

AVG 9.0 File Server

User Manual

Document revision 90.1 (5.10.2009)

Copyright AVG Technologies CZ, s.r.o. All rights reserved.
All other trademarks are the property of their respective owners.

This product uses RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.

This product uses code from C-SaCzech library, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

This product uses compression library zlib, Copyright (c) 1995-2002 Jean-loup Gailly and Mark Adler.

This product uses compression library libzip2, Copyright (c) 1996-2002 Julian R. Seward.

Contents

1. Introduction	6
2. Conditions de l'installation	7
2.1 Systèmes d'exploitation pris en charge	7
2.2 Configuration matérielle	7
3. Options d'installation	9
4. Gestionnaire de téléchargement AVG	10
4.1 Sélection de la langue	10
4.2 Vérification de la connectivité	11
4.3 Paramètres proxy	13
4.4 Choix du type de licence	14
4.5 Télécharger les fichiers à installer	15
5. Processus d'installation d'AVG	16
5.1 Lancement de l'installation	16
5.2 Contrat de licence	17
5.3 Vérification de l'état du composant	18
5.4 Sélection du type d'installation	19
5.5 Activer votre licence AVG	19
5.6 Installation personnalisée - Dossier de destination	21
5.7 Installation personnalisée - Sélection des composants	22
5.8 Installation d'AVG	23
5.9 Programmation des analyses et des mises à jour	24
5.10 La configuration de la protection AVG est terminée	25
6. Opérations à effectuer après l'installation	26
6.1 Enregistrement du produit	26
6.2 Accès à l'interface utilisateur	26
6.3 Analyse complète	26
6.4 Test EICAR	26
6.5 Configuration par défaut d'AVG	27
7. Interface utilisateur AVG	28
7.1 Menu système	29
7.1.1 Fichier	29

7.1.2 Composants	29
7.1.3 Historique	29
7.1.4 Outils	29
7.1.5 Aide	29
7.2 Informations sur l'état de la sécurité	31
7.3 Liens d'accès rapide	33
7.4 Présentation des composants	34
7.5 Statistiques	35
7.6 Icône de la barre d'état système	35
8. Composants AVG	37
8.1 Anti-Virus	37
8.1.1 Principes de l'Anti-Virus	37
8.1.2 Interface de l'Anti-Virus	37
8.2 Anti-Spyware	39
8.2.1 Principes de l'Anti-Spyware	39
8.2.2 Interface de l'Anti-Spyware	39
8.3 Licence	41
8.4 Bouclier résident	42
8.4.1 Principes du Bouclier résident	42
8.4.2 Interface du Bouclier résident	42
8.4.3 Détection du Bouclier résident	42
8.5 Mise à jour	47
8.5.1 Principes du composant Mise à jour	47
8.5.2 Interface du composant Mise à jour	47
9. AVG pour Serveur SharePoint Portal	50
9.1 Maintenance du programme	50
9.2 Configuration d'AVG pour SPPS - Sharepoint 2007	51
9.3 Configuration d'AVG pour SPPS - Sharepoint 2003	53
9.4 AVG pour SPPS - Edition Diagnostics	55
10. Paramètres avancés d'AVG	57
10.1 Affichage	57
10.2 Sons	59
10.3 Ignorer les erreurs	61
10.4 Quarantaine	62
10.5 Exceptions PUP	63
10.6 Analyses	65

10.6.1	<i>Analyse complète</i>	65
10.6.2	<i>Analyse contextuelle</i>	65
10.6.3	<i>Analyse zones sélectionnées</i>	65
10.6.4	<i>Analyse du dispositif amovible</i>	65
10.7	Programmations	72
10.7.1	<i>Analyse programmée</i>	72
10.7.2	<i>Programmation de la mise à jour de la base de données virale</i>	72
10.7.3	<i>Programmation de la mise à jour du programme</i>	72
10.8	Bouclier résident	82
10.8.1	<i>Paramètres avancés</i>	82
10.8.2	<i>Répertoires exclus</i>	82
10.8.3	<i>Fichiers exclus</i>	82
10.9	Mise à jour	87
10.9.1	<i>Proxy</i>	87
10.9.2	<i>Numérotation</i>	87
10.9.3	<i>URL</i>	87
10.9.4	<i>Gérer</i>	87
11.	Analyse AVG	95
11.1	Interface d'analyse	95
11.2	Analyses prédéfinies	96
11.2.1	<i>Analyse complète</i>	96
11.2.2	<i>Analyse zones sélectionnées</i>	96
11.3	Analyse contextuelle	104
11.4	Analyse depuis la ligne de commande	105
11.4.1	<i>Paramètres d'analyse CMD</i>	105
11.5	Programmation de l'analyse	108
11.5.1	<i>Paramètres de la programmation</i>	108
11.5.2	<i>Comment faire l'analyse</i>	108
11.5.3	<i>Objets à analyser</i>	108
11.6	Résultats d'analyse	118
11.7	Détails des résultats d'analyse	120
11.7.1	<i>Onglet Résultats d'analyse</i>	120
11.7.2	<i>Onglet Infections</i>	120
11.7.3	<i>Onglet Spywares</i>	120
11.7.4	<i>Onglet Avertissements</i>	120
11.7.5	<i>Onglet Informations</i>	120
11.8	Quarantaine	128

12. Mises à jour d'AVG	130
12.1 Niveaux de mise à jour	130
12.2 Types de mises à jour	130
12.3 Processus de mise à jour	130
13. Journal des évènements	132
14. FAQ et assistance technique	133

1. Introduction

Ce manuel utilisateur fournit une documentation complète sur **AVG 9.0 File Server**.

Nous vous remercions d'avoir choisi AVG 9.0 File Server.

AVG 9.0 File Server figure parmi les produits AVG primés et a été conçu pour assurer la sécurité de votre ordinateur et vous permettre de travailler en toute sérénité. Comme toute la gamme des produits AVG, la solution **AVG 9.0 File Server** a été entièrement repensée, afin de livrer une protection AVG reconnue et certifiée sous une présentation nouvelle, plus conviviale et plus efficace.

Votre tout nouveau produit **AVG 9.0 File Server** bénéficie d'une interface transparente associée à une analyse encore plus approfondie et plus rapide. D'avantage de fonctions de sécurité ont été automatisées pour plus de commodité et des options utilisateur "intelligentes" ont été incluses de manière à adapter les fonctions de sécurité à vos tâches quotidiennes. La convivialité n'a fait aucun compromis à la sécurité !

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

2. Conditions de l'installation

2.1. Systèmes d'exploitation pris en charge

AVG 9.0 File Server sert à protéger les postes de travail fonctionnant avec les systèmes d'exploitation suivants :

- Windows 2000
- Windows XP, Windows XP Pro Edition x64
- Windows Vista, Windows Vista Edition x64
- Windows 2000 Server
- Windows 2003 Server, Windows 2003 Server Edition x64
- Windows 2008 Server, Windows 2008 Server x64 Edition

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

2.2. Configuration matérielle

Voici la configuration matérielle minimale pour **AVG 9.0 File Server** :

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

Voici la configuration matérielle minimale pour **AVG 9.0 File Server** :

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

- 512 Mo libres de RAM

3. Options d'installation

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

Avant de procéder à l'installation du programme AVG, nous vous recommandons vivement de consulter le site Web d'AVG (<http://www.avg.com>) pour vérifier la présence de nouveaux fichiers d'installation. Ainsi, vous êtes sûr de posséder le dernier fichier d'installation AVG 9.0 File Server en date.

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

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

4. Gestionnaire de téléchargement AVG

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

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

AVG Download Manager disponible en téléchargement sur le site Web d'AVG (<http://www.avg.com>) Vous trouverez ci-dessous une brève description de chaque action à réaliser au sein de l'outil **AVG Download Manager** :

4.1. Sélection de la langue



A la première étape de l'assistant **AVG Download Manager**, sélectionnez la langue d'installation dans le menu déroulant. Notez que la langue que vous sélectionnez s'applique uniquement au processus d'installation ; une fois l'installation terminée, vous pourrez changer la langue directement à partir des paramètres du programme. Cliquez ensuite sur le bouton **Suivant** pour passer à l'écran suivant.

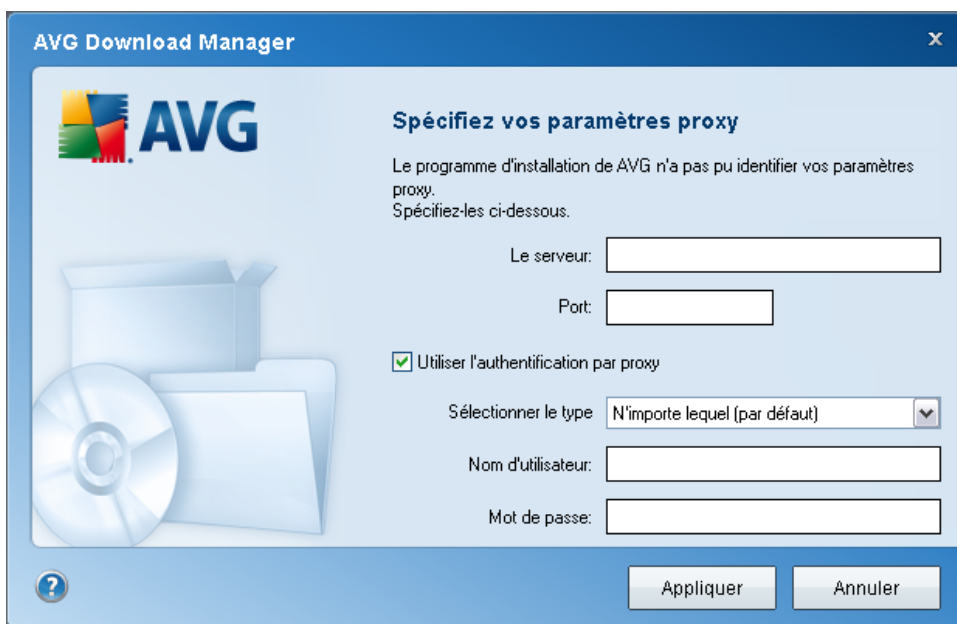
4.2. Vérification de la connectivité

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

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



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



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

4.3. Paramètres proxy

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

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

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

4.4. Choix du type de licence



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

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

4.5. Télécharger les fichiers à installer



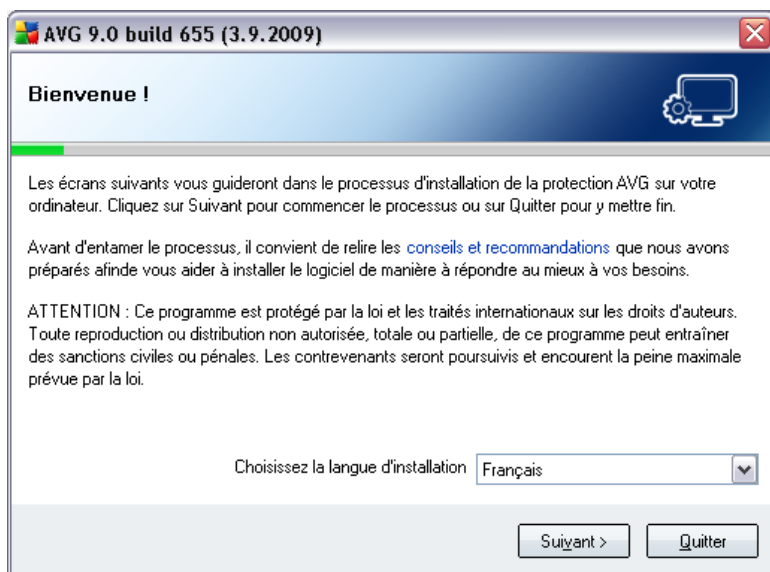
Vous avez maintenant fourni toutes les informations nécessaires pour que le **AVG Download Manager** entame le téléchargement du fichier d'installation et lance le processus d'installation. Vous pouvez maintenant passer au [Processus d'installation d'AVG](#).

5. Processus d'installation d'AVG

Pour installer **AVG 9.0 File Server sur l'ordinateur, il est nécessaire d'obtenir le dernier fichier d'installation disponible**. Vous pouvez utiliser le fichier d'installation figurant sur le CD et fourni avec votre édition, mais il est fort probable qu'il soit déjà périmé. En conséquence, nous vous recommandons de bien vouloir télécharger de dernier fichier d'installation, depuis Internet. Téléchargez le fichier depuis le site Web d'AVG (<http://www.avg.com>) / section **Téléchargements**. Vous pouvez également utiliser notre nouvel outil **AVG Download Manager** qui vous aidera à créer et à télécharger le conditionnement d'installation adapté à vos besoins, puis à lancer le processus de téléchargement.

L'installation consiste à réaliser une série de tâches décrites à l'intérieur de boîtes de dialogue. Dans la suivante, vous trouverez une explication de chaque boîte de dialogue :

5.1. Lancement de l'installation

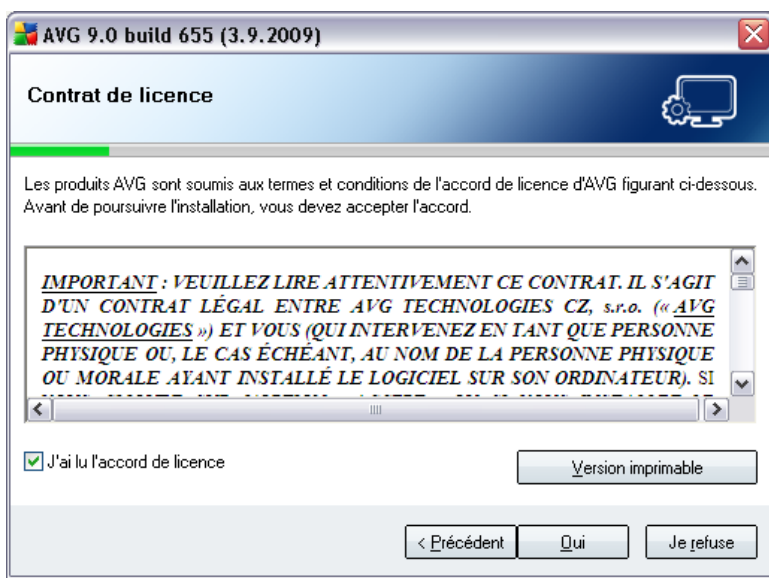


Le processus d'installation commence par l'affichage de la fenêtre **Bienvenue dans le programme d'installation AVG**. Dans cette fenêtre, vous sélectionnez la langue qui sera utilisée au cours de l'installation. Dans la partie inférieure de la fenêtre, localisez l'option **Choisissez la langue d'installation**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

Attention : vous choisissez ici la langue qui sera utilisée pour l'installation uniquement.

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

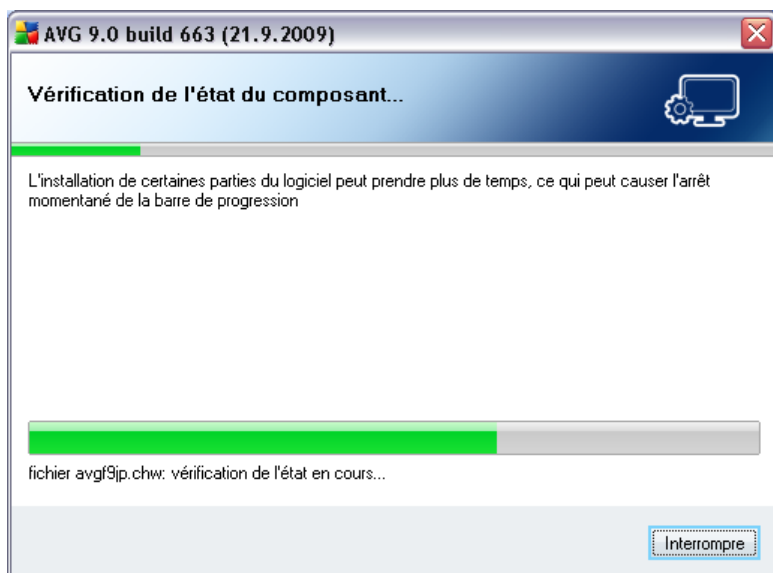
5.2. Contrat de licence



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

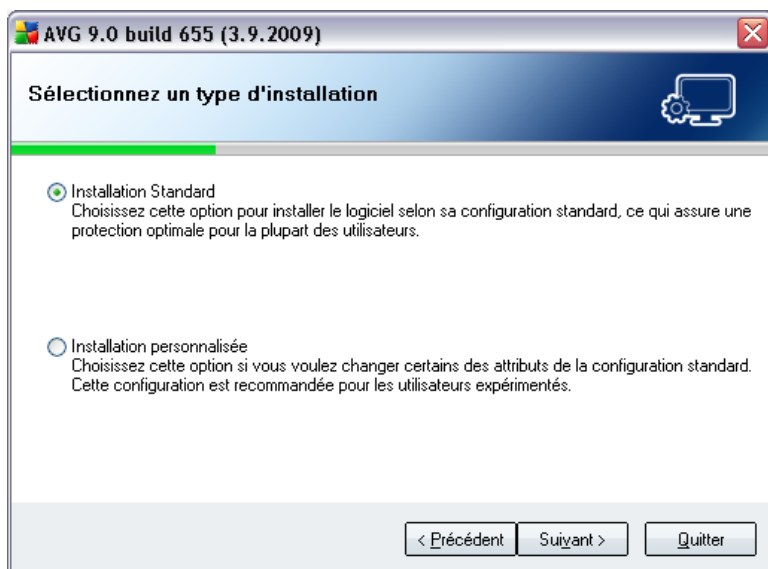
Si vous n'acceptez pas les conditions de l'accord de licence, cliquez sur le bouton **Je refuse** ; le processus d'installation prendra fin immédiatement.

5.3. Vérification de l'état du composant



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

5.4. Sélection du type d'installation



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

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

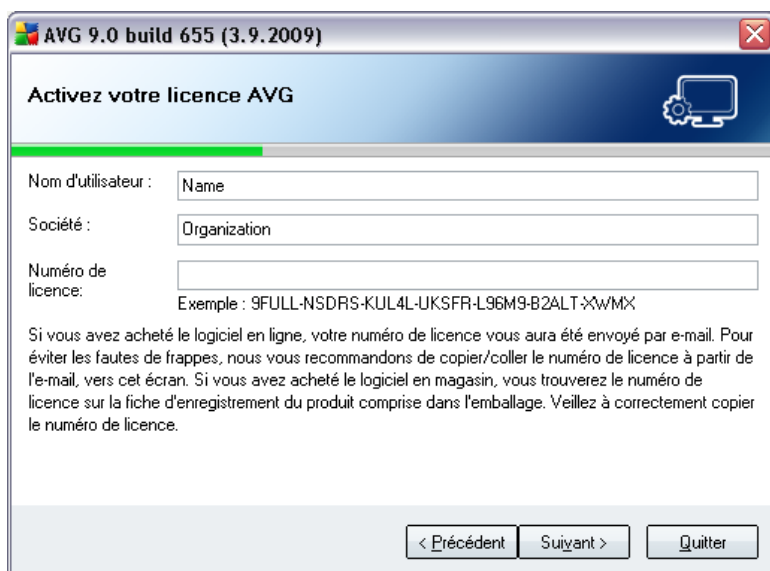
Installation personnalisée - exclusivement réservée aux utilisateurs expérimentés qui ont une raison valable d'installer AVG selon des paramètres non standard (par exemple, cela leur permet d'adapter le programme à une configuration matérielle spécifique).

5.5. Activer votre licence AVG

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

Saisissez ensuite votre numéro de licence/d'achat dans le champ **Numéro de licence**. Le numéro d'achat se trouve sur la pochette du CD-ROM dans l'emballage du produit **AVG 9.0 File Server**. Le numéro de licence figure dans le mail de confirmation que

vous avez reçu après avoir acheté le produit **AVG 9.0 File Server** par Internet. Vous devez saisir le numéro tel qu'il apparaît. Si le numéro de licence est disponible au format électronique (*par exemple, dans un mail*), il est recommandé de l'insérer à l'aide de la méthode copier-coller.



AVG 9.0 build 655 (3.9.2009)

Activez votre licence AVG

Nom d'utilisateur :

Société :

Numéro de licence:

Exemple : 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX

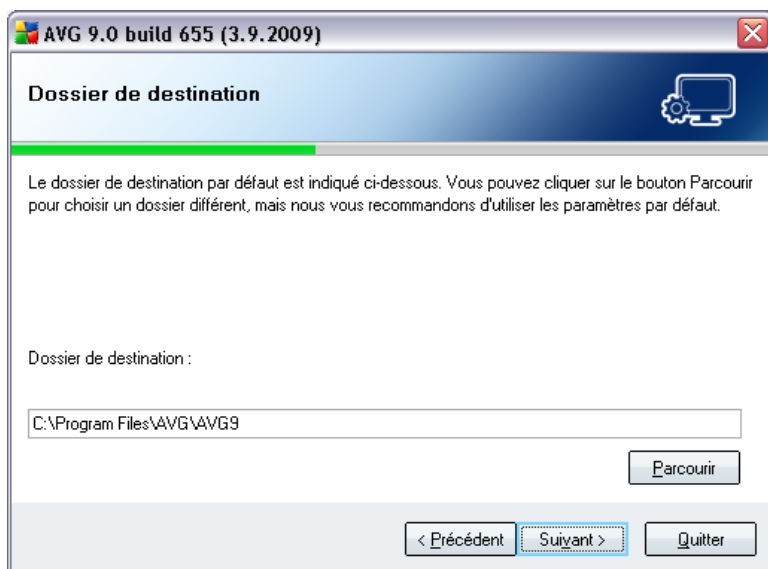
Si vous avez acheté le logiciel en ligne, votre numéro de licence vous aura été envoyé par e-mail. Pour éviter les fautes de frappe, nous vous recommandons de copier/coller le numéro de licence à partir de l'e-mail, vers cet écran. Si vous avez acheté le logiciel en magasin, vous trouverez le numéro de licence sur la fiche d'enregistrement du produit comprise dans l'emballage. Veuillez à correctement copier le numéro de licence.

< Précédent Suivant > Quitter

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

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

5.6. Installation personnalisée - Dossier de destination

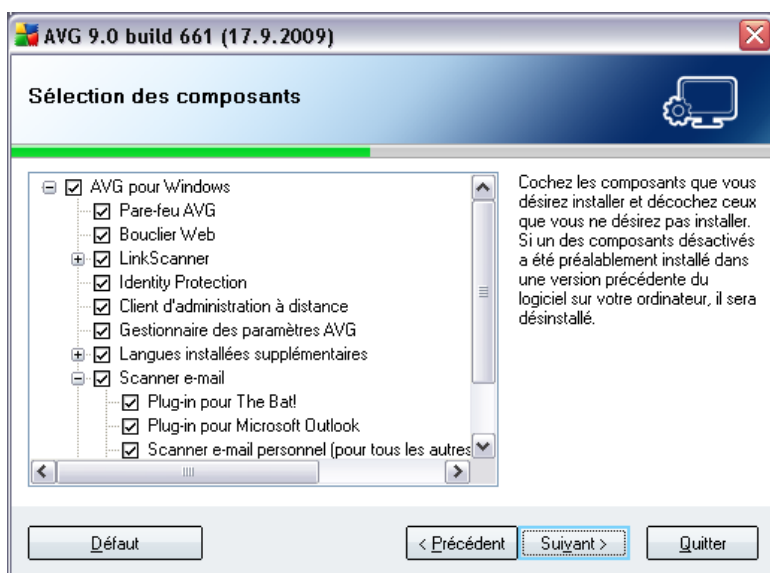


La boîte de dialogue **Dossier de destination** permet d'indiquer le dossier dans lequel les fichiers d'installation sont enregistrés. **AVG 9.0 File Server** Par défaut, AVG est installé dans le dossier contenant les fichiers de programme sur le lecteur C:.. Si un tel dossier n'existe pas, vous serez invité à confirmer, dans une nouvelle boîte de dialogue, que vous acceptez qu'AVG le crée maintenant.

Si vous optez pour un autre emplacement, cliquez sur le bouton **Parcourir** pour consulter l'organisation du lecteur, puis sélectionnez le dossier souhaité.

Cliquez sur le bouton **Suivant** pour confirmer votre choix.

5.7. Installation personnalisée - Sélection des composants



La boîte de dialogue **Sélection des composants** présente tous les composants qui peuvent être installés. **AVG 9.0 File Server** Si les paramètres par défaut ne vous satisfont pas, vous pouvez supprimer ou ajouter certains composants.

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

- **Sélection de la langue**

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

- **Plugins pour le scanner e-mail**

Cliquez sur l'élément **Scanner E-mail** pour ouvrir et choisir le plugin à installer afin d'assurer la sécurité de la messagerie. Par défaut, le **Plugin pour Microsoft Outlook** sera installé. Une autre option spécifique est le **Plugin pour The Bat!** Si vous utilisez un autre client de messagerie (*MS Exchange, Qualcomm Eudora, ...*), sélectionnez l'option **Scanner e-mail personnel** afin de sécuriser votre communication automatiquement, quel que soit le programme que vous utilisez.

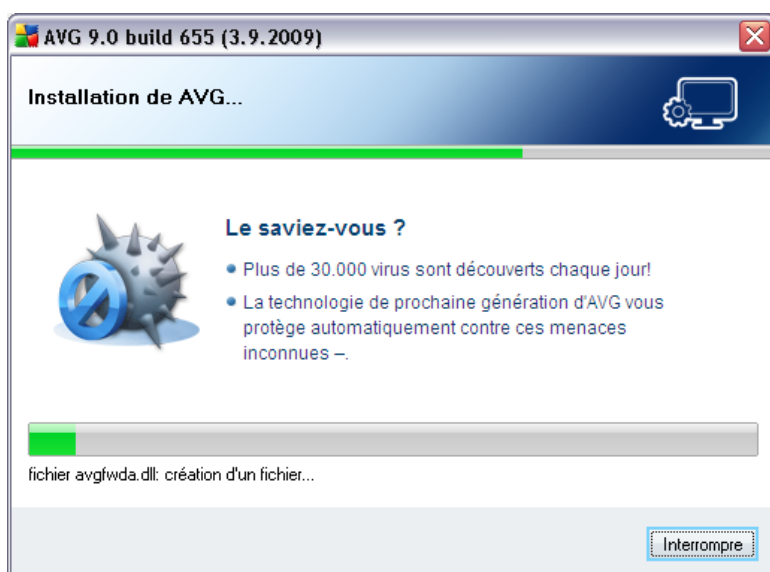
- **Administration à distance**

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

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

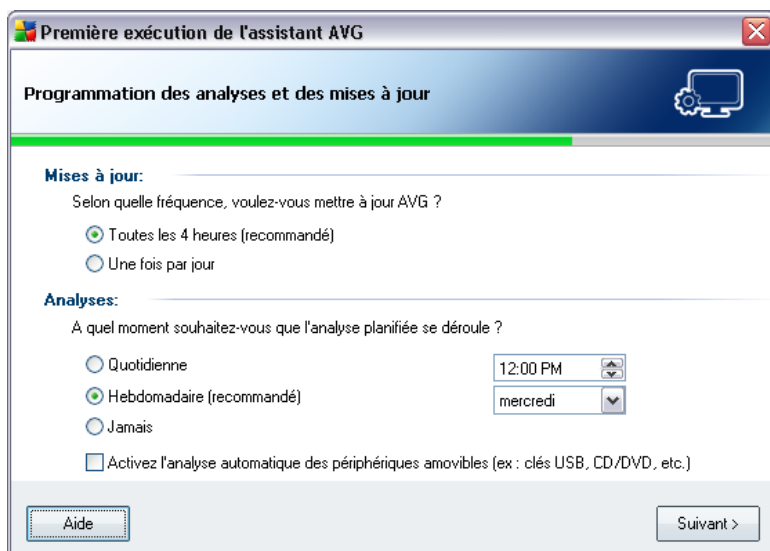
5.8. Installation d'AVG

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



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

5.9. Programmation des analyses et des mises à jour



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

5.10. La configuration de la protection AVG est terminée



AVG 9.0 File Server est maintenant configuré.

