits** permet de détecter et de supprimer les rootkits dangereux de manière efficace. Ces derniers sont des programmes et technologies de camouflage destinés à masquer la présence de logiciels malveillants sur l'ordinateur. Un rootkit est conçu pour prendre le contrôle du système, sans l'autorisation de son propriétaire et de son administrateur légitime. L'analyse peut détecter des rootkits selon un ensemble de règles prédéfinies. Si un rootkit est trouvé, il n'est pas nécessairement infecté. Certains rootkits peuvent être utilisés comme pilotes ou faire partie d'applications valides.

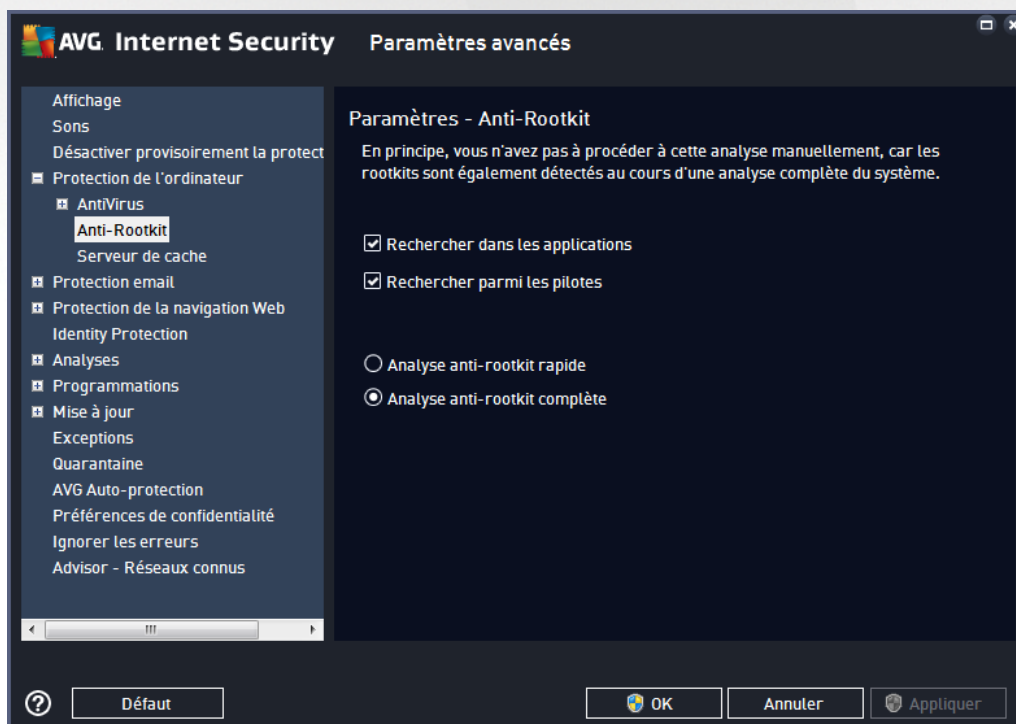
#### Lancement de l'analyse

**Analyse de l'ordinateur à la recherche de rootkits** peut être lancée directement depuis la boîte de dialogue [Options d'analyse](#) en cliquant sur le bouton **Analyse de l'ordinateur à la recherche de rootkits**. Une nouvelle boîte de dialogue nommée **Analyse anti-rootkit en cours** affiche la progression de l'analyse lancée :



### Modification de la configuration de l'analyse

Vous pouvez modifier la configuration de l'analyse anti-rootkit dans la boîte de dialogue **Paramètres de l'anti-rootkit** (accessible par le biais du lien Paramètres associé à Analyse de l'ordinateur à la recherche de rootkits dans la boîte de dialogue [Options d'analyse](#)). **Il est recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité.**



**Rechercher dans les applications** et **Rechercher parmi les pilotes** vous permettent de préciser en détail les éléments à inclure dans l'analyse anti-rootkit. Ces paramètres sont destinés à des utilisateurs expérimentés ;



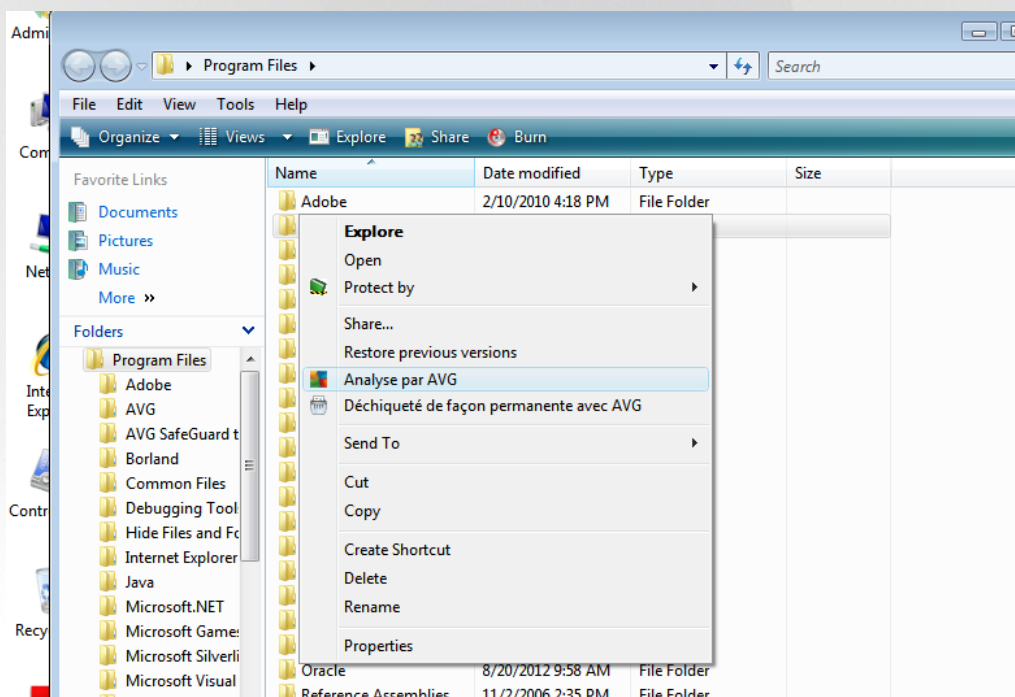


nous vous recommandons de conserver toutes les options actives. Vous pouvez ensuite choisir le mode d'analyse des rootkits :

- **Analyse anti-rootkit rapide** : analyse tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows généralement*)
- **Analyse anti-rootkit complète** : analyse tous les processus en cours d'exécution, tous 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*)

## 9.2. Analyse contextuelle

Outre les analyses prédéfinies exécutées sur l'ensemble ou des zones sélectionnées de l'ordinateur, **AVG Internet Security** 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 Internet Security**

## 9.3. Analyse en ligne de commande

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



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

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

### 9.3.1. 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 /parameter /parameter** .. si plusieurs paramètres sont précisés, spécifiez-les les uns à la suite des autres en les séparant par un espace et une barre oblique)
- si un paramètre requiert la saisie d'une valeur spécifique (par exemple, pour le paramètre **/scan**, le ou les chemins vers les zones de l'ordinateur à analyser), il faut séparer ces valeurs par un point-virgule, par exemple : **avgscanx /scan=C:\;D:\**

### 9.3.2. Paramètres d'analyse

Pour afficher la liste complète des paramètres disponibles, saisissez la commande concernée ainsi que le paramètre **/?** ou **/HELP** (par 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**. Durant l'analyse, vous pouvez arrêter le processus en appuyant simultanément sur les touches **Ctrl+C** ou **Ctrl+Pause**.



