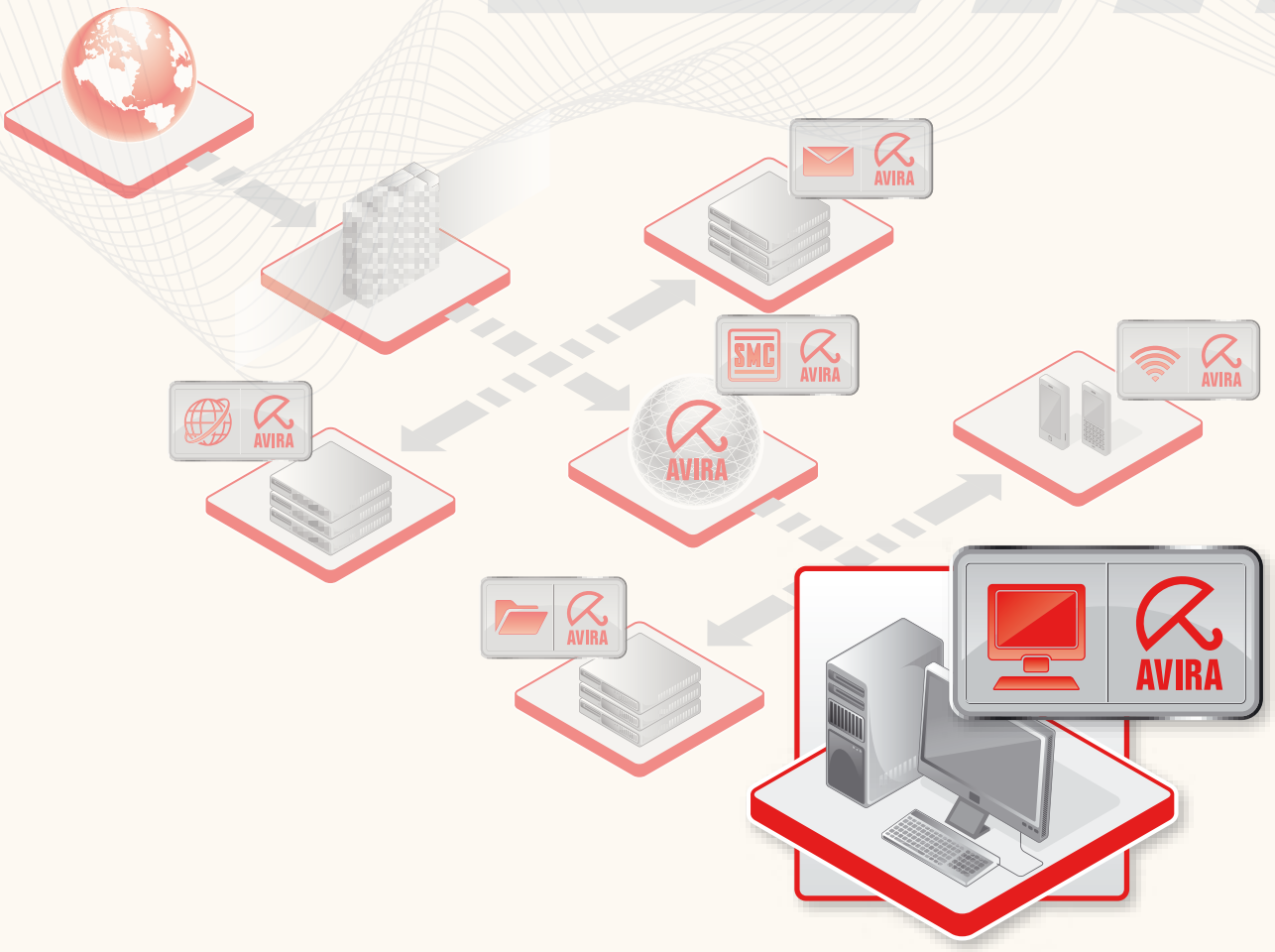
AVIRA
More Than Security

Manuel de l'utilisateur

Avira AntiVir Professional



www.avira.com/fr

Marque de fabrication et copyright

Marque de fabrication

AntiVir est une marque déposée de Avira GmbH.
Windows est une marque déposée de Microsoft Corporation aux Etats-Unis et dans d'autres pays.
Tous les autres noms de marques et de produits sont des marques ou marques déposées de leurs propriétaires.
Les marques protégées ne sont pas désignées comme telles dans le présent manuel. Cela signifie pas qu'elles peuvent être utilisées librement.

Remarques concernant le copyright

Des codes de fournisseurs tiers ont été utilisés pour Avira AntiVir Professional. Nous remercions les détenteurs des copyrights d'avoir mis leur code à notre disposition. Vous trouverez des informations détaillées concernant le copyright dans l'aide de Avira AntiVir Professional sous Third Party Licenses.

Table des matières

1 Introduction 1

2 Symboles et mises en avant 2

3 Informations produit 3

3.1 Prestations 3
3.2 Configuration minimale 4
3.3 Attribution de licence 5
3.3.1 Gestion des licences 5

4 Installation et désinstallation 7

4.1 Installation 7
4.2 Installation modifiée 11
4.3 Modules d'installation 11
4.4 Désinstallation 12
4.5 Installation et désinstallation dans le réseau 13
4.5.1 Installation dans le réseau 13
4.5.2 Désinstallation dans le réseau 14
4.5.3 Paramètres des lignes de commande pour le programme d'installation 14
4.5.4 Paramètres du fichier setup.inf 15

5 Aperçu de AntiVir Professional 19

5.1 Interface et commande 19
5.1.1 Control Center 19
5.1.2 Configuration 22
5.1.3 Icône de programme 25
5.2 Comment procéder 26
5.2.1 Activer la licence 26
5.2.2 Actualiser Avira AntiVir Professional de manière automatisée 27
5.2.3 Démarrer manuellement une mise à jour 28
5.2.4 Recherche directe : chercher des virus et logiciels malveillants avec un profil de recherche 29
5.2.5 Recherche directe : chercher des virus et logiciels malveillants par glisser&déplacer 30
5.2.6 Recherche directe : chercher des virus et logiciels malveillants via le menu contextuel 31
5.2.7 Recherche directe : recherche automatisée de virus et logiciels malveillants 31
5.2.8 Recherche directe : chercher les rootkits actifs de manière ciblée 32
5.2.9 Réagir aux virus et logiciels malveillants détectés 32
5.2.10 Quarantaine : manipuler les fichiers (*.qua) en quarantaine 36
5.2.11 Quarantaine : restaurer les fichiers dans la quarantaine 37
5.2.12 Quarantaine : déplacer un fichier suspect en quarantaine 38
5.2.13 Profil de recherche : compléter ou supprimer un type de fichier dans un profil de recherche 39
5.2.14 Profil de recherche : créer un lien sur le Bureau pour le profil de recherche 39
5.2.15 Evénements: Filtrer les événements 40
5.2.16 MailGuard: Exclure des adresses email de la vérification 40

6 Scanner 43

7 Mises à jour 44

8 FAQ, astuces 46

8.1 Aide en cas de problème 46
8.2 Commandes clavier 49
8.2.1 Dans les champs de dialogue 49
8.2.2 Dans l'Aide 50
8.2.3 Dans le Control Center 51
8.3 Centre de sécurité Windows 52
8.3.1 Généralités 52
8.3.2 Le Centre de sécurité Windows et Avira AntiVir Professional 52

9 Virus et autres 55

9.1 Catégories de dangers étendues 55
9.2 Virus et autres logiciels malveillants 58

10 Info et service 62

10.1 Adresse de contact 62
10.2 Support technique 62
10.3 Fichier suspect 63
10.4 Signaler une fausse alerte 63
10.5 Vos réactions pour plus de sécurité 63

11 Référence : options de configuration 64

11.1 Scanner 64
11.1.1 Recherche 64
11.1.1.1. Action en cas de résultat positif 67
11.1.1.2. Autres actions 70
11.1.1.3. Exceptions 71
11.1.1.4. Heuristique 72
11.1.2 Rapport 73
11.2 Guard 74
11.2.1 Recherche 74
11.2.1.1. Action en cas de résultat positif 76
11.2.1.2. Autres actions 79
11.2.1.3. Exceptions 80
11.2.1.4. Heuristique 82
11.2.2 Rapport 83
11.3 MailGuard 84
11.3.1 Recherche 84
11.3.1.1. Action en cas de résultat positif 85
11.3.1.2. Autres actions 87
11.3.1.3. Heuristique 88
11.3.2 Généralités 88
11.3.2.1. Exceptions 89
11.3.2.2. Mémoire tampon 89
11.3.3 Rapport 90
11.4 WebGuard 91
11.4.1 Recherche 91
11.4.1.1. Action en cas de résultat positif 92
11.4.1.2. Accès bloqués 93
11.4.1.3. Exceptions 95

11.4.1.4. Heuristique....98
11.4.2 Rapport....99
11.5 Généralités....99
11.5.1 Configuration :: Généralités....100
11.5.1.1. Email....100
11.5.2 Configuration :: Généralités....101
11.5.2.1. Catégories de dangers étendues....101
11.5.3 Configuration :: Généralités....101
11.5.3.1. Mot de passe....101
11.5.4 Sécurité....103
11.5.5 WMI....105
11.5.6 Répertoires....105
11.5.7 Mise à jour....106
11.5.7.1. Serveur de fichiers....107
11.5.7.2. Serveur web....108
11.5.8 Avertissements....110
11.5.8.1. Réseau....110
11.5.8.2. Email....112
11.5.8.3. Avertissements acoustiques....114
11.5.9 Evénements....115
11.5.10 Limiter les rapports....115
11.5.11 Avertissements acoustiques....115

1 Introduction

Avira AntiVir Professional de la société Avira GmbH protège votre ordinateur des virus, logiciels malveillants, logiciels publicitaires et espions, programmes indésirables et autres dangers. Ce manuel aborde de manière simplifiée les virus et logiciels malveillants.

Le manuel décrit l'installation et la commande du programme.

Sur notre site Web http://www.avira.com/fr, vous pouvez télécharger le manuel de Avira AntiVir Professional sous forme de PDF, actualiser Avira AntiVir Professional ou renouveler votre licence.

En outre, vous trouverez sur notre site Web des informations comme par exemple le numéro de téléphone du support technique ainsi que notre bulletin d'actualité à laquelle vous pouvez vous abonner.

L'équipe d'Avira GmbH

2 Symboles et mises en avant

Les symboles suivants sont utilisés :

Symbole / Désignation	Explication
✓	Se trouve devant une condition à remplir avant d'exécuter une manipulation.
▸	Se trouve devant une manipulation que vous effectuez.
→	Se trouve devant un résultat qui découle de la manipulation précédente.
Avertissement	Se trouve devant un avertissement en cas de risque de perte critique de données.
Remarque	Se trouve devant une remarque contenant des informations particulièrement importantes ou devant une astuce qui facilite la compréhension et l'utilisation du logiciel Avira AntiVir Professional.

Les mises en avant suivantes sont utilisées :

Mise en avant	Explication
Italique	Nom du fichier ou indication du chemin.
	Eléments de l'interface logicielle qui s'affichent (par ex. intitulé de fenêtre, zone de fenêtre ou champ d'option).
Gras	Éléments de l'interface logicielle sur lesquels vous cliquez (par ex. option de menu, rubrique ou bouton).

3 Informations produit

Ce chapitre vous donne toutes les informations pour l'acquisition et l'utilisation de Avira AntiVir Professional :

- voir le chapitre : Prestations
- voir le chapitre : Configuration minimale
- voir le chapitre : Attribution de licence
- voir le chapitre : Gestion des licences

Avira AntiVir Professional est un outil complet et flexible permettant de protéger avec fiabilité votre ordinateur des virus, des logiciels malveillants, des programmes indésirables et autres dangers.

▶ Tenez compte des remarques suivantes :

Remarque
La perte de données précieuses a souvent des conséquences dramatiques. Même le meilleur programme de protection contre les virus ne peut pas vous protéger à cent pour cent de la perte de données. Effectuez régulièrement des copies de sauvegarde (back-ups) de vos données.

Remarque
Un programme qui protège des virus, logiciels malveillants, programmes indésirables et autres dangers n'est fiable et efficace que s'il est actuel. Assurez-vous de l'actualité de Avira AntiVir Professional grâce aux mises à jour automatiques. Configurez le programme en conséquence.

3.1 Prestations

Avira AntiVir Professional vous propose les fonctions suivantes :

- Control Center pour la surveillance, la gestion et la commande de l'intégralité du programme
- Configuration centrale intuitive standard ou expert et aide contextuelle
- Le Scanner (On-Demand Scan) avec recherche commandée par profil et configurable de tous les types de virus et logiciels malveillants connus
- Intégration dans la commande des comptes d'utilisateurs Windows Vista (User Account Control) pour pouvoir effectuer les tâches nécessitant des droits d'administrateur
- Le Guard (On-Access Scan) pour la surveillance permanente de tous les accès aux données
- MailGuard (scanner POP3, scanner IMAP et scanner SMTP) pour le contrôle permanent de vos emails à la recherche de virus et logiciels malveillants. Inclut la vérification des pièces jointes aux emails
- Le WebGuard pour la vérification des données et fichiers en provenance d'Internet via le protocole HTTP (vérification des ports 80, 8080, 3128)

- Gestion de quarantaines intégrée pour l'isolation et le traitement des fichiers suspects
- Protection anti-rootkit pour localiser les logiciels malveillants installés de manière cachée dans le système de l'ordinateur (appelés rootkits) (pour systèmes 32 bits uniquement)
- Accès direct aux informations détaillées sur les virus et logiciels malveillants trouvés via Internet
- Mise à jour simple et rapide du programme, des définitions de virus (VDF) et du moteur de recherche grâce à la mise à jour de fichiers individuels et à la mise à jour incrémentielle VDF via un serveur Web basé sur Internet ou Intranet
- Attribution de licence intuitive dans la gestion des licences
- Le Planificateur intégré pour la planification des tâches uniques ou répétées comme les mises à jour et les contrôles
- Identification extrêmement efficace des virus et logiciels malveillants grâce à des technologies de recherche innovantes (moteur de recherche) comprenant des procédés de recherche heuristique
- Identification de tous les types d'archives courants, y compris des extensions d'archives imbriquées et des extensions intelligentes
- Grande performance grâce à la capacité de multithreading (scannage simultané de nombreux fichiers à vitesse élevée)

3.2 Configuration minimale

Pour que Avira AntiVir Professional fonctionne parfaitement, l'ordinateur doit remplir les conditions suivantes :

- Processeur Pentium et plus, au moins 266 MHz
- Système d'exploitation
  - Windows 2000, SP4 et le cumul de mises à jour 1 ou
  - Windows XP, SP2 (32 ou 64 bits) ou
  - Windows Vista (32 ou 64 bits, SP1 recommandé)
- 100 Mo minimum d'espace mémoire disponible sur le disque dur (voire plus en cas d'utilisation de la fonction de quarantaine et pour la mémoire temporaire)
- 192 Mo minimum de mémoire vive sous Windows 2000/XP/ Windows 2000 Server
- 512 Mo minimum de mémoire vive sous Windows Vista, Windows Server 2003 et Windows Server 2008
- Pour l'installation de Avira AntiVir Professional : droits d'administrateur
- Pour toutes les installations : Windows Internet Explorer 6.0 ou ultérieur
- Connexion Internet, le cas échéant (voir Installation)

Consignes pour les utilisateurs de Windows Vista

Sous Windows 2000 et Windows XP, de nombreux utilisateurs travaillent avec des droits d'administrateurs. Ceci n'est toutefois pas souhaitable pour des raisons de sécurité, car les virus et programmes indésirables ont beau jeu de s'immiscer dans l'ordinateur.

Pour cette raison, Microsoft introduit avec Windows Vista le "contrôle du compte de l'utilisateur" (User Account Control). Cette fonction offre plus de protection aux utilisateurs connectés en tant qu'administrateur : un administrateur dispose ainsi sur Windows Vista d'abord uniquement des privilèges d'un utilisateur normal. Les actions pour lesquelles des droits d'administrateur sont nécessaires sont repérées par une icône par Windows Vista. En outre, l'utilisateur doit confirmer l'action souhaitée. Ce n'est qu'après avoir donné son accord que l'accroissement des privilèges est octroyé et que le système d'exploitation exécute la tâche administrative en question.