Dans la boîte de dialogue, vous avez la possibilité d'activer la fonction qui signale les exploits et les sites Web malveillants aux laboratoires d'AVG. Pour ce faire, cochez l'option ***J'accepte de fournir des informations ANONYMES sur les menaces détectées pour améliorer ma sécurité.***

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

6. Opérations à effectuer après l'installation

6.1. Enregistrement du produit

Après l'installation d'**AVG 9.0 File Server**, veuillez enregistrer votre produit en ligne sur le site Web d'AVG (<http://www.avg.com>), page **Enregistrement** (*suivez les instructions fournies à la page*). Après l'enregistrement, vous bénéficierez de tous les avantages associés à votre compte utilisateur AVG et aurez accès à la lettre d'informations d'AVG ainsi qu'aux autres services réservés exclusivement aux utilisateurs enregistrés.

6.2. Accès à l'interface utilisateur

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

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

6.3. Analyse complète

Le risque de contamination de l'ordinateur par un virus avant l'installation d'**AVG 9.0 File Server** ne doit pas être écarté. C'est pour cette raison qu'il est recommandé de lancer une **analyse complète** afin de s'assurer qu'aucune infection ne s'est déclarée dans votre ordinateur.

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

6.4. Test EICAR

Pour confirmer que l'installation d'**AVG 9.0 File Server** est correcte, effectuez un test EICAR.

Cette méthode standard et parfaitement sûre sert à tester le fonctionnement de l'anti-virus en introduisant un pseudo-virus ne contenant aucun fragment de code viral et ne présentant absolument aucun danger. La plupart des produits réagissent comme s'il s'agissait d'un véritable virus (*en lui donnant un nom significatif du type « EICAR-AV-Test »*). Vous pouvez télécharger le test Eicar à partir du site Web Eicar à l'adresse

www.eicar.com où vous trouverez toutes les informations nécessaires.

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



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

6.5. Configuration par défaut d'AVG

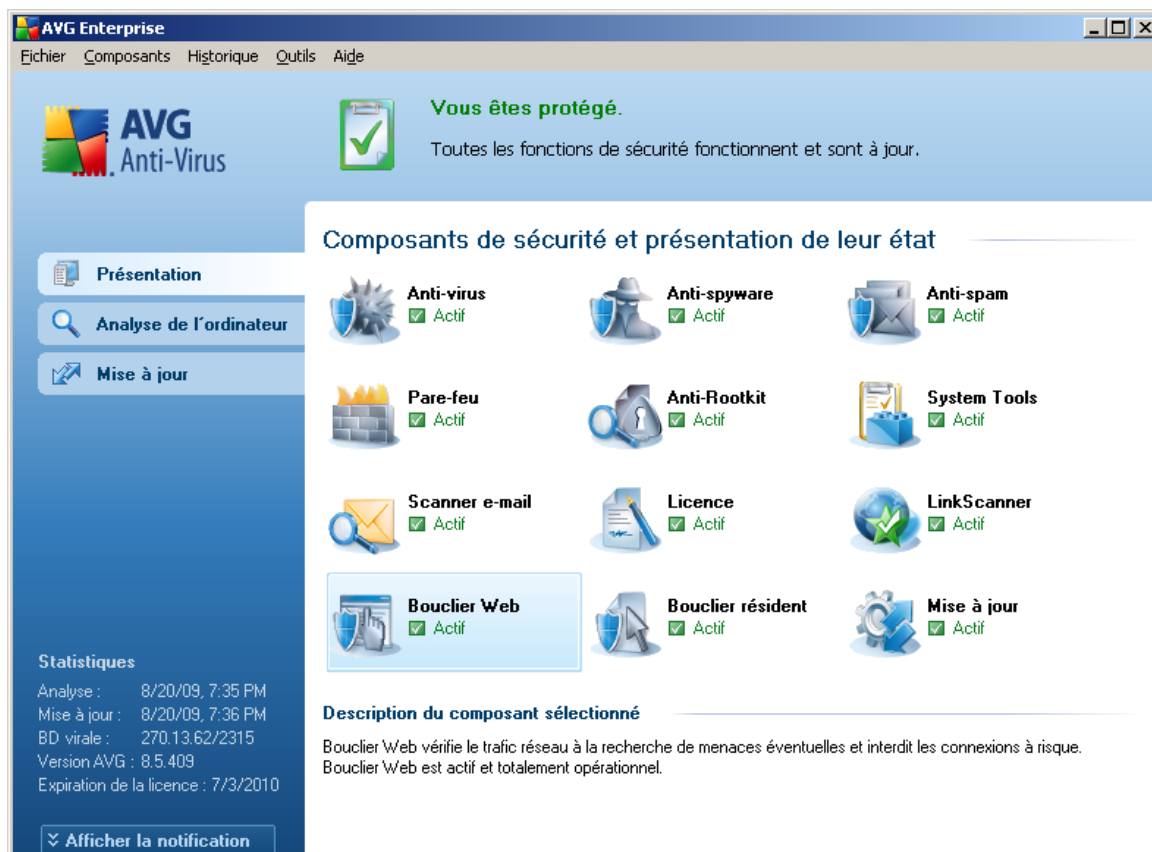
La configuration par défaut (c'est-à-dire la manière dont l'application est paramétrée à l'issue de l'installation) d'**AVG 9.0 File Server** est définie par le fournisseur du logiciel, qui ajuste les composants et les fonctions de manière à obtenir des performances optimales.

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

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

7. Interface utilisateur AVG

AVG 9.0 File Server apparaît dans la fenêtre principale :



La fenêtre principale comprend plusieurs parties :

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

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

7.1. Menu système

Le **menu système** est le système de navigation standard propre à toutes les applications Windows. Il se présente sous la forme d'une barre horizontale en haut de la fenêtre principale d'**AVG 9.0 File Server**. Servez-vous du menu système pour accéder aux composants, fonctions et services AVG de votre choix.

Le menu système inclut cinq sections principales :

7.1.1. Fichier

- **Quitter** - ferme l'interface utilisateur d'**AVG 9.0 File Server**. L'application AVG continue néanmoins de s'exécuter en arrière-plan de sorte que l'ordinateur reste protégé !

7.1.2. Composants

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

- **Présentation du système** - bascule sur l'interface utilisateur par défaut et affiche [une présentation générale de tous les composants installés et leur état](#)
- **Anti-Virus** - ouvre la page par défaut du composant [Anti-Virus](#)
- **Anti-Rootkit** - ouvre la page par défaut du composant **Anti-Rootkit**
- **Anti-Spyware** - ouvre la page par défaut du composant [Anti-Spyware](#)
- **Licence** - ouvre la page par défaut du composant [Licence](#)
- **Bouclier résident** - ouvre la page par défaut du composant [Bouclier résident](#)
- **Mise à jour** - ouvre la page par défaut du composant [Mise à jour](#)

7.1.3. Historique

- **Résultats des analyses** - bascule sur l'interface d'analyse AVG et ouvre notamment la boîte de dialogue **Résultats d'analyse**
- **Détection du Bouclier résident** - ouvre la boîte de dialogue contenant une vue générale des menaces détectées par le **Bouclier résident**
- **Quarantaine** - ouvre l'interface de la zone de confinement (**Quarantaine**) dans laquelle AVG place les infections détectées qui n'ont pu, pour une raison quelconque, être réparées automatiquement. A l'intérieur de cette quarantaine, les fichiers infectés sont isolés. L'intégrité de la sécurité de l'ordinateur est donc garantie et les fichiers infectés sont stockés en vue d'une éventuelle réparation future.
- **Journal de l'historique des événements** - ouvre l'interface de l'historique des événements présentant toutes les actions d'**AVG 9.0 File Server** qui ont été consignées.

7.1.4. Outils

- **Analyse complète** - ouvre l'**interface d'analyse AVG** et procède à l'analyse de l'intégralité des fichiers de l'ordinateur
- **Analyser le dossier sélectionné** - ouvre l'**interface d'analyse AVG** et permet de spécifier, au sein de l'arborescence de l'ordinateur, les fichiers et les dossiers à analyser
- **Analyser le fichier** - permet de lancer sur demande l'analyse d'un fichier sélectionné dans l'arborescence du disque
- **Mise à jour** - lance automatiquement le processus de mise à jour du composant **AVG 9.0 File Server**
- **Mise à jour depuis le répertoire** - procède à la mise à jour grâce aux fichiers de mise à jour situés dans le dossier spécifié de votre disque local. Notez que cette option n'est recommandée qu'en cas d'urgence, c'est-à-dire si vous ne disposez d'aucune connexion Internet (*si, par exemple, l'ordinateur est infecté et déconnecté d'Internet ou s'il est relié à un réseau sans accès à Internet, etc.*). Dans la nouvelle fenêtre qui apparaît, sélectionnez le dossier dans lequel vous avez placé le fichier de mise à jour et lancez la procédure de mise à jour.
- **Paramètres avancés** - ouvre la boîte de dialogue **Paramètres avancés AVG** dans laquelle vous modifiez au besoin la **AVG 9.0 File Server** configuration. En général, il est recommandé de conserver les paramètres par défaut de

l'application tels qu'ils ont été définis par l'éditeur du logiciel.

7.1.5. Aide

- **Sommaire** - ouvre les fichiers d'aide du programme AVG
- **Obtenir de l'aide en ligne** - affiche le site Web d'AVG (<http://www.avg.com>) à la page du centre de support clients
- **Site Internet AVG** - ouvre le site Web d'AVG (<http://www.avg.com>)
- **A propos des virus et des menaces** - ouvre l'[Encyclopédie des virus en ligne](#), où vous pouvez consulter des informations détaillées sur le virus identifié
- **Réactiver** - ouvre la boîte de dialogue **Activer AVG** avec les données que vous avez saisies dans la boîte de dialogue [Personnaliser AVG](#) au cours du [processus d'installation](#). Dans cette boîte de dialogue, vous indiquez votre numéro de licence en lieu et place de la référence d'achat (*le numéro indiqué lors de l'installation d'AVG*) ou de votre ancien numéro (*si vous installez une mise à niveau du produit AVG, par exemple*).
- **Enregistrer maintenant** - renvoie à la page d'enregistrement du site Web d'AVG (<http://www.avg.com>). Merci de compléter le formulaire d'enregistrement ; seuls les clients ayant dûment enregistré leur produit AVG peuvent bénéficier de l'assistance technique gratuite.
- **A propos de AVG** - ouvre la boîte de dialogue **Informations** comportant cinq onglets, où sont précisés le nom du programme, la version du programme, la version de la base de données virale, des informations système, le contrat de licence et des informations de contact d'**AVG Technologies CZ**.

7.2. Informations sur l'état de la sécurité

La section contenant les **informations sur l'état de la sécurité** figure dans la partie supérieure de la fenêtre principale AVG. Les informations sur l'état en cours de la sécurité du programme **AVG 9.0 File Server** sont toujours présentées à cet emplacement. Les icônes illustrées ont la signification suivante :



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



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

Cette icône s'affiche également si, pour une raison quelconque, vous décidez d'[ignorer l'erreur d'un composant](#) (l'option *Ignorer l'état du composant* est disponible dans le menu contextuel apparaissant suite à un clic droit sur l'icône du composant en question, dans la vue des composants de la fenêtre principale AVG). Vous pouvez être amené à utiliser cette option dans certaines situations, mais il est vivement conseillé de désactiver l'option **Ignorer l'état du composant** dès que possible.



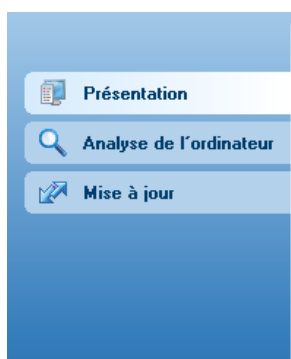
L'icône de couleur rouge signale que le programme AVG est dans un état critique. Un ou plusieurs composants ne fonctionnent pas convenablement et AVG n'est plus en mesure d'assurer la protection de l'ordinateur. Veuillez immédiatement vous porter sur le problème signalé. Si vous ne pouvez pas le résoudre,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

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

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

7.3. Liens d'accès rapide

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



- **Présentation** - ce lien permet de passer de l'interface AVG affichée à l'interface par défaut, qui affiche tous les composants installés - voir le chapitre [Présentation des composants >>](#)
- **Analyse de l'ordinateur** - ce lien affiche l'interface d'analyse d'AVG dans laquelle vous pouvez lancer directement des analyses, programmer des analyses ou modifier leurs paramètres - voir le chapitre [Analyse AVG >>](#)
- **Mise à jour** - ce lien ouvre l'interface de mise à jour et lance immédiatement le processus de mise à jour du programme AVG - voir le chapitre [Mises à jour AVG >>](#)

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

7.4. Présentation des composants

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

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

Dans **AVG 9.0 File Server** , le panneau de **présentation des composants** contient des renseignements sur les composants suivants :

- **Le composant Anti-Virus** garantit que l'ordinateur est protégé contre les virus essayant de pénétrer dans le système- [détails >>](#)
- **Le composant Anti-Spyware** analyse vos applications en arrière-plan lorsqu'elles sont activées - [détails >>](#)
- **Le composant Anti-Rootkit** détecte les programmes et les technologies cherchant à dissimuler des codes malveillants - [détails >>](#)
- **Le composant Licence** affiche le texte complet de l'accord de licence AVG - [détails >>](#)
- **Le composant Bouclier résident** s'exécute en arrière-plan et analyse les fichiers lorsqu'il sont copiés, ouverts ou enregistrés - [détails >>](#)

- **Le composant Mise à jour** recherche la présence d'une mise à jour AVG - [détails >>](#)

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

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

7.5. Statistiques

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


- **Analyse** - indique la date à laquelle la dernière analyse a eu lieu
- **Mise à jour** - indique la date à laquelle une mise à jour a été exécutée pour la dernière fois
- **BD virale** - précise la version de la base de données virale actuellement installée
- **Versión d'AVG** - indique la version du programme actuellement installée (*le numéro se présente sous la forme 8.0.xx. 8.0 désigne la version du produit et xx le numéro du build*)
- **Expiration de la licence** - précise la date à laquelle votre licence AVG cessera d'être valide

7.6. Icône de la barre d'état système

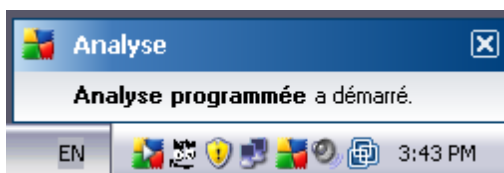
L'**icône de la barre d'état système** (dans la barre des tâches Windows) précise l'état actuel du programme **AVG 9.0 File Server**. Elle est toujours visible dans la barre d'état, que la fenêtre principale AVG soit ouverte ou fermée.

Lorsqu'elle est simplement en couleur , l'icône de la **barre d'état système** indique que tous les composants AVG sont actifs et entièrement opérationnels. Par ailleurs,

l'icône AVG dans la barre d'état s'affiche en couleurs. Si AVG signale une erreur mais que vous en avez été averti et avez choisi d'**ignorer l'état du composant**.

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

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



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

- **Ouvrir l'Interface utilisateur AVG** - cette commande permet d'afficher l'[interface utilisateur AVG](#)
- **Mise à jour** - cette option permet de lancer une [mise à jour](#)

8. Composants AVG

8.1. Anti-Virus

8.1.1. Principes de l'Anti-Virus

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

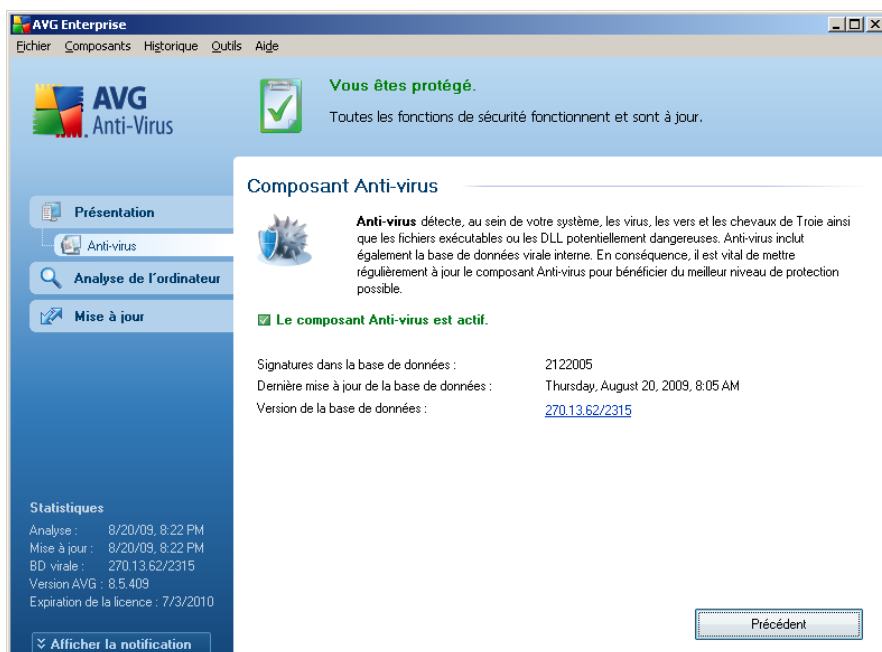
Rappelons que la fonction essentielle d'une protection anti-virus consiste à empêcher l'exécution de tout virus inconnu sur l'ordinateur.

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

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

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

8.1.2. Interface de l'Anti-Virus



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

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

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

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

sélectionnez le menu **Outils / Paramètres avancés** et modifiez la configuration d'AVG dans la boîte de dialogue [Paramètres avancés d'AVG](#) qui apparaît.

8.2. Anti-Spyware

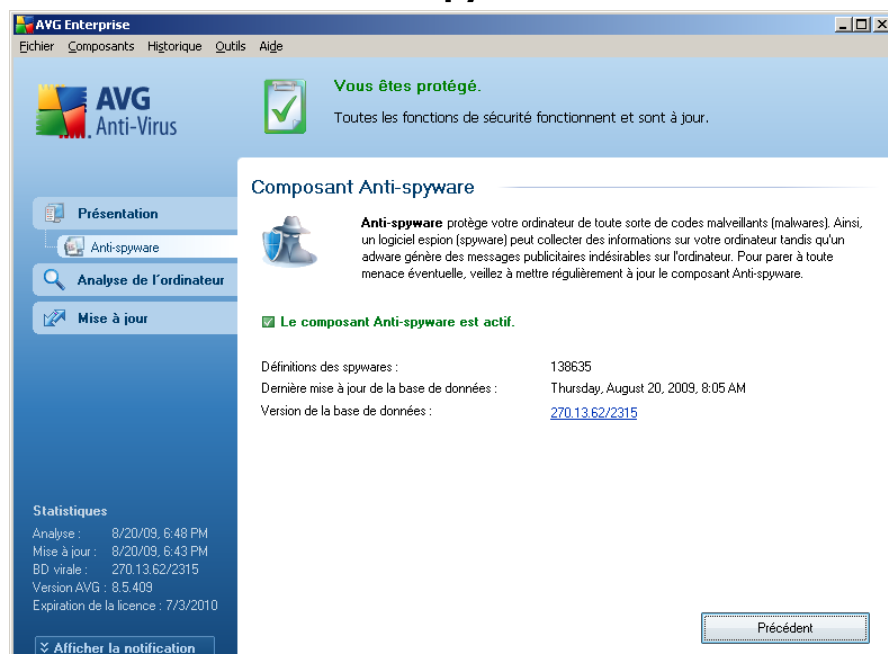
8.2.1. Principes de l'Anti-Spyware

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

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

L'introduction de codes malicieux dans votre ordinateur, avant installation du programme **AVG 9.0 File Server**, ou en cas d'oubli de l'application des dernières [mises à jour](#) de la base de données et du programme est un risque potentiel. Pour cette raison, AVG vous offre la possibilité d'analyser intégralement votre ordinateur à l'aide d'une fonction prévue à cet effet. Il se charge également de détecter les codes malicieux inactifs ou en sommeil (ceux qui ont été téléchargés, mais non activés).

8.2.2. Interface de l'Anti-Spyware



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

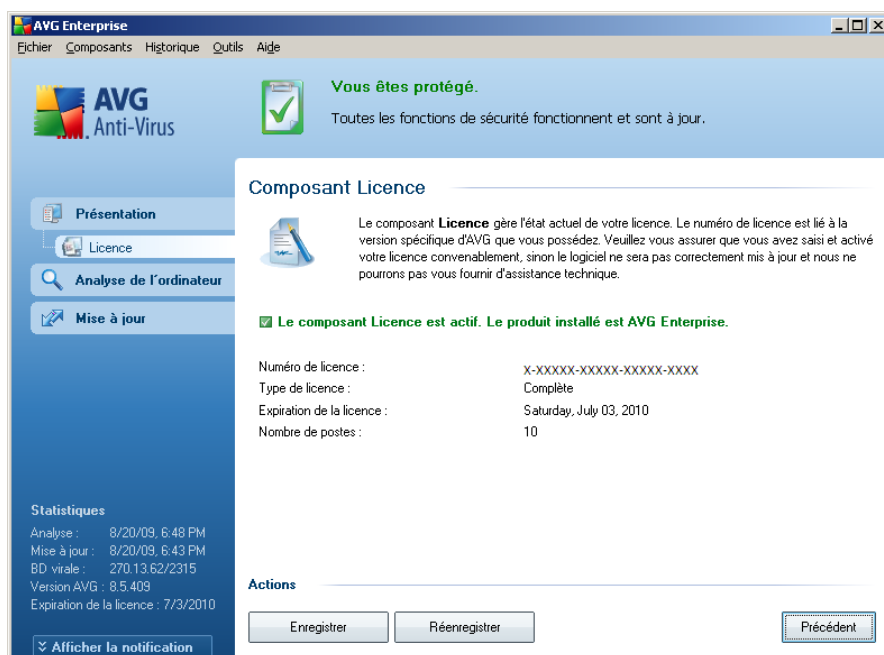
- **Signatures de spywares** : - indique le nombre d'exemples de spywares définis dans la dernière version de la base de données
- **Dernière mise à jour de la base de données** - précise la date et l'heure à laquelle la base de données a été mise à jour
- **Version de la base de données** - spécifie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

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

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

sélectionnez le menu **Outils / Paramètres avancés** et modifiez la configuration d'AVG dans la boîte de dialogue [Paramètres avancés d'AVG](#) qui apparaît.

8.3. Licence



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

- **Numéro de licence** - précise le numéro de licence complet. Lorsque vous saisissez un numéro de licence, vous devez le saisir exactement tel qu'il est affiché. Par conséquent, nous vous conseillons vivement de toujours procéder par "copier-coller" pour toute utilisation du numéro de licence.
- **Type de licence** - indique le type de produit installé.
- **Expiration de la licence** - cette date détermine la durée de validité de la licence. Pour continuer d'utiliser **AVG 9.0 File Server** après cette date, il est nécessaire de renouveler votre licence. Le [renouvellement peut être réalisé en ligne](http://www.avg.com) sur le site Web d'AVG (<http://www.avg.com>).
- **Nombre de postes** - nombre de postes de travail sur lequel vous êtes autorisé à installer le produit **AVG 9.0 File Server**.

Boutons de commande

- **Enregistrer** - renvoie à la page d'enregistrement du site Web d'AVG (<http://www.avg.com>). Merci de compléter le formulaire d'enregistrement ; seuls les clients ayant dûment enregistré leur produit AVG peuvent bénéficier de l'assistance technique gratuite.
- **Réactiver** - affiche la boîte de dialogue **Activer AVG** avec les données saisies dans la boîte de dialogue **Personnaliser AVG** au cours du [processus d'installation](#). Dans cette boîte de dialogue, vous indiquez votre numéro de licence en lieu et place de la référence d'achat (*le numéro indiqué lors de l'installation d'AVG*) ou de votre ancien numéro (*si vous installez une mise à niveau du produit AVG, par exemple*).
- **Précédent** - cliquez sur ce bouton pour revenir à l'[interface utilisateur AVG](#) par défaut (présentation des composants).