### 9.3.3. 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 :



En mode sans échec, l'analyse elle-même se lance depuis la ligne de commande. Cette boîte de dialogue vous permet uniquement de spécifier les paramètres d'analyse depuis l'interface graphique confortable.

Sélectionnez d'abord les zones de l'ordinateur que vous souhaitez analyser : Vous avez le choix entre l'**Analyse complète** prédéfinie ou l'option **Analyse des fichiers ou des dossiers sélectionnés**. La troisième option, **Analyse rapide**, lance une analyse spécifique conçue pour le mode sans échec qui inspecte toutes les zones critiques de votre ordinateur nécessaires pour démarrer.

Les paramètres d'analyse présentés dans la section suivante vous permettent de spécifier en détail les paramètres d'analyse. Tous les paramètres sont cochés par défaut. Il est recommandé de les laisser ainsi et de n'en désactiver un que dans un but précis

- **Analyser les « applications potentiellement dangereuses »** : analyse le système à la recherche de spywares (en plus des virus)
- **Analyser les flux de données alternatifs (NTFS uniquement)** : analyse les flux de données NTFS ; il s'agit d'une fonction Windows que les hackers peuvent détourner en vue de masquer des données et notamment des codes malveillants.
- **Réparer ou supprimer les infections automatiquement** : toute détection éventuelle sera prise en charge et automatiquement réparée/supprimée de votre ordinateur
- **Analyser les processus actifs** : analyse les processus et les applications chargés dans la mémoire de votre ordinateur.
- **Analyser la base de registre** : analyse le registre Windows.



- **Activer la vérification Master Boot Record** : analyse la table de partition et le secteur d'amorce.

Enfin, dans la partie inférieure de cette boîte de dialogue, vous pouvez spécifier le nom et le type du fichier à utiliser pour le rapport d'analyse.

### 9.3.4. Paramètres d'analyse CMD

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

- `/?` Affichage de l'aide sur un sujet
- `/@` Fichier de commande /nom du fichier/
- `/ADS` Analyser les flux de données alternatifs (*NTFS uniquement*)
- `/ARC` Analyser les archive
- `/ARCBOMBSW` Signaler les fichiers archives recompressés
- `/ARCBOMBSW` Signaler les bombes d'archives (*archives recompressées*)
- `/BOOT` Activer la vérification MBR/BOOT
- `/BOOTPATH` Lancer QuickScan
- `/CLEAN` Nettoyer automatiquement
- `/CLOUDCHECK` Vérifier les fausses détections
- `/COMP` [Analyse complète](#)
- `/COO` Analyser les cookies
- `/EXCLUDE` Fichiers ou chemin exclus de l'analyse
- `/EXT` Analyser ces extensions (*par exemple EXT=EXE,DLL*)
- `/FORCESHUTDOWN` Forcer l'arrêt de l'ordinateur à la fin de l'analyse
- `/HELP`  
affiché Afficher la rubrique d'aide en rapport avec l'élément actuellement sélectionné ou affiché
- `/HEUR` Utiliser l'analyse heuristique
- `/HIDDEN` Signaler des fichiers dont l'extension est masquée
- `/IGNLOCKED` Ignorer les fichiers verrouillés
- `/INFECTABLEONLY` Analyser uniquement les fichiers qui, d'après leur extension, sont susceptibles d'être infectés
- `/LOG` Générer un fichier contenant le résultat de l'analyse

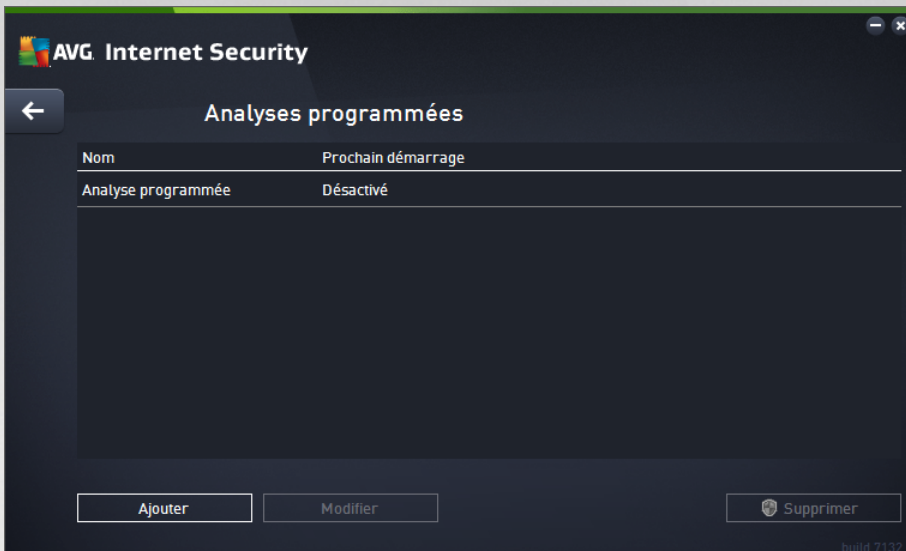


- /MACROW Signaler les macros
- /NOBREAK Ne pas autoriser CTRL-PAUSE pour arrêter
- /NOEXT Ne pas analyser ces extensions (*par exemple NOEXT=JPG*)
- /PRIORITY Définir la priorité de l'analyse (*Faible, Auto, Élevée - voir [Paramètres avancés / Analyses](#)*)
- /PROC Analyser les processus actifs
- /PUP Signaler les programmes potentiellement dangereux
- /PUPEXT Signaler un jeu amélioré de programmes potentiellement dangereux
- /PWDW Signaler les fichiers protégés par un mot de passe
- /QT Analyse rapide
- /REG Analyser la base de registre
- /REPAPPEND Inclure dans le fichier de rapport
- /REPOK Avertir l'utilisateur des fichiers non infectés
- /REPORT Reporter dans le fichier (*nom du fichier*)
- /SCAN [Analyse de fichiers ou de dossiers spécifiques](#) (*SCAN=chemin ; chemin (ex. : / SCAN=C:\;D:\)*)
- /SHUTDOWN Arrêter l'ordinateur à la fin de l'analyse
- /THOROUGHSCAN Exécuter une analyse approfondie
- /TRASH Mettre les fichiers en [Quarantaine](#)

## 9.4. Programmation d'une analyse


Avec **AVG Internet Security**, 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 allumé », vous pouvez programmer l'analyse en dehors de vos heures de travail. Si l'ordinateur est parfois éteint, programmez une analyse [au démarrage de l'ordinateur lorsqu'elle n'a pas pu être effectuée](#).