Avira AntiVir Professional nécessite des droits d'administrateur pour quelques actions sous Windows Vista. Ces actions sont identifiées par le caractère suivant :  . Si ce symbole apparaît en outre sur un bouton, des droits d'administrateur sont nécessaires pour cette action. Si votre compte utilisateur actuel ne dispose pas de droits d'administrateur, le dialogue de contrôle du compte de l'utilisateur Windows Vista vous demande de saisir le mot de passe d'administrateur. Si vous ne disposez pas du mot de passe d'administrateur, vous ne pouvez pas exécuter cette action.

3.3 Attribution de licence

Pour pouvoir utiliser Avira AntiVir Professional, il vous faut une licence. Vous acceptez ainsi les conditions de licence de Avira AntiVir Professional.

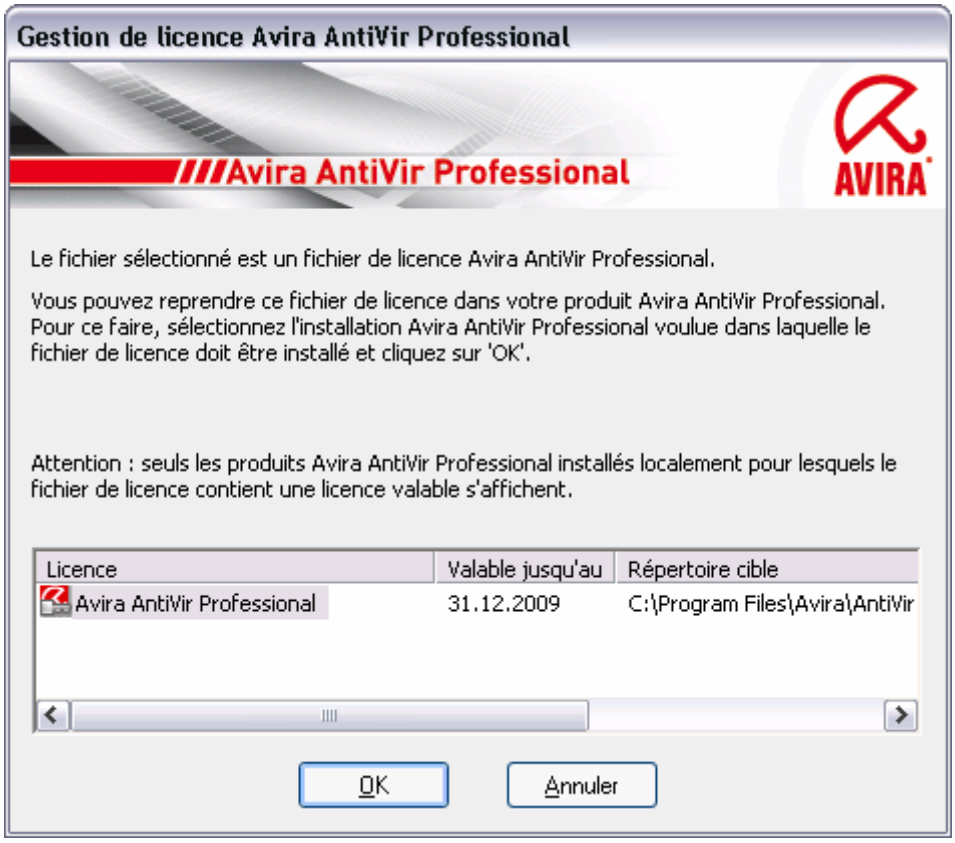
La licence est octroyée via une clé de licence numérique sous forme de fichier hbedv.key. Cette clé de licence numérique est la centrale d'activation de votre licence personnelle. Elle contient des indications précises sur les programmes et les périodes pour lesquels vous avez une licence. Une clé de licence numérique peut donc contenir la licence pour plusieurs produits.

La clé de licence numérique vous est transmise par email si vous avez acheté AntiVir Professional sur Internet ou se trouve sur le CD/DVD du programme Avira AntiVir Professional. Vous pouvez charger la clé de licence lors de l'installation de AntiVir Professional ou l'installer ultérieurement dans la gestion des licences.

3.3.1 Gestion des licences

La gestion des licences Avira AntiVir Professional permet une installation très simple de la licence Avira AntiVir Professional.

Gestion des licences Avira AntiVir Professional



Vous pouvez effectuer une installation de la licence en sélectionnant le fichier de licence dans votre gestionnaire de fichiers ou l'email d'activation en cliquant deux fois dessus et suivre les instructions à l'écran.

Remarque
La gestion des licences Avira AntiVir Professional copie la licence correspondante automatiquement dans le dossier de produit correspondant. Si une licence est déjà disponible, un message s'affiche demandant si le fichier de licence doit être remplacé. Le fichier existant est ensuite renommé en hbedv.old.

4 Installation et désinstallation

Dans ce chapitre, vous obtenez des informations sur l'installation et la désinstallation de votre Avira AntiVir Professional :

- voir le chapitre Installation : conditions, types d'installation, exécuter l'installation
- voir le chapitre Modules d'installation
- voir le chapitre Installation modifiée
- Installation et désinstallation dans le réseau
- voir le chapitre Désinstallation : exécuter la désinstallation

4.1 Installation

Avant l'installation de Avira AntiVir Professional, vérifiez que votre ordinateur présente la configuration minimale requise. Si votre ordinateur présente la configuration minimale requise, vous pouvez installer Avira AntiVir Professional.

Remarque
A partir de Windows XP, Avira AntiVir Professional génère un point de restauration de votre ordinateur avant l'installation de Avira AntiVir Professional. Cela vous permet de supprimer Avira AntiVir Professional de manière sûre en cas d'échec de l'installation. Attention, pour cela l'option **Désactiver la restauration du système** sous : "Démarrer | Panneau de configuration | Performances et maintenance | Système | onglet Restauration du système" ne doit pas être sélectionnée.
Si vous souhaitez restaurer votre ordinateur avant, vous pouvez le faire via la fonction "Démarrer | Tous les programmes | Accessoires | Outils système | Restauration du système". L'entrée AntiVir Professional vous indique le point de restauration généré par Avira AntiVir Professional.

Types d'installation

Pendant l'installation, vous pouvez choisir un type de set-up dans l'assistant d'installation :

Intégrale

AntiVir Professional est installé intégralement avec tous les composants de programme. Les fichiers de programme sont installés dans un répertoire par défaut sous `C:\Programme`.

Personnalisé

Vous avez la possibilité de sélectionner les divers composants du programme pour l'installation (voir le chapitre Installation et désinstallation::Modules d'installation). Vous pouvez choisir un répertoire cible pour les fichiers de programme à installer. Vous pouvez désactiver la création d'une icône de bureau et d'un groupe de programmes dans le menu de démarrage.

Avant le démarrage de la procédure d'installation

- Fermez votre programme de messagerie électronique. Il est en outre recommandé de fermer toutes les applications ouvertes.
- Assurez-vous qu'aucune autre solution antivirus n'est installée. Les fonctions de protection automatiques des différentes solutions de sécurité peuvent s'entraver.
- Connectez vous à Internet. La connexion Internet est nécessaire à l'exécution des étapes d'installation suivantes :
- Téléchargement des fichiers programme actuels et du moteur de recherche, ainsi que des fichiers de définitions des virus du jour par le biais du programme d'installation (en cas d'installation basée sur Internet)
- Si nécessaire, exécution d'une mise à jour de AntiVir Professional une fois l'installation terminée
- Enregistrez le fichier de licence hbedv.key sur votre système informatique, si vous souhaitez activer Avira AntiVir Professional.

Remarque
Installation basée sur Internet :
Pour l'installation basée sur Internet de Avira AntiVir Professional, Avira GmbH met à disposition un programme d'installation qui charge les fichiers programme actuels des serveurs web de la société Avira GmbH, avant l'exécution de l'installation. Cette procédure garantit que le programme AntiVir Professional est installé avec le fichier de définitions des virus du jour.
Installation à l'aide d'un pack d'installation :
Le pack d'installation contient non seulement le programme d'installation mais aussi tous les fichiers programme nécessaires. Il n'y a toutefois pas de possibilité de sélection de la langue pour AntiVir Professional, lors d'une installation à l'aide d'un pack d'installation. Il est recommandé, à l'issue de l'installation, d'effectuer une mise à jour afin d'actualiser le fichier de définitions des virus.

Exécuter l'installation

Le programme d'installation fonctionne en mode de dialogue auto-explicatif. Chaque fenêtre contient une sélection définie de boutons pour la commande du processus d'installation.

Les principaux boutons disposent des fonctions suivantes :

- **OK :** confirmer l'action.
- **Abandonner :** abandonner l'action.
- **Continuer :** passer à l'étape suivante.
- **Précédent :** retourner à l'étape précédente.

Voici comment installer AntiVir Professional :

- Démarrez le programme d'installation par un double clic sur le fichier d'installation que vous avez téléchargé d'Internet ou insérez le CD du programme.

Installation basée sur Internet

La fenêtre de dialogue *Bienvenue...* apparaît.

- Cliquez sur **Continuer** pour poursuivre l'installation.

La fenêtre de dialogue *Sélection de la langue* s'affiche à l'écran.

- Sélectionnez la langue dans laquelle vous souhaitez installer AntiVir Professional et validez votre sélection de langue avec **Continuer**.

La fenêtre de dialogue *Téléchargement* s'affiche à l'écran. Tous les fichiers nécessaires à l'installation sont téléchargés des serveurs web de la société Avira GmbH. Une fois le téléchargement terminé, la fenêtre *Téléchargement* se referme.

Installation à l'aide d'un pack d'installation

L'assistant d'installation s'ouvre avec la fenêtre de dialogue *Avira AntiVir Professional*.

- Cliquez sur *Accepter* pour commencer l'installation.

Le fichier d'installation est décompressé. La routine d'installation démarre.

La fenêtre de dialogue *Bienvenue...* apparaît.

- Cliquez sur **Suivant**.

Suite de l'installation basée sur Internet et de l'installation à l'aide d'un pack d'installation

L'installation se poursuit avec la fenêtre de dialogue *Catégories étendues de dangers*. La fenêtre de dialogue vous informe des fonctions de protection du programme AntiVir Professional et apporte des informations sur l'extension des fonctions de protection AntiVir Professional.

- Cliquez sur **Suivant**.

La fenêtre de dialogue avec l'accord de licence s'affiche.

- Confirmez que vous acceptez l'accord de licence et cliquez sur **Continuer**.

La fenêtre de dialogue *Sélectionner un type d'installation* s'affiche.

- Décidez si vous voulez effectuer une installation complète ou personnalisée.
- Activez l'option **Complète** ou **Personnalisée** et confirmez avec **Continuer**.

Installation personnalisée

La fenêtre de dialogue *Choisir le répertoire cible* s'affiche.

- Confirmez le répertoire cible indiqué avec **Continuer**.

- OU -

Avec **Parcourir**, choisissez un autre répertoire cible et confirmez avec **Continuer**.

La fenêtre de dialogue *Installer les composants* s'affiche :

- Activez ou désactivez les composants souhaités et confirmez avec **Continuer**.

Dans la fenêtre de dialogue suivante, vous pouvez décider si un lien doit être créé sur votre bureau et/ou un groupe de programmes dans le menu démarrer.

- Cliquez sur **Suivant**.

Suite de l'installation complète et personnalisée

La fenêtre de dialogue *Installer la licence* s'affiche :

- Sélectionnez le répertoire dans lequel vous avez enregistré le fichier de licence, suivez les consignes de la fenêtre de dialogue et confirmez avec **Continuer**.

Le fichier de licence est copié, les composants installés et démarrés.

Dans la fenêtre de dialogue suivante, vous pouvez décider si le fichier Lisez-moi doit être ouvert, une fois l'installation terminée.

- Acceptez-le le cas échéant et finissez l'installation avec *Terminer*.

  L'assistant d'installation se referme.

  Le fichier Lisez-moi s'ouvre le cas échéant.

L'assistant de configuration s'ouvre à l'étape suivante. Vous pouvez effectuer d'importants préréglages pour AntiVir Professional dans l'assistant de configuration. Si vous annulez la configuration, AntiVir Professional démarre avec des réglages par défaut.

Préréglages dans l'assistant de configuration

Vous pouvez choisir un degré d'identification pour la technologie Ahead dans la fenêtre de dialogue *Configurer AHeAD*. Le degré d'identification choisi est validé pour le réglage de la technologie AHeAD du Scanner (recherche directe) et du Guard (recherche en temps réel).

- Choisissez un degré d'identification et poursuivez la configuration avec **Continuer**.

La fenêtre de dialogue suivante *Choisir des catégories étendues de dangers* vous permet d'adapter les fonctions de protection de AntiVir Professional grâce à la sélection de catégories de dangers.

- Activez d'autres catégories de danger le cas échéant et poursuivez la configuration avec *Continuer*.
- Activez l'option souhaitée et poursuivez la configuration avec *Continuer*.

Dans la fenêtre de dialogue suivante *Choisir les réglages email*, vous pouvez procéder aux réglages du serveur pour l'envoi d'emails. AntiVir Professional utilise l'envoi d'emails par SMTP pour envoyer des avertissements email.

- Procédez aux indications nécessaires concernant les réglages du serveur, le cas échéant et poursuivez la configuration avec *Continuer*.

La fenêtre de dialogue suivante *Contrôle du système* permet d'activer ou de désactiver l'exécution d'un bref contrôle du système. Le bref contrôle du système est exécuté une fois la configuration terminée et avant le redémarrage de l'ordinateur. Il contrôle les programmes lancés et les fichiers système les plus importants, à la recherche de virus et de logiciels malveillants.

- Activez ou désactivez l'option *Bref contrôle du système* et poursuivez la configuration avec *Continuer*.

La fenêtre de dialogue suivante vous permet de finir la configuration avec *Terminer*.

- Cliquez sur *Terminer* pour quitter la configuration.

  Les réglages indiqués et sélectionnés sont validés.

  Si vous avez activé l'option *Bref contrôle du système*, la fenêtre Luke Filewalker s'ouvre. Le Scanner effectue un bref contrôle du système.

  La fenêtre de dialogue *Quitter l'installation* s'affiche.

  Si vous avez installé AntiVir Professional sous Windows XP et désactivé le pare-feu Windows, une fenêtre s'affiche, indiquant que l'ordinateur doit être redémarré.

- Finissez l'installation avec **Terminer**.

Une fois l'installation réussie, il est recommandé de contrôler dans le Control Center sous *Aperçu :: État*, si AntiVir Professional est à jour.

- Effectuez le cas échéant une mise à jour de AntiVir Professional afin d'actualiser le fichier de définitions des virus.
- Effectuez ensuite un contrôle intégral du système.

4.2 Installation modifiée

Vous avez la possibilité d'ajouter ou de supprimer certains composants de programmes de l'installation actuelle de Avira AntiVir Professional (voir chapitre Installation et désinstallation::Modules d'installation)

Si vous souhaitez ajouter ou supprimer des composants de programme de l'installation actuelle de Avira AntiVir Professional, vous pouvez utiliser l'option **Ajout/Suppression de programmes** pour **Modifier/Supprimer** des programmes dans le **panneau de configuration Windows**.

Sélectionnez Avira AntiVir Professional et cliquez sur **Modifier**. Dans le dialogue de bienvenue de Avira AntiVir Professional, sélectionnez l'option **Modifier le programme**. Vous êtes guidé à travers l'installation modifiée.

4.3 Modules d'installation

Lors d'une installation personnalisée ou modifiée, les modules suivants peuvent être sélectionnés pour l'installation ou ajoutés et supprimés :

- **AntiVir Professional**
  Ce module contient tous les composants nécessaires pour l'installation correcte de Avira AntiVir Professional.
- **AntiVir Guard**
  AntiVir Guard fonctionne en arrière-plan. Il surveille et répare si nécessaire les fichiers lors des opérations comme l'ouverture, l'écriture et la copie en temps réel (On-Access = à l'accès). Si un utilisateur effectue une opération sur le fichier (charger, exécuter ou copier le fichier), Avira AntiVir Professional parcourt automatiquement le fichier. Lors de l'opération Renommer, aucune recherche de AntiVir Guard n'est effectuée.
- **AntiVir MailGuard**
  Le MailGuard est l'interface entre votre ordinateur et le serveur d'email à partir duquel votre programme de messagerie électronique (client email) télécharge les emails. Le MailGuard se place comme proxy entre le programme d'email et le serveur d'email. Tous les emails entrants sont transférés via ce proxy, la présence de virus et de programmes indésirables est recherchée, puis ils sont transmis à votre programme email. Selon la configuration, le programme traite les emails automatiquement ou demande à l'utilisateur quoi faire.