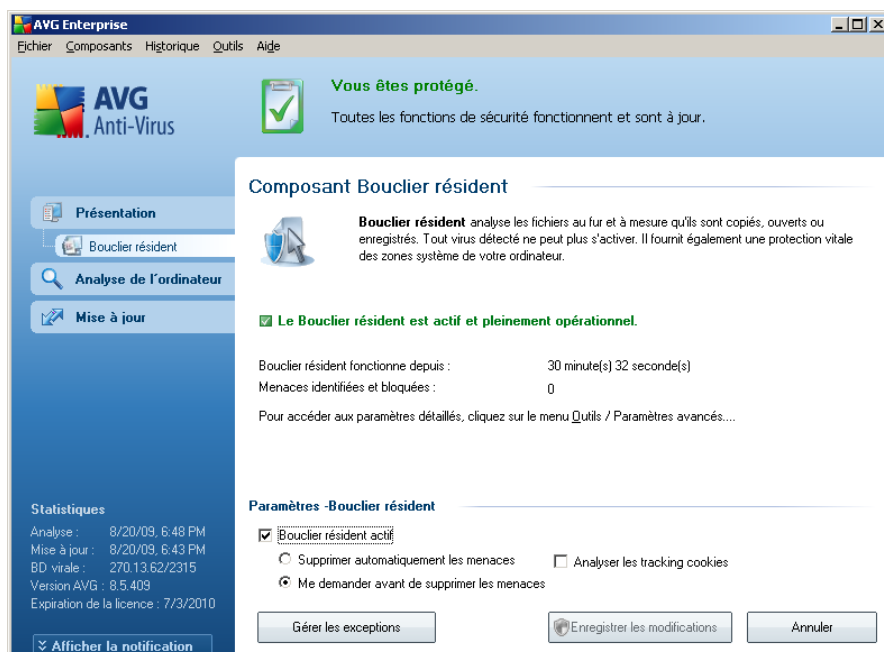
8.4. Bouclier résident

8.4.1. Principes du Bouclier résident

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

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

8.4.2. Interface du Bouclier résident



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

- **Le Bouclier résident est actif depuis** - indique le temps écoulé depuis le lancement du composant
- **Menaces identifiées et bloquées** - indique le nombre d'infections détectées dont l'exécution ou l'ouverture a été bloquée (*il est possible de réinitialiser cette valeur, si besoin est, à des fins statistiques par exemple - Réinitialiser la valeur*)

Configuration standard du composant

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

L'option **Le Bouclier résident est actif** permet d'activer ou désactiver la protection résidente. Par défaut, cette fonction est activée. Si la protection résidente est activée, vous pouvez définir plus précisément la manière dont les infections détectées sont traitées (c'est-à-dire supprimées) :

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

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

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

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

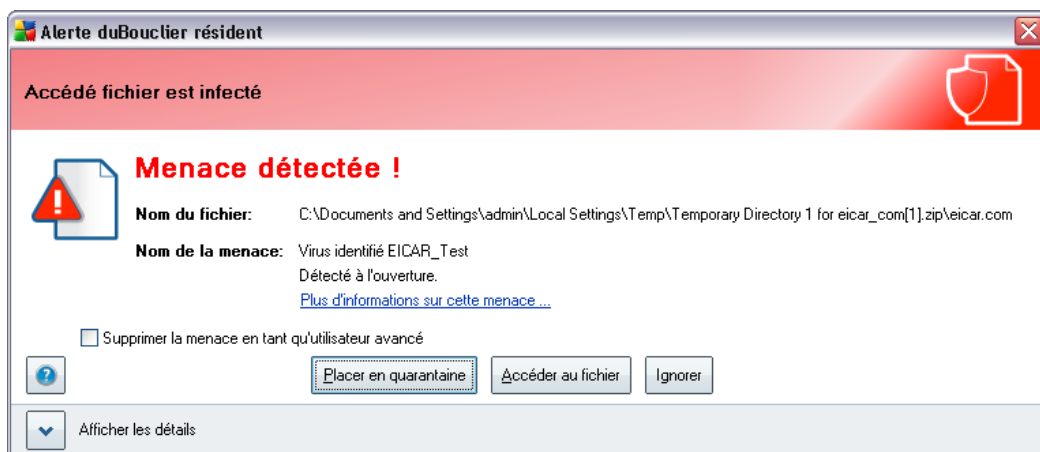
Boutons de commande

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

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

8.4.3. Détection du Bouclier résident

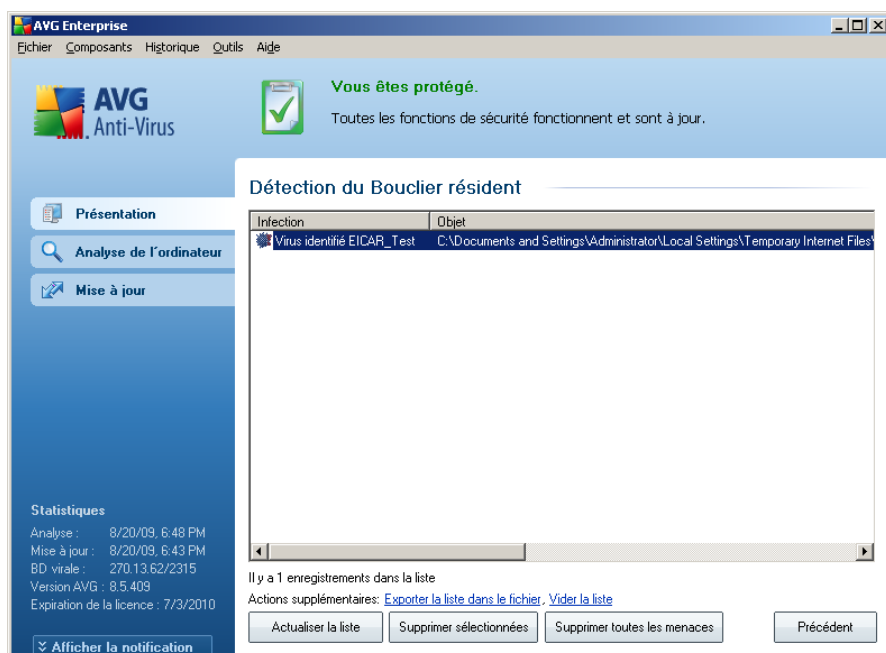
Le composant Bouclier résident analyse les fichiers lorsqu'ils sont copiés, ouverts ou enregistrés. Lorsqu'un virus ou tout autre type de menace est détecté, vous êtes averti immédiatement via la boîte de dialogue suivante :



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

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

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



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

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

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

basculer vers l'[Interface utilisateur AVG](#) par défaut (présentation des composants).

8.5. Mise à jour

8.5.1. Principes du composant Mise à jour

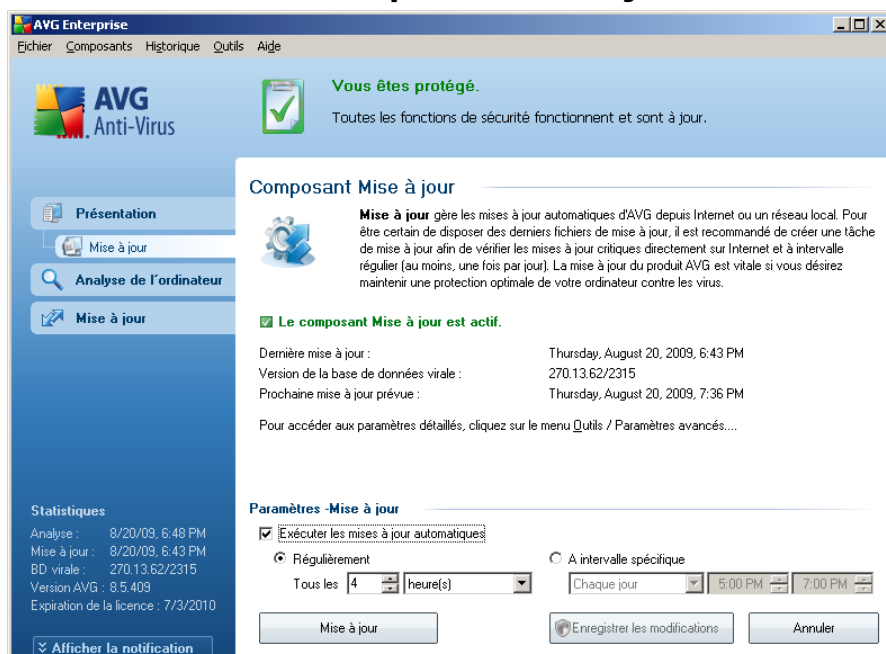
Aucun logiciel de sécurité ne peut garantir une protection fiable contre la diversité des menaces à moins d'une mise à jour régulière. Les auteurs de virus sont toujours à l'affût de nouvelles failles des logiciels ou des systèmes d'exploitation. Chaque jour apparaissent de nouveaux virus, malwares et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

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

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

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

8.5.2. Interface du composant Mise à jour



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

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

Configuration standard du composant

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

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

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

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

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

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

Boutons de commande

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

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

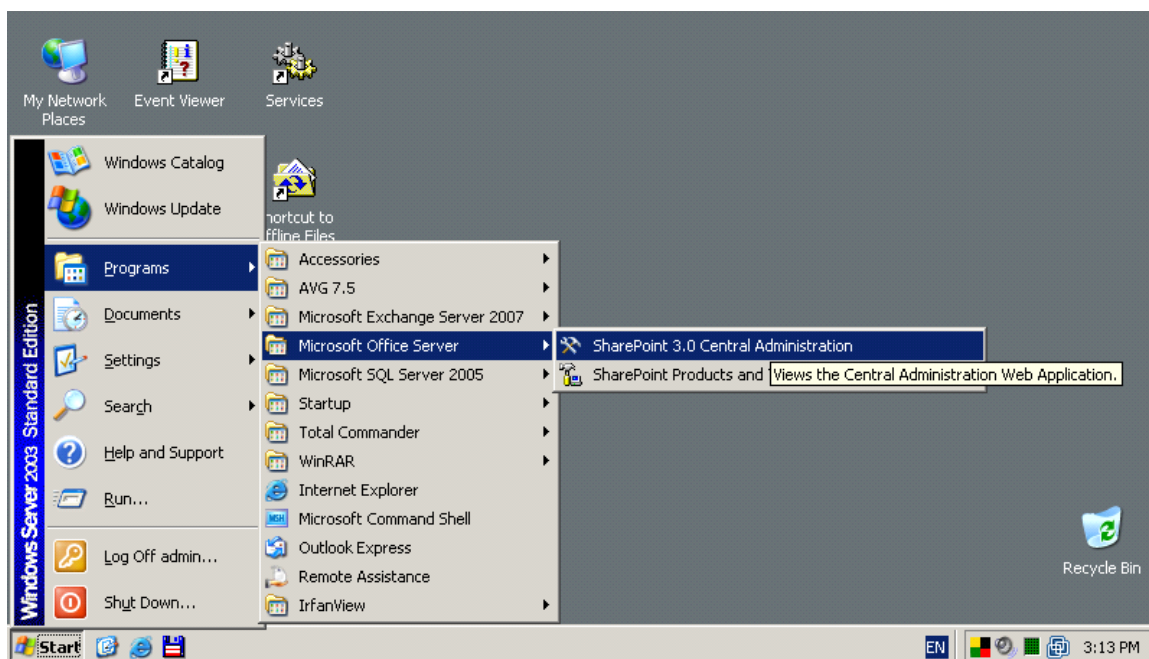
9. AVG pour Serveur SharePoint Portal

Ce chapitre est consacré à la maintenance d'AVG sur **MS SharePoint Portal Server** qui peut être considéré comme un type particulier de serveur de fichiers.

9.1. Maintenance du programme

AVG for SharePoint Portal Server utilise l'interface d'analyse antivirus Microsoft SP VSAPI 1.4 pour la protection de votre serveur contre toute forme d'infection. Les objets sur le serveur sont analysés pour détecter la présence d'un code malveillant lorsqu'ils sont téléchargés depuis ou sur le serveur par vos utilisateurs. La configuration de la protection antivirus peut être installée grâce à l'interface **Administration Centrale** de votre SharePoint Portal Server. Au sein de l'**Administration centrale**, vous pouvez également visualiser et gérer le fichier journal **AVG for SharePoint Portal Server**.

Vous pouvez lancer l'**Administration centrale de SharePoint Portal Server** lorsque vous ouvrez une session depuis l'ordinateur sur lequel votre serveur est exécuté. L'interface d'administration est accessible en ligne (*de même que l'interface utilisateur SharePoint Portal Server*) et vous pouvez l'ouvrir grâce à l'option **Administration Centralisée SharePoint (3.0)** dans le dossier **Programs/Microsoft Office Server** (ou grâce à l'option **SharePoint Portal Server**) du menu **Démarrer** de Windows :



Vous pouvez également accéder à la page Web **Administration centrale de SharePoint Portal Server** à distance en utilisant les droits d'accès et l'URL nécessaires.

9.2. Configuration d'AVG pour SPPS - Sharepoint 2007

Dans l'interface de l'**Administration centrale de Sharepoint 3.0**, vous pouvez facilement configurer les paramètres de performance et les tâches du scanner **AVG for SharePoint Portal Server**. Choisissez l'option **Opérations** dans la section **Administration centrale**. Une nouvelle boîte de dialogue s'affiche. Sélectionnez **Anti-virus** dans la section **Configuration de la sécurité**.

Security Configuration

- ▣ Service accounts
- ▣ Information Rights Management
- ▣ Antivirus
- ▣ Blocked file types
- ▣ Update farm administrator's group
- ▣ Information management policy configuration
- ▣ Manage settings for single sign-on

La fenêtre suivante va s'afficher :

Central Administration > Operations > Antivirus

Antivirus

Use this page to configure settings for virus scanning. You must install virus scanning software on all Web servers that are hosting documents before these settings can take effect. [Learn about configuring antivirus settings.](#)

Antivirus Settings

Specify when you want documents stored in document libraries and lists to be virus scanned, and whether you want your virus scanner to attempt to clean infected documents.

- Scan documents on upload
- Scan documents on download
- Allow users to download infected documents
- Attempt to clean infected documents

Antivirus Time Out

You can specify how long the virus scanner should run before timing out. If server response time is slow while scanning, you may want to decrease the number of seconds.

Time out duration (in seconds):

Antivirus Threads

You can specify the number of execution threads on the server that the virus scanner may use. If server response time is slow while scanning, you may want to decrease the number of threads allowed for virus scanning.

Number of threads:

Vous pouvez, à partir d'ici, configurer différentes tâches d'analyse **AVG for SharePoint Portal Server** ainsi que les caractéristiques de performance :

- **Analyser les documents lors du chargement** – activer/désactiver l'analyse des documents qui sont en train d'être chargés
- **Analyser les documents lors du téléchargement** – activer/désactiver l'analyse des documents qui sont en train d'être téléchargés
- **Autoriser les utilisateurs à télécharger des documents infectés** – autoriser/empêcher le téléchargement de documents infectés par les utilisateurs
- **Nettoyer les documents infectés** – activer/désactiver la suppression automatique des documents infectés
- **Durée du délai d'expiration (en secondes)** – la valeur maximale en secondes de la durée de la procédure d'analyse des virus après chaque lancement (diminuez cette valeur lorsque le serveur devient relativement lent lors de

l'analyse de documents)

- **Nombre de threads** - vous pouvez spécifier le nombre de threads d'analyse de virus qui peuvent s'exécuter simultanément ; l'augmentation de ce nombre peut entraîner une accélération de l'analyse du fait du niveau de parallélisme qui est plus élevé, mais elle peut en outre accroître le temps de réaction du serveur

9.3. Configuration d'AVG pour SPPS - Sharepoint 2003

Dans l'interface de l'**Administration centrale de Sharepoint Portal Server**, vous pouvez facilement configurer les paramètres de performance et les tâches du scanner **AVG for SharePoint Portal Server**. Choisissez l'option **Configuration des tâches de l'anti-virus** dans la section **Configuration de la sécurité**

Component Configuration



Use these links to manage search settings, configure single sign-on, manage shared services, configure usage analysis, HTML viewer settings and configure diagnostic settings. If you have installed the optional document library component, you can configure document libraries (Web Storage System-based) from here.

- ▣ [Manage the Search Service](#)
- ▣ [Manage settings for single sign-on](#)
- ▣ [Manage shared services for the server farm](#)
- ▣ [Configure usage analysis processing](#)
- ▣ [Configure HTML viewer](#)
- ▣ [Configure diagnostic settings](#)

La fenêtre suivante va s'afficher :

Windows SharePoint Services

Configure Antivirus Settings

Use this page to configure settings for virus scanning. You must install virus scanning software on all Web servers that are hosting documents before these settings can take effect. [Show me more information.](#)

Antivirus Settings

Specify when you want documents stored in document libraries and lists to be virus scanned, and whether you want your virus scanner to attempt to clean infected documents. You can also specify how long the virus scanner should run before timing out, and the number of execution threads on the server that it may use. If server response time is slow while scanning, you may want to decrease the number of seconds and threads allowed for virus scanning.

- Scan documents on upload
- Scan documents on download
- Allow users to download infected documents
- Attempt to clean infected documents
- Time out scanning after seconds
- Allow scanner to use up to threads

OK

Cancel

Vous pouvez, à partir d'ici, configurer différentes tâches d'analyse **AVG for SharePoint Portal Server** ainsi que les caractéristiques de performance :

- **Analyser les documents lors du chargement** – activer/désactiver l'analyse des documents qui sont en train d'être chargés
- **Analyser les documents lors du téléchargement** – activer/désactiver l'analyse des documents qui sont en train d'être téléchargés
- **Autoriser les utilisateurs à télécharger des documents infectés** – autoriser/empêcher le téléchargement de documents infectés par les utilisateurs
- **Nettoyer les documents infectés** - activer/désactiver la suppression automatique des documents infectés
- **Durée maximale de l'analyse** – valeur maximale en secondes de la procédure d'analyse de virus après chaque lancement (*diminuez la valeur si le serveur devient relativement lent lors de l'analyse de documents*)
- **Utilisez au maximum X sous-processus lors de l'analyse de documents** – Le nombre X désigne le nombre de threads d'analyse de virus qui peuvent

s'exécuter simultanément ; l'augmentation de ce nombre peut entraîner une accélération de l'analyse du fait du niveau de parallélisme qui est plus élevé, mais elle peut aussi accroître le délai de réaction du serveur

9.4. AVG pour SPSS - Edition Diagnostics

Vous pouvez visualiser les messages de diagnostic de **AVG for SharePoint Portal Server** après avoir choisi la **Configuration des paramètres de diagnostic** dans la section **Configuration du composant de l'administration centralisée SharePoint** :

Component Configuration



Use these links to manage search settings, configure single sign-on, manage shared services, configure usage analysis, HTML viewer settings and configure diagnostic settings. If you have installed the optional document library component, you can configure document libraries (Web Storage System-based) from here.

- ▣ [Manage the Search Service](#)
- ▣ [Manage settings for single sign-on](#)
- ▣ [Configure usage analysis processing](#)
- ▣ [Configure HTML viewer](#)
- ▣ [Configure diagnostic settings](#)

Toutes les informations de diagnostic liées à la performance de **AVG for SharePoint Portal Server** sont stockées dans le fichier *_AVG4SPS.LOG. Vous pouvez visualiser le contenu de ce fichier après l'avoir choisi dans la section **Afficher les protocoles de diagnostic** dans la fenêtre **Configuration des paramètres de diagnostic** :

SharePoint Portal Server Central Administration
 Configure Diagnostic Settings for PC28-2003-EN

Use this page to change logging settings and review diagnostic logs.

Logging Settings

Click the component for which you want to change the settings and then click **Edit**.

Components:

- WWW Worker Process
- Notification Service
- Single Sign-on Service
- Administrative Service
- Search Service
- Search Filter Process
- Backup - Restore
- Audience Job
- Third Party Applications

View Diagnostic Logs

Click the diagnostic log that you want to view or delete.

Diagnostic logs:

2005-01-21 12:52:48 SiteCreation_Grisoft Testing SharePoint F
2005-01-21 11:37:44 00000656_MSIB6B.LOG
2005-01-21 19:30:01 00003180_MSSDMN.LOG
2005-01-21 12:57:42 00003012_MSSEARCH.LOG
2005-01-21 19:22:39 00000668_MSSEARCH.LOG
2005-01-21 19:23:52 00000672_MSSEARCH.LOG
2005-01-21 11:42:29 00001508_SPSADM.LOG
2005-01-21 19:23:47 00001844_SPSADMIN.LOG
2005-01-21 19:23:53 00000692_SPSNOTIFICATIONSERVICE.L
2005-01-21 11:43:02 00001924_W3WP.LOG

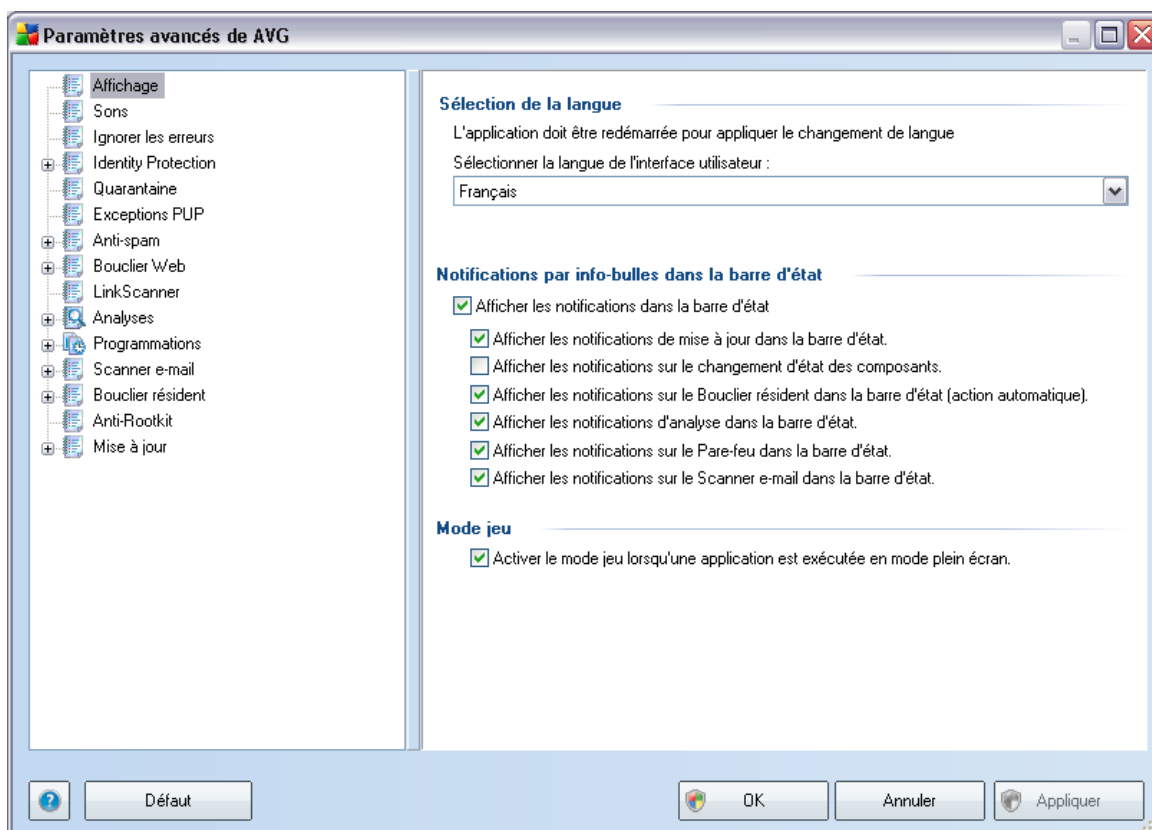
Cliquez sur le bouton **Afficher le journal** pour consulter le fichier journal de **AVG for SharePoint Portal Server**.

10. Paramètres avancés d'AVG

La boîte de dialogue de configuration avancée d'**AVG 9.0 File Server** a pour effet d'ouvrir une nouvelle fenêtre intitulée **Paramètres avancés d'AVG**. Cette fenêtre se compose de deux parties : la partie gauche présente une arborescence qui permet d'accéder aux options de configuration du programme. Sélectionnez le composant dont vous voulez corriger la configuration (*ou celle d'une partie spécifique*) pour ouvrir la boîte de dialogue correspondante dans la partie droite de la fenêtre.

10.1. Affichage

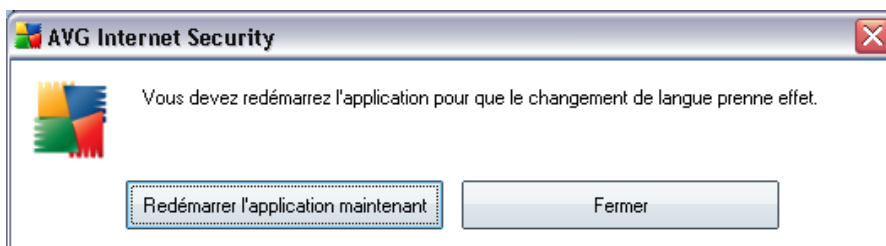
Le premier élément de l'arborescence de navigation, **Affichage**, porte sur les paramètres généraux de l'[interface utilisateur AVG](#) et sur des options élémentaires du comportement de l'application :



Sélection de la langue

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

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



Notifications par info-bulles dans la barre d'état

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

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

- **Afficher les notifications dans la barre d'état système** - par défaut, activée (*cochée*) ; les notifications s'affichent. Désélectionnez cette option pour désactiver l'affichage de toutes les notifications par info-bulles. Lorsqu'elle est active, vous pouvez sélectionner les notifications qui doivent s'afficher :
 - **Afficher les notifications de [mise à jour](#)** dans la barre d'état - indiquez

s'il faut afficher les informations sur le lancement de la mise à jour AVG, la progression et la fin du processus ;

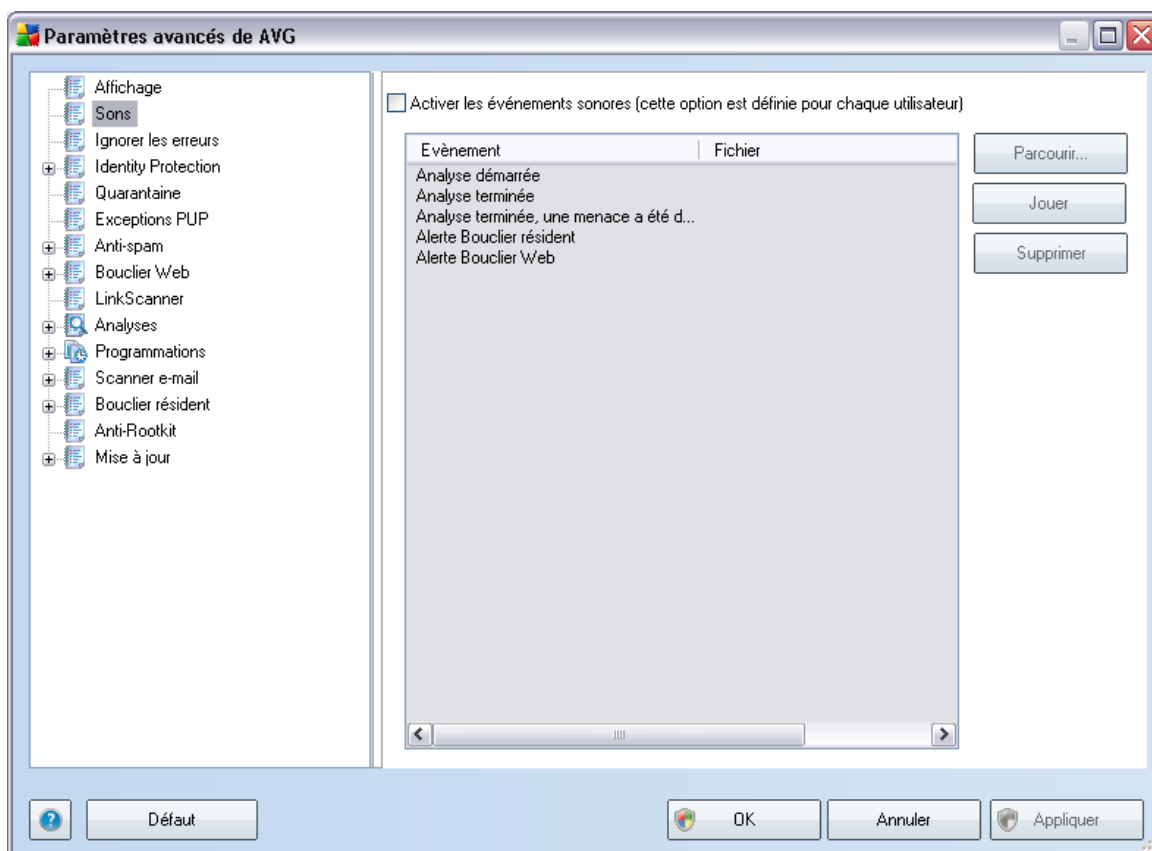
- **Afficher les notifications sur le changement d'état des composants** - indiquez s'il faut afficher des informations sur l'activité/ arrêt d'activité des composants ou les problèmes éventuels. Lorsque cette option signale une anomalie d'un composant, elle remplit la même fonction d'information que l'[icône dans la barre d'état système](#) (changement de couleur) indiquant un problème lié à un composant AVG;
- **Afficher des notifications sur le [Bouclier résident](#) dans la barre d'état** - indiquez s'il faut afficher ou supprimer les informations sur les processus d'enregistrement, de copie et d'ouverture de fichier ;
- **Afficher les notifications d'analyse** dans la barre d'état - indiquez s'il faut afficher les informations sur le lancement automatique de l'analyse programmée, sa progression et ses résultats.