Le programme d'analyse peut être créé / modifié dans la boîte de dialogue **Analyses programmées**, accessible par le biais du bouton **Gérer les analyses planifiées** dans la boîte de dialogue [Options d'analyse](#). Cette boîte de dialogue répertorie toutes les analyses actuellement programmées :

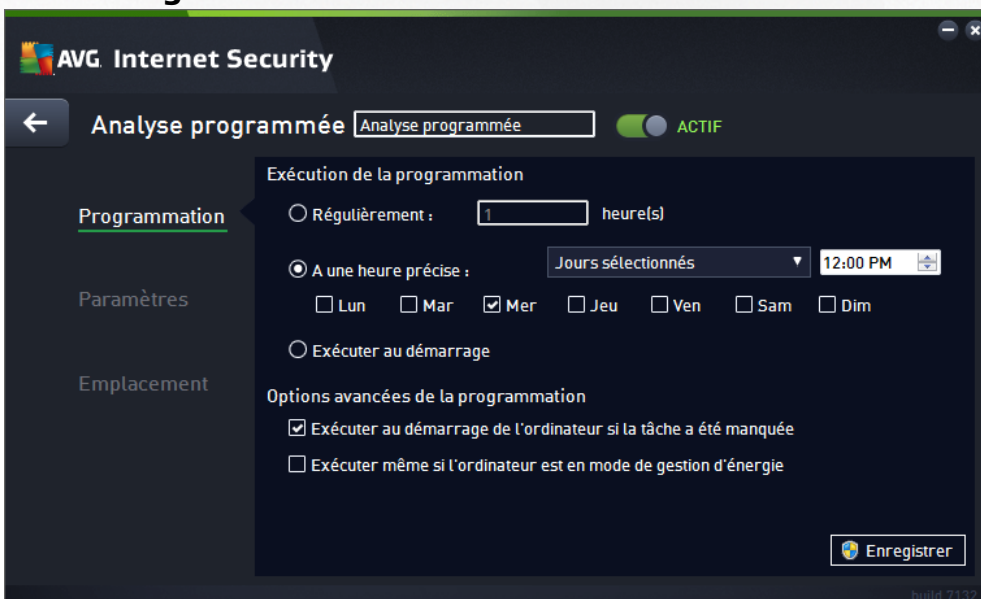


Dans la boîte de dialogue, vous pouvez spécifier vos propres analyses. Cliquez sur le bouton **Ajouter** pour créer votre propre programmation d'analyse. Les paramètres de l'analyse programmée peuvent être modifiés (ou une nouvelle analyse peut être programmée) depuis les trois onglets :

- [Programmation](#)
- [Paramètres](#)
- [Emplacement](#)

Dans chaque onglet, cliquez simplement sur le bouton de « feu tricolore »  pour désactiver temporairement l'analyse programmée et la réactiver au moment opportun.

### 9.4.1. Programmation






Dans la partie supérieure de l'onglet **Programmation**, vous pouvez spécifier le nom du programme d'analyse actuellement défini dans la zone de texte correspondante. Veillez à utiliser toujours des noms courts, descriptifs et appropriés pour distinguer facilement les différentes analyses par la suite. Par 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. À l'inverse, "Analyser l'environnement système" est un nom descriptif précis.

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

- **Exécution de la programmation** : spécifiez ici l'intervalle entre chaque exécution de la nouvelle analyse. La périodicité de l'analyse peut être programmée à des intervalles réguliers (*Régulièrement*), à une date et une heure précises (*A une heure précise*) ou encore être associée à un événement (*Exécuter au démarrage*).
- **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, vous en êtes informé par le biais d'une fenêtre contextuelle sur 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.

### Commandes de la boîte de dialogue

- **Enregistrer** : enregistre toutes les modifications entrées dans l'onglet en cours, ou dans un autre onglet de cette boîte de dialogue, et retourne à la vue [Analyses programmées](#). Par conséquent, si vous désirez configurer les paramètres d'analyse répartis dans tous les onglets, cliquez uniquement sur ce bouton après avoir défini tous vos choix.
-  : utilisez la flèche verte située dans la partie supérieure gauche de la fenêtre pour retourner à la vue [Analyses programmées](#).



## 9.4.2. Emplacement



Dans la partie supérieure de l'onglet **Paramètres**, vous pouvez spécifier le nom du programme d'analyse actuellement défini dans la zone de texte correspondante. Veillez à utiliser toujours des noms courts, descriptifs et appropriés pour distinguer facilement les différentes analyses par la suite. Par 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. À l'inverse, "Analyser l'environnement système" est un nom descriptif précis.

Sous l'onglet **Paramètres de l'analyse**, vous trouverez une liste de paramètres d'analyse qui peuvent être activés ou désactivés. **Il est vivement conseillé de ne pas modifier la configuration prédéfinie sans motif valable :**

- **Désinfecter/supprimer les infections virales sans me demander** (option activée par défaut) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement, si cela est possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en [Quarantaine](#).
- **Signaler les applications potentiellement dangereuses et les spyware** (option activée par défaut) : cochez cette case pour activer la recherche de spyware et de virus. Les spyware désignent une catégorie de programmes malveillants : 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 ordinateur.
- **Signaler le jeu amélioré d'applications potentiellement dangereuses** (option désactivée par défaut) : l'indication permet de détecter les jeux étendus de spyware 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 utilisés 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) : avec ce paramètre, les cookies sont 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).

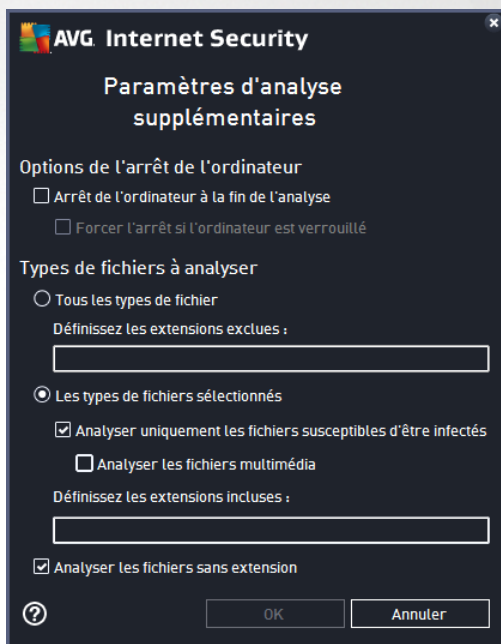




- **Analyser les archives** (*option désactivée par défaut*) : ce paramètre indique que l'analyse doit examiner tous les fichiers, y compris ceux stockés dans des formats d'archives (archives ZIP, RAR etc.).
- **Utiliser la méthode heuristique** (*option activée par défaut*) : l'analyse heuristique (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*) est l'une des méthodes employées pour détecter des virus pendant l'analyse.
- **Analyser l'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 qui analyseront jusqu'aux zones de l'ordinateur les moins susceptibles d'être infectées. Gardez à l'esprit que cette méthode prend énormément de temps.
- **Analyser les rootkits** : (*option activée par défaut*) 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.