- **AntiVir WebGuard**
  En 'naviguant' sur Internet, vous demandez des données en provenance d'un serveur Web via votre navigateur Web. Les données transmises par le serveur Web (fichiers HTML, script et images, fichiers flash, flux vidéo et musique, etc.) arrivent normalement de la mémoire cache du navigateur directement pour être exécutées dans le navigateur Web, ce qui exclut un contrôle par une recherche en temps réel comme AntiVir Guard le propose. De cette manière, des virus et programmes indésirables peuvent arriver sur votre système. Le WebGuard est un proxy HTTP qui surveille les ports (80, 8080, 3128) servant à la transmission des données et contrôle l'absence de virus et de programmes indésirables sur les données transférées. Selon la configuration, le programme traite les emails concernés automatiquement ou demande à l'utilisateur quoi faire.
- ***Protection AntiVir Rootkit***
  La Protection AntiVir Rootkit contrôle si un logiciel s'est déjà installé sur votre ordinateur qui ne peut être détecté par les méthodes habituelles après infiltration dans votre système.
- **Shell Extension**
  Les Shell Extensions Avira AntiVir Professional génèrent dans le menu contextuel de l'explorateur Windows (bouton droit de la souris) une entrée Contrôler les fichiers sélectionnés avec AntiVir. Avec cette entrée, vous pouvez scanner directement certains fichiers ou répertoires.

4.4 Désinstallation

Si vous souhaitez supprimer Avira AntiVir Professional de votre ordinateur, vous pouvez utiliser l'option **Logiciels** pour **Modifier ou supprimer** des programmes dans le panneau de configuration Windows.

Voici comment désinstaller Avira AntiVir Professional (exemple avec Windows XP et Windows Vista) :

- Ouvrez le **panneau de configuration** via le menu **Démarrer** de Windows.
- Double-cliquez sur **Programmes** (Windows XP : **Logiciels**).
- Sélectionnez **Avira AntiVir Professional** et cliquez sur **Supprimer**.

  Le système vous demande si vous souhaitez réellement supprimer le programme.
- Confirmez avec **Oui**.

  Tous les composants du programme sont supprimés.
- Cliquez sur **Terminer** pour terminer la désinstallation.

  Une fenêtre de dialogue peut s'afficher vous conseillant de redémarrer l'ordinateur.
- Confirmez avec **Oui**.

  Avira AntiVir Professional est désinstallé, votre ordinateur est redémarré si besoin est, ce faisant, tous les répertoires, tous les fichiers et toutes les entrées de registre de Avira AntiVir Professional sont supprimés.

4.5 Installation et désinstallation dans le réseau

Pour simplifier l'installation de Avira AntiVir Professional dans un réseau à plusieurs ordinateurs clients pour l'administrateur du système, Avira AntiVir Professional propose une procédure spéciale pour l'installation initiale et l'installation modifiée.

Pour l'installation automatique de Avira AntiVir Professional, le programme de set-up fonctionne avec le fichier de commande setup.inf. Le programme de set-up (presetup.exe) est compris dans le pack d'installation de Avira AntiVir Professional. L'installation démarre avec un script ou un fichier batch et contient toutes les informations nécessaires en provenance du fichier de commande. Les commandes dans le script remplacent les saisies manuelles habituelles pendant une installation.

Remarque
Attention : pour l'installation initiale dans le réseau, un fichier de licence est obligatoire.

Remarque
Veuillez noter que vous avez besoin d'un pack d'installation de Avira AntiVir Professional pour l'installation via le réseau. Il n'est pas possible d'utiliser un fichier d'installation pour l'installation basée sur Internet.

Avec un script de connexion du serveur ou par SMS, Avira AntiVir Professional peut être réparti de manière confortable dans le réseau.

Vous trouverez ici des informations sur l'installation et la désinstallation dans le réseau :

- voir le chapitre : Paramètres des lignes de commande pour le programme d'installation
- voir le chapitre : Paramètres du fichier setup.inf
- voir le chapitre : Installation dans le réseau
- voir le chapitre : Désinstallation dans le réseau

Remarque
AntiVir Security Management Center offre une autre possibilité confortable pour l'installation et la désinstallation de Avira AntiVir Professional dans le réseau. AntiVir Security Management Center sert à l'installation et à la maintenance à distance de AntiVir produits dans le réseau. Vous trouverez de plus amples informations sur notre site Web http://www.avira.com/fr.

4.5.1 Installation dans le réseau

L'installation peut être exécutée en mode batch commandée par script.

Le set-up est adapté aux installations suivantes :

- Installation initiale via le réseau (unattended setup)
- Installation des ordinateurs monopostes

▶ Installation modifiée ou mise à jour

Remarque
Nous recommandons de tester l'installation automatique avant d'effectuer la routine d'installation dans le réseau.

Voici comment installer Avira AntiVir Professional automatiquement dans le réseau :

Droits d'administration disponibles (nécessaires également en mode batch)

- Configurez les paramètres du fichier *setup.inf* et mémorisez le fichier.
- Démarrez l'installation de Avira AntiVir Professional avec le paramètre/inf ou liez le paramètre au script de connexion du serveur.
  - Exemples : `presetup.exe /inf="c:\temp\setup.inf"`

    L'installation se fait automatiquement.

4.5.2 Désinstallation dans le réseau

Voici comment désinstaller Avira AntiVir Professional automatiquement dans le réseau :

Droits d'administration disponibles (nécessaires également en mode batch)

- Démarrez la désinstallation de Avira AntiVir Professional avec le paramètre `/remsilent` ou `/remsilentaskreboot` ou intégrez le paramètre dans le script de connexion du serveur.

  En outre, vous pouvez indiquer le paramètre pour la documentation de la désinstallation.
  - Exemples : `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

    La désinstallation se fait automatiquement.

4.5.3 Paramètres des lignes de commande pour le programme d'installation

Toutes les indications sur les chemins et fichiers doivent être placées entre "...".

Pour l'installation, le paramètre suivant est possible :

- `/inf`

  Le programme d'installation démarre avec le script indiqué et lui prend tous les paramètres nécessaires.

  Exemple : `presetup.exe /inf="c:\temp\setup.inf"`

Pour la désinstallation, les paramètres suivants sont possibles :

- `/remove`

  Le programme d'installation désinstalle Avira AntiVir Professional.

  Exemple : `presetup.exe /remove`

- `/remsilent`

  Le programme d'installation désinstalle Avira AntiVir Professional, sans afficher de dialogues. L'ordinateur redémarre après la désinstallation.

  Exemple : `presetup.exe /remsilent`

– `/remsilentaskreboot`

Le programme d'installation désinstalle Avira AntiVir Professional sans afficher de dialogues et demande si l'ordinateur doit être redémarré après la désinstallation.

Exemple : `presetup.exe /remsilentaskreboot`

Pour la documentation de la désinstallation, les paramètres en option suivants sont possibles :

– `/unsetuplog`

Toutes les actions sont enregistrées à la désinstallation.

Exemple : `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

4.5.4 Paramètres du fichier setup.inf

Dans le fichier de commande setup.inf, vous pouvez régler les paramètres suivants de la zone [DATA] pour l'installation automatique de Avira AntiVir Professional. L'ordre des paramètres n'a aucune importance. Lorsqu'un paramètre manque ou est mal configuré, la routine de set-up s'arrête avec un message d'erreur.

– `DestinationPath`

Chemin cible où Avira AntiVir Professional est installé. Il doit être indiqué dans le script. Veuillez noter que le setup joint automatiquement le nom de l'entreprise et celui du produit. Il est possible d'utiliser des variables d'environnement.

Exemple : DestinationPath=`%PROGRAMFILES%`
donne par ex. le chemin d'installation `C:\Programme\Avira\AntiVir Desktop`

– `ProgramGroup`

Crée un groupe de programmes pour tous les utilisateurs de l'ordinateur dans le menu de démarrage de Windows.

`1`: créer un groupe de programmes

`0`: ne pas créer de groupe de programmes

Exemple : `ProgramGroup=1`

– `DesktopIcon`

Crée une icône sur le Bureau pour tous les utilisateurs de l'ordinateur.

`1`: créer une icône de bureau

`0`: ne pas créer d'icône de bureau

Exemple : `DesktopIcon=1`

– `ShellExtension`

Annonce la Shell-Extension dans le registre. Avec la Shell-Extension, l'absence de virus et logiciels malveillants peut être contrôlée sur les fichiers ou répertoires avec le menu contextuel du bouton droit de la souris.

`1`: enregistrer l'extension du shell

`0`: ne pas enregistrer l'extension du shell

Exemple : `ShellExtension=1`

– `Guard`

Installe AntiVir Guard (On-Access-Scanner).

`1`: installer AntiVir Guard

`0`: ne pas installer AntiVir Guard

Exemple : `Guard=1`

– `MailScanner`

Installe AntiVir MailGuard.

`1`: installer AntiVir MailGuard

`0`: ne pas installer AntiVir MailGuard

Exemple : `MailScanner=1`

– `KeyFile`

Indique le chemin du fichier de licence qui est copié lors de l'installation. Lors de l'installation initiale : obligatoire. Le nom du fichier doit être intégralement indiqué (qualification intégrale). (Lors d'une installation modifiée : facultatif.)

Exemple : `KeyFile=D:\inst\license\hbedv.key`

– `ShowReadMe`

Affiche le fichier readme.txt après l'installation.

`1`: afficher le fichier

`0`: ne pas afficher le fichier

Exemple : `ShowReadMe=1`

– `RestartWindows`

Redémarre l'ordinateur après l'installation. Cette entrée a la priorité en tant que ShowRestartMessage.

`1`: redémarrer l'ordinateur

`0`: ne pas redémarrer l'ordinateur

Exemple : `RestartWindows=1`

– `ShowRestartMessage`

Affiche une information pendant le setup avant un redémarrage automatique

`0`: ne pas afficher l'information

`1`: afficher l'information

Exemple : `ShowRestartMessage=1`

– `SetupMode`

Non nécessaire lors de l'installation initiale. Le programme de set-up reconnaît si une installation initiale est en cours. Etablit le type d'installation. En présence d'une installation déjà effectuée, vous devez indiquer avec le SetupMode si seule une mise à jour, une modification (reconfiguration) ou une désinstallation est exécutée pour cette installation.

`Update` : exécute une mise à jour d'une installation existante. Ce faisant, les paramètres de configuration, par ex. Guard, sont ignorés.

`Modify` : effectue une modification (reconfiguration) d'une installation existante. Aucun fichier n'est copié vers le chemin cible.
`Remove` : désinstalle AntiVir Professional du système.

Exemple : `SetupMode=Update`

– `AVWinIni (option)`

Indique le chemin cible du fichier de configuration qui peut être copié lors de l'installation. Le nom du fichier doit être intégralement indiqué (qualification intégrale).

Exemple : `AVWinIni=d:\inst\config\avwin.ini`

– `ScanMode`

Cette option active la recherche dans tous les lecteurs, une fois l'installation réussie :

`1`: démarrer la recherche

`0`: pas de recherche

Exemple : `ScanMode=1`

– `Mot de passe`

Cette option transmet à la routine de configuration le mot de passe mis en place pour l'installation (de modification) et la désinstallation. L'entrée n'est ensuite contrôlée par la routine de configuration que si un mot de passe a été créé. Si un mot de passe a été créé et que son paramètre manque ou est erroné, la routine de configuration est annulée.

Exemple : `Mot de passe=Mot de passe123`

– `WebGuard`

Installe le AntiVir WebGuard .

1: installer AntiVir WebGuard

0: ne pas installer AntiVir WebGuard

Exemple : WebGuard=1

– RootKit

Installe le module Protection AntiVir Rootkit Sans la Protection AntiVir Rootkit, le Scanner ne peut pas rechercher de rootkits sur le système !

1: installer la Protection AntiVir Rootkit

0: ne pas installer la Protection AntiVir Rootkit

Exemple : RootKit=1

5 Aperçu de AntiVir Professional

Dans ce chapitre vous obtenez une vue d'ensemble des fonctionnalités et de la commande de AntiVir Professional.

- voir le chapitre Interface et commande
- voir le chapitre Comment procéder

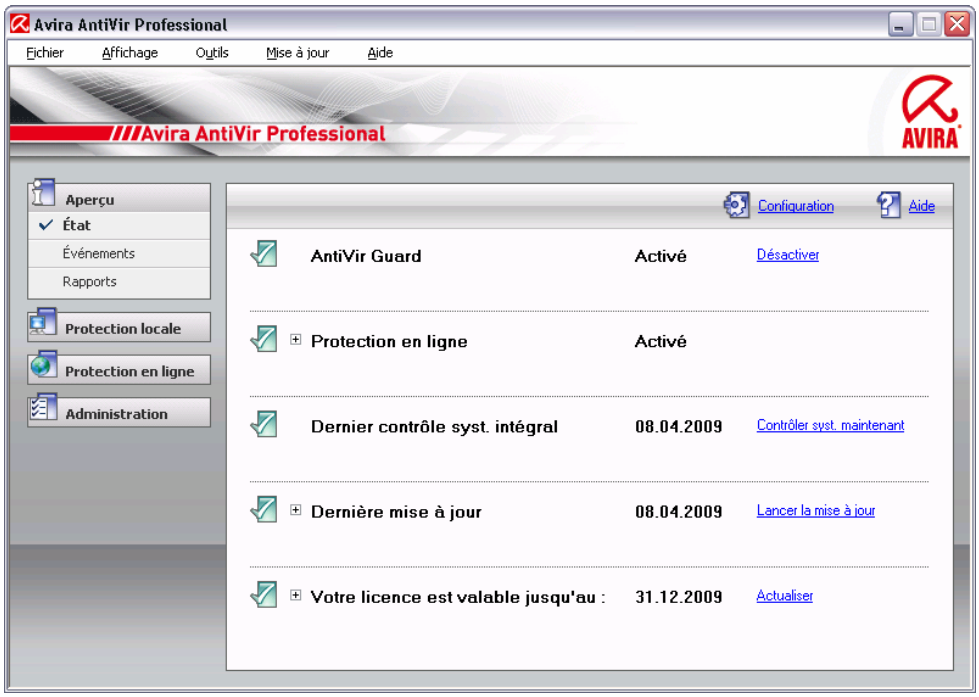
5.1 Interface et commande

La commande de AntiVir Professional se fait via trois éléments d'interface du programme :

- Control Center: surveillance et commande de AntiVir Professional
- Configuration Avira AntiVir Professional: configuration de AntiVir Professional
- Icône de programme dans la zone de notification de la barre des tâches : Ouverture du Control Center et autres fonctions

5.1.1 Control Center

Le Control Center sert à vérifier le statut de protection de votre ordinateur et à commander et utiliser les composants de protection et les fonctions de AntiVir Professional.



La fenêtre du Control Center se divise en trois zones : la **barre de menus**, la **barre de navigation** et la fenêtre de détail **Vue** :

- **Barre de menus :** dans les menus du Control Center, vous pouvez accéder aux fonctions générales du programme et à des informations sur AntiVir Professional.

- **Zone de navigation :** la zone de navigation vous permet de passer d'une rubrique à l'autre du Control Center. Les diverses rubriques contiennent des informations et fonctions des composants du programme AntiVir Professional et sont classées dans la barre de navigation selon les secteurs des tâches. Exemple : secteur de tâches *Aperçu* - Rubrique **État**.
- **Vue :** la rubrique sélectionnée dans la zone de navigation s'affiche dans cette fenêtre. Selon la rubrique, vous trouverez dans la barre supérieure de la fenêtre de détail les boutons pour exécuter les fonctions et actions. Dans les diverses rubriques, les données ou objets de données s'affichent dans des listes. Vous pouvez trier les listes en cliquant sur le champ situé derrière la liste à trier.

Démarrage et arrêt du Control Center

Vous avez les possibilités suivantes pour démarrer le Control Center :

- Cliquez deux fois sur l'icône du programme sur le Bureau
- Via l'entrée de programme AntiVir Professional dans le menu Démarrer | Programmes.
- Via l'icône de programme Avira AntiVir Professional.

Vous quittez le Control Center via la commande de menu **Quitter** dans le menu **Fichier** ou en cliquant sur la croix de fermeture dans Control Center.