Mode jeu

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

10.2. Sons

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

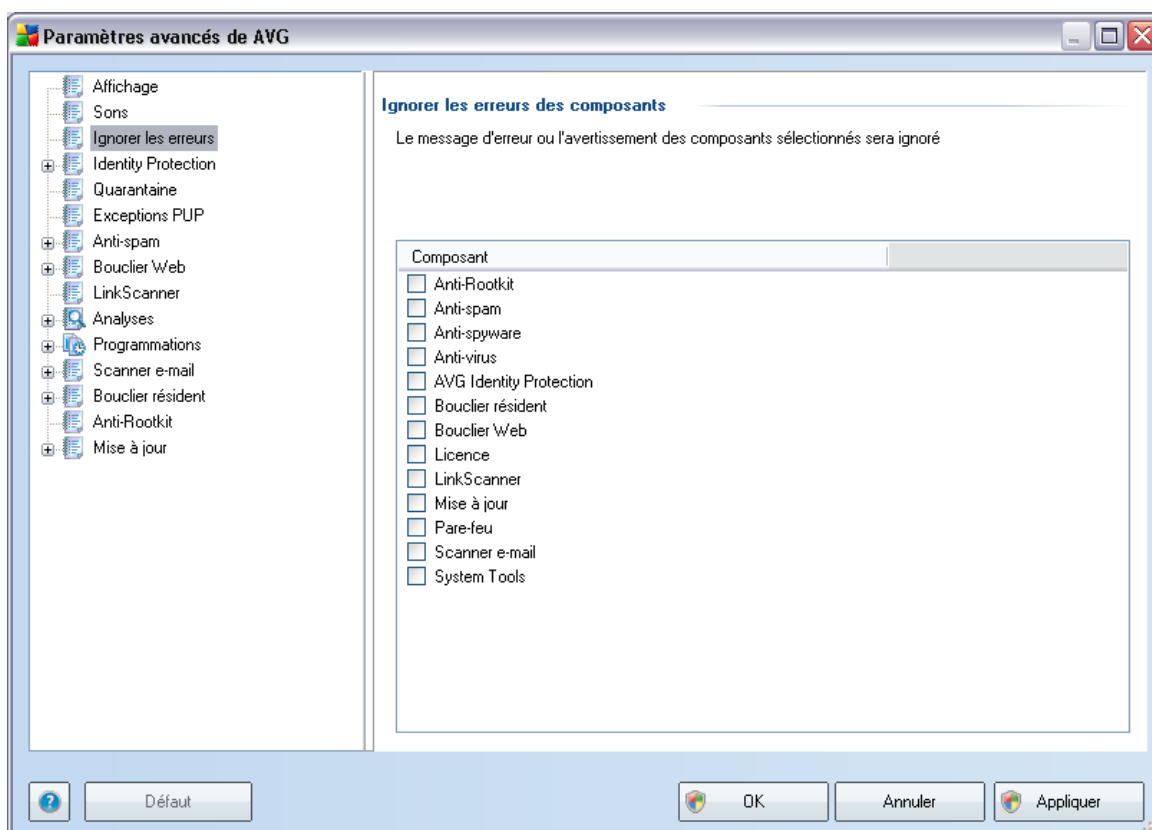


Ainsi, sélectionnez l'évènement correspondant à partir de la liste et recherchez (**Parcourir**) un son approprié que vous souhaitez affecter à cet évènement. Pour écouter le son sélectionné, mettez en surbrillance l'évènement dans la liste et cliquez sur le bouton **Jouer**. Utilisez le bouton **Supprimer**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

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

10.3. Ignorer les erreurs

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



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

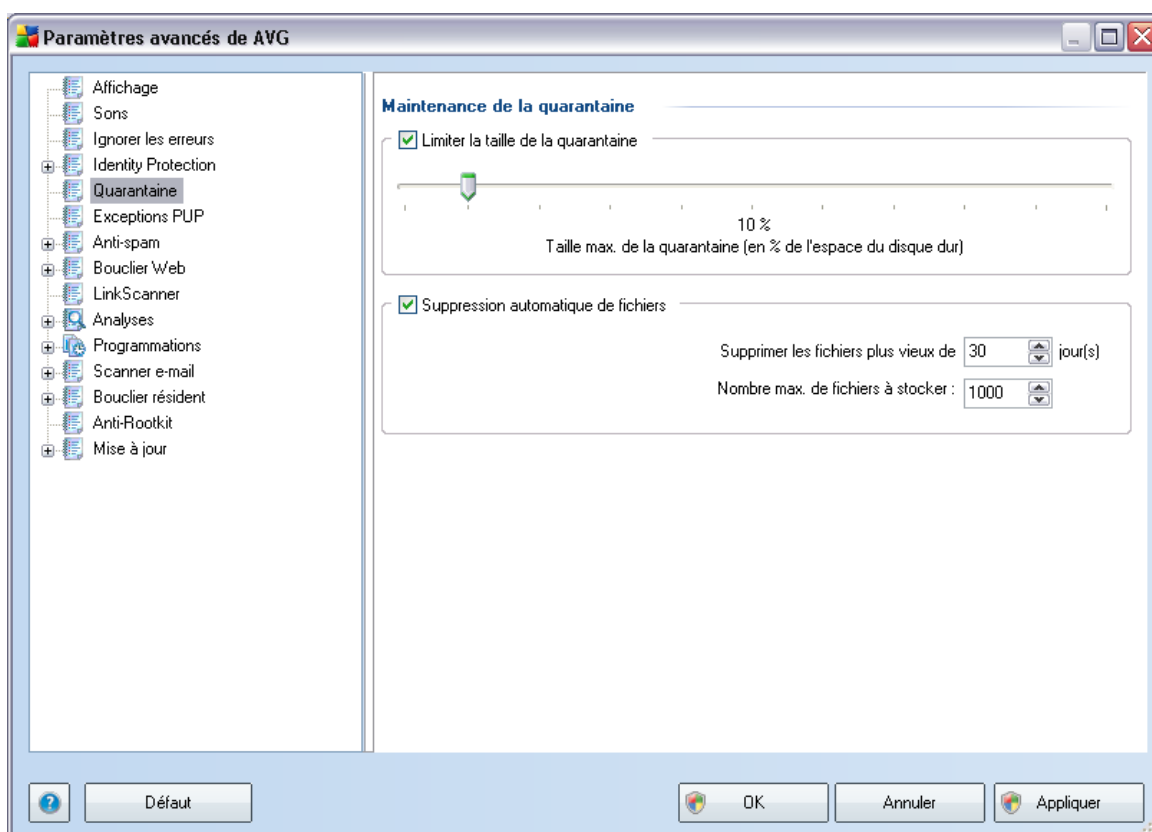
- **icône de la barre d'état système** - si tous les composants d'AVG fonctionnent correctement, l'icône apparaît en quatre couleurs ; cependant, si une erreur se produit l'icône apparaît avec un point d'exclamation de couleur jaune,
- description du problème existant dans la section relative à l'**état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

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

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

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

10.4. Quarantaine



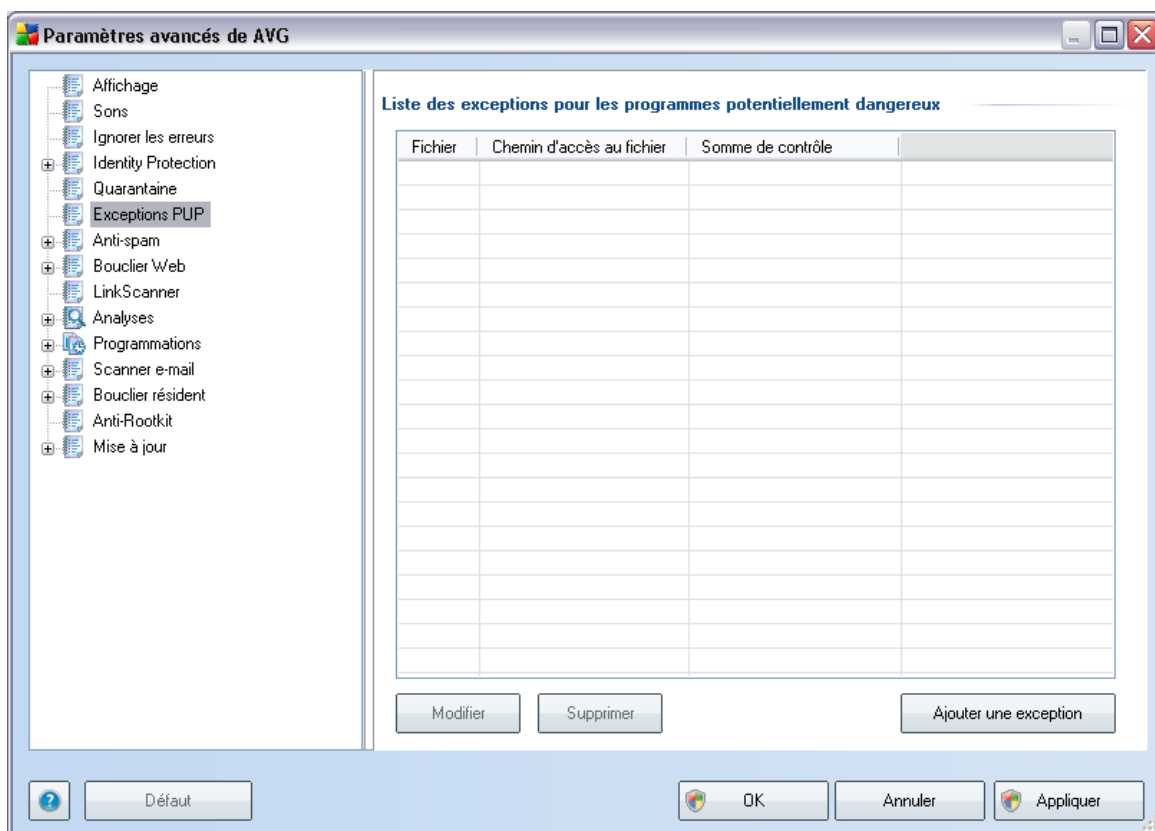
La boîte de dialogue **Maintenance de la quarantaine** permet de définir plusieurs

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**)

10.5. Exceptions PUP

AVG 9.0 File Server est en mesure d'analyser et de détecter des exécutables ou bibliothèques DLL qui peuvent s'avérer malveillants envers le système. Dans certains cas, il est possible que l'utilisateur souhaite conserver certains programmes considérés comme potentiellement dangereux sur son ordinateur (*ceux installés volontairement, par exemple*). Certains programmes, et notamment ceux fournis gratuitement, font partie de la famille des adwares. Or, ce type de programme peut être signalé par AVG comme un **programme potentiellement dangereux**. Si vous souhaitez malgré tout le conserver sur votre ordinateur, il suffit de le définir comme une exception de programme potentiellement dangereux :

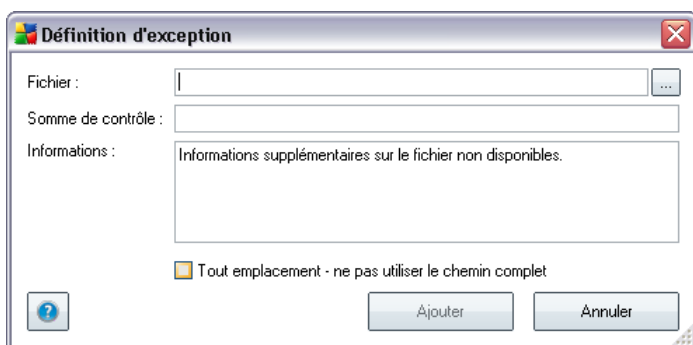


La boîte de dialogue **Liste des exceptions pour les programmes potentiellement dangereux** dresse la liste des exceptions déjà définies et actuellement valides par rapport aux programmes indésirables. Vous pouvez modifier la liste, supprimer des éléments existants ou ajouter une nouvelle exception.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

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

Boutons de commande

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



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

10.6. Analyses

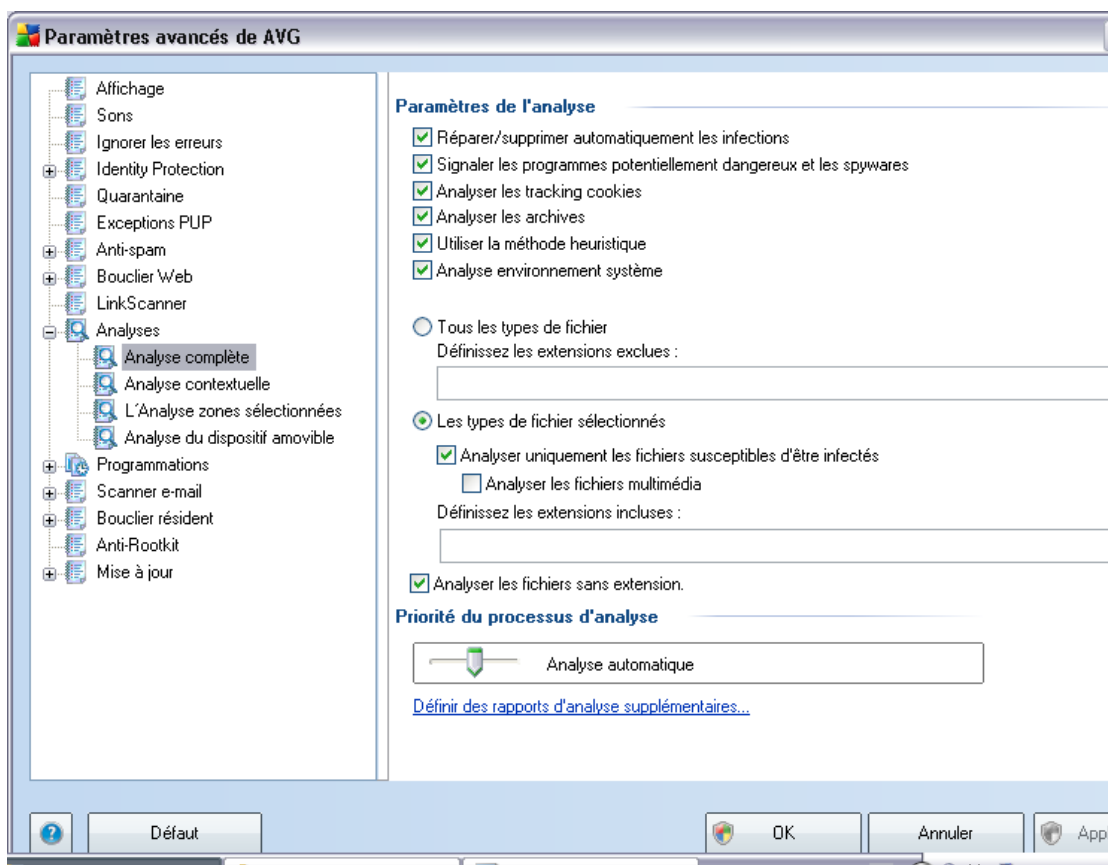
Les paramètres d'analyse avancés sont répartis en trois catégories selon le type d'analyse spécifique tel qu'il a été défini par le fournisseur du logiciel :

- **Analyse complète** - analyse standard prédéfinie appliquée à l'ensemble des fichiers contenus dans l'ordinateur

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

10.6.1. Analyse complète

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



Paramètres de l'analyse

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

- **Réparer/supprimer automatiquement les infections** - lorsqu'un virus est détecté au cours de l'analyse, il sera réparé automatiquement si une solution est disponible. Si la désinfection automatique du fichier n'est pas possible (ou si cette option est désactivée), un message de détection de virus s'affiche. Il vous appartient alors de déterminer le traitement à appliquer à l'infection. La procédure recommandée consiste à confiner le fichier infecté en [quarantaine](#).
- **Signaler les programmes potentiellement dangereux et les spywares** - ce paramètre contrôle la fonctionnalité [Anti-Virus](#) qui [détecte les programmes potentiellement dangereux](#) (fichiers exécutables fonctionnant comme des spywares ou des adwares) et les bloque ou les supprime.
- **Analyser les tracking cookies** - ce paramètre du composant [Anti-Spyware](#) indique qu'il faut détecter les cookies ; (les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique).
- **Analyser les archives** - ce paramètre indique que l'analyse doit examiner tous les fichiers même ceux stockés dans des archives ZIP, RAR, etc.
- **Utiliser la méthode heuristique** - l'analyse heuristique (émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel) est l'une des méthodes employées pour détecter des virus pendant l'analyse.
- **Analyser environnement système** - l'analyse vérifie aussi l'environnement système de l'ordinateur.

Ensuite, vous pouvez choisir d'analyser

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

analyse.

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

Priorité du processus d'analyse

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

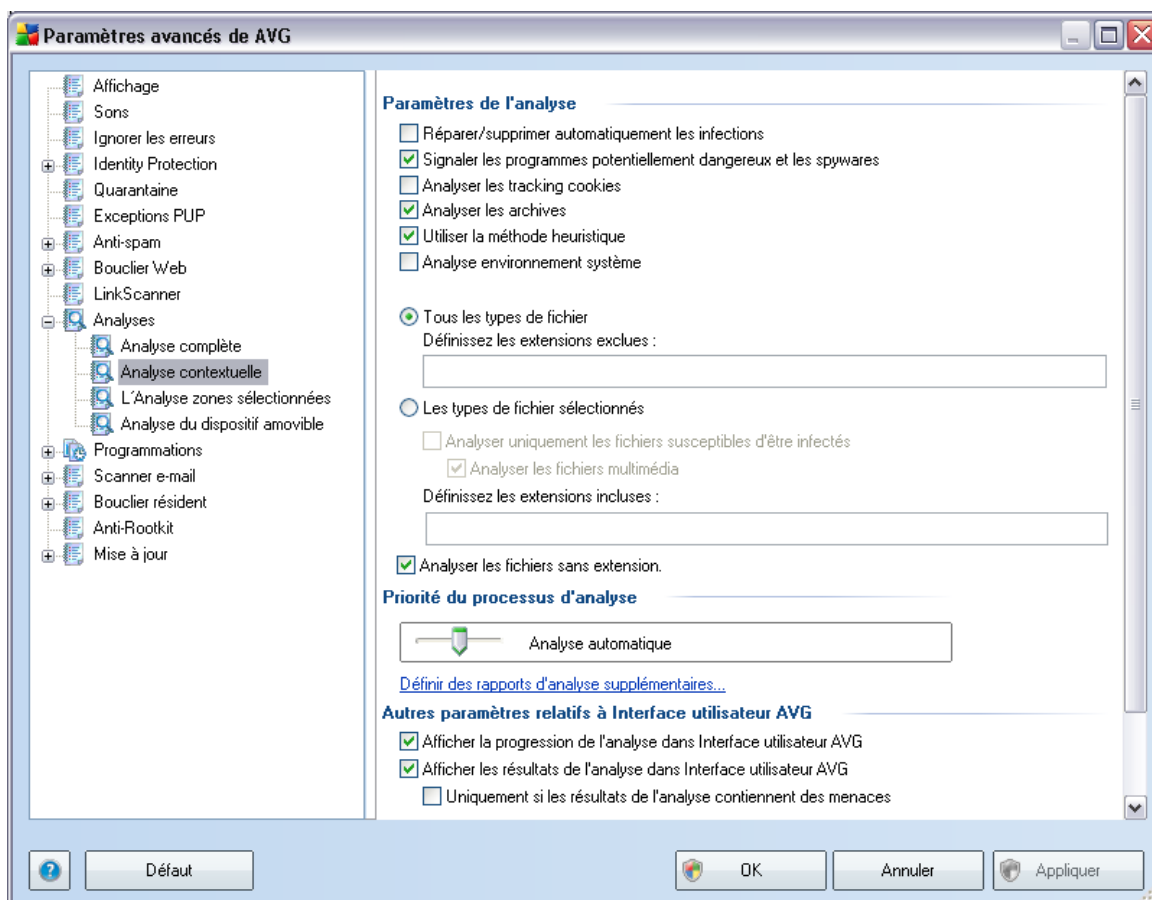
Définir des rapports d'analyse supplémentaires ...

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



10.6.2. Analyse contextuelle

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

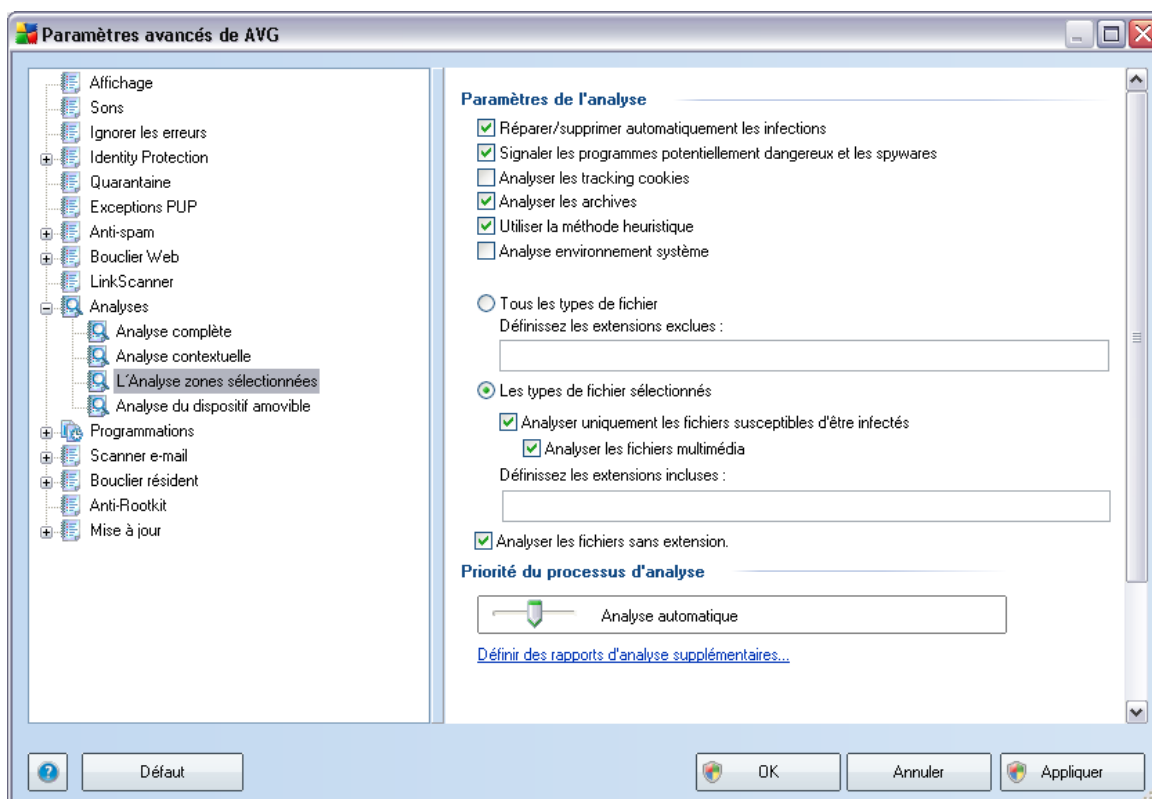


La liste des paramètres correspond à celle proposée pour l'**[Analyse complète](#)**. Cependant, la configuration par défaut est différente : dans l'**[Analyse complète](#)**, les principaux paramètres sont sélectionnés tandis que pour l'**[analyse contextuelle \(analyse dans l'Explorateur Windows\)](#)**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

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

10.6.3. Analyse zones sélectionnées

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

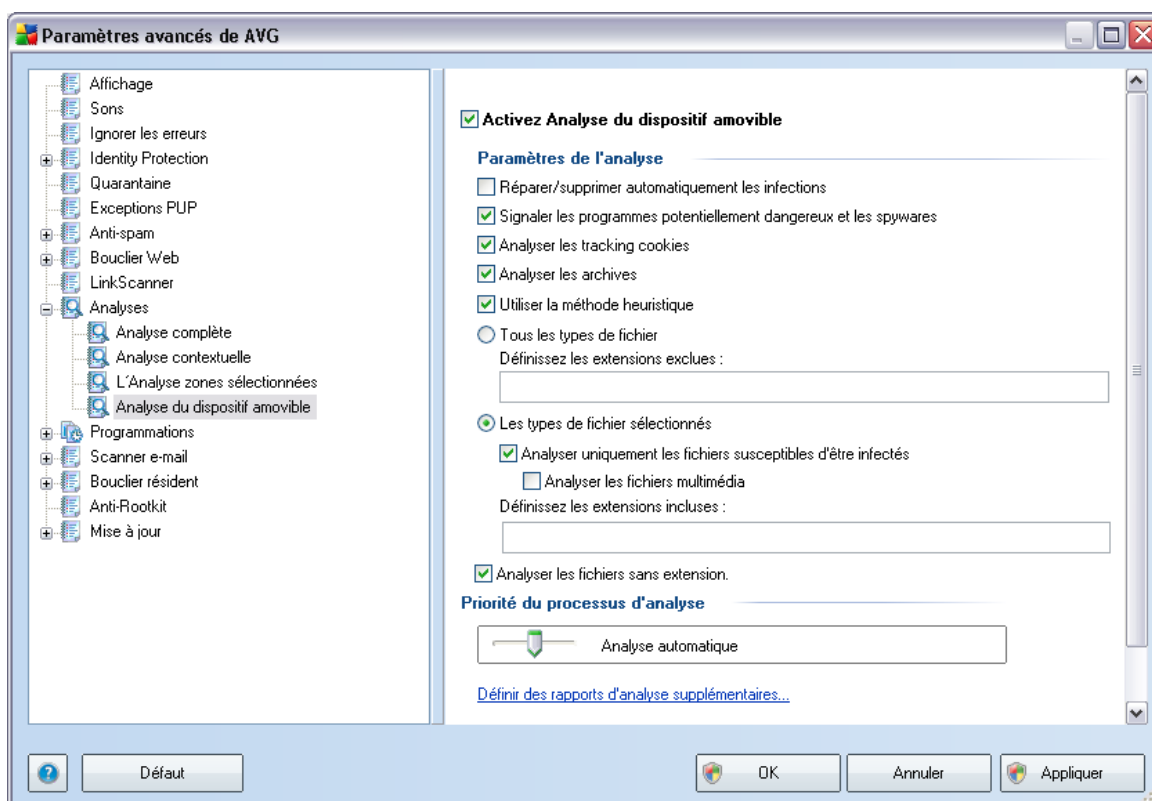


Tous les paramètres définis dans cette boîte de dialogue de configuration s'appliquent uniquement aux zones sélectionnées pour analyse dans l'option **Analyse zones sélectionnées**! Si vous cochez l'option **Analyser les rootkits** dans cette boîte de dialogue de configuration, une recherche rapide de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

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

10.6.4. Analyse du dispositif amovible

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



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

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

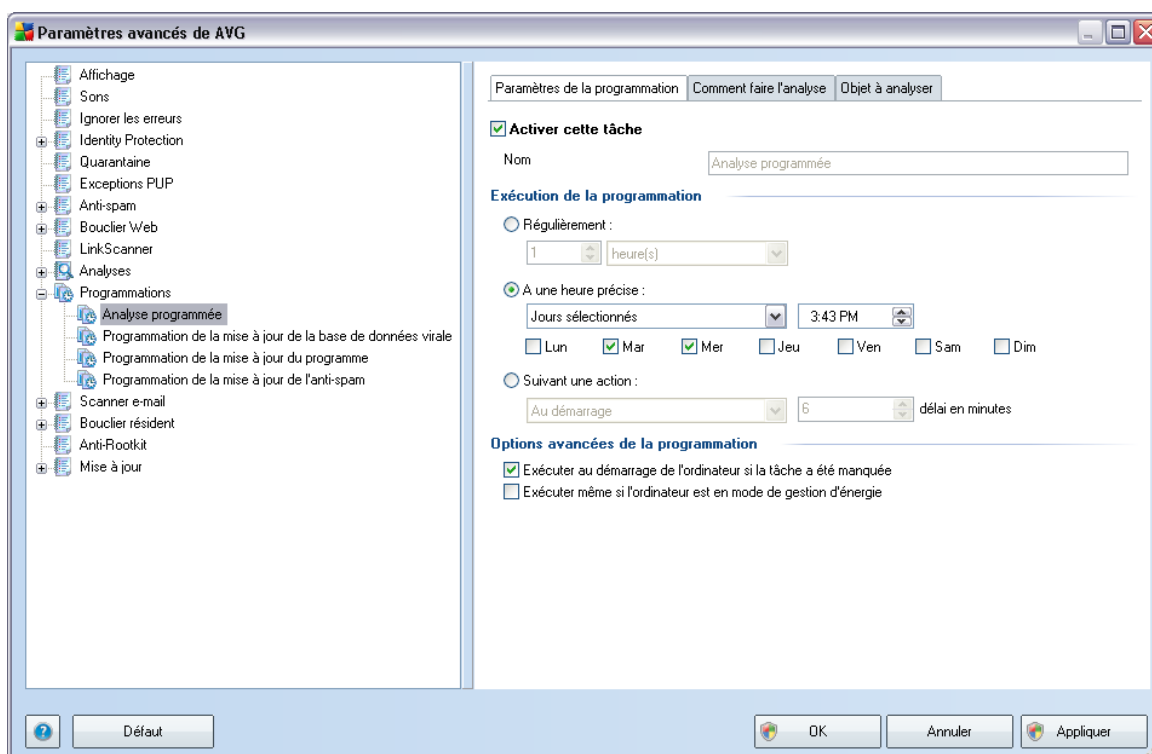
10.7. Programmations

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

- [Programmation de l'analyse complète de l'ordinateur](#)
- [Programmation de la mise à jour de la base de données virale](#)
- [Programmation de la mise à jour du programme](#)

10.7.1. Analyse programmée

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



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

le réactiver au moment opportun.