### Paramètres d'analyse supplémentaires

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



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



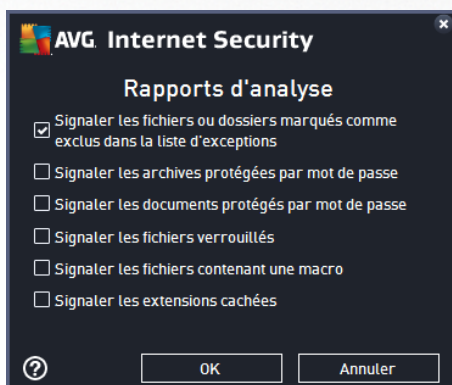
- **Types de fichiers à analyser** : vous devez également choisir d'analyser :
  - **Tous les types de fichier** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers à ne pas analyser (séparées par des virgules) ;
  - **Types de fichiers sélectionnés** : vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent être infectés 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 multimédias (*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 cette section, il est possible de régler la vitesse d'analyse en fonction des ressources système. Par défaut, cette option est réglée sur le niveau *automatique* d'utilisation des ressources. Cette configuration permet d'accélérer l'analyse : elle réduit le temps 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 la quantité de ressources système utilisées en augmentant la durée de l'analyse.

### Définir des rapports d'analyse supplémentaires

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




### Commandes de la boîte de dialogue

- **Enregistrer** : enregistre toutes les modifications entrées dans l'onglet en cours, ou dans un autre onglet de cette boîte de dialogue, et retourne à la vue [Analyses programmées](#). Par conséquent, si



vous désirez configurer les paramètres d'analyse répartis dans tous les onglets, cliquez uniquement sur ce bouton après avoir défini tous vos choix.

-  : utilisez la flèche verte située dans la partie supérieure gauche de la fenêtre pour retourner à la vue [Analyses programmées](#).

### 9.4.3. des paramètres



Sous l'onglet **Localisation**, 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 sont 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**
  - pour Windows XP : C:\Documents and Settings\Utilisateur\Mes Documents\
    - pour Windows 7 : C:\Users\Utilisateur\Documents



- pour Windows Vista/7 : C:\Utilisateurs\utilisateur\Documents\
- **Documents partagés**
  - pour Windows XP : C:\Documents and Settings\All Users\Documents\
  - pour Windows Vista/7 : C:\Users\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)

### Commandes de la boîte de dialogue

- **Enregistrer** : enregistre toutes les modifications entrées dans l'onglet en cours, ou dans un autre onglet de cette boîte de dialogue, et retourne à la vue [Analyses programmées](#). Par conséquent, si vous désirez configurer les paramètres d'analyse répartis dans tous les onglets, cliquez uniquement sur ce bouton après avoir défini tous vos choix.
-  : utilisez la flèche verte située dans la partie supérieure gauche de la fenêtre pour retourner à la vue [Analyses programmées](#).



## 9.5. Résultats des analyses

Nom	Heure de début	Heure de fin	Objets analysés	Infections	Supér
Analyse anti-rootkit	9/11/2015, 8:12	9/11/2015, 8:12	19132	0	0
Analyse complète	9/11/2015, 8:12	9/11/2015, 8:12	4844	0	0

La vue **Résultats d'analyse** contient une liste des résultats de toutes les analyses effectuées jusqu'à présent. Ce tableau fournit les informations suivantes sur chaque processus d'analyse :

- **Icônes**  : dans la première colonne, l'état de l'analyse est indiqué par une icône :
  - Aucune infection détectée ; analyse terminée
  - Aucune infection détectée ; l'analyse a été interrompue prématurément
  - Des infections ont été trouvées, mais n'ont pas été traitées ; analyse terminée
  - Des infections ont été trouvées, mais n'ont pas été traitées ; l'analyse a été interrompue prématurément
  - Des infections ont été trouvées et entièrement traitées ou supprimées ; analyse terminée
  - Des infections ont été trouvées et entièrement traitées ou supprimées ; l'analyse a été interrompue prématurément
- **Nom** : cette colonne précise le nom de chaque analyse. Il peut s'agir de l'une des [analyses prédéfinies](#) ou d'une [analyse programmée](#) par vous.
- **Heure de début** : date et heure précises de lancement de l'analyse.
- **Heure de fin** : date et heure précises de fin ou d'interruption de l'analyse.
- **Objets analysés** : indique le nombre total de tous les objets analysés.
- **Infections** : indique le nombre d'infections supprimées/totales.
- **Elevé / Moyen / Faible** : ces trois colonnes consécutives indiquent le nombre d'infections de risque




élevé, moyen ou faible détectées pour chaque analyse.

- **Rootkits** : indique le nombre total de [rootkits](#) détectés pendant l'analyse.

### Commandes de la boîte de dialogue

**Voir les détails** : permet d'afficher des [informations détaillées sur une analyse sélectionnée](#) (*en surbrillance dans le tableau ci-dessus*).


**Supprimer ce résultat** : supprime les résultats d'une analyse dans la liste.

 : utilisez la flèche verte située dans la partie supérieure gauche de la fenêtre pour retourner à [l'interface utilisateur principale](#) qui répertorie les composants.


## 9.6. Détails des résultats d'analyse

Pour ouvrir une vue détaillée des résultats de l'analyse sélectionnée, cliquez sur le bouton **Afficher les détails** dans la boîte de dialogue [Résultats d'analyse](#). Vous êtes redirigé vers la même interface qui fournit des informations détaillées sur les résultats d'une analyse spécifique. Ces informations sont réparties dans trois onglets :

- **Récapitulatif** : ce tableau vous donne des informations de base relatives à l'analyse : si elle a été effectuée avec succès, si des menaces ou des objets suspects ont été trouvés et le traitement qui leur a été appliqué.
- **Détails** : cet onglet affiche toutes les informations relatives à l'analyse, y compris les détails des menaces détectées. L'option Exporter les données dans le fichier permet de les enregistrer au format .csv.
- **Détections** : Ce tableau ne s'affiche que si des menaces ont été détectées au cours de l'analyse, et fournit des informations détaillées sur les menaces :

 **Gravité informationnelle** : informations ou avertissements, il ne s'agit pas de menaces réelles. Généralement, des documents contenant des macros, documents ou archives protégés par mot de passe, fichiers verrouillés etc.

 **Gravité moyenne** : généralement des applications potentiellement indésirables (*telles que les adwares*) ou des cookies de suivi.