Utiliser le Control Center

Voici comment naviguer dans le Control Center

▶ Dans la barre de navigation, sélectionnez une zone de tâches.

La zone de tâches s'ouvre et d'autres rubriques s'affichent. La première rubrique de la zone des tâches est sélectionnée et s'affiche.

▶ Cliquez éventuellement sur une rubrique pour l'afficher dans la fenêtre de détail.

- OU -

▶ Sélectionnez une rubrique via le menu *Vue*.

Remarque
La navigation au clavier dans la barre des menus s'active avec la touche [Alt]. Si la navigation est activée, vous pouvez vous déplacer dans le menu avec les touches flèches. La touche Entrée vous permet d'activer la rubrique actuellement repérée.
Pour ouvrir, fermer des menus dans le Control Center, ou naviguer dans les menus, vous pouvez également utiliser des combinaisons de touches : touche [Alt] + la lettre soulignée dans le menu ou la commande de menu. Maintenez la touche [Alt] enfoncée quand vous souhaitez accéder à une commande de menu ou à un sous-menu à partir du menu.

Voici comment traiter les données ou objets affichés dans la fenêtre de détail :

▶ Repérez les données ou objets que vous souhaitez traiter.

Pour repérer plusieurs éléments, maintenez la touche Ctrl ou Shift (sélection d'éléments situés les uns sous les autres) pendant la sélection des éléments.

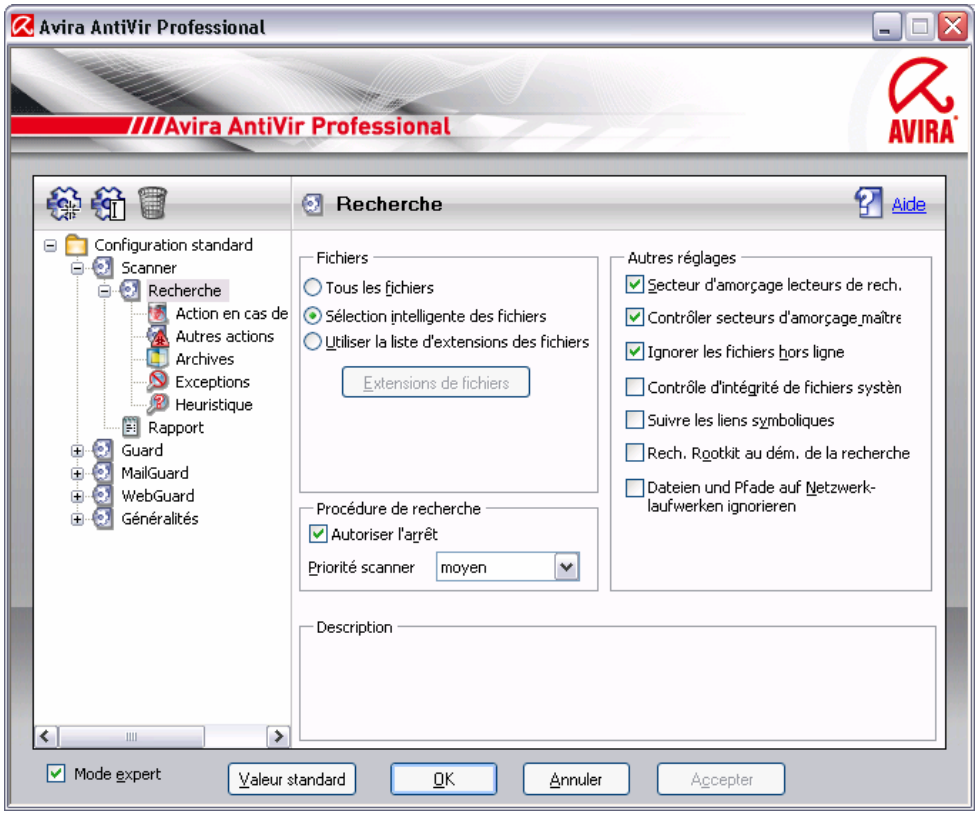
▶ Cliquez sur le bouton souhaité dans la barre supérieure de la fenêtre de détail pour traiter l'objet.

Aperçu du Control Center

- **Aperçu** : vous trouverez sous **Aperçu** toutes les rubriques vous permettant de surveiller le fonctionnement de Avira AntiVir Professional.
- La rubrique **État** offre la possibilité de voir d'un seul coup d'œil quels modules Avira AntiVir Professional sont actifs et fournit des informations sur la dernière mise à jour effectuée. De plus, elle vous permet de voir en si vous êtes détenteur d'une licence valable.
- La rubrique Evénements vous donne la possibilité de vous informer sur les événements générés par les modules Avira AntiVir Professional.
- La rubrique Rapports vous permet de visualiser les résultats des actions effectuées par Avira AntiVir Professional.
- **Protection locale** : vous trouverez sous **Protection locale** les composants vous permettant de contrôler l'absence de virus et de logiciels malveillants dans les fichiers de votre ordinateur.
- La rubrique Contrôler vous permet de configurer et de démarrer simplement la recherche directe. Les profils prédéfinis permettent d'effectuer une recherche avec des options standard adaptées. À l'aide de la sélection manuelle (qui n'est pas enregistrée) ou en créant des profils personnalisés, vous pouvez également adapter la recherche de virus et de programmes indésirables à vos besoins personnels.
- La rubrique Guard vous fournit des informations sur les fichiers contrôlés, ainsi que d'autres données statistiques qu'il est possible de réinitialiser à tout moment, et vous permet d'afficher le fichier de rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles quasiment "par pression d'un bouton".
- **Protection en ligne** : vous trouverez sous **protection en ligne** les composants vous permettant de protéger votre ordinateur contre les virus et logiciels malveillants provenant d'Internet ainsi que des accès réseau indésirables.
- La rubrique MailGuard vous indique les emails contrôlés par le MailGuard, leurs propriétés ainsi que d'autres données statistiques.
- La rubrique WebGuard vous fournit des informations sur les URL contrôlées et les virus trouvés, ainsi que d'autres données statistiques qu'il est possible de réinitialiser à tout moment et vous permet d'afficher le fichier de rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles quasiment "par pression d'un bouton".
- **Administration** : vous trouverez sous **Administration** des outils vous permettant d'isoler et de gérer les fichiers suspects ou infectés par des virus ainsi que de planifier des tâches récurrentes.
- Sous la rubrique Quarantaine se trouve le gestionnaire de quarantaine. Emplacement central pour les fichiers déjà en quarantaine ou suspects que vous souhaitez mettre en quarantaine. En outre, vous avez la possibilité d'envoyer un fichier par email à Avira Malware Research Center.
- La rubrique Planificateur vous donne la possibilité de créer des tâches de contrôle et de mise à jour programmées et d'ajuster ou de supprimer les tâches existantes.

5.1.2 Configuration

Dans la Configuration Avira AntiVir Professional, vous pouvez effectuer les réglages pour AntiVir Professional. Après l'installation, AntiVir Professional est configuré avec les réglages standard qui garantissent une protection optimale de votre ordinateur. Toutefois, votre ordinateur ou vos exigences envers AntiVir Professional peuvent présenter des particularités nécessitant l'ajustement de la configuration des composants de protection de AntiVir Professional.



La Configuration Avira AntiVir Professional a la structure d'une fenêtre de dialogue : Les boutons OK ou Valider vous permettent d'enregistrer les réglages effectués dans la configuration, Annuler vous permet de rejeter vos réglages et le bouton Valeurs par défaut vous permet de réinitialiser les réglages de la configuration aux réglages par défaut. Dans la barre de navigation gauche, vous pouvez choisir les diverses rubriques de configuration.

Accès à la Configuration Avira AntiVir Professional

Vous avez plusieurs possibilités pour accéder à la configuration :

- Via le panneau de configuration Windows.
- Via le Centre de sécurité Windows - à partir de Windows XP Service Pack 2.
- Via l'icône de programme Avira AntiVir Professional.
- Dans le Control Center Avira AntiVir Professional via la rubrique Outils | Configuration.
- Dans le Control Center Avira AntiVir Professional via le bouton Configuration.

Remarque
Si vous accédez à la configuration via le bouton **Configuration** du Control Center, vous arrivez au répertoire de configuration de la rubrique active dans le Control Center. Pour sélectionner les divers répertoires de configuration, le mode expert de la configuration doit être activé. Dans ce cas, un dialogue s'affiche vous invitant à activer le mode expert.

Utiliser Configuration Avira AntiVir Professional

Vous naviguez dans la fenêtre de configuration comme dans l'explorateur de Windows :

- Cliquez sur une entrée de l'arborescence pour afficher cette rubrique de configuration dans la fenêtre de détail.
- Cliquez sur le signe plus devant une entrée pour étendre la rubrique de configuration et afficher les sous-rubriques de la configuration dans l'arborescence.
- Pour masquer les sous-rubriques de la configuration, cliquez sur le signe moins devant la rubrique de configuration étendue.

Remarque
Pour activer ou désactiver des options ou appuyer sur des boutons dans la Configuration Avira AntiVir Professional, vous pouvez également utiliser des combinaisons de touches : touche [Alt] + la lettre soulignée dans le nom de l'option ou la désignation du bouton.

Remarque
Seul le mode expert permet d'afficher la totalité des rubriques de configuration. Activez le mode expert pour voir toutes les rubriques de configuration. Le mode expert peut être doté d'un mot de passe pour son activation.

Si vous souhaitez valider vos réglages dans la configuration :

- Cliquez sur le bouton **OK**.

  La fenêtre de configuration se ferme et les réglages sont validés.

  - OU -

- Cliquez sur le bouton **Valider**.

  Les réglages effectués sont validées. La fenêtre de configuration reste ouverte.

Si vous souhaitez terminer la configuration sans valider vos réglages :

- Cliquez sur le bouton **Annuler**.

  La fenêtre de configuration se ferme et les réglages sont rejetés.

Si vous souhaitez réinitialiser tous les réglages de la configuration aux valeurs par défaut :

- Cliquez sur **Valeurs par défaut**.

  Tous les réglages de la configuration sont réinitialisés aux valeurs par défaut.

Toutes les modifications et vos saisies sont perdues en cas de réinitialisation aux valeurs par défaut.

Profils de configuration

Vous avez la possibilité d'enregistrer vos réglages effectués dans la configuration en tant que profils de configuration. Dans le profil de configuration, c'est-à-dire une configuration, toutes les options de configuration sont réunies dans un groupe. La configuration est représentée dans la barre de navigation sous forme de nœud. Vous pouvez ajouter d'autres configurations à la configuration par défaut. Vous pouvez passer à une autre configuration dans le menu contextuel de l'icône de programme. Il est également possible de définir des règles pour la commutation d'une certaine configuration :
La commutation de la configuration basée sur des règles permet de coupler des configurations à l'utilisation d'une connexion LAN ou Internet (identification via une passerelle par défaut) : vous pouvez ainsi créer par exemple des profils de configuration pour les différents scénarios d'utilisation d'un ordinateur portable :

- Utilisation dans le réseau de l'entreprise : mise à jour via le serveur Intranet, WebGuard désactivé
- Utilisation à domicile : mise à jour via le serveur web par défaut de la société Avira GmbH, WebGuard activé

Les boutons disponibles sur la barre de navigation ou les commandes du menu contextuel des rubriques de configuration vous permettent d'ajouter, de renommer, d'effacer, de copier, de réinitialiser des configurations ainsi que de définir des règles pour la commutation d'une configuration.

Remarque
La commutation automatique d'une configuration n'est pas prise en charge sous Windows 2000. Il n'est pas possible de définir des règles de commutation d'une configuration sous Windows 2000.

Aperçu des options de configuration

Vous disposez des options de configuration suivantes :

- **Scanner**: Configuration de la recherche directe

  Options de recherche

  Actions en cas de résultat positif

  Options pour la recherche dans les archives

  Exceptions de la recherche directe

  Heuristique de la recherche directe

  Réglage de la fonction de rapport

- **Guard**: Configuration de la recherche en temps réel

  Options de recherche

  Actions en cas de résultat positif

  Exceptions de la recherche en temps réel

  Heuristique de la recherche en temps réel

  Réglage de la fonction de rapport

- **MailGuard**: Configuration du MailGuard

  Options de recherche : activation de la surveillance des comptes POP3, des comptes IMAP, des emails sortants (SMTP)

  Actions en cas de logiciel malveillant

Heuristique de la recherche du MailGuard

Exceptions de la recherche du MailGuard

Configuration de la mémoire tampon, vider la mémoire tampon

Réglage de la fonction de rapport

– **WebGuard**: Configuration du WebGuard

Options de recherche, activation et désactivation du WebGuard

Actions en cas de résultat positif

Accès bloqués : Types de fichiers et types MIME indésirables, filtre Web pour les URL connues indésirables (logiciels malveillants, hameçonnage, etc.)

Exceptions de la recherche du WebGuard : URL, types de fichiers, types MIME

Heuristique du WebGuard

Réglage de la fonction de rapport

– Généralités :

Configuration de l'envoi d'emails par SMTP

Catégories étendues de dangers pour la recherche directe et en temps réelle

Protection par mot de passe pour l'accès au Control Center et à la Configuration Avira AntiVir Professional

Sécurité : affichage d'état de la mise à jour, affichage d'état du contrôle intégral du système, protection du produit

WMI : activer la prise en charge WMI

Configuration de la documentation des événements

Configuration des fonctions de rapport

Réglage des répertoires utilisés

Mise à jour : configuration de la connexion au serveur de téléchargement , méthode de téléchargement (via serveur Web ou serveur de fichiers), réglage des mises à jour produits

Avertissements : Configuration des avertissements email du/des composant(s) :
Scanner
Guard
Updater
Configuration des avertissements réseau du/des composant(s) Scanner, Guard

Configuration des avertissements acoustiques en cas de détection de logiciel malveillant

5.1.3 Icône de programme

Après l'installation, l'icône de AntiVir Professional s'affiche dans la zone de notification de la barre des tâches :

Symbole	Description
	AntiVir Guard est activé

	AntiVir Guard est désactivé

L'icône de programme indique le statut du service AntiVir Guard.

Via le menu contextuel de l'icône de programme, les fonctions centrales de Avira AntiVir Professional sont rapidement accessibles. Pour accéder au menu contextuel, cliquez avec le bouton droit de la souris sur l'icône de programme.

Entrées dans le menu contextuel

- **Activer AntiVir Guard**: active ou désactive Avira AntiVir Guard.
- **Démarrer AntiVir**: ouvre le Control Center Avira AntiVir Professional.
- **Configurer AntiVir**: ouvre la Configuration Avira AntiVir Professional.
- **Lancer la mise à jour**: démarre une mise à jour.
- **Aide**: ouvre cette aide en ligne.
- **Avira sur Internet**: ouvre le portail Web de l'éditeur du logiciel AntiVir Professional sur Internet. La condition est de disposer d'un accès actif à Internet.

5.2 Comment procéder

5.2.1 Activer la licence

Voici comment activer la licence de AntiVir Professional :

Avec le fichier de licence hbedv.key, vous activez votre licence pour Avira AntiVir Professional. Vous recevez votre fichier de licence par Avira GmbH par email. Le fichier de licence contient la licence pour tous les produits que vous avez commandés.

Si vous n'avez pas encore installé Avira AntiVir Professional :

- ▶ Enregistrez le fichier de licence dans un répertoire local de votre ordinateur.
- ▶ installez Avira AntiVir Professional.
- ▶ Lors de l'installation, indiquez où vous avez enregistré le fichier de licence.

Si vous avez déjà installé Avira AntiVir Professional :

- ▶ Cliquez deux fois dans votre gestionnaire de fichiers ou dans l'email d'activation sur le fichier de licence et suivez les instructions à l'écran du gestionnaire de licences Avira AntiVir Professional qui s'ouvre.

  - OU -

- ▶ Dans le Control Center Avira AntiVir Professional, cliquez sur la rubrique Aide/Charger le fichier de licence....

Remarque
Sous Windows Vista, la fenêtre de dialogue de contrôle du compte d'utilisateur s'ouvre. Connectez-vous comme administrateur le cas échéant. Cliquez sur **Continuer**.

- ▶ Sélectionnez le fichier de licence et cliquez sur **Ouvrir**.

  Un message apparaît.

- ▶ Validez avec **OK**.

  La licence est activée.

- Redémarrez le système si nécessaire.