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

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

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

Exécution de la programmation

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

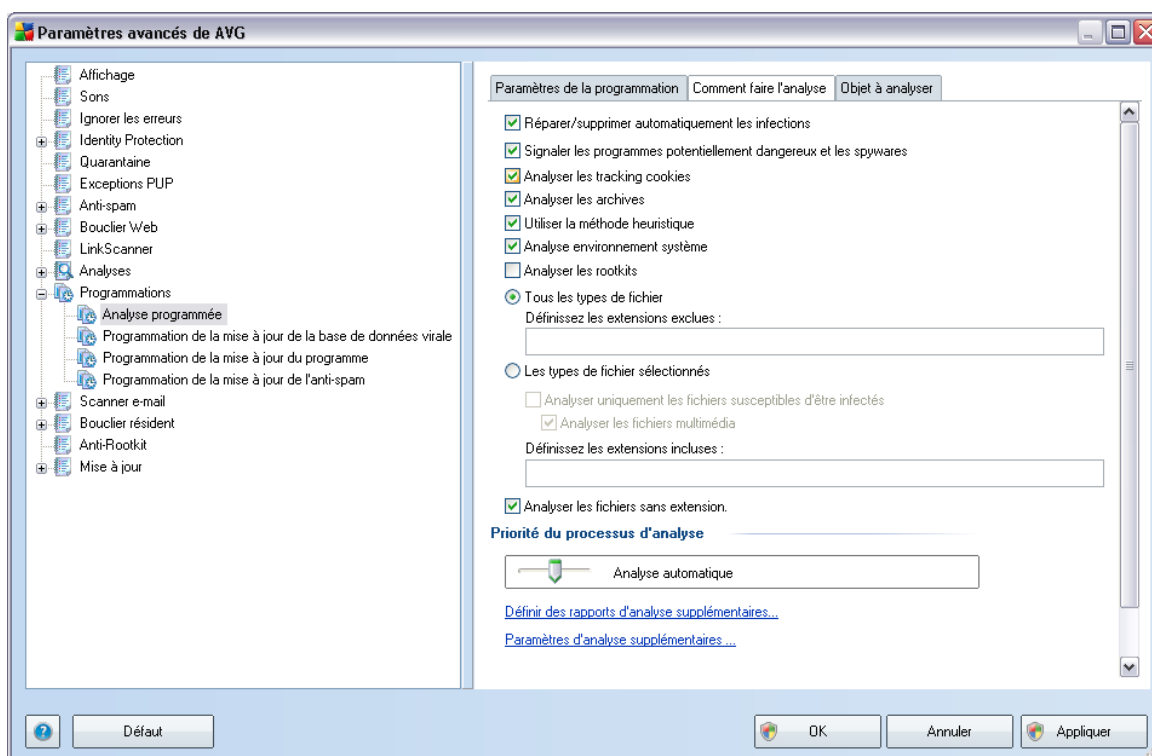
Options avancées de la programmation

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

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



Une nouvelle [icône de la barre d'état système AVG](#) s'affiche alors (en couleurs avec une flèche blanche - voir illustration ci-dessus) et signale qu'une analyse programmée est en cours.



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

- **Réparer/supprimer automatiquement les infections** - (option activée par défaut) : lorsqu'un virus est détecté au cours de l'analyse, il sera réparé automatiquement si une solution est disponible. Si la désinfection automatique

du fichier n'est pas possible (ou si cette option est désactivée), un message de détection de virus s'affiche. Il vous appartient alors de déterminer le traitement à appliquer à l'infection. L'action recommandée consiste à confiner le fichier infecté en [quarantaine](#).

- **Signaler les programmes potentiellement dangereux et les spywares** - (option activée par défaut) : ce paramètre contrôle la fonctionnalité [Anti-Virus](#) qui [détecte les programmes potentiellement dangereux](#) (fichiers exécutables fonctionnant comme des spywares ou des adwares) afin de les bloquer ou de les supprimer.
- **Analyser les tracking cookies** - (option activée par défaut) : ce paramètre du composant [Anti-Spyware](#) indique que les cookies doivent être détectés au cours de l'analyse ; les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique)
- **Analyser les archives** - (option activée par défaut) : ce paramètre indique que l'analyse doit examiner tous les fichiers même ceux stockés dans des archives (archives ZIP, RAR, par exemple).
- **Utiliser la méthode heuristique** - (option activée par défaut) : l'analyse heuristique (émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel) est l'une des méthodes employées pour détecter des virus pendant l'analyse.
- **Analyser environnement système** - (option activée par défaut) : l'analyse vérifie les fichiers système de l'ordinateur.
- **Analyser les rootkits** - cochez cette option si vous souhaitez inclure la détection de rootkits dans l'analyse complète de l'ordinateur. La détection seule de rootkits est aussi proposée dans le composant **Anti-Rootkit**;

Ensuite, vous pouvez choisir d'analyser

- **Tous les types de fichiers** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers (séparées par des virgules) à ne pas analyser ; ou
- **Types de fichier sélectionnés** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables), y compris les fichiers média (vidéo, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers

qui sont rarement infectés par un virus). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.

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

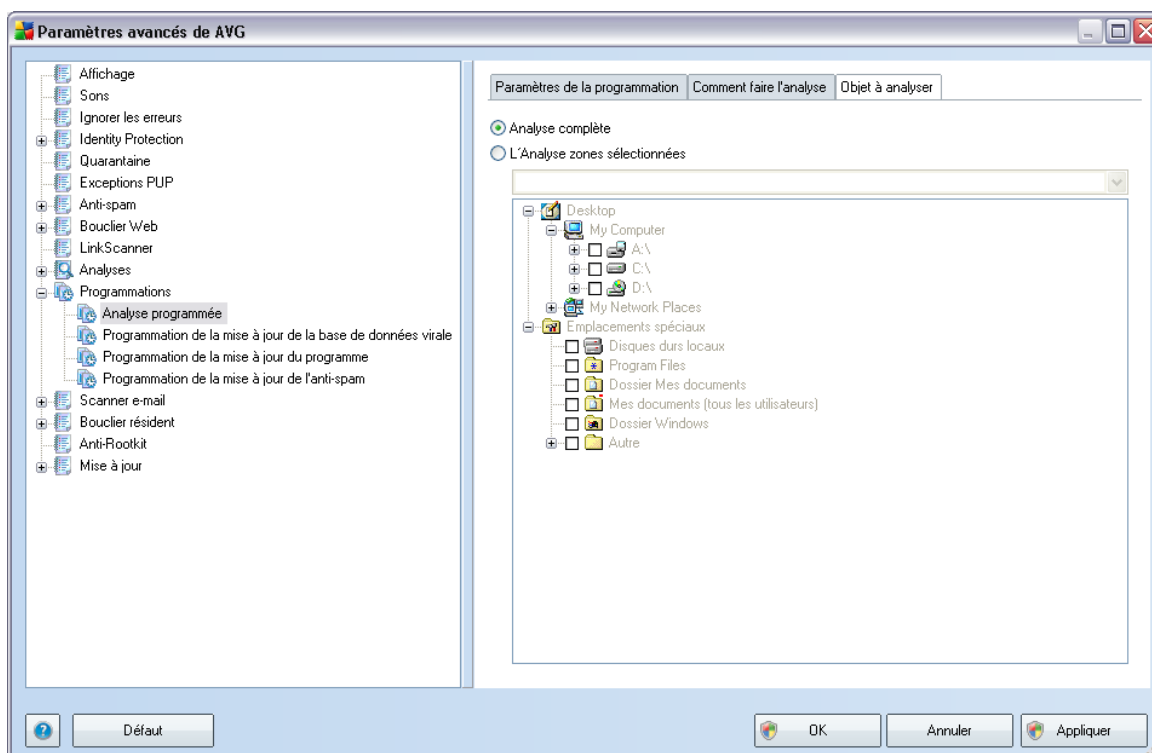
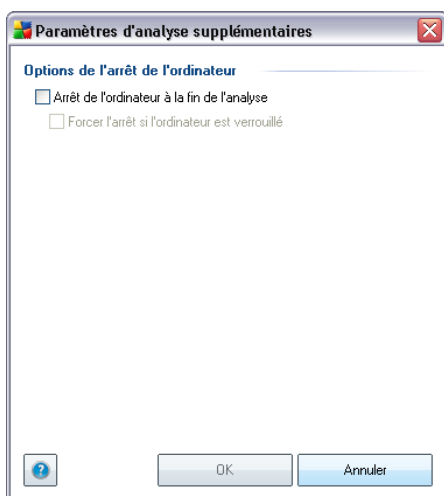
Priorité du processus d'analyse

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

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



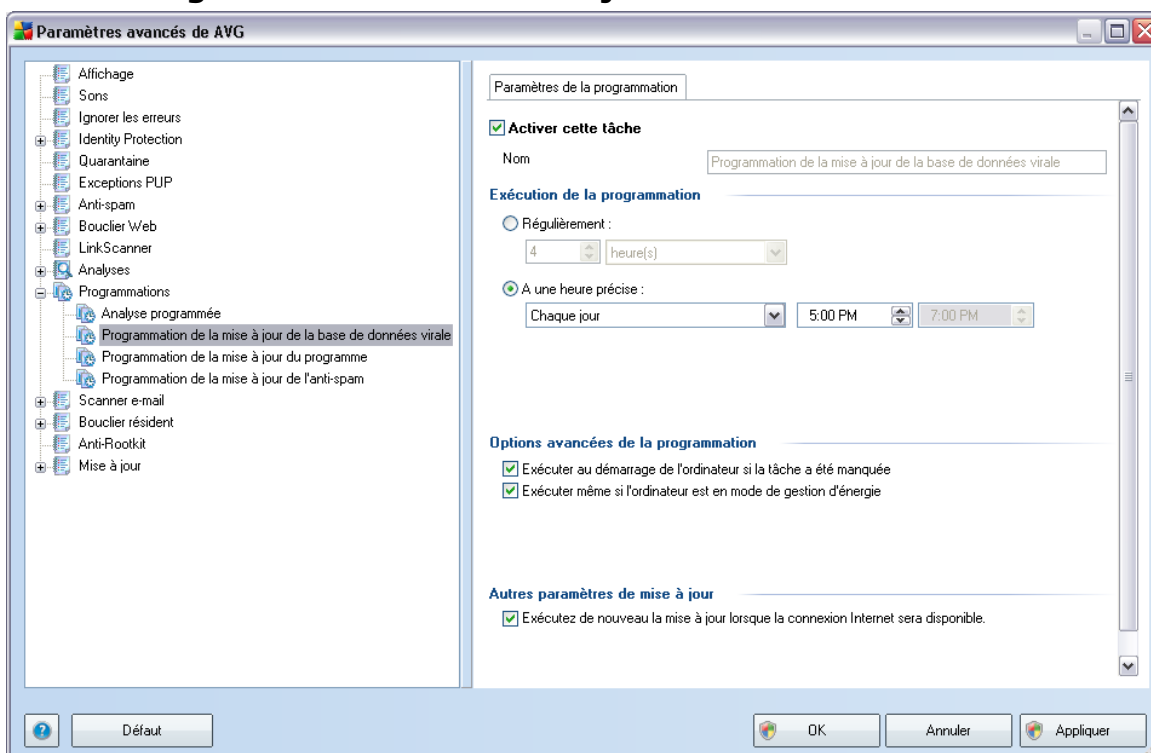
Cliquez sur **Paramètres d'analyse supplémentaires ...** pour ouvrir la boîte de dialogue **Options de l'arrêt de l'ordinateur**, où vous indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Une fois l'option **Arrêt de l'ordinateur à la fin de l'analyse** confirmée,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



Sous l'onglet **Objet à analyser**, indiquez si vous voulez programmer l'[analyse complète](#) ou l'[analyse des zones sélectionnées](#). Si vous optez pour la deuxième solution, la

structure de l'arborescence affichée dans la partie inférieure de la boîte de dialogue devient active et permet de définir les dossiers qui vous intéressent.

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



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

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

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

toujours utiliser des noms courts, descriptifs et appropriés pour distinguer facilement les différentes programmations par la suite.

Exécution de la programmation

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

Options avancées de la programmation

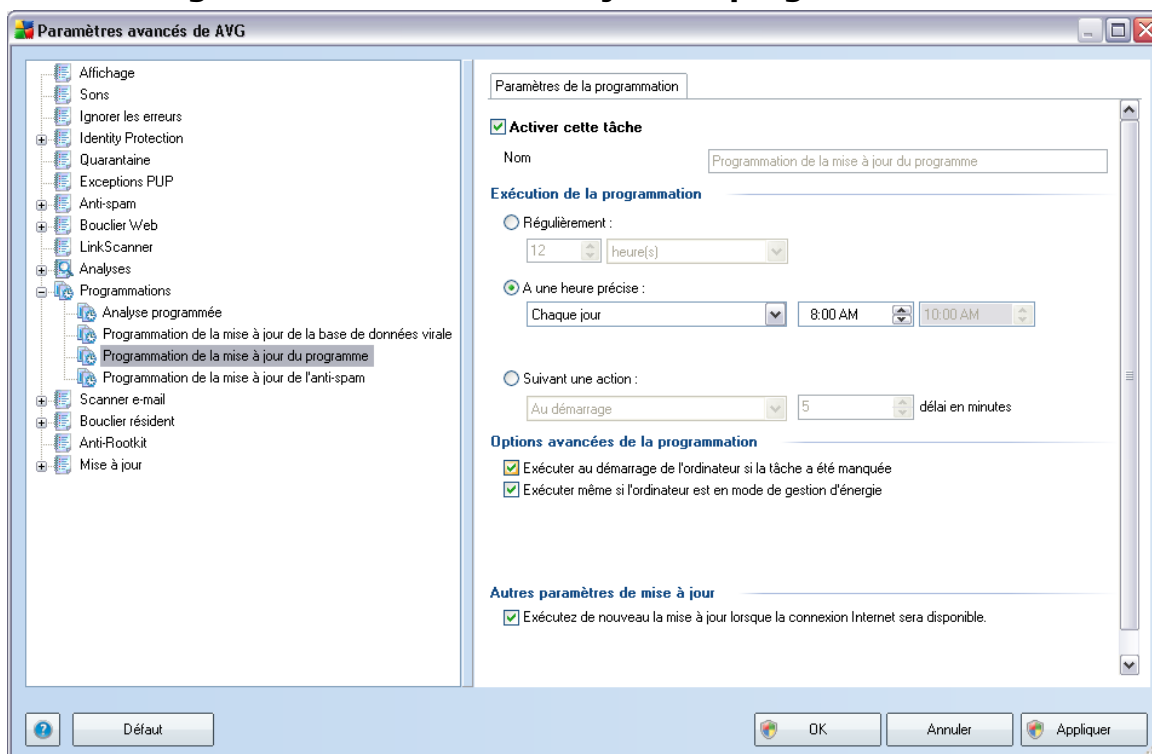
Cette section permet de définir dans quelles conditions la mise à jour de la base de données virale doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

Autres paramètres de mise à jour

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

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

10.7.3. Programmation de la mise à jour du programme



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

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

Exécution de la programmation

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

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

Options avancées de la programmation

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

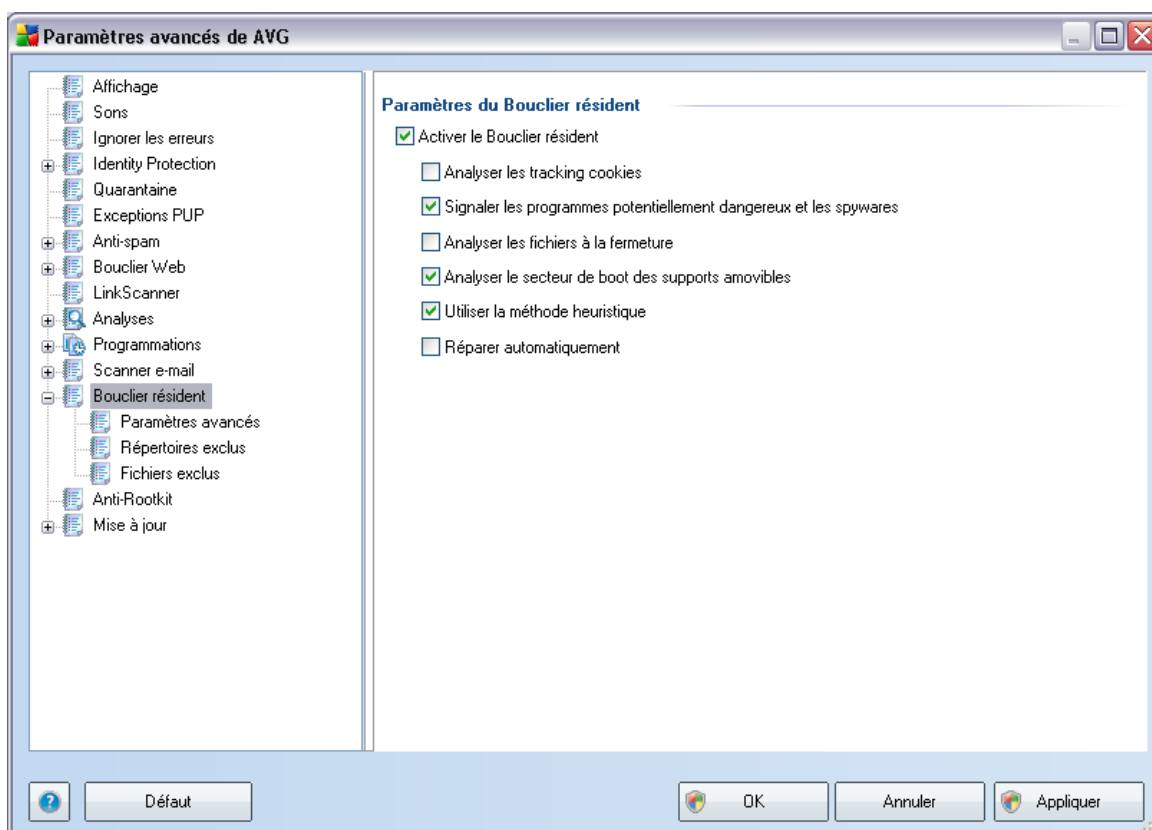
Autres paramètres de mise à jour

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

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

10.8. Bouclier résident

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



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

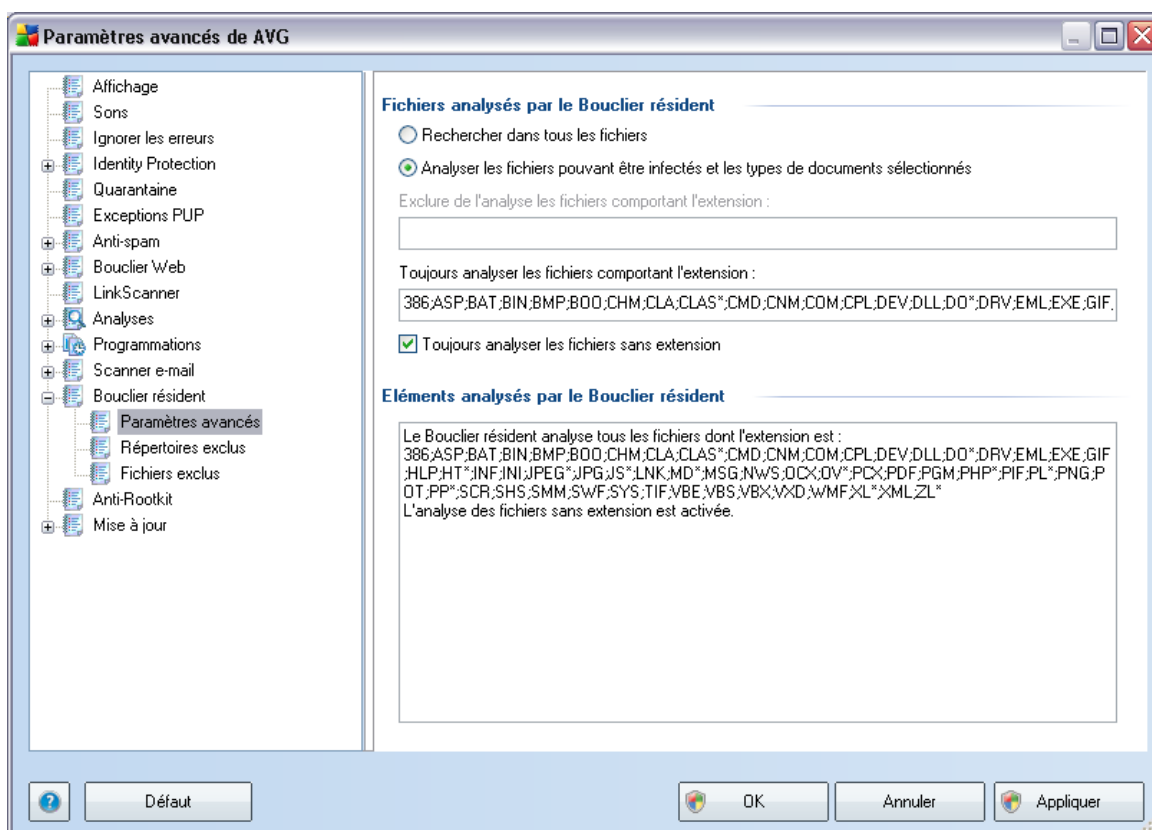
- **Analyser les cookies** - ce paramètre définit les cookies à détecter au cours de l'analyse. (Les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique).
- **Signaler les programmes potentiellement dangereux et les spywares** - (paramètre activé par défaut) analyse des [programmes potentiellement dangereux](#) (applications exécutables se comportant comme des spywares ou

des adwares)

- **Analyser les fichiers à la fermeture** - ce type d'analyse garantit qu'AVG vérifie les objets actifs (par exemple, les applications, les documents...) à leur ouverture et à leur fermeture. Cette fonction contribue à protéger l'ordinateur contre certains types de virus sophistiqués
- **Analyser le secteur d'initialisation (boot) des supports amovibles** - (*option activée par défaut*)
- **Utiliser la méthode heuristique**- (*option activée par défaut*) [l'analyse heuristique](#) est un moyen de détection (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*)
- **Réparer automatiquement** - toute infection détectée sera automatiquement réparée si un traitement est disponible

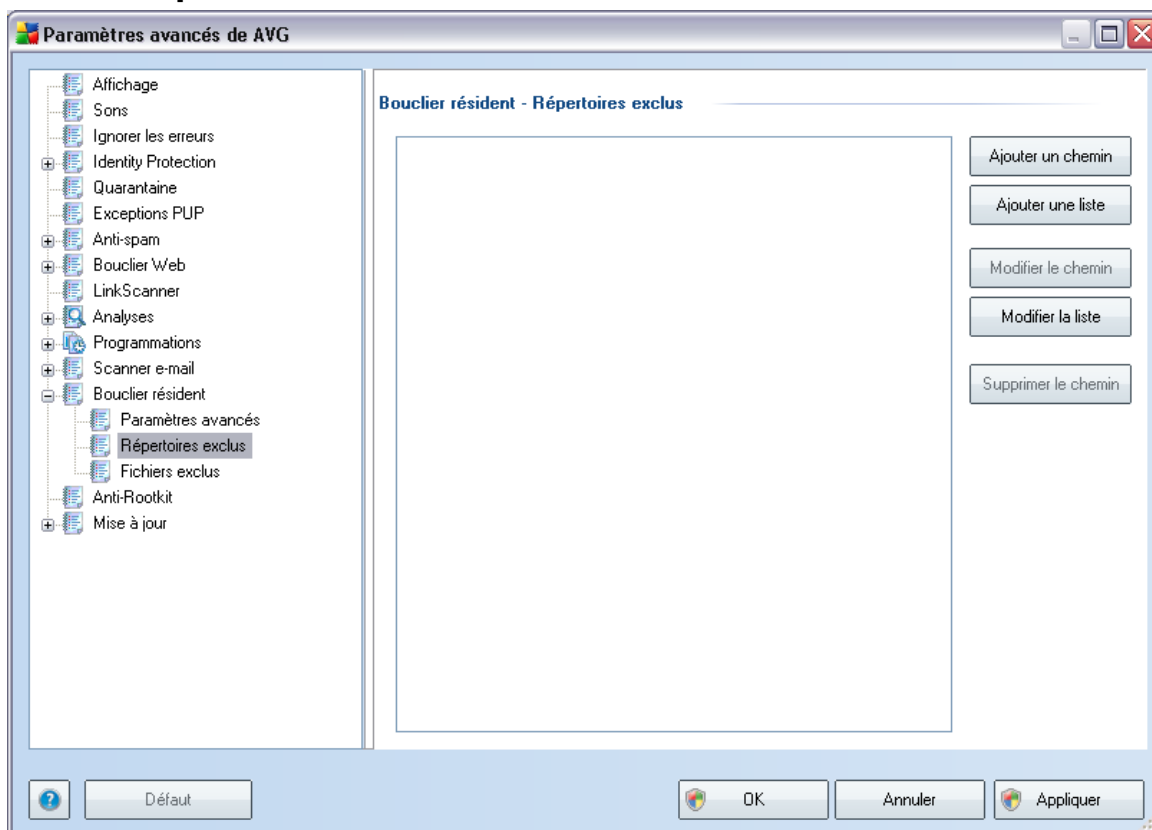
10.8.1. Paramètres avancés

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



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

10.8.2. Répertoires exclus



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

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

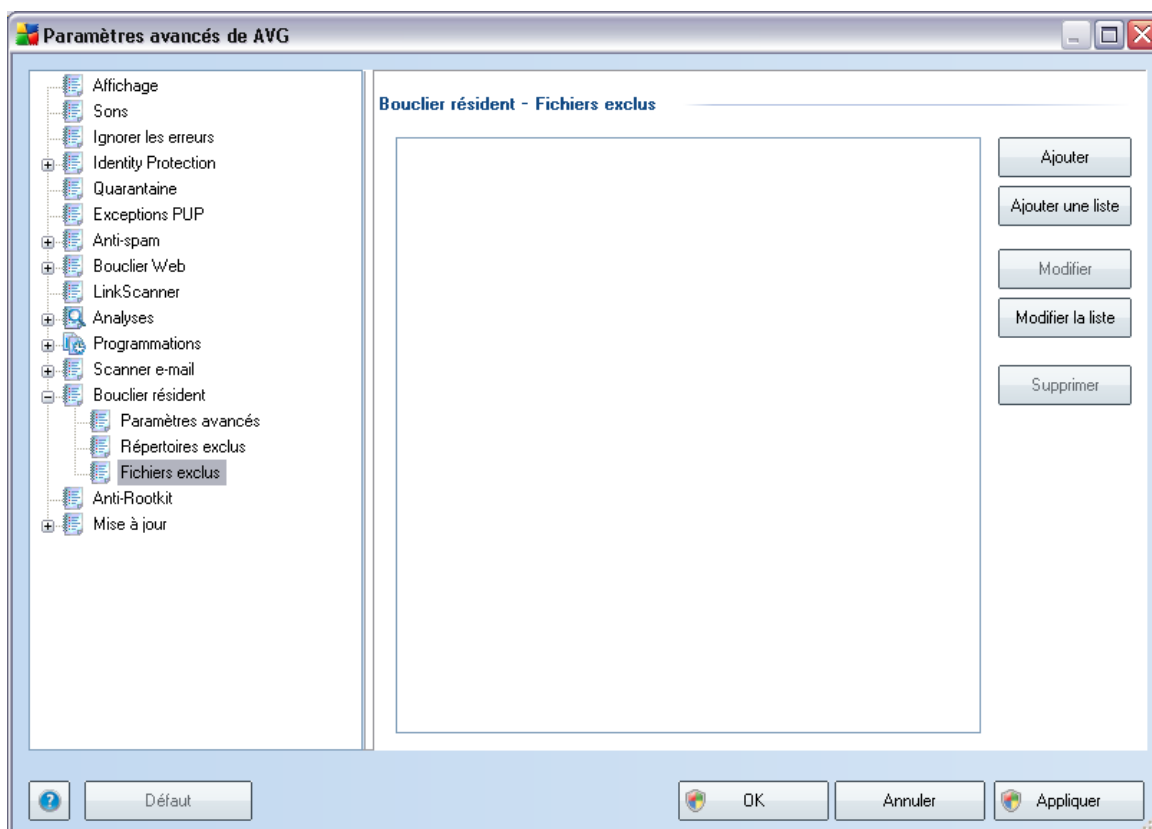
Cette boîte de dialogue présente les boutons de fonction suivantes :