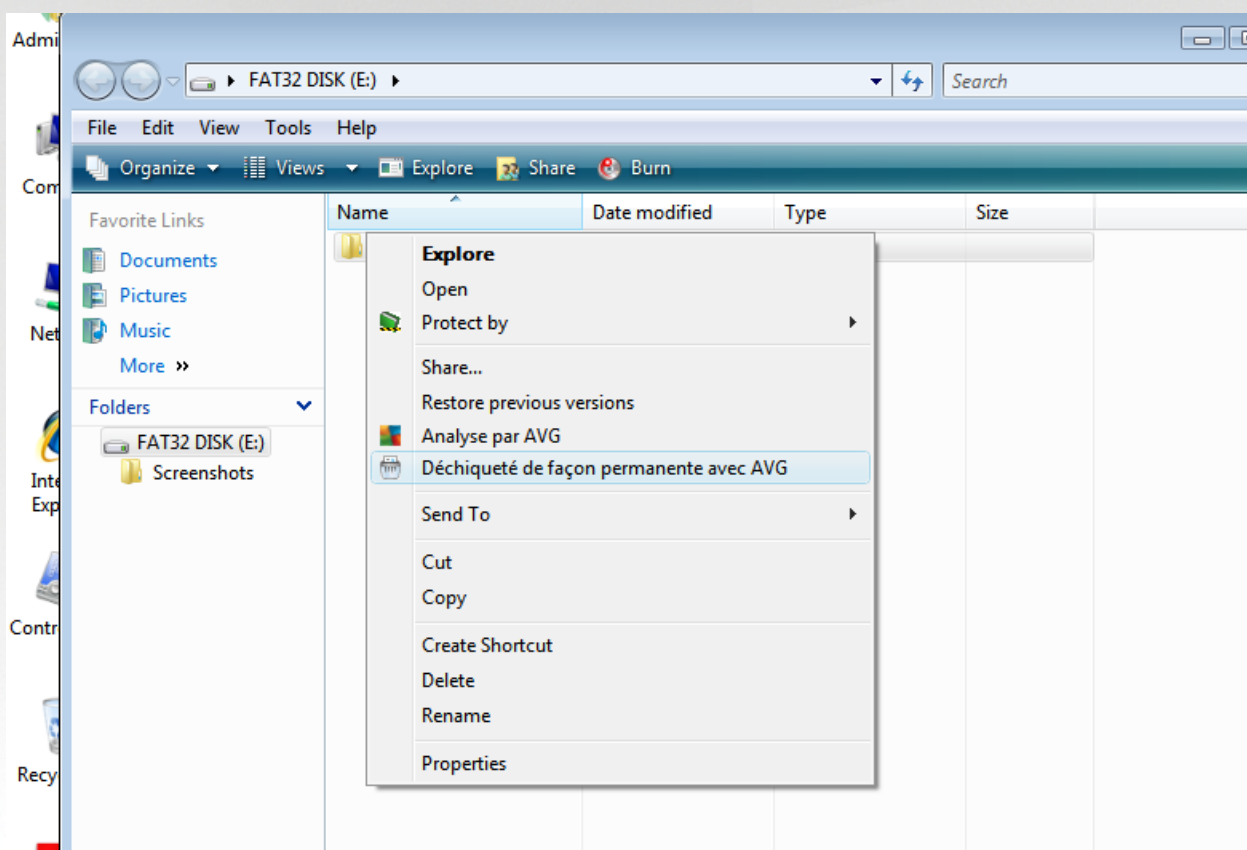
 **Gravité supérieure** : menaces sérieuses telles que des virus, chevaux de Troie, programmes d'intrusion etc. Il peut également s'agir d'objets détectés au moyen de la méthode de détection heuristique, par exemple des menaces non décrites dans la base de données virales.



## 10. AVG File Shredder

**AVG File Shredder** a été conçu pour effacer des fichiers de façon totalement sécurisée, c'est-à-dire de manière à ne laisser aucune possibilité de les récupérer, même à l'aide de logiciels spécialisés.

Pour détruire un fichier ou un dossier, cliquez dessus avec le bouton droit de la souris dans le gestionnaire de fichiers (*Windows Explorer, Total Commander, ...*) et sélectionnez **Détruire définitivement avec AVG** depuis le menu contextuel. Les fichiers contenus dans la corbeille peuvent également être détruits. Si un fichier spécifique dans un emplacement spécifique (*par exemple, un CD-ROM*) ne peut être détruit de manière fiable, vous en êtes informé ou l'option correspondante du menu contextuel n'est pas disponible.



**Veillez garder à l'esprit que : Une fois qu'un fichier est détruit, vous ne pouvez plus jamais le récupérer.**



## 11. 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 mis en quarantaine :

- **Date d'ajout** : date et heure auxquelles le fichier a été trouvé et placé en quarantaine.
- **Menace** : si vous avez décidé d'installer le composant [Identité](#) dans votre **AVG Internet Security**, une identification graphique de la gravité du résultat sera fournie dans cette section : elle oscillera entre acceptable (*trois points verts*) et très dangereux (*trois points rouges*). Cette section fournit également des informations sur le type d'infection et son emplacement d'origine. Le lien *Plus d'informations* vous redirige vers une page fournissant des informations détaillées sur la menace détectée dans [l'encyclopédie des virus en ligne](#).
- **Source** : spécifie le composant de **AVG Internet Security** qui a détecté la menace.
- **Notifications** : dans de très rares cas, cette colonne peut contenir des commentaires détaillés sur la menace détectée.

### 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** : transfère le fichier infecté dans le dossier sélectionné
- **Envoyer pour analyse** : ce bouton est uniquement actif lorsqu'un objet est sélectionné dans la liste des détections située au-dessus. Le cas échéant, vous pouvez envoyer la détection sélectionnée aux laboratoires de virus AVG pour une analyse plus approfondie. Veuillez noter que cette fonction est principalement réservée à l'envoi des faux positifs, c'est-à-dire des fichiers signalés comme étant infectés ou suspects, alors qu'ils vous semblent inoffensifs.
- **Détails** : pour obtenir des informations détaillées sur une menace spécifique en **Quarantaine**, sélectionnez la menace dans la liste, puis cliquez sur le bouton **Détails** pour afficher sa description.
- **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. Historique

La section **Historique** contient des informations sur tous les événements passés (*mises à jour, analyses, détections, etc.*) et établit des rapports sur ces événements. Pour y accéder depuis l'[interface utilisateur principale](#), cliquez sur **Options / Historique**. L'historique de tous les événements enregistrés se divise en plusieurs thèmes :

- [Résultats des analyses](#)
- [Résultats du Bouclier résident](#)
- [Résultats de la Protection email](#)
- [Résultats du Bouclier Web](#)
- [Journal de l'historique des événements](#)
- [Journal du Pare-feu](#)

### 12.1. Résultats des analyses




La boîte de dialogue **Résultats d'analyse** est accessible depuis **Options / Historique / Résultats d'analyse**, sur la ligne de navigation en haut de la fenêtre principale d'**AVG Internet Security**. 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
- **Élevé / Moyen** : ces colonnes indiquent le nombre d'infections de risque élevé ou moyen détectées pour chaque analyse
- **Infos** : informations sur le déroulement de l'analyse et sur les résultats (*finalisation ou interruption du processus*)
- **Rootkits** : nombre de [rootkits](#) trouvés

### 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
-  : permet de revenir à la [boîte de dialogue principale d'AVG](#) par défaut (*présentation des composants*), à l'aide de la flèche située dans le coin supérieur gauche de la boîte de dialogue

## 12.2. Résultats du Bouclier résident

Le service **Bouclier résident** fait partie du composant [Ordinateur](#) et 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 :