5.2.2 Actualiser Avira AntiVir Professional de manière automatisée

Remarque
Une tâche de mise à jour est préinstallée qui actualise Avira AntiVir Professional toutes les 60 minutes en présence d'une connexion Internet, ainsi qu'à l'établissement d'une connexion Internet.

Voici comment créer une tâche d'actualisation automatisée de Avira AntiVir Professional avec Planificateur AntiVir :

- Dans le Control Center, sélectionnez la rubrique **Administration :: Planificateur**.
- Cliquez sur le symbole  *Créer une nouvelle tâche avec l'assistant*.

  La fenêtre de dialogue *Nom et description de la tâche* apparaît.
- Nommez la tâche et décrivez-la si besoin est.
- Cliquez sur **Suivant**.

  La fenêtre de dialogue *Type de tâche* s'affiche.
- Sélectionnez **Tâche de mise à jour** dans la liste de sélection.
- Cliquez sur **Suivant**.

  La fenêtre de dialogue *Point de démarrage de la tâche* s'affiche.
- Sélectionnez quand la mise à jour doit être effectuée :
  - **Immédiatement**
  - **Tous les jours**
  - **Toutes les semaines**
  - **Par intervalle**
  - **Une fois**
  - **Connexion**

Remarque
Nous conseillons vivement d'actualiser Avira AntiVir Professional régulièrement et souvent, par ex. toutes les 60 minutes.

- Le cas échéant, saisissez la date selon votre sélection.
- Le cas échéant, sélectionnez des options supplémentaires (disponibles en fonction du type de tâche) :
  - **Démarrer la tâche en plus à chaque connexion à Internet**

    Outre la fréquence définie, la tâche est exécutée à chaque démarrage d'une connexion Internet.
  - **Rattraper la tâche quand la date est déjà passée**

    Le programme effectue les tâches situées dans le passé qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.
- Cliquez sur **Suivant**.

  La fenêtre de dialogue *Sélection du mode d'affichage* apparaît.
- Sélectionnez le mode d'affichage de la fenêtre de tâche :
  - **Réduit** : uniquement la barre de progression

- **Agrandi** : fenêtre de tâche intégrale
- **Invisible** : pas de fenêtre de tâche

▶ Cliquez sur **Terminer**.

La tâche que vous venez de créer apparaît comme activée (cochée) sur la page d'accueil de la rubrique **Administration ::Contrôler**.

▶ Désactivez éventuellement les tâches qui ne doivent pas être exécutées.

Les symboles suivants vous permettent de continuer à éditer les tâches :

 Afficher les caractéristiques d'une tâche

 Modifier la tâche

 Supprimer la tâche

 Démarrer la tâche

 Arrêter la tâche

5.2.3 Démarrer manuellement une mise à jour

Vous avez différentes possibilités de démarrer manuellement une mise à jour de Avira AntiVir Professional : Dans le cas d'une mise à jour démarrée manuellement, une mise à jour du fichier de définitions des virus et du moteur de recherche est effectuée systématiquement. Une mise à jour n'est effectuée que si vous activez l'option **Télécharger et installer automatiquement les mises à jour** dans la configuration sous Généralités :: Mise à jour.

Voici comment démarrer manuellement une mise à jour de Avira AntiVir Professional :

▶ Cliquez avec le bouton droit de la souris sur l'icône de programme Avira AntiVir Professional dans la barre des tâches.

Un menu contextuel s'affiche.

▶ Sélectionnez **Lancer la mise à jour**.

La fenêtre de dialogue *Avira AntiVir Professional Updaterr* apparaît.

- OU -

▶ Dans le Control Center, sélectionnez la rubrique**Aperçu :: État**.

▶ Dans la zone *Dernière mise à jour*, cliquez sur le lien **Lancer la mise à jour**.

La fenêtre de dialogue Avira AntiVir Professional Updaterr apparaît.

- OU -

▶ Dans le Control Center, sélectionnez la rubrique *Démarrer la mise à jour* dans le menu **Mise à jour**.

La fenêtre de dialogue Avira AntiVir Professional Updaterr apparaît.

Remarque
Nous conseillons vivement d'actualiser Avira AntiVir Professional régulièrement de manière automatisée, par ex. toutes les 60 minutes.

Remarque
Voici comment vous pouvez effectuer une mise à jour manuelle directement via le Centre de sécurité Windows.

5.2.4 Recherche directe : chercher des virus et logiciels malveillants avec un profil de recherche

Un profil de recherche est un regroupement de lecteurs et répertoires à parcourir.

Vous avez la possibilité suivante pour chercher via un profil de recherche :

– Utiliser un profil de recherche prédéfini

Si les profils de recherche prédéfinis répondent à vos besoins.

– Ajuster et utiliser le profil de recherche (sélection manuelle)

Si vous souhaitez chercher avec un profil de recherche individualisé.

– Créer et utiliser un nouveau profil de recherche

Si vous souhaitez créer votre propre profil de recherche.

En fonction du système d'exploitation, divers symboles sont disponibles pour le démarrage d'un profil de recherche :

– Sous Windows XP et 2000 :

À l'aide de ce symbole, vous démarrez la recherche d'un profil de recherche.

– Sous Windows Vista :

Sous Microsoft Windows Vista, le Centre de contrôle n'a d'abord que des droits restreints, par ex. pour l'accès aux répertoires et fichiers. Le Centre de contrôle ne peut exécuter certaines actions et accès aux fichiers qu'avec des droits d'administrateur étendus. Ces droits d'administrateur étendus doivent être attribués à chaque démarrage d'une recherche via un profil de recherche.

À l'aide de ce symbole, vous démarrez une recherche limitée d'un profil de recherche. Seuls les répertoires et fichiers pour lesquels Windows Vista a attribué les droits d'accès sont parcourus.

À l'aide de ce symbole, vous démarrez la recherche avec des droits d'administrateur étendus. Après confirmation, tous les répertoires et fichiers dans le profil de recherche sélectionné sont parcourus.

Voici comment chercher des virus et logiciels malveillants avec un profil de recherche :

▶ Dans le Control Center, sélectionnez la rubrique **Protection locale :: Contrôler**.

Les profils de recherche prédéfinis apparaissent.

▶ Sélectionnez l'un des profils de recherche prédéfinis.

-OU-

▶ Ajustez le profil de recherche *Sélection manuelle*.

-OU-

▶ Créez un nouveau profil de recherche

- Cliquez sur le symbole (Windows XP :  ou Windows Vista : ).
- La fenêtre *Luke Filewalker* apparaît et la recherche directe démarre.

  A la fin du processus de recherche, les résultats s'affichent.

Si vous souhaitez ajuster un profil de recherche :

- Déployez dans le profil de recherche **Sélection manuelle** l'arborescence des fichiers de manière que tous les lecteurs et répertoires à contrôler soient ouverts.
  - Clic sur le signe **+** : le niveau de répertoire suivant s'affiche.
  - Clic sur le signe **-** : le niveau de répertoire suivant est masqué.
- Sélectionnez les nœuds et répertoires à contrôler en cliquant une fois dans la case correspondante du niveau de répertoire concerné.

  Vous avez les possibilités suivantes pour sélectionner des répertoires :
  - Répertoire avec ses sous-répertoires (coche noire)
  - Répertoire sans les sous-répertoires (coche verte)
  - Uniquement les sous-répertoires d'un répertoire (coche grise, les sous-répertoires ont une coche noire)
  - Aucun répertoire (pas de coche)

Si vous souhaitez créer un nouveau profil de recherche :

- Cliquez sur le symbole  **Créer un nouveau profil.**

  Le profil *Nouveau profil* apparaît sous les profils existants.
- Renommez le profil de recherche si nécessaire, en cliquant sur le symbole 
- Sélectionnez les nœuds et répertoires à contrôler en cliquant une fois dans la case du niveau de répertoire concerné.

  Vous avez les possibilités suivantes pour sélectionner des répertoires :
  - Répertoire avec ses sous-répertoires (coche noire)
  - Répertoire sans les sous-répertoires (coche verte)
  - Uniquement les sous-répertoires d'un répertoire (coche grise, les sous-répertoires ont une coche noire)
  - Aucun répertoire (pas de coche)

5.2.5 Recherche directe : chercher des virus et logiciels malveillants par glisser&déplacer

Voici comment chercher par glisser&déplacer des virus et logiciels malveillants de manière ciblée :

Le Control Center Avira AntiVir Professional est ouvert.

- Sélectionnez le fichier ou le répertoire, qui doit être contrôlé.
- Glissez avec le bouton gauche de la souris le fichier ou le répertoire sélectionné dans le *Control Center*.

  La fenêtre *Luke Filewalker* apparaît et la recherche directe démarre.

  A la fin du processus de recherche, les résultats s'affichent.

5.2.6 Recherche directe : chercher des virus et logiciels malveillants via le menu contextuel

Voici comment chercher via le menu contextuel des virus et logiciels malveillants de manière ciblée :

- Cliquez (par ex. dans l'explorateur Windows, sur le bureau ou dans un répertoire Windows ouvert) avec le bouton droit de la souris sur le fichier ou le répertoire que vous souhaitez contrôler.

  Le menu contextuel de l'explorateur Windows apparaît.

- Dans le menu contextuel, sélectionnez **Contrôler les fichiers sélectionnés avec AntiVir**.

  La fenêtre *Luke Filewalker* apparaît et la recherche directe démarre.

  A la fin du processus de recherche, les résultats s'affichent.

5.2.7 Recherche directe : recherche automatisée de virus et logiciels malveillants

Voici comment créer une tâche de recherche automatisée des virus et logiciels malveillants :

- Dans le Control Center, sélectionnez la rubrique **Administration :: Planificateur**.
- Cliquez sur le symbole 

  La fenêtre de dialogue *Nom et description de la tâche* apparaît.

- Nommez la tâche et décrivez-la si besoin est.
- Cliquez sur **Suivant**.

  La fenêtre de dialogue *Type de tâche* apparaît.

- Sélectionnez la **tâche de contrôle**.
- Cliquez sur **Suivant**.

  La fenêtre de dialogue *Sélection du profil* apparaît.

- Choisissez le profil qui doit être contrôlé.
- Cliquez sur **Suivant**.

  La fenêtre de dialogue *Point de démarrage de la tâche* s'affiche.

- Sélectionnez quand la recherche doit être effectuée :
  - **Immédiatement**
  - **Tous les jours**
  - **Toutes les semaines**
  - **Par intervalle**
  - **Une fois**
  - **Connexion**
- Le cas échéant, saisissez la date selon votre sélection.
- Sélectionnez le cas échéant l'option supplémentaire suivante (disponible en fonction du type de tâche) :
  - **Rattraper la tâche quand la date est déjà passée**

Le programme effectue les tâches situées dans le passé qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.

- Cliquez sur **Suivant**.

  La fenêtre de dialogue *Sélection du mode d'affichage* apparaît.

- Sélectionnez le mode d'affichage de la fenêtre de tâche :
  - **Réduit** : uniquement la barre de progression
  - **Agrandi** : fenêtre de tâche intégrale
  - **Invisible** : pas de fenêtre de tâche
- Cliquez sur **Terminer**.

  La tâche que vous venez de créer apparaît comme activée (cochée) sur la page d'accueil de la rubrique *Administration :: Planificateur*.

- Désactivez éventuellement les tâches qui ne doivent pas être exécutées.

Les symboles suivants vous permettent de continuer à éditer les tâches :

 Afficher les caractéristiques d'une tâche

 Modifier la tâche

 Supprimer la tâche

 Démarrer la tâche

 Arrêter la tâche

5.2.8 Recherche directe : chercher les rootkits actifs de manière ciblée

Pour rechercher les rootkits actifs, utilisez le profil de recherche prédéfini *Recherche des rootkits*.

Voici comment rechercher les rootkits actifs de manière ciblée :

- Dans le Control Center, sélectionnez la rubrique **Protection locale :: Contrôler**.

  Les profils de recherche prédéfinis apparaissent.

- Sélectionnez le profil de recherche prédéfini **Recherche de rootkits**.
- Sélectionnez les éventuels autres nœuds et répertoires à contrôler en cliquant une fois dans la case du niveau de répertoire concerné.
- Cliquez sur le symbole (Windows XP :  ou Windows Vista : ).

  La fenêtre *Luke Filewalker* apparaît et la recherche directe démarre.

  A la fin du processus de recherche, les résultats s'affichent.

5.2.9 Réagir aux virus et logiciels malveillants détectés

Pour les divers composants de protection de AntiVir Professional, vous pouvez régler sous la rubrique *Action en cas de résultat positif* de la configuration, comment AntiVir Professional doit réagir en cas de détection d'un virus ou d'un programme indésirable :

Options disponibles pour le Scanner :

– **Interactif**

En mode d'action interactif, les résultats positifs de la recherche du Scanner sont signalés dans une fenêtre de dialogue. Ce réglage est activé par défaut.
Lors de la recherche de **rootkits**, **de virus de secteurs d'amorçage** et du **contrôle de processus actifs**, une fenêtre de dialogue s'affiche vous permettant de sélectionner l'action à effectuer avec l'objet affecté.
Lors de la **recherche de fichiers**, la notification et la possibilité de sélection du traitement des fichiers affectés dépendent du mode de notification choisi :
Mode de notification : combiné

En mode de notification combiné, vous recevez à l'issue de la recherche de fichiers, un message d'avertissement comportant une liste des fichiers contaminés qui ont été trouvés. Aucune possibilité de sélection n'est disponible pour le traitement des fichiers affectés. Vous pouvez exécuter l'action par défaut du Scanner pour tous les fichiers contaminés ou interrompre le Scanner. L'action par défaut du Scanner concernant le traitement des fichiers contaminés consiste à déplacer le fichier contaminé en quarantaine.

Mode de notification : combiné (expert)

En mode de notification expert, vous recevez à l'issue de la recherche de fichiers, un message d'avertissement comportant une liste des fichiers contaminés qui ont été trouvés. Vous avez la possibilité de sélectionner une action à exécuter pour les différents fichiers contaminés, via le menu contextuel. Vous pouvez exécuter les actions choisies pour tous les fichiers contaminés ou quitter le Scanner.

Mode de notification : individuel

En mode de notification individuel, chaque résultat positif de virus est signalé dans une fenêtre séparée lors de la recherche de fichiers. Vous pouvez sélectionner dans la fenêtre de dialogue ce qui doit advenir du fichier contaminé.

– **Automatique**

En mode d'action automatique, l'action que vous avez choisie dans cette zone est exécutée automatiquement en cas de détection d'un virus ou d'un programme indésirable. Si l'option *Afficher le message d'avertissement* est activée, vous recevez un message d'avertissement affichant l'action exécutée, en cas de détection d'un virus.

Options disponibles pour le Guard, MailGuard, WebGuard :

– **Interactif**

En mode d'action interactif, une fenêtre de dialogue s'affiche en cas de détection d'un virus ou d'un programme indésirable, vous permettant de choisir ce qu'il doit advenir de l'objet contaminé. Ce réglage est activé par défaut.

– **Automatique**

En mode d'action automatique, l'action que vous avez choisie dans cette zone est exécutée automatiquement en cas de détection d'un virus ou d'un programme indésirable. Si l'option *Afficher le message d'avertissement* est activée, vous recevez un message d'avertissement affichant l'action exécutée, en cas de détection d'un virus.

En mode d'action interactif, vous réagissez aux virus et programmes indésirables détectés en sélectionnant dans le message d'avertissement une action pour les objets contaminés et en exécutant l'action choisie par votre validation. Les actions suivantes de traitement des objets contaminés sont disponibles :

Remarque
Les actions disponibles à la sélection dépendent du système d'exploitation, du composant de protection (AntiVir Guard, AntiVir Scanner, AntiVir MailGuard, AntiVir WebGuard) qui signale le résultat positif et du logiciel malveillant détecté.

Actions du Scanner et du Guard .

– **Réparer**

Le fichier est réparé.

Cette option n'est activable que si une réparation du fichier trouvé est possible.

– **Déplacer en quarantaine**

Le fichier est compressé dans un format spécial (*.*qua*) et déplacé dans le répertoire de quarantaine *INFECTED* sur votre disque dur pour empêcher tout accès direct. Les fichiers de ce répertoire peuvent ensuite être réparés en quarantaine ou - si nécessaire - envoyés à Avira GmbH.