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

dossier sélectionné

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

10.8.3. Fichiers exclus



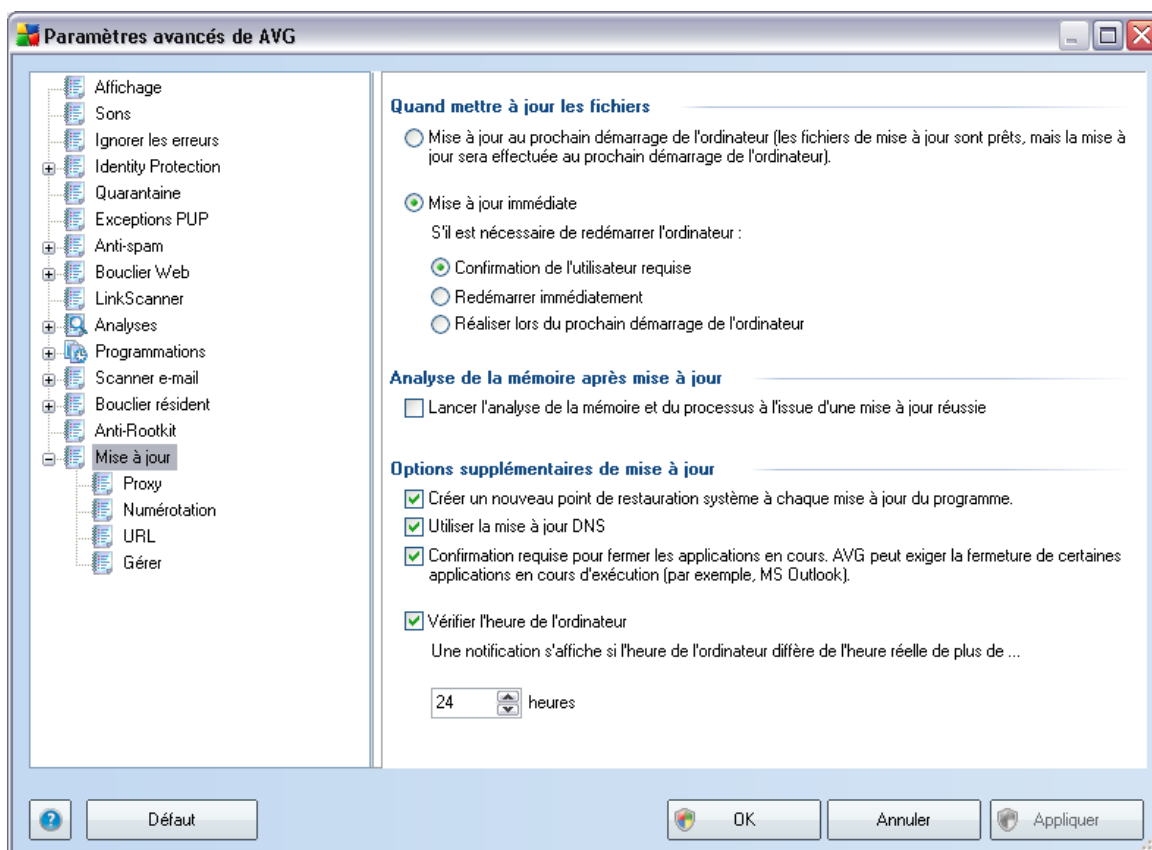
La boîte de dialogue **Bouclier résident - Fichiers exclus** se comporte comme celle précédemment décrite, à savoir **Bouclier résident - Répertoires exclus** mais à la place des dossiers, vous avez maintenant la possibilité de définir des fichiers spécifiques à exclure de l'analyse effectuée par le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

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

Cette boîte de dialogue présente les boutons de fonction suivantes :

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

10.9. Mise à jour



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

Quand mettre à jour les fichiers

Dans cette section, vous avez le choix entre deux options : la [mise à jour](#) peut être programmée pour être lancée au redémarrage de l'ordinateur ou être exécutée immédiatement. Par défaut, l'option de mise à jour immédiate est sélectionnée, car de cette façon AVG offre le niveau de sécurité optimal. Programmer une mise à jour au redémarrage suivant est seulement recommandé si l'ordinateur est régulièrement réamorcé (au moins une fois par jour).

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

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

Analyse de la mémoire après mise à jour

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

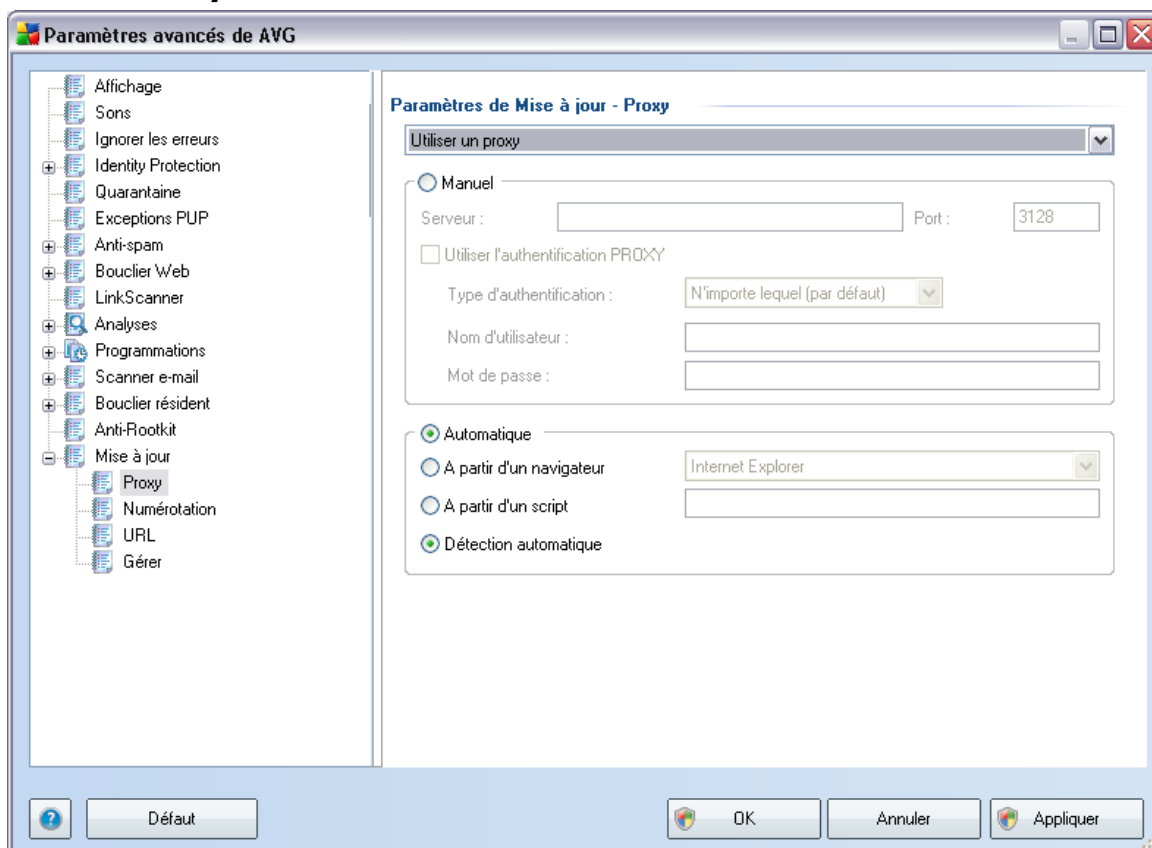
Options supplémentaires de mise à jour

- **Créer un nouveau point de restauration après chaque nouvelle mise à jour du programme** : un point de restauration est créé avant le lancement d'une mise à jour du programme AVG. En cas d'échec de la mise à jour et de blocage de votre système d'exploitation, vous avez alors la possibilité de restaurer le système d'exploitation tel qu'il était configuré à partir de ce point.

Cette option est accessible via Démarrer / Tous les programmes / Accessoires / Outils système / Restauration du système, mais seuls les utilisateurs expérimentés devraient effectuer des changements à ce niveau! Laissez cette case cochée si vous voulez utiliser cette fonctionnalité.

- **Utiliser la mise à jour DNS** : cochez cette case si vous voulez confirmer que vous voulez utiliser la méthode de détection des fichiers de mise à jour qui élimine la quantité de données transférée entre le serveur de mise à jour et le client AVG ;
- **Confirmation requise pour fermer les applications en cours** (*option activée par défaut*) : cette option permet de vous assurer qu'aucune application actuellement en cours d'exécution ne sera fermée sans votre autorisation, si cette opération est requise pour la finalisation du processus de mise à jour ;
- **Vérifier l'heure de l'ordinateur** : cochez cette case si vous voulez être informé lorsque l'heure du système et l'heure correcte diffèrent de plus du nombre d'heures spécifié.

10.9.1. Proxy



Un serveur proxy est un serveur ou un service autonome s'exécutant sur un PC dans le but de garantir une connexion sécurisée à Internet. En fonction des règles de réseau spécifiées, vous pouvez accéder à Internet directement, via le serveur proxy ou en combinant les deux possibilités. Dans la première zone (liste déroulante) de la boîte de dialogue **Paramètres de mise à jour - Proxy**, vous êtes amené à faire un choix parmi les options suivantes :

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

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

manuellement ou automatiquement.

Configuration manuelle

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

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

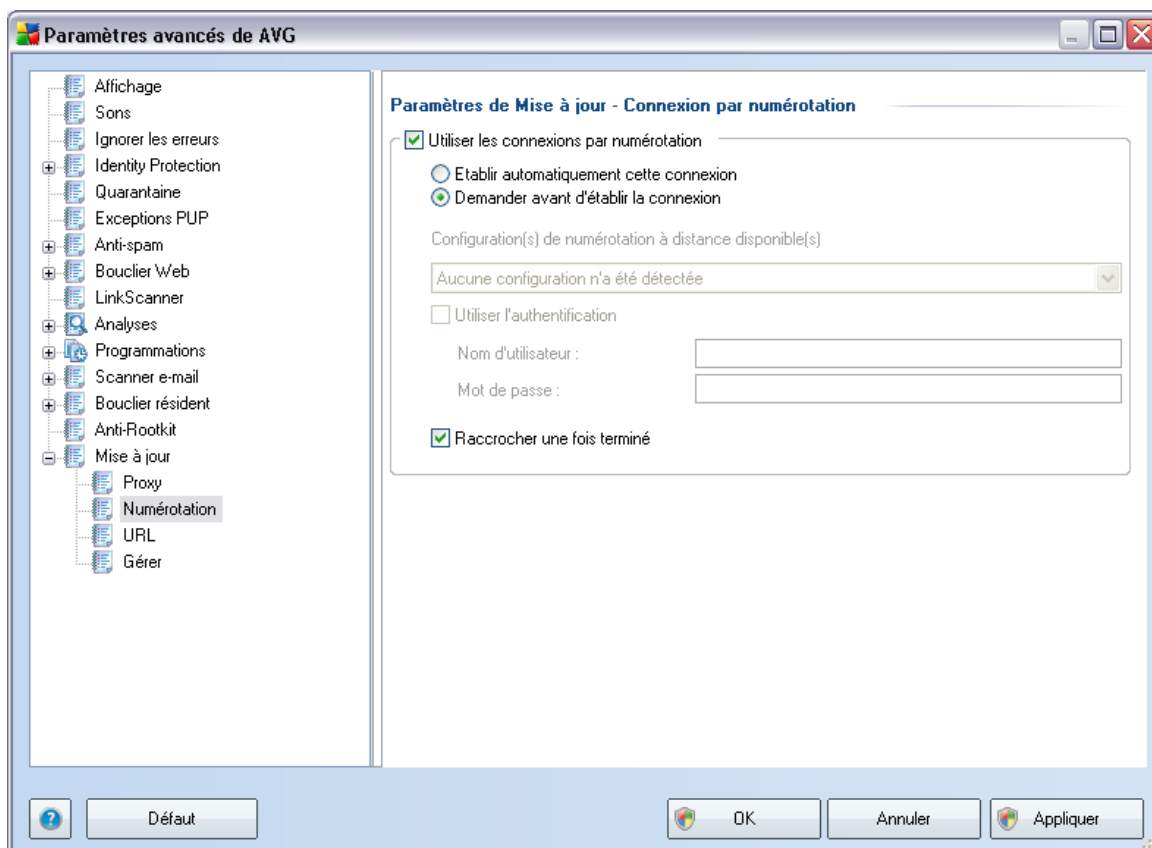
Il est aussi possible de définir des règles spécifiques à chaque utilisateur pour le serveur proxy. Si votre serveur proxy est configuré de cette manière, cochez l'option **Utiliser l'authentification PROXY** pour vous assurer que votre nom d'utilisateur et votre mot de passe sont valides pour établir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

Configuration automatique

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

- **A partir 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

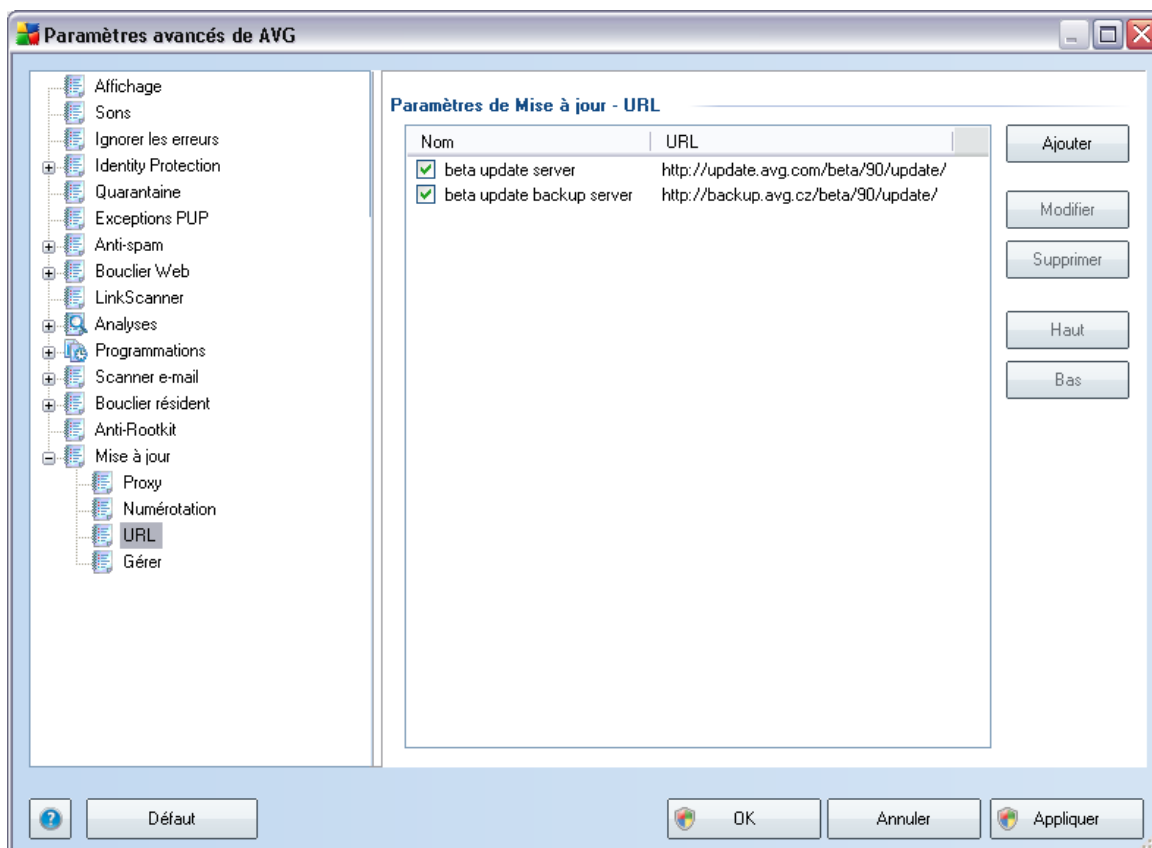
10.9.2. Numérotation



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

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

10.9.3. URL

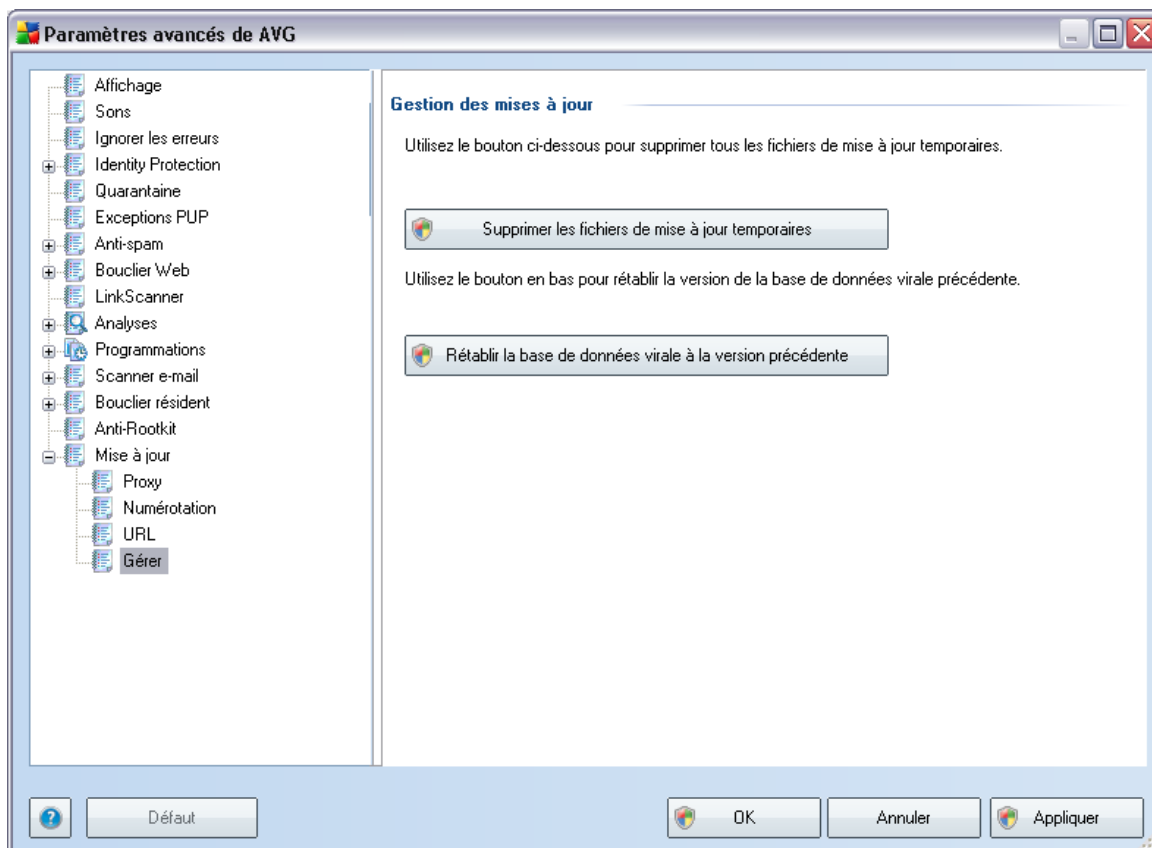


La boîte de dialogue **URL** contient une liste d'adresses Internet à partir desquelles il est possible de télécharger les fichiers de mise à jour. Vous pouvez redéfinir le contenu de cette liste à l'aide des boutons de fonction suivants :

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

10.9.4. Gérer

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



- **Supprimer les fichiers de mise à jour temporaires** - cliquez sur ce bouton pour supprimer tous les fichiers redondants de votre disque dur (*par défaut, ces fichiers sont conservés pendant 30 jours*)
- **Revenir à la version précédente de la base virale** – cliquez sur ce bouton pour supprimer la dernière version de la base virale de votre disque dur et revenir à la version précédente enregistrée (*la nouvelle version de la base de données sera incluse dans la mise à jour suivante*)

11. Analyse AVG

L'analyse constitue une partie fondamentale de la fonctionnalité d'**AVG 9.0 File Server**. Vous avez la possibilité d'exécuter des analyses à la demande ou de [programmer une analyse quotidienne](#) à l'heure qui vous convient le mieux.

11.1. Interface d'analyse



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

- présentation des [analyses prédéfinies](#) - trois types d'analyse (définis par l'éditeur du logiciel) sont prêts à l'emploi sur demande ou par programmation :
 - [Analyse complète](#)
 - [Analyse zones sélectionnées](#)
 - [Analyse anti-rootkit](#)
- [programmation de l'analyse](#) - dans cette section, vous définissez de nouvelles analyses et planifiez d'autres programmations selon vos besoins.

Boutons de commande

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

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

11.2. Analyses prédéfinies

Une des principales fonctions d'**AVG 9.0 File Server** est l'**analyse à la demande**. Ce type d'analyse est prévu pour analyser différentes zones de l'ordinateur en cas de doute concernant la présence éventuelle de virus. Il est vivement recommandé d'effectuer fréquemment de telles analyses même si vous pensez qu'aucun virus ne s'est introduit dans votre système.

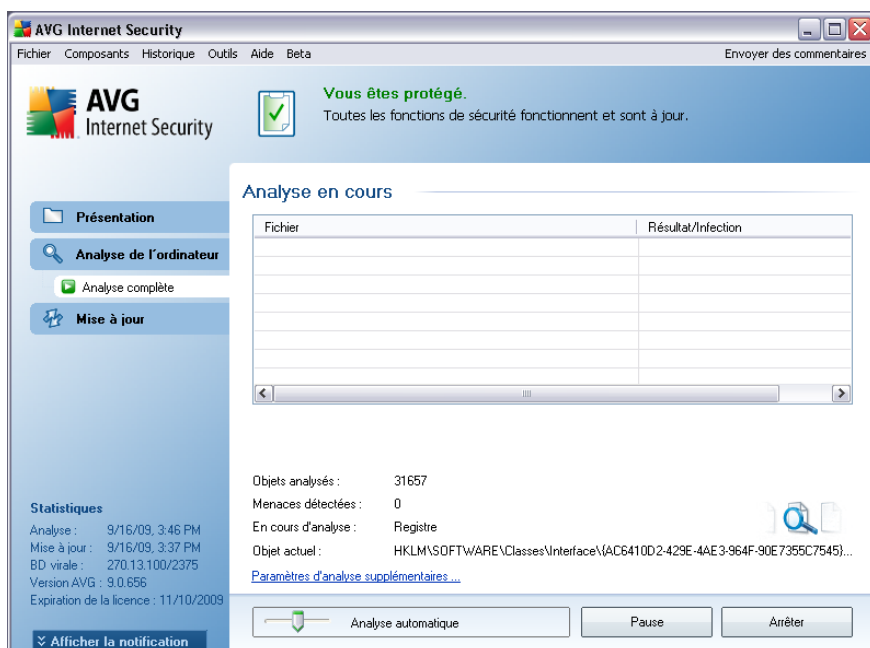
Dans **AVG 9.0 File Server**, vous trouverez les types d'analyse prédéfinies par l'éditeur du logiciel suivantes :

11.2.1. Analyse complète

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

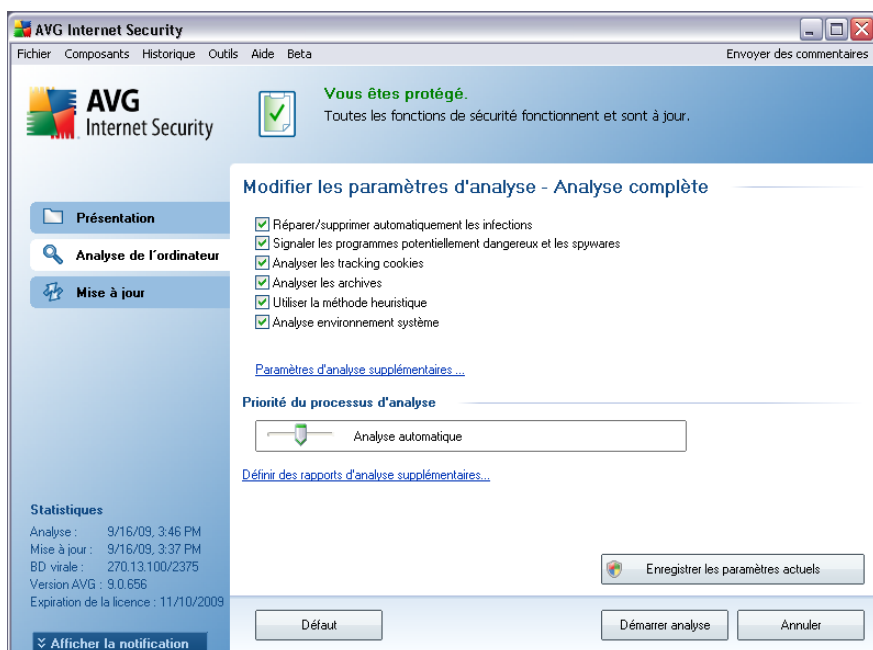
Lancement de l'analyse

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

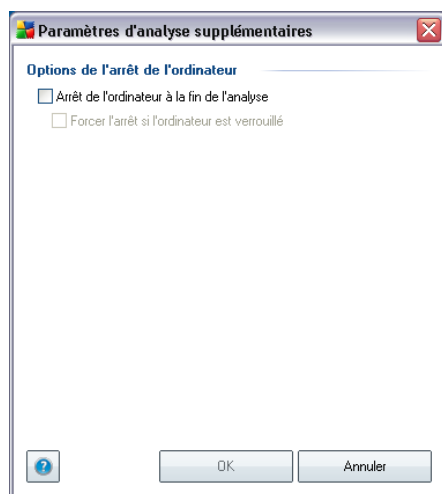


Modification de la configuration de l'analyse

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



- **Paramètres d'analyse** - dans la liste des paramètres d'analyse, vous pouvez activer/désactiver des paramètres spécifiques en fonction de vos besoins. Par défaut, la plupart des paramètres sont activés et seront appliqués automatiquement au cours de l'analyse.
- **Paramètres d'analyse supplémentaires** - ce lien ouvre une nouvelle boîte de dialogue **Paramètres d'analyse supplémentaires** permettant de spécifier les paramètres suivants :



- **Options d'arrêt de l'ordinateur** - indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Une fois l'option **Arrêt de l'ordinateur à la fin de l'analyse** confirmée, l'option **Forcer l'arrêt si l'ordinateur est verrouillé** s'active et vous permet d'arrêter l'ordinateur même s'il est verrouillé.
- **Définir les types de fichiers à analyser** - vous devez également choisir d'analyser :
 - **Tous les types de fichiers** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers (séparées par des virgules) à ne pas analyser ; ou
 - **Types de fichier sélectionnés** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers média (*vidéo, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.
 - Vous pouvez également choisir l'option **Analyser les fichiers sans extension** - cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent

toujours faire l'objet d'une analyse.