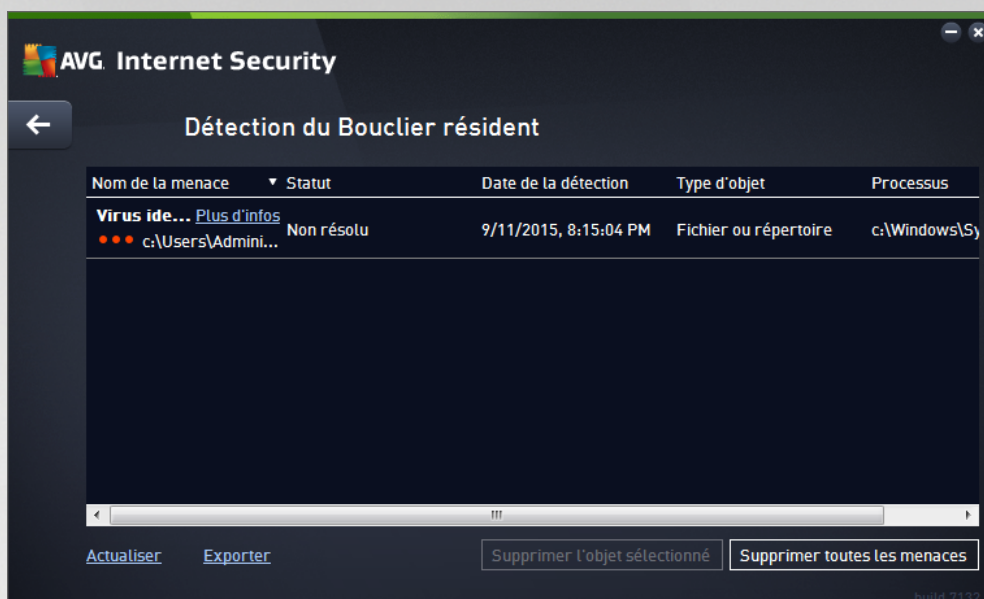


Dans cette boîte de dialogue d'avertissement, vous trouverez des informations sur l'objet qui a été détecté et défini comme infecté (*Menace*), ainsi qu'une brève description de l'infection reconnue (*Description*). Le lien *Plus d'informations* vous redirige vers une page offrant des informations détaillées sur la menace détectée dans l'[encyclopédie des virus en ligne](#), lorsque celles-ci sont connues. Cette boîte de dialogue décrit également les solutions disponibles pour résoudre cette menace détectée. L'une d'entre elles sera recommandée : **Me protéger (recommandé)**. **Choisissez systématiquement cette solution, dans la mesure du possible.**

**Remarque :** il peut arriver que la taille de l'objet détecté dépasse les limites d'espace de la Quarantaine. En pareil cas, un message d'avertissement s'affiche et vous en informe. Notez, toutefois, que la taille de la quarantaine est modifiable. Elle est définie sous la forme d'un pourcentage ajustable de la taille de votre disque dur. Pour augmenter la taille de la zone de quarantaine, ouvrez la boîte de dialogue [Quarantaine](#) dans [Paramètres avancés AVG](#), via l'option « Limiter la taille de la quarantaine ».

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

Une liste des détections du Bouclier résident est disponible dans la boîte de dialogue **Détection du Bouclier résident**. Cette boîte de dialogue est accessible depuis **Options / Historique / Détection du Bouclier résident**, sur la ligne de navigation en haut de la [fenêtre principale](#) d'AVG Internet Security. Elle répertorie les objets détectés par le Bouclier résident comme étant dangereux, puis réparés ou déplacés en [Quarantaine](#).



Les informations suivantes accompagnent chaque objet détecté :

- **Nom de la menace** : description (et éventuellement le nom) de l'objet détecté et son emplacement. Le lien *Plus d'informations* vous redirige vers une page fournissant des informations détaillées sur la menace détectée dans l'[encyclopédie des virus en ligne](#).
- **Etat** : 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 appeler l'objet potentiellement dangereux en vue de sa détection

### Boutons de commande

- **Actualiser la liste** : met à jour la liste des menaces détectées par le **Bouclier résident**
- **Exporter** : exporte la liste complète des objets détectés dans un fichier
- **Supprimer l'objet sélectionné** : supprime les éléments de la liste sélectionnés
- **Supprimer toutes les menaces** : supprime tous les éléments répertoriés dans la boîte de dialogue
- **←** : permet de revenir à la [boîte de dialogue principale d'AVG](#) par défaut (présentation des composants), à l'aide de la flèche située dans le coin supérieur gauche de la boîte de dialogue



### 12.3. Résultats d'Identity Protection

La boîte de dialogue **Identity Protection** est accessible depuis **Options / Historique / Résultats d'Identity Protection**, sur la ligne de navigation en haut de la fenêtre principale d'AVG Internet Security .




Cette boîte de dialogue dresse la liste de tous les objets détectés par le composant [Identity Protection](#). Les informations suivantes accompagnent chaque objet détecté :

- **Nom de la menace** : description (et éventuellement le nom) de l'objet détecté et son emplacement. Le lien *Plus d'informations* vous redirige vers une page fournissant des informations détaillées sur la menace détectée dans l'[encyclopédie des virus en ligne](#).
- **Etat** : 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 appeler 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**).

#### Boutons de commande

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

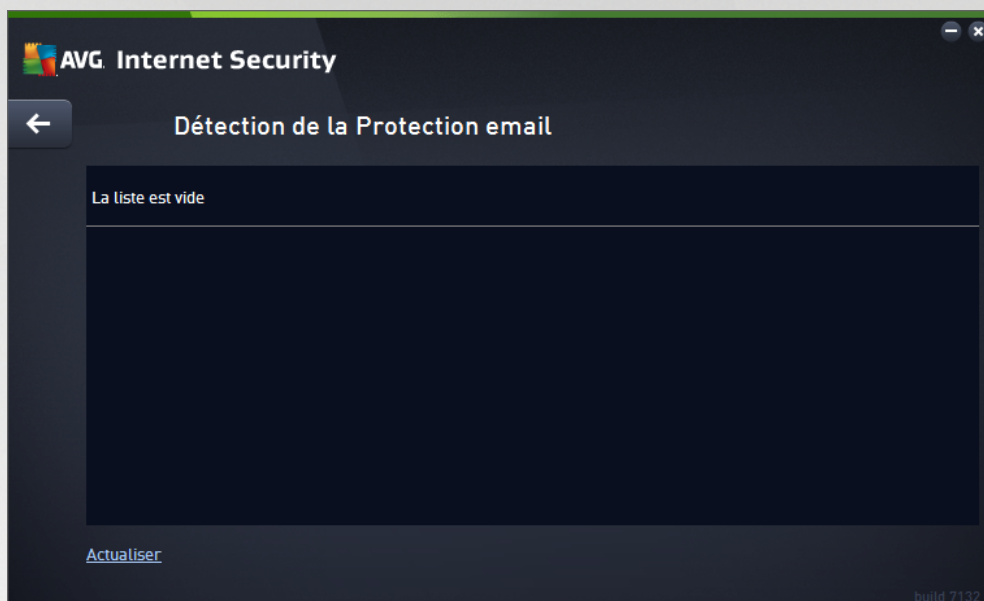
- **Actualiser la liste** : met à jour la liste des menaces détectées
-  : permet de revenir à la [boîte de dialogue principale d'AVG](#) par défaut (présentation des



composants), à l'aide de la flèche située dans le coin supérieur gauche de la boîte de dialogue

## 12.4. Résultats de la Protection email

La boîte de dialogue **Résultats de Protection email** est accessible depuis **Options / Historique / Résultats de Protection email**, sur la ligne de navigation en haut de la fenêtre principale d'AVG Internet Security .