– **Supprimer**

Le fichier est supprimé, mais peut être restauré avec les outils adéquats (par ex. *Avira UnErase*). Ceci permet de retrouver la signature du virus. Cette procédure est beaucoup plus rapide que *Écraser et supprimer* Si le résultat positif est un virus de secteur d'amorçage, le secteur d'amorçage est effacé en cas de suppression. Un nouveau secteur d'amorçage est écrit.

– **Ecraser et supprimer**

Le fichier est écrasé par un modèle standard puis supprimé. Il ne peut plus être restauré.

– **Renommer**

Le fichier est renommé en *.*vir*. Un accès direct à ces fichiers (en cliquant deux fois par ex.) n'est alors plus possible. Les fichiers peuvent être réparés et renommés ultérieurement.

– **Ignorer**

Avira AntiVir Professional n'effectue aucune autre action. Le fichier touché reste actif sur votre ordinateur.

Avertissement
Risque de perte de données et de dommages sur le système d'exploitation ! Utilisez l'option *Ignorer* uniquement dans des cas exceptionnels le justifiant.

– **Refuser l'accès**

Option d'action en cas de résultats positifs du Guard : l'accès au fichier contaminé est bloqué. Le résultat positif est uniquement entré dans le fichier rapport (si la fonction de rapport est activée).

– **Copier dans la quarantaine**

Option d'action en cas de détection d'un rootkit : le résultat positif est copié en quarantaine.

– **Quitter le programme**

Option d'action en cas de détection d'un processus suspect : le processus est arrêté. Une autre fenêtre de dialogue s'ouvre dans laquelle vous pouvez sélectionner ce qui doit advenir du fichier exécutable.

Actions du MailGuard : Emails entrants

– **Déplacer en quarantaine**

L'email, y compris toutes les pièces jointes, est déplacé en quarantaine. L'email touché est supprimé. Le corps et les pièces jointes éventuelles de l'email sont remplacés par un texte standard.

– **Supprimer**

L'email touché est supprimé. Le corps et les pièces jointes éventuelles sont remplacés par un texte standard.

– **Supprimer la pièce jointe**

La pièce jointe contaminée est remplacée par un texte standard. Si le corps de l'email est touché, celui-ci est supprimé et également remplacé par un texte standard. L'email lui-même est délivré.

– **Déplacer la pièce jointe en quarantaine**

La pièce jointe concernée est placée en quarantaine puis supprimée (remplacée par un texte standard). Le corps de l'email est délivré. La pièce jointe touchée peut être délivrée plus tard par le gestionnaire de quarantaines.

– **Ignorer**

L'email concerné est livré.

Avertissement
Ce faisant, il est possible que des virus et programmes indésirables arrivent sur votre ordinateur. Sélectionnez l'option **Ignorer** uniquement dans des cas exceptionnels le justifiant. Désactivez l'aperçu dans Microsoft Outlook, n'ouvrez pas les pièces jointes par double-clic !

Actions du MailGuard : Emails sortants

– **Déplacer l'email en quarantaine (ne pas envoyer)**

L'email, y compris toutes les pièces jointes, sont copiés dans la quarantaine et ne sont pas envoyés. L'email reste dans la boîte d'envoi de votre client email. Vous recevez un message d'erreur dans votre programme email. Cet email subit un contrôle de recherche de logiciels malveillants à chaque processus d'envoi ultérieur de votre compte email.

– **Bloquer l'envoi d'emails (ne pas envoyer)**

L'email n'est pas envoyé et reste dans la boîte d'envoi de votre client email. Vous recevez un message d'erreur dans votre programme email. Cet email subit un contrôle de recherche de logiciels malveillants à chaque processus d'envoi ultérieur de votre compte email.

– **Ignorer**

L'email concerné est envoyé.

Avertissement
Ce faisant, il est possible que des virus et programmes indésirables arrivent sur l'ordinateur du destinataire de l'email.

Actions du WebGuard :

– **Refuser l'accès**

La page Web demandée par le serveur Web ou les données et fichiers transmis ne sont pas envoyés à votre navigateur Web. Dans le navigateur Web, un message d'erreur de refus d'accès s'affiche.

– **Déplacer en quarantaine**

La page Web demandée par le serveur Web ou les données et fichiers transmis sont déplacés en quarantaine. Le fichier peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou - si nécessaire - être envoyé à Avira Malware Research Center.

– **Ignorer**

La page Web demandée par le serveur Web ou les données et fichiers transmis sont envoyés à votre navigateur Web par le WebGuard.

Avertissement
Ce faisant, il est possible que des virus et programmes indésirables arrivent sur votre ordinateur. Sélectionnez l'option **Ignorer** uniquement dans des cas exceptionnels le justifiant.

Remarque
Nous conseillons de déplacer en quarantaine un fichier suspect qui ne peut être réparé.

Remarque
Envoyez-nous aussi les fichiers annoncés par l'heuristique pour analyse.
Vous pouvez charger ces fichiers sur notre site Web par ex.
:http://analysis.avira.com/samples/?lang=fr
Les fichiers signalés par l'heuristique sont reconnaissables à la désignation *HEUR/* ou *HEURISTIC/* qui précède le nom du fichier, par ex. : *HEUR/fichier_test.**.

5.2.10 Quarantaine : manipuler les fichiers (*.qua) en quarantaine

Voici comment manipuler les fichiers en quarantaine :

- Dans le Control Center, sélectionnez la rubrique **Administration :: Quarantaine**.
- Vérifiez de quels fichiers il s'agit pour pouvoir charger les originaux d'un autre emplacement sur votre ordinateur le cas échéant.

Si vous souhaitez afficher des informations plus détaillées sur un fichier :

- Sélectionnez le fichier et cliquez sur 

La fenêtre de dialogue *Caractéristiques* avec d'autres informations sur le fichier apparaît.

Si vous souhaitez à nouveau contrôler un fichier :

La vérification d'un fichier est recommandée quand le fichier de définitions des virus a été actualisé par Avira AntiVir Professional et qu'il y a un doute de fausse alerte. Voici comment confirmer une fausse alerte lors du nouveau contrôle et restaurer le fichier.

- Sélectionnez le fichier et cliquez sur 

L'absence de virus et logiciels malveillants est contrôlée sur le fichier avec les réglages de la recherche directe.

Après le contrôle, le dialogue *Statistiques de contrôle* s'affiche avec les statistiques sur l'état du fichier avant et après le deuxième contrôle.

Si vous souhaitez supprimer un fichier :

- Sélectionnez le fichier et cliquez sur 

Si vous souhaitez télécharger le fichier sur un serveur web de l'Avira Malware Research Center en vue d'une analyse :

- Sélectionnez le fichier que vous souhaitez télécharger.
- Cliquez sur 

  Une boîte de dialogue s'ouvre, contenant un formulaire pour la saisie de vos coordonnées.
- Entrez tous les données.
- Sélectionnez un type : **Fichier suspect** ou **Fausse alerte**.
- Appuyez sur **OK.**

  Le fichier est téléchargé sur un serveur web de l'Avira Malware Research Center.

Remarque
Une analyse par Avira Malware Research Center est recommandée dans les cas suivants :
Résultat heuristique (fichier suspect) : lors d'une recherche, un fichier a été classé comme suspect par AntiVir Professional et déplacé en quarantaine : L'analyse du fichier par Avira Malware Research Center a été conseillée dans la fenêtre de dialogue du résultat positif de virus ou dans le fichier de rapport de la recherche.
Fichier suspect : vous considérez un fichier comme suspect et l'avez de ce fait ajouté à la quarantaine, mais le contrôle du fichier quant à la présence de virus et de logiciels malveillants est négatif.
Fausse alerte : vous partez du principe qu'un résultat positif de virus est en fait une fausse alerte : AntiVir Professional signale un résultat positif dans un fichier qui toutefois, n'est très vraisemblablement pas contaminé par un logiciel malveillant.

Remarque
La taille des fichiers que vous téléchargez est limitée à 20 Mo au format non compressé ou à 8 Mo en format compressé.

Remarque
Vous pouvez télécharger simultanément plusieurs fichiers en sélectionnant tous les fichiers que vous souhaitez télécharger, puis en cliquant sur le bouton **Envoyer l'objet**.

Vous pouvez aussi restaurer les fichiers en quarantaine :

- voir le chapitre : Quarantaine : restaurer les fichiers en quarantaine

5.2.11 Quarantaine : restaurer les fichiers dans la quarantaine

En fonction du système d'exploitation, divers symboles sont disponibles pour la restauration :

- Sous Windows XP et 2000 :

Ce symbole vous permet de restaurer les fichiers dans le répertoire d'origine.

Ce symbole vous permet de restaurer des fichiers dans un répertoire de votre choix.

- Sous Windows Vista :

Sous Microsoft Windows Vista, le Centre de contrôle n'a d'abord que des droits restreints, par ex. pour l'accès aux répertoires et fichiers. Le Centre de contrôle ne peut exécuter certaines actions et accès aux fichiers qu'avec des droits d'administrateur étendus. Ces droits d'administrateur étendus doivent être attribués à chaque démarrage d'une recherche via un profil de recherche.

Ce symbole vous permet de restaurer des fichiers dans un répertoire de votre choix.

Ce symbole vous permet de restaurer les fichiers dans le répertoire d'origine. Si des droits d'administrateur sont nécessaires pour accéder à ce répertoire, une demande s'affiche.

Voici comment restaurer les fichiers en quarantaine :

Avertissement
Risque de perte de données et de dommages sur le système d'exploitation ! N'utilisez la fonction *Restaurer l'objet sélectionné* que dans les cas exceptionnels. Assurez-vous de ne restaurer que les fichiers qui ont pu être nettoyés au cours d'une nouvelle recherche.

Fichier recontrôlé par une recherche et réparé.

- Dans le Control Center, sélectionnez la rubrique **Administration :: Quarantaine**.

Remarque
Les emails et pièces jointes d'emails peuvent être restaurés uniquement avec l'option  et avec l'extension **.eml*.

Si vous souhaitez restaurer un fichier à son emplacement d'origine :

- Sélectionnez le fichier et cliquez sur le symbole (Windows 2000/XP :  , Windows Vista ).

  Cette option n'est pas disponible pour les emails.

Remarque
Les emails et pièces jointes d'emails peuvent être restaurés uniquement avec l'option  et avec l'extension **.eml*.

Le système vous demande si vous souhaitez restaurer le fichier.

- Cliquez sur **Oui**.

Le fichier est restauré dans le répertoire à partir duquel il avait été placé en quarantaine.

Si vous souhaitez restaurer un fichier dans un répertoire particulier :

- Sélectionnez le fichier et cliquez sur 

  Le système vous demande si vous souhaitez restaurer le fichier.

- Cliquez sur **Oui**.

  La fenêtre standard Windows pour sélectionner un répertoire apparaît.

- Sélectionnez le répertoire dans lequel le fichier doit être restauré et validez.

  Le fichier est restauré dans le répertoire choisi.

5.2.12 Quarantaine : déplacer un fichier suspect en quarantaine

Vous pouvez déplacer manuellement un fichier suspect en quarantaine :

- Dans le Control Center, sélectionnez la rubrique **Administration :: Quarantaine**.
- Cliquez sur 

La fenêtre standard Windows pour sélectionner un fichier apparaît.

- Choisissez un fichier et validez.

  Le fichier est déplacé en quarantaine.

Vous pouvez contrôler les fichiers en quarantaine avec AntiVir Scanner :

- voir Chapitre : Quarantaine : manipuler les fichiers (*.qua) en quarantaine

5.2.13 Profil de recherche : compléter ou supprimer un type de fichier dans un profil de recherche

Voici comment établir pour un profil de recherche que des types de fichiers supplémentaires doivent être parcourus ou que certains types de fichiers doivent être exclus de la recherche (possible uniquement en cas de sélection manuelle et de profils de recherche définis par l'utilisateur) :

Vous vous trouvez dans le Control Center sous la rubrique **Protection locale :: *Contrôler***.

- Cliquez avec le bouton droit de la souris sur le profil de recherche que vous souhaitez éditer.

  Un menu contextuel s'affiche.

- Sélectionnez l'entrée **Filtre de fichiers**.
- Déployez le menu contextuel en cliquant sur le petit triangle à droite du menu contextuel.

  Les entrées *Standard*, *Contrôler tous les fichiers* et *Personnalisé* apparaissent.

- Sélectionnez l'entrée **Personnalisé**.

La fenêtre de dialogue *Extensions de fichiers* s'affiche avec une liste de tous les types de fichiers qui sont parcourus avec le profil de recherche.

Si vous voulez exclure un type de fichier de la recherche :

- Sélectionnez le type de fichier et cliquez sur **Supprimer**.

Si vous voulez ajouter un type de fichier à la recherche :

- Sélectionnez le type de fichier.
- Cliquez sur **Ajouter** et saisissez l'extension de fichier du type de fichier dans le champ de saisie.

  Utilisez au maximum 10 caractères et ne tapez pas le point initial. Les caractères de remplacement (* et ?) sont autorisés.

5.2.14 Profil de recherche : créer un lien sur le Bureau pour le profil de recherche

Le lien sur le Bureau vers un profil de recherche vous permet de démarrer une recherche directe depuis votre Bureau, sans accéder au Control Center Avira AntiVir Professional.

Voici comment créer un lien vers le profil de recherche sur le Bureau :

Vous vous trouvez dans le Control Center sous la rubrique **Protection locale :: *Contrôler***.

- Sélectionnez le profil de recherche vers lequel vous souhaitez créer un lien.
- Cliquez sur le symbole 

Le lien est créé sur le bureau.

5.2.15 Evénements: Filtrer les événements

Dans le Control Center, sont affichés sous **Aperçu :: Evénements**, les événements qui ont été créés par les composants du programme AntiVir Professional. (de manière analogue à l'affichage des événements de votre système d'exploitation Windows). Les composants de programmes sont :

- Updater
- Guard
- MailGuard
- Scanner
- Planificateur

Les types d'événements suivants s'affichent :

- Information
- Avertissement
- Erreur
- Résultat positif

Voici comment filtrer les événements affichés :

- Dans le Control Center, sélectionnez la rubrique **Aperçu :: Événements**.
- Cochez la case des composants de programme pour afficher les événements des composants activés.

  - OU -

  Décochez la case des composants de programme pour masquer les événements des composants désactivés.

- Cochez la case des types d'événements pour afficher ces événements.

  - OU -

  Décochez la case des types d'événements pour masquer ces événements.

5.2.16 MailGuard: Exclure des adresses email de la vérification

Voici comment exclure des adresses email (expéditeur) de la vérification par le MailGuard (mise sur liste blanche) :

- Dans le Control Center, choisissez la rubrique **Protection en ligne :: MailGuard**.

  Vous voyez dans la liste les emails reçus.

- Sélectionnez l'email que vous souhaitez exclure de la vérification du MailGuard.
- Cliquez sur le symbole souhaité pour exclure l'email de la vérification par le MailGuard :

  L'adresse email sélectionnée ne sera plus contrôlée à l'avenir, quant à l'absence de virus et de programmes indésirables.

  L'adresse email de l'expéditeur est ajoutée à la liste d'exceptions et n'est plus

contrôlée quant à l'absence de virus et de logiciels malveillants .

Avertissement
N'excluez de la vérification par le MailGuard que les adresses emails absolument dignes de confiance.

Remarque
Dans la configuration sous MailGuard :: Généralités :: Exceptions, vous pouvez ajouter des adresses email à la liste des exclusions ou supprimer des adresses email de la liste des exclusions.

6 Scanner

Grâce au composant Scanner, vous pouvez rechercher de manière ciblée les virus et programmes indésirables (recherche directe). Vous avez les possibilités suivantes pour rechercher des fichiers contaminés :

- **Recherche directe via le menu contextuel**
  La recherche directe via le menu contextuel (bouton droit de la souris - entrée **Contrôler les fichiers sélectionnés avec AntiVir**) est recommandée si vous voulez contrôler des fichiers et répertoires séparément dans l'explorateur Windows par exemple. Un autre avantage est qu'il n'est pas nécessaire de démarrer le Control Center Avira AntiVir Professional pour la recherche directe via le menu contextuel.
- **Recherche directe via la commande glisser & déplacer**
  En glissant un fichier ou un répertoire dans la fenêtre de programme du Control Center Avira AntiVir Professional, le Scanner contrôle le fichier ou le répertoire, ainsi que tous les sous-répertoires inclus. Cette procédure est recommandée si vous souhaitez contrôler des fichiers et répertoires séparément, que vous avez par ex. déposés sur votre bureau.
- Recherche directe via les profils
  Cette procédure est recommandée si vous souhaitez contrôler régulièrement certains répertoires et lecteurs (par ex. votre répertoire de travail ou les lecteurs sur lesquels vous déposez régulièrement des fichiers). Il n'est alors plus nécessaire de sélectionner ces répertoires et lecteurs à chaque contrôle, il suffit d'une simple sélection avec le profil correspondant.
- **Recherche directe via le Planificateur**
  Le Planificateur offre la possibilité de faire effectuer des tâches de contrôle programmées dans le temps.