- **Priorité du processus d'analyse** - le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, le niveau de priorité attribué est moyen (*Analyse automatique*), qui applique le meilleur compromis entre le processus d'analyse et l'utilisation des ressources système. Vous pouvez aussi choisir le processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse*) ; ou rapide, qui utilise plus de ressources système (*convient notamment lorsque vous quittez temporairement votre poste de travail*).
- **Définir des rapports d'analyse supplémentaires** - ce lien ouvre une nouvelle boîte de dialogue **Rapports d'analyse**, dans laquelle vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :



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

11.2.2. Analyse zones sélectionnées

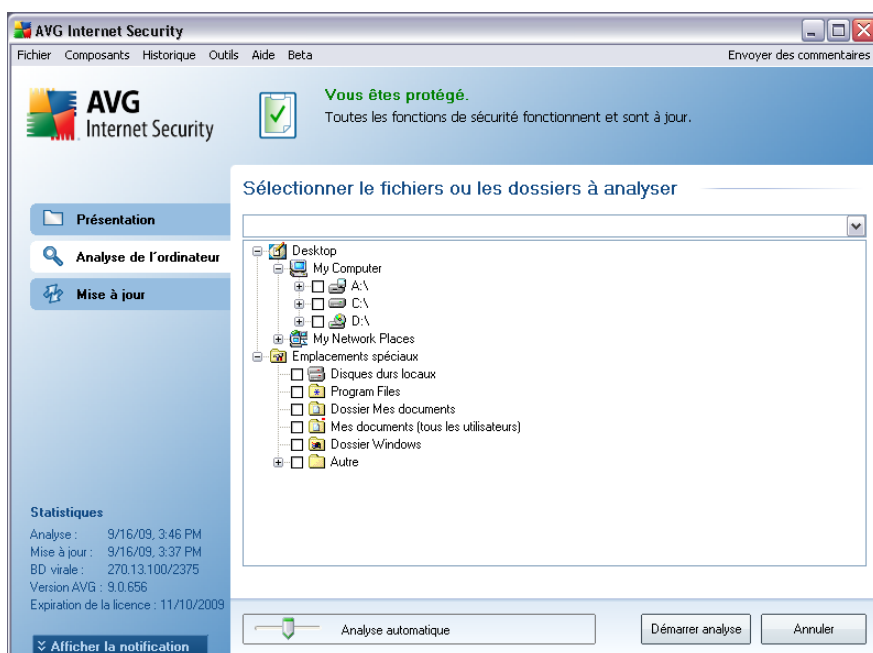
Analyse zones sélectionnées - analyse seulement les zones de l'ordinateur que vous avez sélectionnées en vue d'une analyse (*dossiers, disque durs, disquettes, CD, etc.*). Le déroulement de l'analyse en cas de détection virale, ainsi que la solution appliquée, est le même que pour une analyse complète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

Lancement de l'analyse

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

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

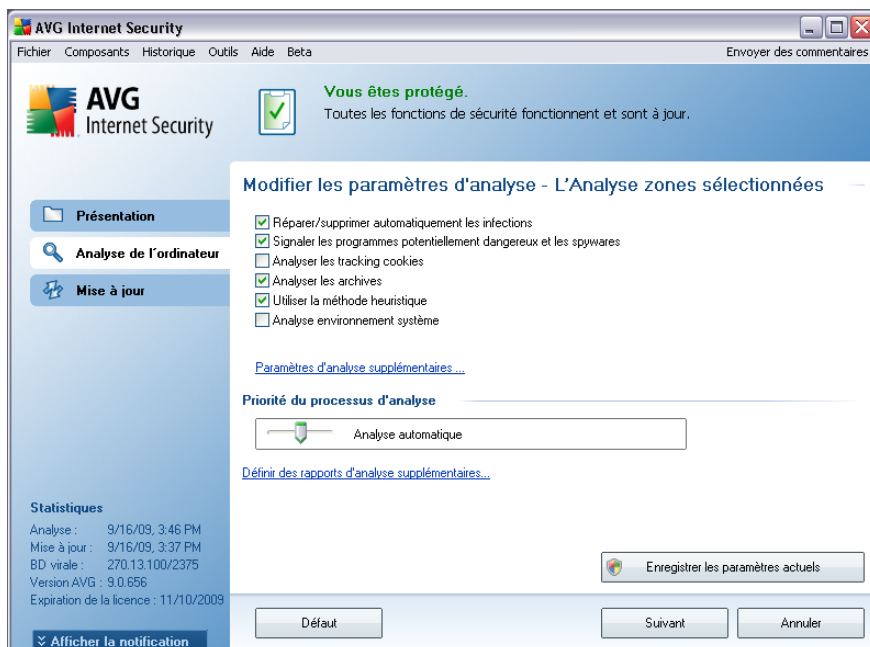
Pour exécuter l'analyse, cliquez sur le bouton **Démarrer l'analyse** ; le processus est fondamentalement identique à celui d'une [analyse complète de l'ordinateur](#).



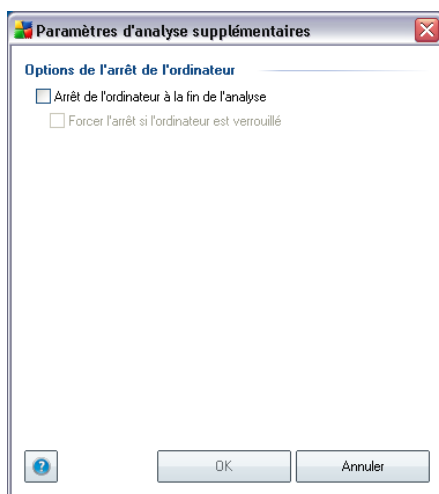
Modification de la configuration de l'analyse

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

nécessité.



- **Paramètres de l'analyse** - dans la liste des paramètres de l'analyse, vous pouvez activer/désactiver des paramètres spécifiques en fonction de vos besoins (*pour une description détaillée de ces paramètres, consultez le chapitre [Paramètres avancés AVG/ Analyses / Analyse zones sélectionnées](#)).*
- **Paramètres d'analyse supplémentaires** - ce lien ouvre une nouvelle boîte de dialogue Paramètres d'analyse supplémentaires permettant de spécifier les paramètres suivants :



- **Options d'arrêt de l'ordinateur** - indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Une fois l'option **Arrêt de l'ordinateur à la fin de l'analyse** confirmée, l'option **Forcer l'arrêt si l'ordinateur est verrouillé** s'active et vous permet d'arrêter l'ordinateur même s'il est verrouillé.
- **Définir les types de fichiers à analyser** - vous devez également choisir d'analyser :
 - **Tous les types de fichiers** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers (séparées par des virgules) à ne pas analyser ; ou
 - **Types de fichier sélectionnés** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers média (*vidéo, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.
 - Vous pouvez également choisir l'option **Analyser les fichiers sans extension** - cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent

toujours faire l'objet d'une analyse.

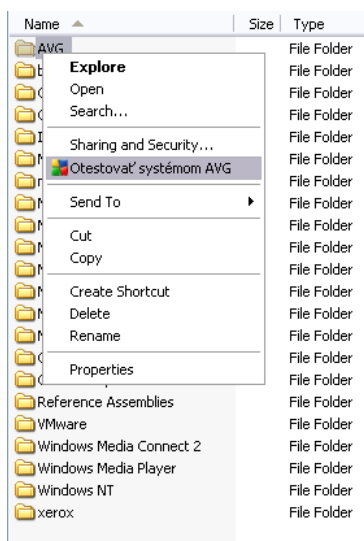
- **Priorité du processus d'analyse** - le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, le niveau de priorité attribué est moyen (*Analyse automatique*), qui applique le meilleur compromis entre le processus d'analyse et l'utilisation des ressources système. Vous pouvez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



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

11.3. Analyse contextuelle

Outre les analyses prédéfinies et exécutées sur l'ensemble de l'ordinateur ou sur des zones sélectionnées, **AVG 9.0 File Server** permet d'analyser rapidement l'objet de votre choix dans l'environnement de l'Explorateur Windows. Si vous désirez ouvrir un fichier inconnu dont le contenu est incertain, vous pouvez le vérifier à la demande. Procédez comme suit :



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

11.4. Analyse depuis la ligne de commande

Dans **AVG 9.0 File Server**, il est possible de lancer l'analyse depuis la ligne de commande. Vous apprécierez cette possibilité sur les serveurs, par exemple, ou lors de la création d'un script de commandes qui doit s'exécuter automatiquement après l'initialisation de l'ordinateur. La plupart des paramètres proposés dans l'interface utilisateur graphique sont disponibles à partir de la ligne de commande.

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

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

Syntaxe de la commande

La syntaxe de la commande est la suivante :

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

Emplacement des fichiers à vérifier

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

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

Analyse CMD lancée depuis l'interface d'analyse

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

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

11.4.1. Paramètres d'analyse CMD

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

- **/SCAN** [Analyse de fichiers ou de dossiers spécifiques](#) /
SCAN=chemin;chemin (ex. : /SCAN=C:\;D:\)

- **/COMP** [Analyse complète](#)
- **/HEUR** Utiliser l'[analyse heuristique](#)
- **/EXCLUDE** Fichiers ou chemin exclus de l'analyse
- **/@** Fichier de commande /nom du fichier/
- **/EXT** Analyser ces extensions /par exemple EXT=EXE,DLL/
- **/NOEXT** Ne pas analyser ces extensions /par exemple NOEXT=JPG/
- **/ARC** Analyser les archives
- **/CLEAN** Nettoyer automatiquement
- **/TRASH** Mettre les fichiers en [Quarantaine](#)
- **/QT** Analyse rapide
- **/MACROW** Signaler les macros
- **/PWDW** Signaler les fichiers protégés par un mot de passe
- **/IGNLOCKED** Ignorer les fichiers verrouillés
- **/REPORT** Reporter dans le fichier /nom du fichier/
- **/REPAPPEND** Inclure dans le fichier de rapport
- **/REPOK** Avertir l'utilisateur des fichiers non infectés
- **/NOBREAK** Ne pas autoriser CTRL-PAUSE pour arrêter
- **/BOOT** Activer la vérification MBR/BOOT
- **/PROC** Analyser les processus actifs
- **/PUP** Signaler les "[programmes potentiellement dangereux](#)"
- **/REG** Analyser la base de registre
- **/COO** Analyser les cookies
- **/?** Affichage de l'aide sur un sujet

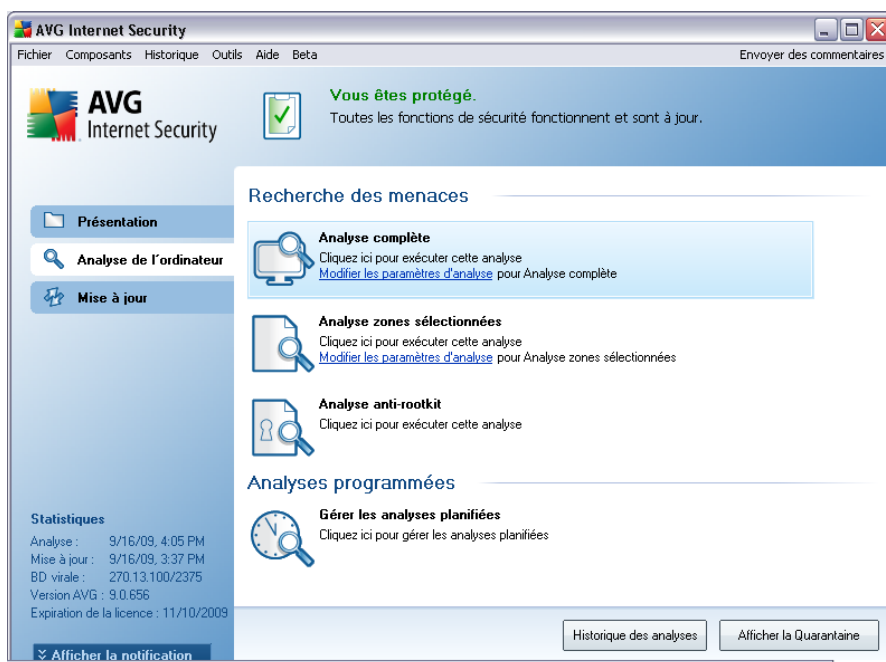
- **/HELP** Affichage de l'aide sur un sujet
- **/PRIORITY** Définir la priorité de l'analyse /Faible, Auto, Elevée (voir [Paramètres avancés / Analyses](#))
- **/SHUTDOWN** Arrêt de l'ordinateur à la fin de l'analyse
- **/FORCESHUTDOWN** Forcer l'arrêt de l'ordinateur à la fin de l'analyse
- **/ADS** Analyser les flux de données NTFS uniquement

11.5. Programmation de l'analyse

Avec **AVG 9.0 File Server**, vous pouvez effectuer une analyse à la demande (par exemple, lorsque vous soupçonnez une infection par un virus dans votre ordinateur) ou selon un programme défini. Il est vivement recommandé d'exécuter des analyses planifiées. Vous serez ainsi assuré que votre ordinateur sera protégé de tout risque d'infection et vous n'aurez plus à vous soucier de la gestion des analyses.

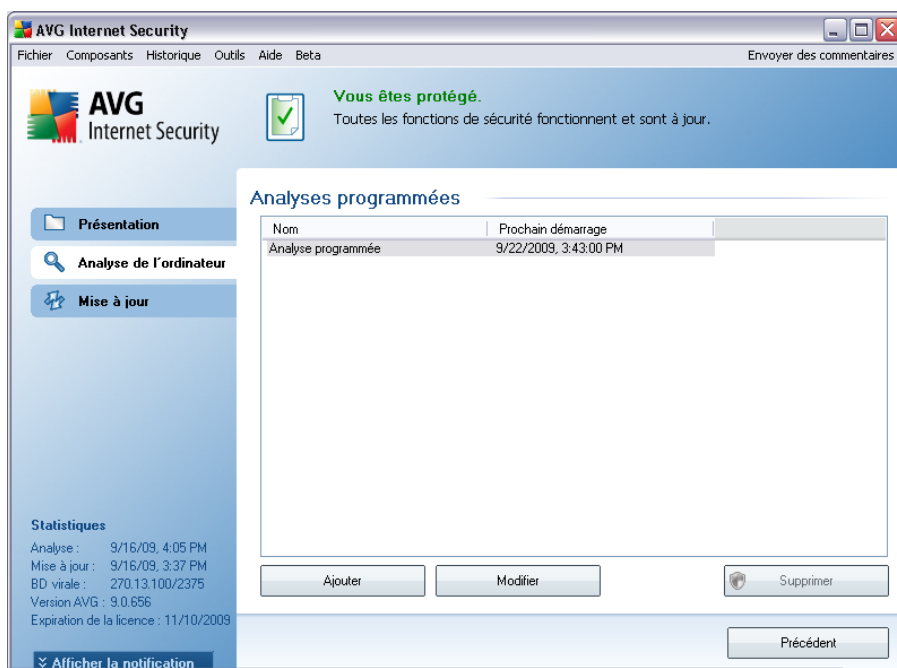
Vous devez effectuer une **analyse complète** régulièrement, au moins une fois par semaine. Si possible, faites aussi une analyse complète l'ordinateur une fois par jour, comme configuré par défaut dans la programmation de l'analyse. Si l'ordinateur est toujours sous tension, vous pouvez programmer l'analyse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

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



Analyses programmées

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

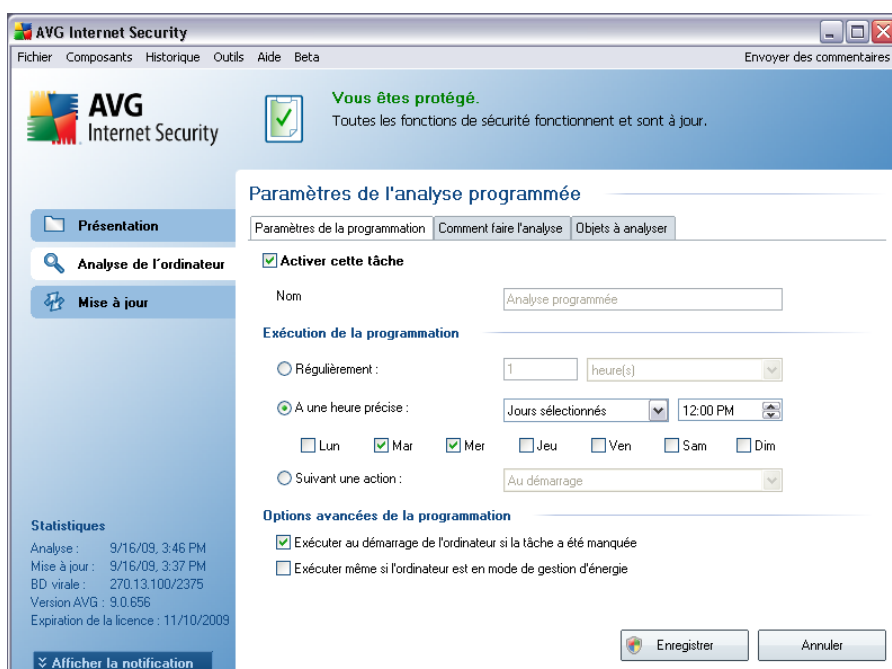


Vous pouvez modifier / ajouter des analyses à l'aide des boutons de commande suivants :

- **Ajouter** - le bouton ouvre la boîte de dialogue **Paramètres de l'analyse programmée**, onglet **Paramètres de la programmation**. Dans cette boîte de dialogue, définissez les paramètres de la nouvelle analyse.
- **Modifier** - ce bouton n'est actif que si vous avez déjà sélectionné une analyse existante dans la liste des analyses programmées. Dans ce cas, le bouton est accessible ; il suffit de cliquer dessus pour accéder à la boîte de dialogue **Paramètres de l'analyse programmée**, onglet **Paramètres de la programmation**. Les paramètres de l'analyse sélectionnée sont pré-renseignés et peuvent être modifiés.
- **Supprimer** - ce bouton est actif si vous avez déjà sélectionné une analyse existante dans la liste des analyses programmées. Cette analyse peut ensuite être supprimée de la liste en cliquant sur ce bouton. Notez néanmoins que vous ne pouvez supprimer que vos propres analyses. Les analyses de type **Programmation de l'analyse complète de l'ordinateur** prédéfinies par défaut ne peuvent jamais être supprimées.
- **Précédent** - permet de revenir à l'[interface d'analyse d'AVG](#)

11.5.1. Paramètres de la programmation

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



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

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

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

l'ordinateur ou une sélection de fichiers ou de dossiers. Notez que les analyses personnalisées sont toujours basées sur l'[Analyse zones sélectionnés](#).

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

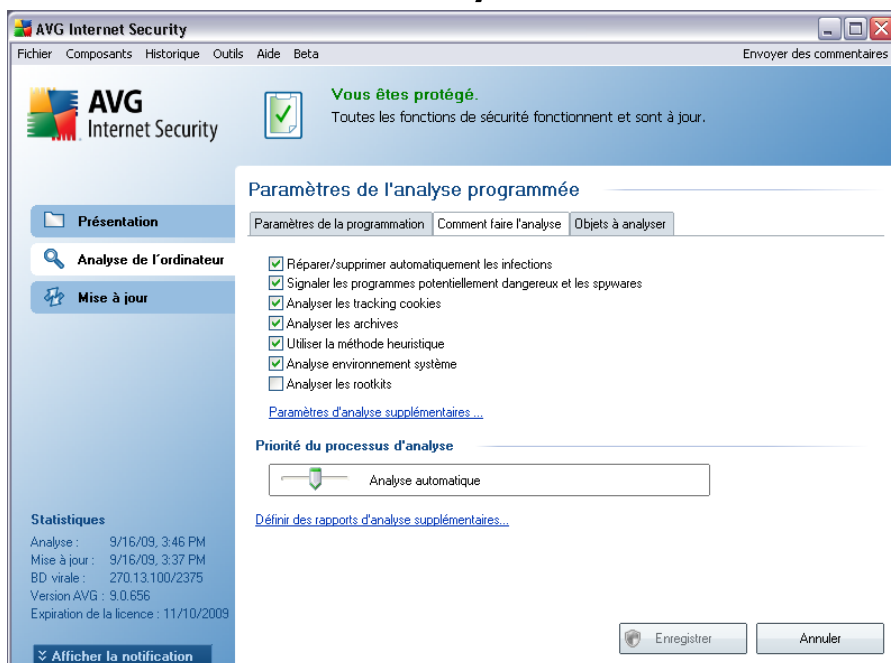
- **Exécution de la programmation** - spécifiez l'intervalle entre chaque exécution de la nouvelle analyse. La périodicité peut être définie à l'aide d'une répétition lancée à l'issue d'un délai déterminé (**Régulièrement**), à une date et à une heure précises (**A une heure précise**) ou encore suivant un événement auquel sera associé le lancement de la mise à jour (**Suivant une action**).
- **Options avancées de la programmation** - cette section permet de définir dans quelles conditions l'analyse doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

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

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

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

11.5.2. Comment faire l'analyse



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

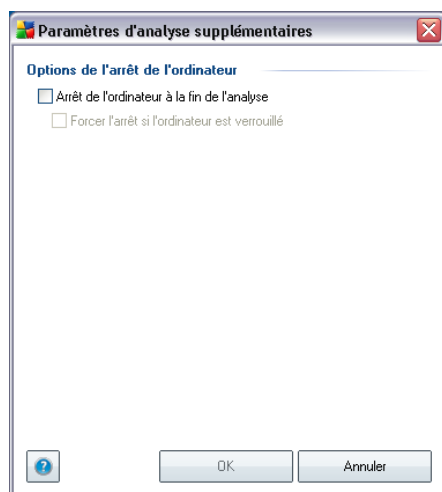
- **Réparer/supprimer automatiquement les infections** - (option activée par défaut) : lorsqu'un virus est détecté au cours de l'analyse, il sera réparé automatiquement si une solution est disponible. Si la désinfection automatique du fichier n'est pas possible (ou si cette option est désactivée), un message de détection de virus s'affiche. Il vous appartient alors de déterminer le traitement à appliquer à l'infection. L'action recommandée consiste à confiner le fichier infecté en **quarantaine**.
- **Signaler les programmes potentiellement dangereux et les spywares** - (option activée par défaut) : ce paramètre contrôle la fonctionnalité **Anti-Virus** qui **détecte les programmes potentiellement dangereux** (fichiers exécutables fonctionnant comme des spywares ou des adwares) afin de les bloquer ou de les supprimer.
- **Analyser les tracking cookies** - (option activée par défaut) : ce paramètre du composant **Anti-Spyware** définit les cookies qui pourront être détectés au

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

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

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

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



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

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

- **Définir les types de fichiers à analyser** - vous devez également choisir d'analyser :
 - **Tous les types de fichiers** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers (séparées par des virgules) à ne pas analyser ; ou
 - **Types de fichier sélectionnés** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers média (*vidéo, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.
 - Vous pouvez également choisir l'option **Analyser les fichiers sans extension** - cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.
- **Priorité du processus d'analyse** - le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, le niveau de priorité attribué est moyen (*Analyse automatique*), qui applique le meilleur compromis entre le processus d'analyse et l'utilisation des ressources système. Vous pouvez aussi choisir le processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse*) ; ou rapide, qui utilise plus de ressources système (*convient notamment lorsque vous quittez temporairement votre poste de travail*).
- **Définir des rapports d'analyse supplémentaires** - ce lien ouvre une nouvelle boîte de dialogue **Rapports d'analyse**, dans laquelle vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :



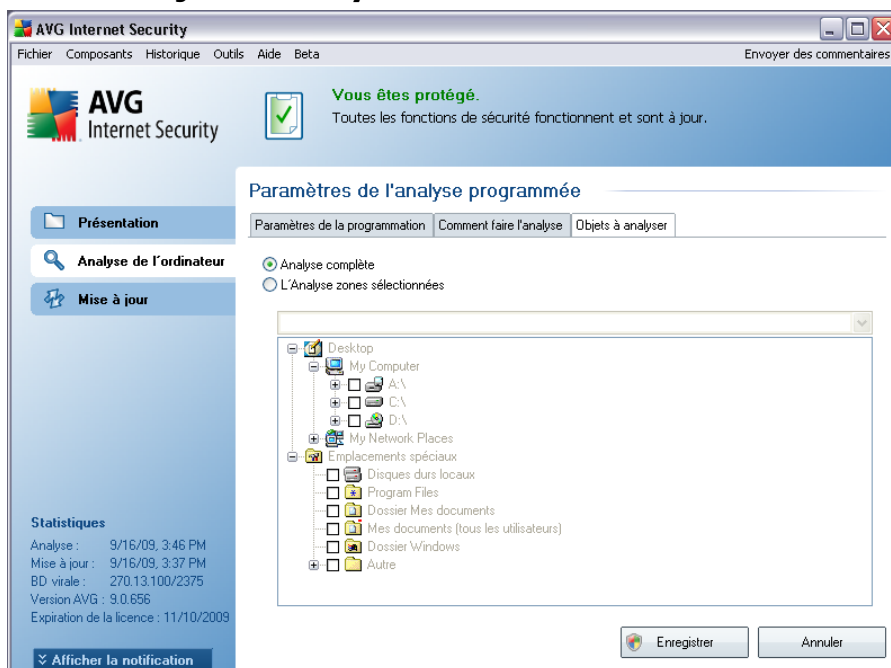
Remarque : par défaut, l'analyse est configurée pour bénéficier de performances optimales. Sauf raison valable, il est fortement conseillé de conserver la configuration telle qu'elle est prédéfinie. Seuls les utilisateurs expérimentés peuvent modifier la configuration. Pour accéder à d'autres options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