Cette boîte de dialogue dresse la liste de tous les objets détectés par le composant [Scanner email](#). Les informations suivantes accompagnent chaque objet détecté :

- **Nom de la détection** : description (et éventuellement nom) de l'objet détecté et de sa source.
- **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
- **Processus** : action réalisée pour appeler 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**).

### Boutons de commande

Les boutons de commande disponibles dans l'interface de **Détection du Scanner email** sont :

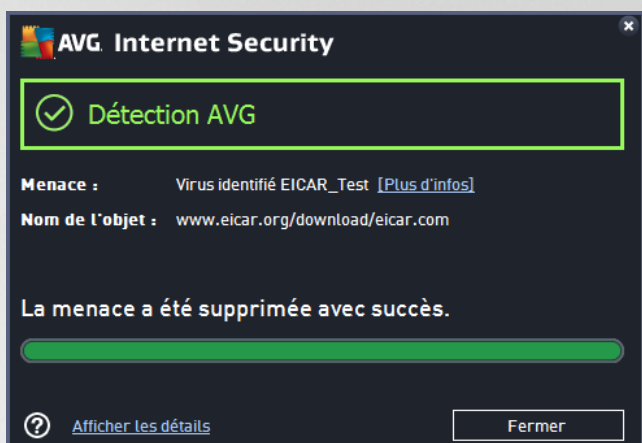
- **Actualiser la liste** : met à jour la liste des menaces détectées
-  : permet de revenir à la [boîte de dialogue principale d'AVG](#) par défaut (présentation des



composants), à l'aide de la flèche située dans le coin supérieur gauche de la boîte de dialogue

## 12.5. Résultats 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 l'objet qui a été détecté et défini comme infecté (*Menace*), ainsi qu'une brève description de l'infection reconnue (*Objet*). Le lien *Plus d'informations* vous redirigera vers l'[encyclopédie des virus en ligne](#) dans laquelle vous pourrez éventuellement obtenir des renseignements supplémentaires sur cette infection. Cette boîte de dialogue présente les commandes suivantes :

- **Afficher les détails** : cliquez sur ce lien pour ouvrir une fenêtre contenant des informations détaillées sur le processus en cours lorsque l'infection a été détectée ainsi que l'identification de cette dernière.
- **Fermer** : cliquez sur ce 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 **Détection du Bouclier web**. Cette liste qui récapitule toutes les menaces détectées est accessible depuis **Options / Historique / Détection du Bouclier Web**, sur la ligne de navigation en haut de la fenêtre principale d'AVG Internet Security .



Les informations suivantes accompagnent chaque objet détecté :

- **Nom de la menace** : description (et éventuellement le nom) de l'objet détecté et son emplacement (page Web) ; le lien *Plus d'informations* vous conduit vers une page fournissant des informations détaillées sur la menace détectée dans l'[encyclopédie des virus en ligne](#).
- **Etat** : 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

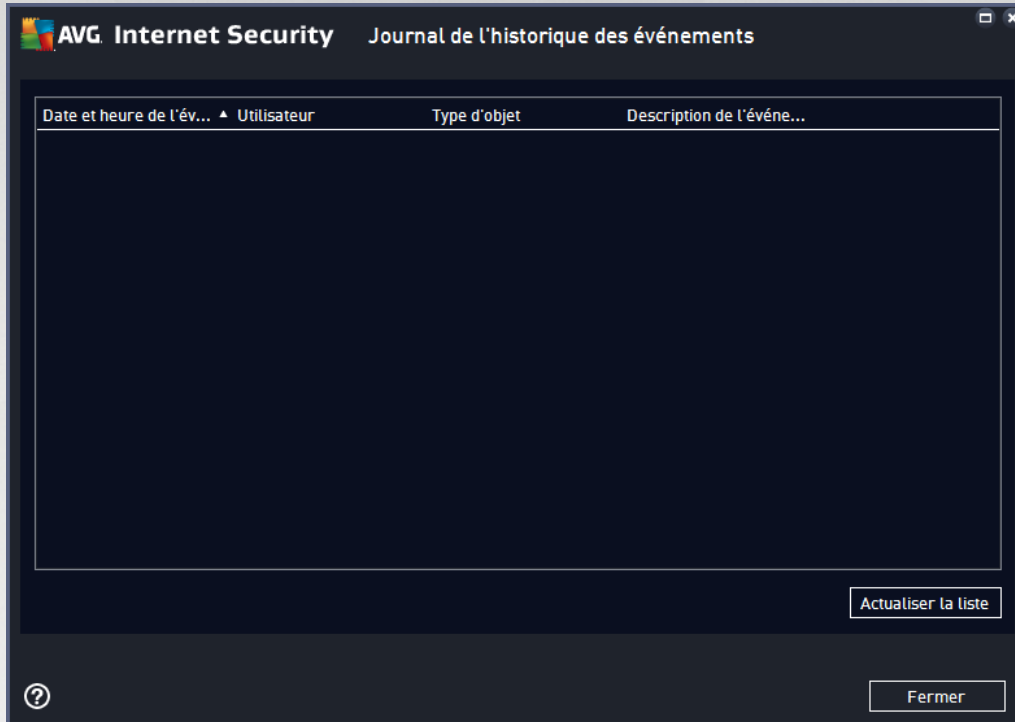
### Boutons de commande

- **Actualiser la liste** : met à jour la liste des menaces détectées par le **Bouclier résident**
- **Exporter** : exporte la liste complète des objets détectés dans un fichier
-  : permet de revenir à la [boîte de dialogue principale d'AVG](#) par défaut (présentation des composants), à l'aide de la flèche située dans le coin supérieur gauche de la boîte de dialogue





## 12.6. Journal de l'historique des événements



La boîte de dialogue **Historique des événements** est accessible depuis **Options / Historique / Historique des événements**, sur la ligne de navigation, en haut de la fenêtre principale d'**AVG Internet Security**. Dans cette boîte de dialogue, vous trouverez un résumé des événements les plus importants survenus pendant l'exécution du programme **AVG Internet Security**. Cette boîte de dialogue enregistre les types d'événement suivants : informations sur les mises à jour de l'application AVG ; informations sur le début, la fin ou l'arrêt de l'analyse (y compris les tests automatiques) ; informations sur les événements liés à la détection des virus (par le Bouclier résident ou résultant de l'[analyse](#)) avec indication de l'emplacement des occurrences et autres événements importants.