Des procédures particulières sont nécessaires lors de la recherche de rootkits, de virus de secteurs d'amorçage et du contrôle de processus actifs. Vous disposez des options suivantes :

- Recherche de rootkits via le profil de recherche *Recherche de rootkits*
- Contrôle des processus actifs via le profil de recherche **Processus actifs**
- Recherche de virus de secteurs d'amorçage via la commande **Contrôler les virus de secteurs d'amorçage** dans le menu **Outils**

7 Mises à jour

L'efficacité d'un logiciel anti-virus dépend de la mise à jour du programme, et tout particulièrement celle du fichier de définitions des virus et du moteur de recherche. Le composant Updater est intégré dans AntiVir Professional pour l'exécution des mises à jour. L'Updater garantit que Avira AntiVir Professional fonctionne toujours au niveau le plus récent et qu'il est en mesure de détecter les nouveaux virus apparaissant chaque jour. L'Updater met à jour les composants suivants :

- Fichier de définitions des virus :

  Le fichier de définitions des virus contient un modèle de détection des programmes malveillants que AntiVir Professional utilise lors de la recherche de virus et de logiciels malveillants, ainsi que pour réparer les objets infectés.

- Moteur de recherche :

  Le moteur de recherche contient des méthodes à l'aide desquelles AntiVir Professional recherche des virus et logiciels malveillants.

- Fichiers programme (mise à jour produit) :

  Les paquets pour les mises à jour produit offrent des fonctions supplémentaires pour les différents composants du programme.

Lors de l'exécution d'une mise à jour, on vérifie que le fichier de définitions des virus et le moteur de recherche sont actuels et ceux-ci sont mis à jour si nécessaire. Selon les réglages effectués dans la configuration, l'Updater effectue en outre une mise à jour produit ou vous informe des mises à jour produit disponibles. Il n'est pas nécessaire de redémarrer AntiVir Professional après une mise à jour.

Remarque
Pour des raisons de sécurité, Avira AntiVir Professional Updaterr contrôle si le fichier hôte Windows de votre ordinateur a été modifié, si l'URL de mise à jour de Avira AntiVir Professional a été manipulée par un logiciel malveillant par exemple et si Avira AntiVir Professional Updaterr a été redirigé sur des pages de téléchargement indésirables. Si le fichier hôte Windows a été manipulé, ceci est visible dans le fichier rapport de Avira AntiVir Professional Updaterr.

Dans le Control Center, sous le Planificateur, vous pouvez configurer des tâches de mise à jour qui seront exécutées par l'Updater aux intervalles indiqués. Une tâche de mise à jour est créée par défaut après l'installation de AntiVir Professional. Vous avez aussi la possibilité de démarrer manuellement une mise à jour :

- dans le Control Center : dans le menu Mise à jour et dans la rubrique État
- via le menu contextuel de l'icône de programme

Vous pouvez obtenir des mises à jour à partir d'Internet, via un serveur Web du fabricant ou bien via un serveur Web ou serveur de fichiers dans l'intranet qui télécharge des fichiers de mise à jour d'Internet et les met à disposition d'autres ordinateurs dans le réseau. Cette option est judicieuse si vous souhaitez mettre à jour AntiVir Professional sur plusieurs ordinateurs dans un même réseau. Grâce à la configuration d'un serveur de mise à jour, il est possible de garantir la mise à jour de AntiVir Professional sur tous les ordinateurs à protéger, sans utiliser trop de ressources.

Remarque
Vous pouvez utiliser AntiVir Internet Update Manager (serveur Web ou serveur de fichiers sous Windows) comme serveur Web ou serveur de fichiers dans l'Intranet. AntiVir Internet Update Manager reflète le serveur de téléchargement des produits Avira AntiVir (de AntiVir Professional entre autres) et peut être obtenu sur Internet à l’adresse suivante http://www.avira.com. Ils peuvent toutefois aussi mettre à jour AntiVir Professional sur les ordinateurs à protéger dans le réseau, par cascadage via un serveur de fichiers central dans l'intranet.

Le téléchargement se fait par protocole HTTP lors de l'utilisation d'un serveur Web. En cas d'utilisation d'un serveur de fichiers, l'accès aux fichiers de mise à jour se fait via le réseau. Vous pouvez configurer la connexion au serveur Web ou de fichiers dans la Configuration Avira AntiVir Professional sous Généralités :: Mise à jour. Pour la configuration standard, la connexion Internet existante est utilisée comme connexion aux serveurs Web de la société Avira GmbH.

8 FAQ, astuces

Dans ce chapitre, vous trouverez un récapitulatif des questions les plus fréquentes concernant Avira AntiVir Professional, l'aide en cas de problèmes ainsi que les trucs et astuces pour l'utilisation de Avira AntiVir Professional.

voir le chapitre Aide en cas de problème

voir le chapitre Commandes clavier

voir le chapitre Centre de sécurité Windows

8.1 Aide en cas de problème

Vous trouverez ici des informations sur les causes et solutions de problèmes possibles.

- Le message d'erreur Le fichier de licence ne s'ouvre pas s'affiche.
- AntiVir MailGuard ne fonctionne pas.
- Un email envoyé via une connexion TSL a été bloqué par le MailGuard.
- Le chat Internet ne fonctionne : les messages du chat ne s'affichent pas

Le message d'erreur *Le fichier de licence ne s'ouvre pas* apparaît.

Cause : le fichier est codé.

▶ Pour activer la licence, il n'est pas nécessaire d'ouvrir le fichier mais de l'enregistrer dans le répertoire de programmes de Avira AntiVir Professional. Voir également Gestion des licences Avira AntiVir Professional.

Le message d'erreur *L'établissement de la connexion a échoué lors du téléchargement du fichier...* apparaît lorsque vous essayez de démarrer une mise à jour.

Cause : votre connexion Internet est inactive. C'est pourquoi, Avira AntiVir Professional ne trouve pas le serveur Web sur Internet.

▶ Testez le fonctionnement d'autres services Internet comme WWW ou le courrier électronique. S'ils ne fonctionnent pas, restaurez la connexion Internet.

Cause : le serveur proxy n'est pas accessible.

▶ Contrôlez si les données de connexion au serveur proxy ont changé et adaptez votre configuration si nécessaire.

Cause : le fichier update.exe n'est pas intégralement autorisé par votre pare-feu personnel.

▶ Assurez-vous d'autoriser complètement le fichier update.exe auprès de votre pare-feu personnel.

Sinon :

▶ Contrôlez vos réglages dans la Configuration Avira AntiVir Professional (mode expert) sous Généralités :: Mise à jour Vos réglages.

Les virus et logiciels malveillants ne peuvent pas être déplacés ou effacés.

Cause : le fichier a été chargé par Windows et se trouve à l'état activé.

▶ Actualisez Avira AntiVir Professional.

▶ Si vous utilisez le système d'exploitation Windows XP, désactivez la restauration du système.

▶ Démarrez l'ordinateur en mode sécurisé.

▶ Démarrez Avira AntiVir Professional et la Configuration Avira AntiVir Professional (mode expert).

▶ Sélectionnez Scanner :: Recherche :: Fichiers :: Tous les fichiers et confirmez la fenêtre avec **OK**.

▶ Démarrez une recherche sur tous les lecteurs locaux.

▶ Démarrez l'ordinateur en mode normal.

▶ Effectuez une recherche en mode normal.

▶ Si aucun autre virus ni logiciel malveillant n'est détecté, activez la restauration du système si elle est disponible et doit être utilisée.

L'icône de programme indique un état de désactivation.

Cause : AntiVir Guard est désactivé.

▶ Dans le Control Center, cliquez sur le lien **Activer** dans la rubrique Aperçu :: État de la zone AntiVir Guard.

Cause : AntiVir Guard est bloqué par un pare-feu.

▶ Dans la configuration de votre pare-feu, définissez une autorisation générale pour AntiVir Guard. AntiVir Guard fonctionne uniquement avec l'adresse 127.0.0.1 (localhost). Aucune connexion à Internet n'est établie. La même chose s'applique à AntiVir MailGuard.

Sinon :

▶ Vérifiez le type de démarrage du service AntiVir Guard. Activez le service si nécessaire : sélectionnez dans la barre de démarrage "Démarrer | Panneau de configuration | Performances et maintenance". Démarrez le panneau de configuration "Services" en cliquant deux fois dessus (sous Windows 2000 et Windows XP, l'applet des services se trouve dans le sous-dossier "Outils d'administration"). Cherchez l'entrée "Avira AntiVir Guard". Le type de démarrage saisi doit être "Automatique" et l'état "Démarré". Démarrez le service manuellement si nécessaire en sélectionnant la ligne correspondante et le bouton "Démarrer". Si un message d'erreur s'affiche, contrôlez l'affichage de l'événement.

L'ordinateur devient très lent quand j'enregistre des données.

Cause : AntiVir Guard parcourt tous les fichiers avec lesquels la sauvegarde des données fonctionne lors du processus de sauvegarde.

▶ Sélectionnez dans la Configuration Avira AntiVir Professional (mode expert) Guard :: Recherche :: Exceptions et saisissez le nom du processus du logiciel de sauvegarde.

Mon pare-feu déclare AntiVir Guard et AntiVir MailGuard dès qu'ils sont activés.

Cause : la communication de AntiVir Guard et AntiVir MailGuard a lieu via le protocole Internet TCP/IP. Un pare-feu surveille toutes les connexions via ce protocole.

▶ Définissez une autorisation générale pour AntiVir Guard et AntiVir MailGuard. AntiVir Guard fonctionne uniquement avec l'adresse 127.0.0.1 (localhost). Aucune connexion à Internet n'est établie. La même chose s'applique à AntiVir MailGuard.

AntiVir MailGuard ne fonctionne pas.

Contrôlez la fonctionnalité de AntiVir MailGuard à l'aide des checklists suivantes, si des problèmes se produisent en combinaison avec AntiVir MailGuard.

Checklists

▶ Contrôlez si votre client de mail communique via IMAP avec le serveur mail. Ce protocole n'est pas pris en charge actuellement.

▶ Vérifiez si votre client de mail se connecte au serveur par Kerberos, APOP ou RPA. Ces méthodes d'identification ne sont pas prises en charge actuellement.

▶ Contrôlez si votre client de mail client se connecte au serveur par SSL (également appelé souvent TSL - Transport Layer Security). AntiVir MailGuard prend en charge SSL mais sans contrôler l'absence de virus et de programmes indésirables dans les emails codés. La condition est que la connexion a lieu via le port 995 et non via le port POP3 normal n° 110. Souvent, ce port est appelé "port alternatif" ou en anglais "alternate port". La plupart des serveurs d'email prend en charge le SSL via ce port également.

▶ Le service AntiVir MailGuard est-il activé ? Activez le service si nécessaire : sélectionnez dans la barre de démarrage "Démarrer | Panneau de configuration | Performances et maintenance". Démarrez le panneau de configuration "Services" en cliquant deux fois dessus (sous Windows 2000 et Windows XP, l'applet des services se trouve dans le sous-dossier "Outils d'administration"). Cherchez l'entrée "Avira AntiVir MailGuard". Le type de démarrage saisi doit être "Automatique" et l'état "Démarré". Démarrez le service manuellement si nécessaire en sélectionnant la ligne correspondante et le bouton "Démarrer". Si un message d'erreur s'affiche, contrôlez l'affichage de l'événement. Si cela ne résout pas le problème, désinstallez complètement Avira AntiVir Professional via "Démarrer | Panneau de configuration | Performances et maintenance | Logiciel", redémarrez l'ordinateur et réinstallez Avira AntiVir Professional.

Généralités

▶ AntiVir MailGuard ne prend pas actuellement en charge IMAP (Internet Message Access Protocol), ce qui signifie que si votre programme de messagerie électronique communique avec le serveur mail via ce protocole, vous n'êtes pas protégé des virus et programmes indésirables.

▶ Via SSL (Secure Sockets Layer), les connexions POP3 (appelées souvent TLS (Transport Layer Security)) ne peuvent pas être protégées actuellement et sont ignorées.

▶ L'identification lors de la connexion au serveur de messagerie électronique est actuellement prise en charge uniquement via des "mots de passe". "Kerberos" et "RPA" ne sont actuellement pas pris en charge.

▶ Avira AntiVir Professional ne contrôle pas l'absence de virus et de programmes indésirables lors de l'envoi d'emails.

Remarque
Nous vous recommandons d'effectuer régulièrement des mises à jour Microsoft pour combler des lacunes éventuelles dans la sécurité.

Un email envoyé via une connexion TSL a été bloqué par le MailGuard.

Cause : Transport Layer Security (TLS : protocole de cryptage pour la transmission de données par Internet) n'est actuellement pas pris en charge par le MailGuard. Vous disposez des possibilités suivantes pour envoyer l'email :

- Utilisez un autre port que le port 25 utilisé par SMTP. Vous contournerez ainsi la surveillance du MailGuard
- Renoncez à utiliser la connexion cryptée TSL et désactivez la prise en charge TSL de votre client email.
- Désactivez (provisoirement) la surveillance des emails sortants par le MailGuard dans la configuration sous MailGuard::Recherche.

Le chat Internet ne fonctionne : les messages du chat ne s'affichent pas, des données sont chargées dans le navigateur.

Ce phénomène peut se produire dans les chats basés sur le protocole HTTP avec 'transfer-encoding= chunked'.

Cause : le WebGuard contrôle d'abord intégralement l'absence de virus et de programmes indésirables sur les données envoyées avant de charger celles-ci dans le navigateur Internet. Lors d'un transfert de données avec ’r;transfer-encoding= chunked', le WebGuard ne peut pas déterminer la longueur des messages ou la quantité de données.

- Indiquez l'URL du chat Internet comme exception dans la configuration (voir Configuration Avira AntiVir Professional: WebGuard::Exceptions).

8.2 Commandes clavier

Les commandes clavier - aussi appelées raccourcis clavier - permettent de naviguer dans Avira AntiVir Professional, d'accéder à divers modules et de démarrer des actions rapidement.

Ci-après une vue d'ensemble des commandes clavier disponibles dans Avira AntiVir Professional. Le chapitre correspondant de l'aide vous donne plus d'informations sur les fonctionnalités et la disponibilité de ces commandes.

8.2.1 Dans les champs de dialogue

Commande clavier	Description
Ctrl + Tab Ctrl + PgDn	Passer à la rubrique suivante.
Ctrl + Shift + Tab Ctrl + PgUp	Passer à la rubrique précédente.

Tab	Passer à l'option suivante ou au groupe d'options suivant.
Shift + Tab	Passer à l'option précédente ou au groupe d'options précédent.
← ↑ → ↓	Changer d'option dans un champ de liste déroulante sélectionné ou dans un groupe d'options.
Touche espace	Activation et désactivation d'une case à cocher lorsque l'option active est une case à cocher.
Alt + lettre soulignée	Sélectionner une option ou exécuter une commande.
Alt + ↓ F4	Ouvrir le champ de liste déroulante sélectionné.
Esc	Fermer le champ de liste déroulante sélectionné. Abandonner la commande et fermer le champ de dialogue.
Touche Enter	Exécuter la commande pour l'option ou le bouton actif.

8.2.2 Dans l'Aide

Commande clavier	**Description**
Alt + touche espace	Afficher le menu système.
Alt + Tab	Commutation entre l'aide et les autres fenêtres ouvertes.
Alt + F4	Fermer l'aide.
Shift + F10	Afficher les menus contextuels de l'aide.
Ctrl + Tab	Passer à la rubrique suivante dans la fenêtre de navigation.
Ctrl + Shift + Tab	Passer à la rubrique précédente dans la fenêtre de navigation.
PgUp	Passer au thème situé au-dessus du thème actuel dans le sommaire, l'index ou la liste des résultats de recherche.
PgDn	Passer au thème situé en dessous du thème actuel dans le sommaire, l'index ou la liste des résultats de recherche.
F6	Commuter entre les fenêtres de navigation et thématique.
PgUp PgDn	Parcourir un thème.