Boutons de commande

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

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

11.5.3. Objets à analyser



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

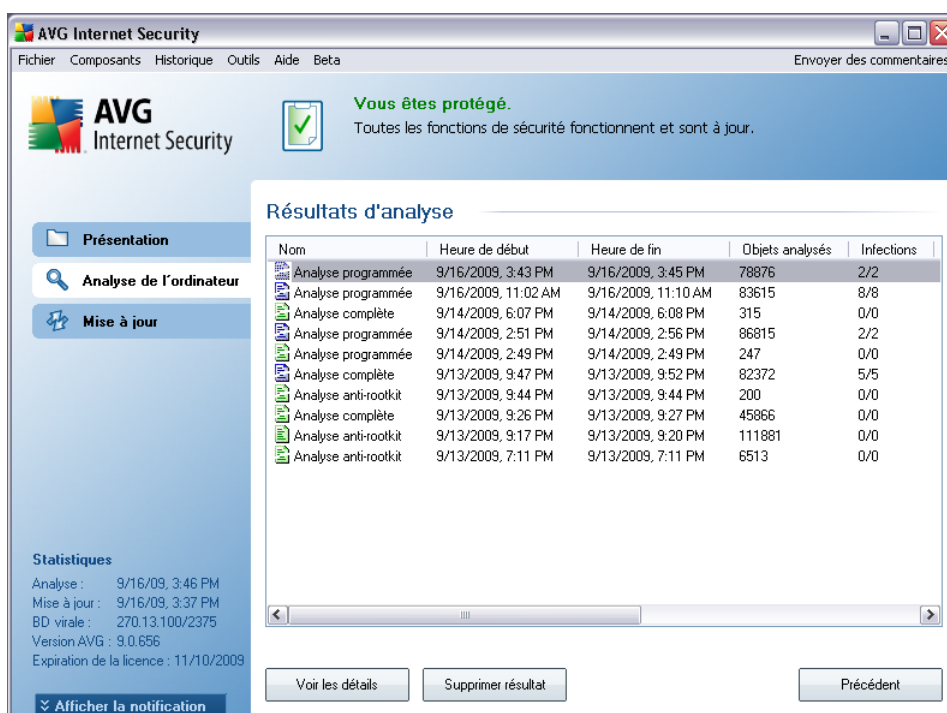
Boutons de commande de la boîte de dialogue Paramètres de l'analyse programmée

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

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

[défaut de l'interface d'analyse AVG.](#)

11.6. Résultats d'analyse



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

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

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

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

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

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

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

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

Boutons de commande

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

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

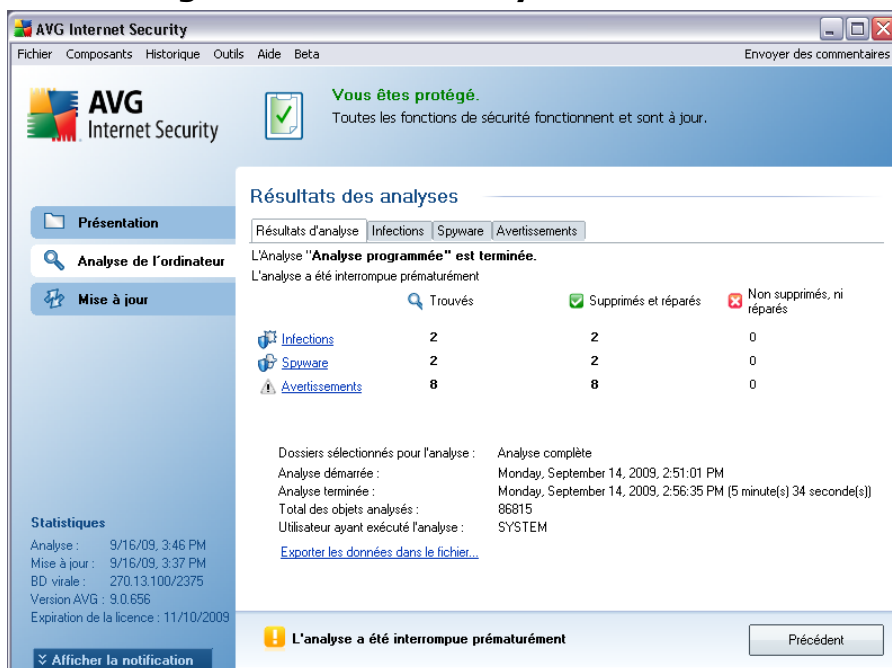
11.7. Détails des résultats d'analyse

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

La boîte de dialogue est subdivisée en plusieurs onglets :

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

11.7.1. Onglet Résultats d'analyse



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

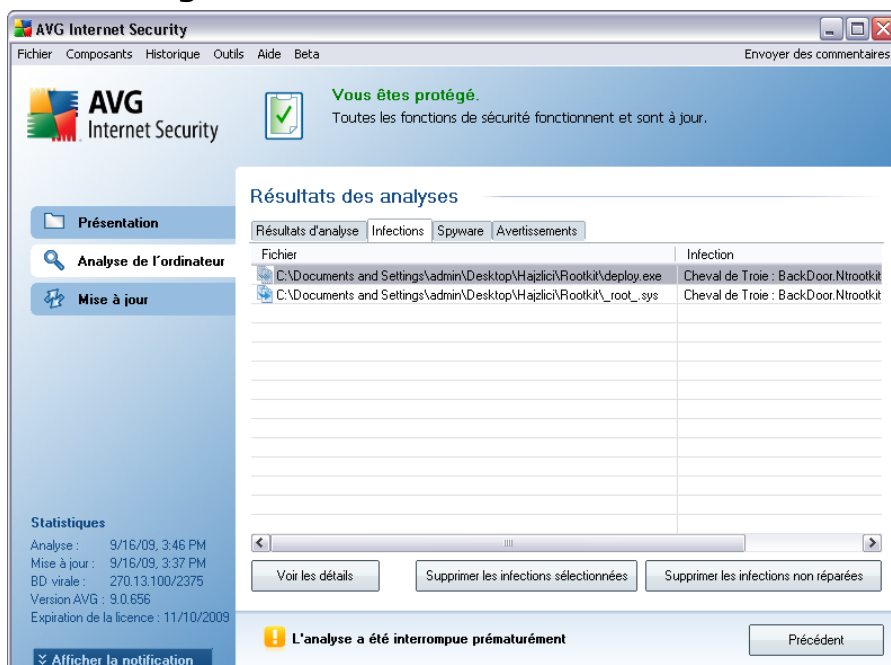
- les [infections](#) / [spywares détectés](#)
- les [infections](#) / [spywares supprimés](#)
- le nombre d'[infections](#) / [de spywares](#) qui n'ont pu être supprimés ou réparés

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

Boutons de commande

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

11.7.2. Onglet Infections



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

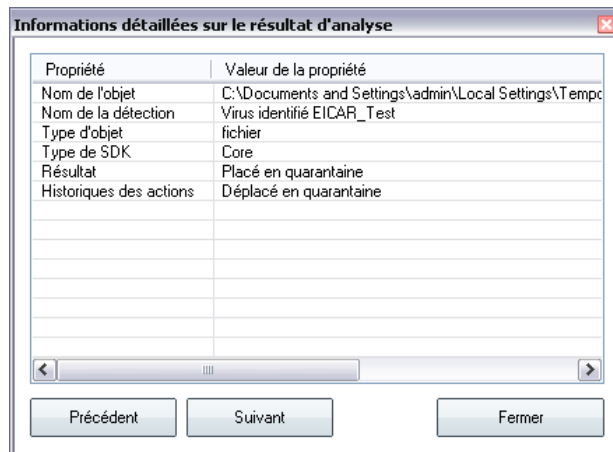
- **Fichier** - chemin complet vers l'emplacement d'origine de l'objet infecté
- **Infections** - nom du [virus](#) détecté (*pour plus de détails sur un virus particulier, consultez l'[Encyclopédie des virus](#) en ligne*)
- **Résultat** - indique l'état actuel de l'objet infecté détecté :
 - **Infecté**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

- **Ajouté aux exceptions PUP** - l'objet détecté est considéré comme une exception et est inclus dans la liste des exceptions PUP (*liste configurée dans la boîte de dialogue **Exceptions PUP** des paramètres avancés*)
- **Fichier verrouillé** - non vérifié - l'objet considéré est verrouillé, AVG ne peut donc pas l'analyser
- **Objet potentiellement dangereux** - l'objet est considéré comme potentiellement dangereux, mais n'est pas infecté (*il contient par exemple des macros*) ; cette information est fournie à titre d'avertissement uniquement
- **Un redémarrage de l'ordinateur est nécessaire pour terminer l'opération** - l'objet infecté ne peut pas être supprimé ; pour ce faire, il faut redémarrer l'ordinateur

Boutons de commande

Cette boîte de dialogue compte trois boutons de commande :

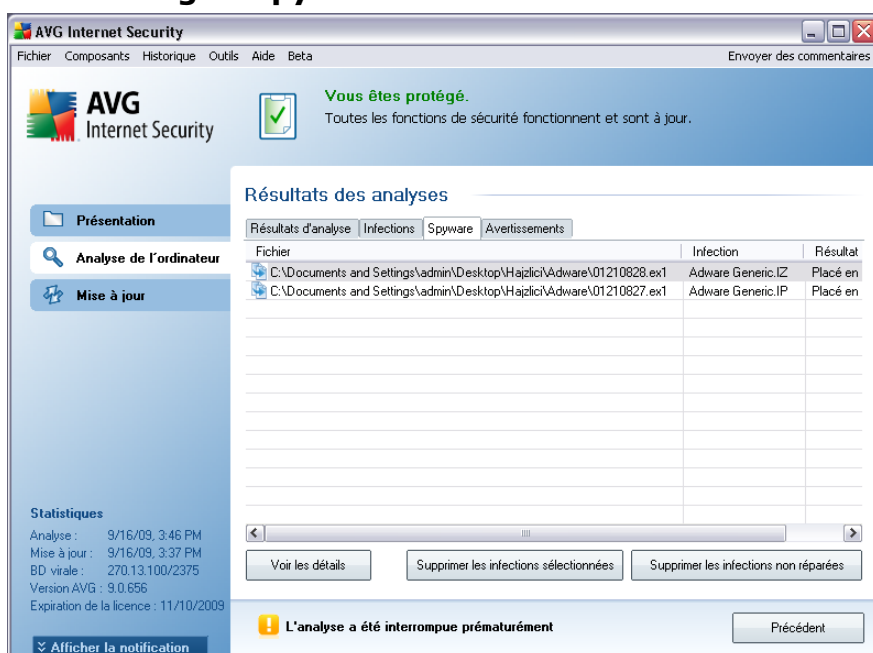
- **Voir les détails** - le bouton ouvre la boîte de dialogue, **Informations détaillées sur le résultat d'analyse** :



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

- **Supprimer les infections sélectionnées** - servez-vous de ce bouton pour mettre les objets trouvés en [quarantaine](#)
- **Supprimer toutes les infections non réparées** - ce bouton supprime tous les objets trouvés qui ne peuvent être désinfectés, ni placés en [quarantaine](#)
- **Fermer résultats** - met fin aux informations détaillées et renvoie la boîte de dialogue [Résultats des analyses](#)

11.7.3. Onglet Spywares



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

- **Fichier** - chemin complet vers l'emplacement d'origine de l'objet infecté
- **Infections** - nom du [spyware](#) détecté (*pour plus de détails sur un virus particulier, consultez l'[Encyclopédie des virus](#) en ligne*)
- **Résultat** - indique l'état actuel de l'objet infecté détecté :
 - **Infecté** - l'objet infecté détecté a été laissé à son emplacement d'origine (si, par exemple, vous avez [désactivé l'option de réparation automatique](#))

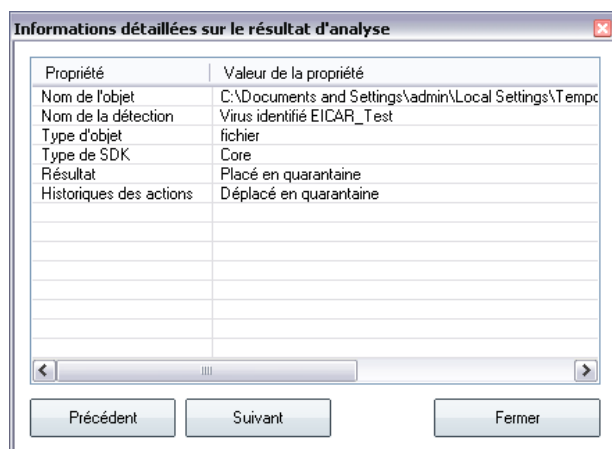
pour une analyse spécifique)

- **Réparé** - l'objet infecté détecté a été réparé et conservé à son emplacement d'origine
- **Placé en quarantaine** - l'objet infecté a été déplacé en [Quarantaine](#)
- **Supprimé** - l'objet infecté a été supprimé
- **Ajouté aux exceptions PUP** - l'objet détecté est considéré comme une exception et est inclus dans la liste des exceptions PUP (*liste configurée dans la boîte de dialogue [Exceptions PUP](#) des paramètres avancés*)
- **Fichier verrouillé - non vérifié** - l'objet considéré est verrouillé, AVG ne peut donc pas l'analyser
- **Objet potentiellement dangereux** - l'objet est considéré comme potentiellement dangereux, mais n'est pas infecté (il contient par exemple des macros) ; cette information est fournie à titre d'avertissement uniquement
- **Un redémarrage de l'ordinateur est nécessaire pour terminer l'opération** - l'objet infecté ne peut pas être supprimé ; pour ce faire, il faut redémarrer l'ordinateur

Boutons de commande

Cette boîte de dialogue compte trois boutons de commande :

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



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

- **Supprimer les infections sélectionnées** - servez-vous de ce bouton pour mettre les objets trouvés en **quarantaine**
- **Supprimer toutes les infections non réparées** - ce bouton supprime tous les objets trouvés qui ne peuvent être désinfectés, ni placés en **quarantaine**
- **Fermer résultats** - met fin aux informations détaillées et renvoie la boîte de dialogue **Résultats des analyses**

11.7.4. Onglet Avertissements

L'onglet **Avertissements** affiche des informations sur les objets "suspects" (*généralement des fichiers*) trouvés au cours de l'analyse. Lorsqu'ils sont détectés par le **Bouclier résident**, l'accès à ces fichiers est bloqué. Voici des exemples types de ce genre d'objets : fichiers masqués, cookies, clés de registre suspectes, documents protégés par un mot de passe, archives, etc. De tels fichiers ne présentent pas de menace directe pour l'ordinateur ou sa sécurité. Les informations relatives à ces fichiers sont généralement utiles lorsque la présence d'adwares ou de spywares est décelée dans votre ordinateur. Si l'analyse AVG ne détecte que des avertissements, aucune action n'est nécessaire.

Cette rubrique décrit brièvement les exemples les plus courants de tels objets :

- **Fichiers masqués** - Les fichiers masqués sont, par défaut, non visibles et certains virus ou autres menaces peuvent empêcher leur détection en stockant

leurs fichiers avec cet attribut. Si AVG signale un fichier masqué que vous soupçonnez d'être dangereux, vous pouvez le confiner en [Quarantaine](#).

- **Cookies** - Les cookies sont des fichiers texte bruts utilisés par les sites Web pour stocker des informations propres à l'utilisateur. Elles permettent ultérieurement de charger un contenu personnalisé d'un site Web, de saisir automatiquement le nom d'utilisateur, etc.
- **Clés de registre suspectes** - Certains programmes malveillants stockent leurs informations dans la base de registre de Windows. De cette manière, elles sont chargées au démarrage ou peuvent s'immiscer dans le système d'exploitation.

11.7.5. Onglet Informations

L'onglet **Informations** contient des renseignements sur des "objets trouvés" qui ne peuvent pas être classés dans les catégories infections, spywares, etc. Il est impossible de les désigner comme positivement dangereux, mais ils réclament malgré tout votre attention. L'analyse AVG permet de détecter des fichiers qui ne sont peut-être pas infectés, mais malicieux. Ces fichiers sont signalés par le biais d'un [avertissement](#) ou d'une **information**.

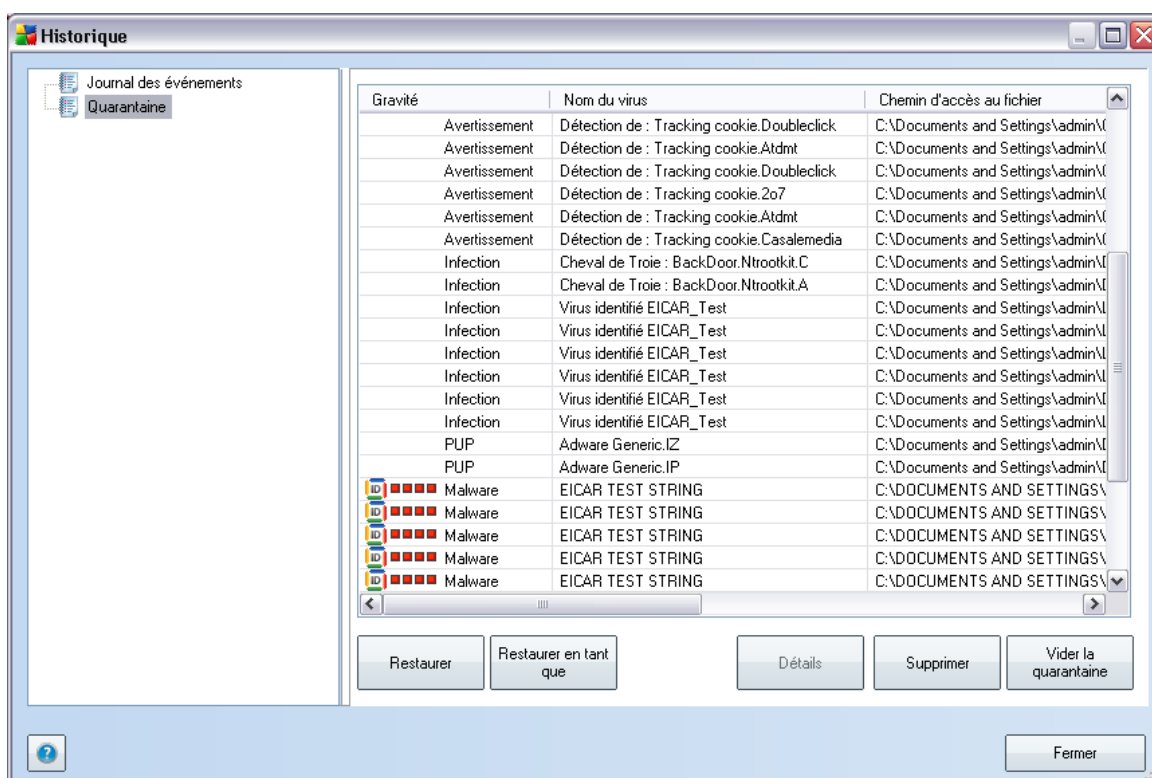
Les raisons suivantes peuvent expliquer la gravité des **informations** :

- **Mode de compression** - Le fichier a été compressé avec l'un des systèmes de compression les moins connus, peut-être dans le but d'en empêcher l'analyse par AVG. Cependant, il n'est pas dit qu'un tel résultat indique que ce fichier contienne un virus.
- **Mode de compression récursif** - Semblable au précédent, mais moins fréquent parmi les logiciels les plus connus. Ces fichiers sont malicieux et leur suppression ou envoi à AVG pour analyse doit être envisagé.
- **Archive ou document protégé par mot de passe** - Les fichiers protégés par mot de passe ne peuvent pas être analysés par AVG (ou par d'autres programmes anti-malwares).
- **Document contenant des macros** - Le document signalé contient des macros potentiellement dangereuses.
- **Extension cachée** - Les fichiers munis d'une extension cachée peuvent apparaître comme des images alors qu'en réalité ce sont des fichiers

exécutables (*exemple : image.jpg.exe*). Par défaut, la deuxième extension n'est pas visible sur Windows et AVG signale ce genre de fichiers afin d'empêcher leur ouverture accidentelle.

- **Chemin d'accès au fichier incorrect** - Si un fichier système important est exécuté à partir d'un chemin d'accès autre que celui par défaut (*exemple : winlogon.exe exécuté à partir d'un dossier autre que Windows*), AVG signale cette contradiction. Dans certains cas, les virus utilisent des noms de processus système standards afin de se dissimuler au système.
- **Fichier verrouillé** - Le fichier signalé est verrouillé et, de ce fait, AVG ne peut pas l'analyser. En général, il s'agit d'un fichier qui est constamment utilisé par le système (*par exemple, un fichier d'échange*).

11.8. Quarantaine



La **quarantaine** offre un environnement parfaitement sûr pour la manipulation des objets infectés ou susceptibles de l'être, détectés au cours des analyses AVG. Lorsqu'un objet infecté est repéré par l'analyse et qu'AVG n'est pas en mesure de le

réparer automatiquement, un message vous invite à indiquer la mesure à prendre. Il est recommandé de placer l'objet en **Quarantaine** afin de le traiter ultérieurement.

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

- **Gravité** - offre une identification graphique du degré de gravité de la recherche en cours sur quatre niveaux allant du moins dangereux (■□□□) au plus grave (■□■□)
- **Type d'infection** - différencie les types d'objets trouvés selon l'importance de leur infection (*les objets répertoriés sont potentiellement infectés ou réellement infectés*)
- **Nom du virus** - spécifie le nom de l'infection décelée conformément à l'[Encyclopédie des virus](#) (disponible en ligne)
- **Chemin d'accès au fichier** - chemin d'accès menant à l'origine du fichier infectieux
- **Nom original de l'objet** - tous les objets détectés figurant dans la liste portent un nom standard attribué par AVG au cours du processus d'analyse. Si le nom initial de l'objet est connu (*telle qu'une pièce jointe qui ne correspond pas au contenu véritable de la pièce jointe*), il sera indiqué dans cette colonne.
- **Date de l'enregistrement** - date et heure à laquelle le fichier a été trouvé et placé en **quarantaine**

Boutons de commande

Les boutons de commande suivants sont accessibles depuis l'interface **Quarantaine** :

- **Restaurer** - rétablit le fichier infecté à sa place d'origine, sur le disque
- **Restaurer en tant que** - si vous décidez de transférer l'objet infecté détecté depuis la zone de **Quarantaine** vers un dossier de votre choix, servez-vous de ce bouton. L'objet suspect détecté sera enregistré sous son nom d'origine. Si le nom d'origine n'est pas connu, le nom standard sera utilisé.
- **Supprimer** - supprime définitivement le fichier infecté de la **Quarantaine**
- **Vider la quarantaine** - Vider intégralement le contenu de la **Quarantaine**

12. Mises à jour d'AVG

Il est essentiel de mettre régulièrement à jour votre programme anti-virus de manière à assurer une détection rapide des virus récemment découverts. Les mises à jour AVG ne sont pas diffusées selon un programme précis, mais sont plutôt la réaction à la détection d'un grand nombre de menaces ou de menaces sérieuses. C'est pourquoi, il est recommandé de vérifier au moins une fois par jour l'existence d'une éventuelle mise à jour. L'option de vérification toutes les 4 heures garantit la protection optimale par la base virale AVG tout au long de la journée.

12.1. Niveaux de mise à jour

AVG présente deux niveaux de mise à jour :

- Une **mise à jour des définitions** prioritaire inclut les modifications nécessaires à une protection efficace contre les virus. En règle générale, cette action ne s'applique pas au code. Seule la base de données de définition est concernée. Il est conseillé d'effectuer cette mise à jour dès qu'elle est disponible.
- **La mise à jour du programme** contient diverses modifications, corrections et améliorations.

Lorsque vous [programmez une mise à jour](#), il est possible de sélectionner le niveau de priorité voulu lors du téléchargement et de l'application de la mise à jour.

12.2. Types de mises à jour

Il existe deux types de mises à jour :

- **Mise à jour à la demande** - une mise à jour immédiate d'AVG que vous exécutez dès que vous en voyez l'utilité.
- **Mise à jour programmée** - [AVG permet également de définir à l'avance un plan de mise à jour](#). La mise à jour planifiée est alors exécutée de façon périodique en fonction de la configuration choisie. Chaque fois que de nouveaux fichiers de mise à jour sont présents à l'emplacement indiqué, ils sont téléchargés directement depuis Internet ou à partir d'un répertoire du réseau. Lorsque aucune mise à jour n'est disponible, le processus n'a pas lieu.

12.3. Processus de mise à jour

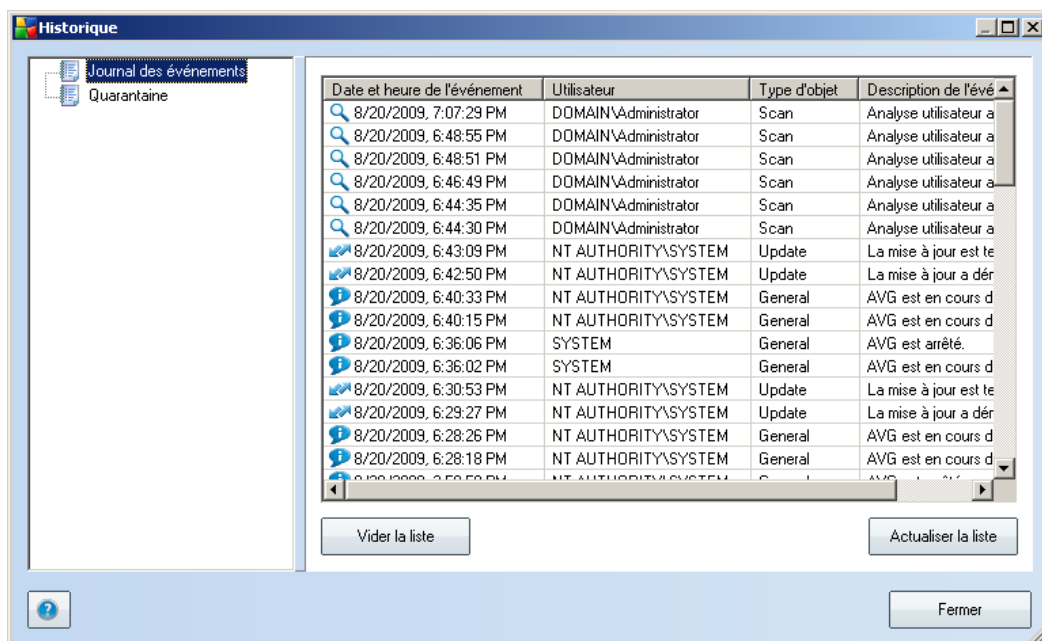
Le processus de mise à jour peut être lancé aussi souvent que nécessaire en cliquant sur **Mise à jour** ([lien d'accès rapide](#)). Ce lien est constamment disponible, quelle que soit la boîte de dialogue ouverte dans l'[interface utilisateur AVG](#). Il est toutefois particulièrement recommandé d'effectuer des mises à jour fréquentes comme établi par

défaut dans le composant [Mise à jour](#).

Lorsque vous lancez la mise à jour, AVG vérifie en premier lieu si de nouveaux fichiers de mise à jour sont disponibles. Le cas échéant, AVG télécharge et exécute ces mises à jour. Pendant ce processus, l'interface **Mise à jour** s'affiche et vous présente le déroulement de l'opération sous une forme graphique avec des données statistiques explicites (*taille du fichier de mise à jour, données reçues, vitesse du téléchargement, temps écoulé...*).

Remarque : avant l'exécution de la mise à jour du programme AVG, un point de restauration est créé. En cas d'échec de la mise à jour et de blocage de votre système d'exploitation, vous avez alors la possibilité de restaurer le système d'exploitation tel qu'il était configuré à partir de ce point. Cette option est disponible dans le menu Démarrer / Tous les programmes / Accessoires / Outils système / Restauration du système. Option destinée aux utilisateurs expérimentés seulement !

13. Journal des événements



La boîte de dialogue **Journal des événements** est accessible par le [menu système](#), commande **Historique/Journal des événements**. Dans cette boîte de dialogue, vous trouverez un résumé des événements les plus importants survenus pendant l'exécution du programme **AVG 9.0 File Server**. La commande **Journal des événements** enregistre les types d'événements suivants :

- Informations au sujet des mises à jour de l'application AVG
- Heure de début, de fin ou d'interruption de l'analyse (y compris pour les analyses effectuées automatiquement)
- Événements liés à la détection des virus (par le [Bouclier résident](#) ou résultant de l'[analyse](#)) avec indication de l'emplacement des occurrences
- Autres événements importants

Boutons de commande

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

14. FAQ et assistance technique

En cas de problème technique ou commercial avec votre produit AVG, consultez la section **FAQ** du site Web d'AVG (<http://www.avg.com>).

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