Pour chaque événement, les informations suivantes s'affichent :

- **Date et heure de l'évènement** donne la date et l'heure exactes de l'évènement.
- **Utilisateur** indique le nom de l'utilisateur actuellement connecté au moment de 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

- **Actualiser la liste** permet de mettre à jour toutes les entrées de la liste des événements
- **Fermer** permet de retourner dans la fenêtre principale d' **AVG Internet Security**

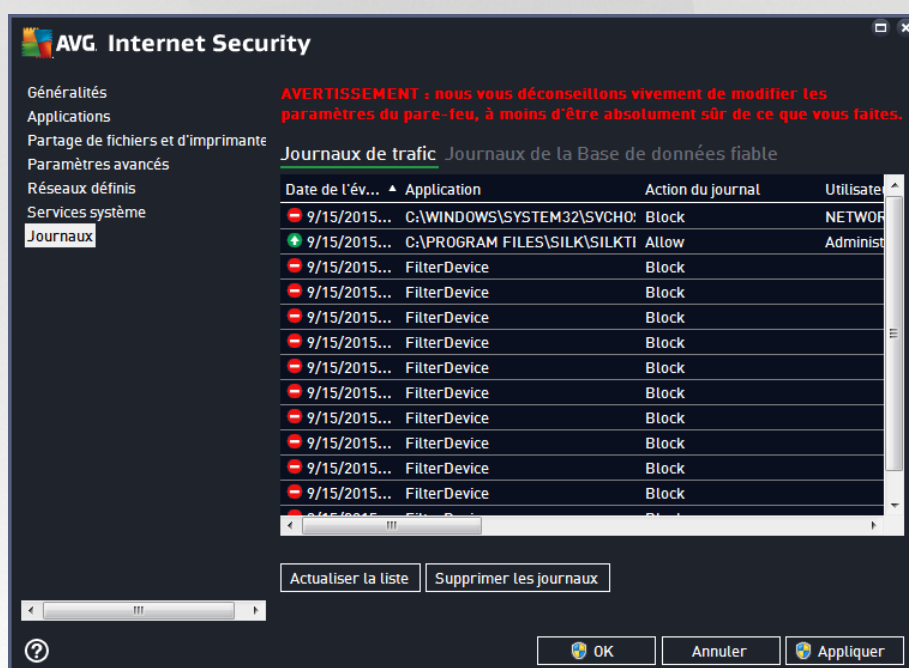


## 12.7. Journal du Pare-feu

**Cette boîte de dialogue de configuration est destinée aux experts. Nous vous recommandons de ne pas modifier ces paramètres, à moins d'être absolument sûr ce que vous modifiez !**

La boîte de dialogue **Journaux** permet de passer en revue l'ensemble des actions et des événements du Pare-feu qui ont été enregistrés ainsi que la description détaillée des paramètres associés sur deux onglets :

- **Journaux de trafic** : cet onglet fournit des informations sur les activités de toutes les applications qui ont essayé de se connecter au réseau. Pour chaque activité, vous pouvez connaître la date de l'événement, le nom de l'application, l'action du journal correspondante, le nom d'utilisateur, le PID, la direction du trafic, le type de protocole, les numéros des ports locaux et distants, etc.



- **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.

### 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.



- **Supprimer les journaux** : ce bouton supprime toutes les entrées du tableau.



## 13. Mises à jour AVG

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. Au regard de toutes les menaces informatiques apparues récemment et de la vitesse à laquelle elles se propagent, il est absolument essentiel de mettre à jour régulièrement le programme **AVG Internet Security**. La meilleure solution est de conserver les paramètres par défaut du programme en ce qui concerne les mises à jour automatiques. Notez que si la base virale d'**AVG Internet Security** n'est pas à jour, ce dernier ne sera pas en mesure de détecter les menaces les plus récentes !

***C'est pourquoi il est essentiel de mettre régulièrement à jour votre produit AVG ! Les mises à jour 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.***

Afin d'optimiser la sécurité, **AVG Internet Security** est programmé par défaut pour rechercher de nouvelles mises à jour de la base de données virale toutes les quatre heures. Les mises à jour d'AVG n'étant pas publiées selon un calendrier fixe, mais plutôt en réaction au nombre et à la gravité des nouvelles menaces, il est très important d'effectuer cette vérification pour garantir la mise à jour permanente de votre base de données virale AVG.

Pour rechercher immédiatement de nouvelles mises à jour, cliquez sur le lien d'accès rapide [Mise à jour](#) de l'interface utilisateur principale. Ce lien est constamment disponible, quelle que soit la boîte de dialogue ouverte dans l'[interface utilisateur](#). Lorsque vous lancez la mise à jour, AVG vérifie en premier lieu si de nouveaux fichiers de mise à jour sont disponibles. Si tel est le cas, **AVG Internet Security** lance leur téléchargement et exécute le processus qui effectue la mise à jour. Vous serez prévenu des résultats de la mise à jour dans la boîte de dialogue contextuelle, affichée au-dessus de l'icône AVG dans la barre d'état système.

Si vous souhaitez réduire le nombre de mises à jour, vous pouvez définir vos propres paramètres d'exécution pour ce type d'opération. Toutefois, **il est fortement recommandé d'exécuter au moins une mise à jour par jour !** Pour modifier la configuration, ouvrez les boîtes de dialogue de la section [Paramètres avancés/ Programmations](#) suivantes :

- [Programmation de la mise à jour des définitions](#)
- [Programmation des mises à jour de l'Anti-Spam](#)



## 14. FAQ et Assistance technique

Si vous rencontrez des difficultés d'ordre commercial ou technique avec votre application **AVG Internet Security**, il existe plusieurs méthodes pour obtenir de l'aide. Choisissez l'une de ces trois options :

- **Obtenir de l'aide** : vous pouvez accéder à la page dédiée du support client du site Web d'AVG directement à partir de l'application AVG (<http://www.avg.com/>). Sélectionnez la commande du menu principal **Aide / Obtenir de l'aide** pour être redirigé vers le site Web d'AVG contenant toutes les solutions de support disponibles. Suivez les instructions fournies sur la page Web pour poursuivre la procédure.
- **Support** (lien du menu principal) : Le menu de l'application AVG (dans la partie supérieure de l'interface utilisateur principale) comporte un lien **Support** qui permet d'ouvrir une nouvelle boîte de dialogue contenant toutes les informations dont vous pourriez avoir besoin pour rechercher de l'aide. Vous y trouverez des données de base relatives à l'application AVG installée (version de l'application / de la base de données), les informations de licence et une liste de liens d'accès rapide au support.
- **Résolution des problèmes dans le fichier d'aide** : Une nouvelle section **Résolution des problèmes** est disponible directement dans le fichier d'aide inclus dans **AVG Internet Security** (pour ouvrir le fichier d'aide, appuyez sur la touche F1 à partir de n'importe quelle boîte de dialogue de l'application). Cette section fournit la liste des situations les plus courantes que peut rencontrer un utilisateur lorsqu'il recherche une aide professionnelle pour résoudre un problème technique. Cliquez sur la situation qui décrit le mieux votre problème afin d'obtenir des instructions détaillées sur la manière de le résoudre.
- **Site Web du Centre de support d'AVG** : vous pouvez également rechercher la solution à votre problème sur le site Web d'AVG (<http://www.avg.com/>). La section **Support** contient une présentation des groupes thématiques abordant à la fois les problèmes d'ordre commercial et technique, une section structurée de la foire aux questions et tous les contacts disponibles.
- **AVG ThreatLabs** : un site Web AVG spécifique (<http://www.avg.com/about-viruses>) est dédié aux problèmes liés aux virus et fournit un aperçu structuré des informations liées aux menaces en ligne. Vous y trouverez également des instructions sur la manière de supprimer les virus et spyware et des conseils sur la manière de rester protégé.
- **Forum de discussion** : vous pouvez également utiliser le forum de discussion des utilisateurs d'AVG à l'adresse : <http://community.avg.com/>.