8.2.3 Dans le Control Center

Généralités

Commande clavier	Description
F1	Afficher l'aide
Alt + F4	Fermer le Control Center
F5	Actualiser la vue
F8	Ouvrir la configuration
F9	Lancer la mise à jour

Rubrique Contrôler

Commande clavier	Description
F2	Renommer le profil sélectionné
F3	Démarrer la recherche avec le profil choisi
F4	Créer un lien sur le Bureau pour le profil sélectionné
Ins	Créer un nouveau profil
Suppr	Supprimer le profil sélectionné

Rubrique Quarantaine

Commande clavier	Description
F2	Contrôler à nouveau l'objet
F3	Restaurer l'objet
F4	Envoyer l'objet
F6	Restaurer l'objet après...
Enter	Caractéristiques
Ins	Ajouter le fichier
Suppr	Supprimer l'objet

Rubrique Planificateur

Commande clavier	Description
F2	Modifier la tâche
Enter	Caractéristiques
Ins	Ajouter une nouvelle tâche
Suppr	Supprimer la tâche

Rubrique Rapports

Commande clavier	Description
F3	Afficher le fichier de rapport
F4	Imprimer le fichier de rapport
Enter	Afficher le rapport
Suppr	Supprimer le(s) rapport(s)

Rubrique Evénements

Commande clavier	Description
F3	Exporter le(s) événement(s)
Enter	Afficher l'événement
Suppr	Supprimer le(s) événement(s)

8.3 Centre de sécurité Windows

- à partir de Windows XP Service Pack 2 -

8.3.1 Généralités

Le Centre de sécurité Windows vérifie l'état d'un ordinateur concernant les aspects importants de la sécurité.

Si un problème est constaté sur l'un de ces points importants (par ex. un programme antivirus expiré), le Centre de sécurité envoie un avertissement et donne des recommandations pour mieux protéger l'ordinateur.

8.3.2 Le Centre de sécurité Windows et Avira AntiVir Professional

Logiciel antivirus/Protection contre les logiciels nuisibles

Vous pouvez recevoir les consignes suivantes du Centre de sécurité Windows, concernant votre protection antivirus.

Protection antivirus NON TROUVÉE

Antivirus EXPIRÉ

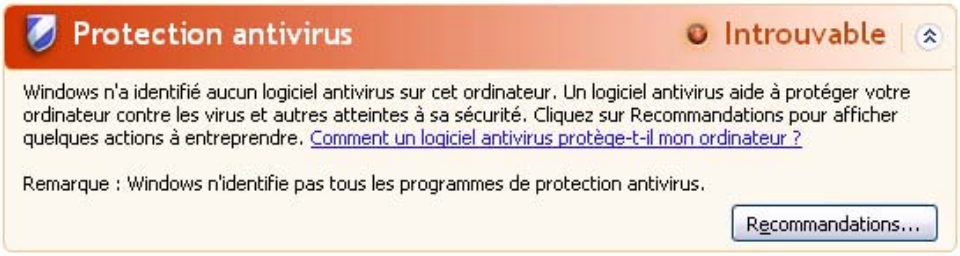
Protection antivirus ACTIVÉE

Protection antivirus DÉSACTIVÉE

Protection antivirus NON SURVEILLÉE

Protection antivirus NON TROUVÉE

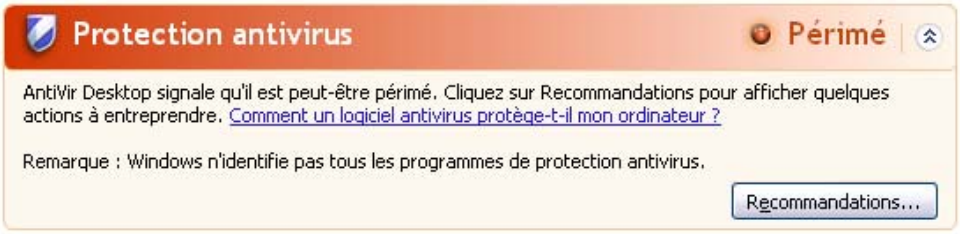
Cette remarque du Centre de sécurité Windows apparaît si le Centre de sécurité Windows n'a trouvé aucun logiciel antivirus sur votre ordinateur.



Remarque
Installez Avira AntiVir Professional sur votre ordinateur pour le protéger des virus et autres programmes indésirables !

Antivirus EXPIRÉ

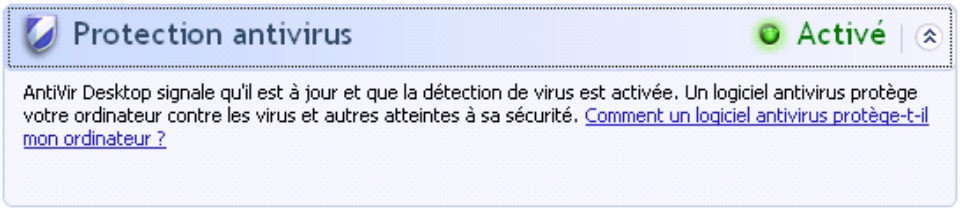
Si vous avez installé Windows XP Service Pack 2 ou Windows Vista puis Avira AntiVir Professional ou si vous avez installé Windows XP Service Pack 2 ou Windows Vista sur un système accueillant déjà Avira AntiVir Professional, vous recevez le message suivant :



Remarque
Pour que le Centre de sécurité Windows reconnaisse Avira AntiVir Professional comme actuel, une mise à jour est obligatoire après l'installation. Vous actualisez votre système en effectuant une mise à jour de Avira AntiVir Professional.

Protection antivirus ACTIVÉE

Après l'installation de Avira AntiVir Professional et une mise à jour immédiatement après, vous recevez le message suivant :



Avira AntiVir Professional est actuel et AntiVir Guard est activé.

Antivirus DÉSACTIVÉ

Vous recevez le message suivant si vous désactivez AntiVir Guard ou si vous arrêtez le service Guard.



Remarques
Vous pouvez activer ou désactiver AntiVir Guard dans la rubrique Aperçu :: Activez ou désactivez l'état du Avira AntiVir Professional Control Center. Vous voyez en outre que AntiVir Guard est activé si le parapluie rouge est ouvert dans votre barre des tâches.

Protection antivirus NON SURVEILLÉE

Si vous recevez le message suivant du Centre de sécurité Windows, c'est que vous avez choisi de surveiller vous-même votre logiciel antivirus.

Remarque
Windows Vista ne prend pas en charge la fonction.



Remarque
Le Centre de sécurité Windows est pris en charge par Avira AntiVir Professional. Vous pouvez activer cette option à tout moment via le bouton "Recommandations...".

Remarque
Même si vous avez installé Windows XP Service Pack 2 ou Windows Vista, il vous faut toujours une protection antivirus, par ex. Avira AntiVir Professional. Bien que Windows XP Service Pack 2 surveille votre logiciel antivirus, il ne dispose d'aucune fonction antivirus. Sans protection antivirus supplémentaire, vous ne seriez donc pas protégé des virus et autres logiciels malveillants !

9 Virus et autres

9.1 Catégories de dangers étendues

Programmes de numérotation payants (DIALER)

Certaines prestations de service sur Internet sont payantes. La facturation a lieu en Allemagne via les programmes de numérotation en 0190/0900 (en Autriche et en Suisse via des numéros en 09x0 ; en Allemagne le passage à des numéros en 09x0 aura lieu à moyen terme). Installés sur l'ordinateur, ces programmes - appelés dialers - assurent l'établissement de la connexion via un numéro surtaxé dont le prix peut être très variable.

La commercialisation de contenus en ligne via la facture téléphonique est légale et peut être avantageuse pour l'utilisateur. Les dialers sérieux affichent clairement leur utilisation consciente et réfléchie par le client. Ils ne s'installent sur l'ordinateur de l'utilisateur que si ce dernier a donné son accord, cet accord étant donné sur la base d'une présentation ou d'une incitation claire. L'établissement de la connexion via des programmes de numérotation sérieux s'affiche sans ambigüité. En outre, les dialers sérieux indiquent clairement les frais de connexion.

Malheureusement, il existe des dialers qui s'installent sur les ordinateurs de manière cachée et douteuse, voire même de manière trompeuse. Ils remplacent par ex. la connexion de télétransmission standard de l'utilisateur Internet vers le FAI (fournisseur d'accès Internet) et appellent à chaque connexion un numéro en 0190/0900 surtaxé, parfois très cher. L'utilisateur ne remarque qu'à l'arrivée de la facture téléphonique suivante qu'un programme de numérotation indésirable en 0190/0900 a été utilisé sur son ordinateur à chaque connexion à Internet - avec pour conséquence des coûts très élevés.

Pour vous protéger des programmes de numérotation indésirables (dialers 0190/0900), nous vous conseillons de vous faire bloquer auprès de votre opérateur téléphonique pour ce type de numéros.

En général, Avira AntiVir Professional identifie les programmes de numérotation payants qu'il connaît.

Si dans la configuration l'option Programmes de numérotation payants (DIALER) est cochée sous **Catégories étendues de dangers**, vous recevez un avertissement en cas de détection d'un programme de numérotation payant. Vous avez alors la possibilité de supprimer le programme de numérotation en 0190/0900. S'il s'agit d'un programme de numérotation souhaité, vous pouvez le déclarer comme fichier d'exclusion afin qu'il ne soit plus examiné à l'avenir.

Jeux (GAMES)

Les jeux vidéo ont leur raison d'être - mais pas obligatoirement sur le poste de travail (à part peut-être pour la pause déjeuner). Toutefois, dans les entreprises privées comme publiques, il n'est pas rare que les employés jouent. Internet permet de télécharger de nombreux jeux. Les jeux par email aussi sont de plus en plus populaires : des simples échecs à la "bataille navale" (bataille de torpilles incluse), de nombreuses variantes circulent : les jeux sont envoyés via les programmes de courrier électronique aux partenaires qui répondent.

Des analyses ont montré que le temps de travail passé à jouer aux jeux vidéo a atteint depuis longtemps des proportions économiques non négligeables. Il est d'autant plus compréhensible que de plus en plus d'entreprises décident de bannir les jeux des postes de travail.

Avira AntiVir Professional détecte les jeux vidéo. Si dans la configuration l'option Jeux (GAMES) est cochée sous **Catégories étendues de dangers**, vous recevez un avertissement quand Avira AntiVir Professional a détecté un jeu. Le jeu est donc éradiqué au sens premier du terme, car vous avez la possibilité de le supprimer.

Programmes de blagues (JOKES)

Les programmes de blagues sont faits pour effrayer ou pour amuser, sans être nuisibles ni se multiplier. Souvent l'ordinateur se met à jouer une mélodie une fois le programme de blague ouvert ou à afficher quelque chose d'inhabituel. On peut citer pour exemples la machine à laver dans le lecteur de disquettes (DRAIN.COM) et le mangeur d'écran (BUGSRES.COM).

Mais prudence ! Tous les symptômes des programmes de blagues peuvent aussi provenir d'un virus ou d'un cheval de Troie. Au mieux on se fait une belle frayeur, au pire on peut vraiment faire des dégâts à cause de la panique.

Avira AntiVir Professional est capable de détecter les programmes de blagues grâce à l'élargissement de ses routines de recherche et d'identification pour les éliminer éventuellement comme programmes indésirables. Si dans la configuration l'option Programmes de blagues (JOKES) est cochée sous **Catégories étendues de dangers**, vous êtes prévenu.

Security Privacy Risk (SPR)

Logiciel qui compromet la sécurité de votre système, déclenche des activités de programmes non souhaitées, qui viole votre sphère privée ou espionne votre comportement d'utilisateur et peut donc être indésirable.

Avira AntiVir Professional détecte les logiciels "Security Privacy Risk". Si dans la configuration l'option Security Privacy Risk (SPR) est cochée sous **Catégories étendues de dangers**, vous recevez un avertissement quand Avira AntiVir Professional en détecte un.

Logiciel de commande Backdoor (BDC)

Pour voler des données ou manipuler l'ordinateur, un programme de serveur backdoor passe par la "porte arrière" sans que l'utilisateur le remarque. Via Internet ou le réseau, ce programme peut être commandé via un logiciel de commande backdoor (client) par des tiers.

Avira AntiVir Professional détecte les "logiciels de commande backdoor". Si dans la configuration l'option Logiciel de commande backdoor est cochée sous **Catégories de dangers étendues (BDC)**, vous recevez un avertissement quand Avira AntiVir Professional en détecte un.

Logiciel publicitaire/Logiciel espion (ADSPY)

Logiciel affichant de la publicité ou logiciel envoyant des informations personnelles de l'utilisateur à des tiers, le plus souvent sans son accord ou sans qu'il en ait connaissance et qui est donc éventuellement indésirable.

Avira AntiVir Professional détecte les "logiciels publicitaires/espions". Si dans la configuration, l'option Logiciels publicitaires/logiciels espions est coché sous **Catégories étendues de dangers**, vous recevez un avertissement si Avira AntiVir Professional en détecte un.

Programmes de compression dans le temps d'exécution (PCK) inhabituels

Fichiers compressés avec un programme de compression dans le temps d'exécution inhabituel et qui peuvent donc être considérés comme suspects.

Avira AntiVir Professional détecte les "programmes de compression dans le temps d'exécution inhabituels". Si dans la configuration, l'option Programmes de compression dans le temps d'exécution (PCK) inhabituels est cochée sous **Catégories étendues de dangers**, vous recevez un avertissement quand Avira AntiVir Professional en a détecté un.

Fichiers à extensions déguisées (HEUR-DBLEXT)

Fichiers exécutables qui déguisent leur extension de manière suspecte. Cette méthode de déguisement est souvent utilisée par les logiciels malveillants.

Avira AntiVir Professional détecte les "fichiers à extensions déguisées". Si dans la configuration, l'option Fichiers à extensions déguisées (HEUR-DBLEXT) est cochée sous **Catégories étendues de dangers**, vous recevez un avertissement si Avira AntiVir Professional en détecte un.

Hameçonnage

L'hameçonnage, également connu sous le nom de *brand spoofing*, est une forme raffinée de vol de données qui vise les clients ou clients potentiels des FAI, banques, services bancaires en lignes, autorités d'enregistrement.
Grâce à la transmission d'une adresse email sur Internet, au remplissage de formulaires en ligne, à la participation à des groupes d'information ou des pages Web, il est possible que vos données soient volées par des "Internet crawling spiders" et utilisées sans votre accord pour une escroquerie ou d'autres forfaits.

Avira AntiVir Professional détecte l'"hameçonnage". Si dans la configuration, l'option Hameçonnage est cochée sous **Catégories étendues de dangers**, vous recevez un avertissement si Avira AntiVir Professional détecte ce type de comportement.

Application (APPL)

L'appellation APPL recoupe une application dont l'utilisation peut être liée à un risque ou dont l'origine est douteuse.

Avira AntiVir Professional détecte les "applications (APPL)". Si dans la configuration l'option Application (APPL) est cochée sous **Catégories étendues de dangers**, vous recevez un avertissement quand Avira AntiVir Professional détecte ce type de comportement.

9.2 Virus et autres logiciels malveillants

Logiciels publicitaires

On appelle logiciel publicitaire un logiciel qui, en plus de sa fonctionnalité réelle, montre à l'utilisateur des bannières publicitaires ou fenêtres intempestives publicitaires. Ces affichages de pubs ne peuvent en général être coupés et restent toujours visibles. Ici, les données de connexion permettent de tirer de nombreux enseignements sur le comportement d'utilisation et sont problématiques en matière de protection des données.

Backdoors

Un backdoor (porte arrière en français) peut accéder à un ordinateur en passant outre sa protection.

Un programme fonctionnant de manière cachée offre à un agresseur des droits quasi illimités. A l'aide du backdoor, il est possible d'espionner les données personnelles de l'utilisateur. Mais ils servent surtout à installer des virus ou vers sur le système concerné.

Virus d'amorçage

Le secteur d'amorçage ou le secteur d'amorçage maître des disques durs s'infecte de préférence de virus de secteurs d'amorçage. Ils écrasent des informations importantes pour le démarrage du système. L'une des conséquences désagréables : le système d'exploitation ne peut plus être chargé...

Bot-Net

Un Bot-Net est un réseau commandable à distance (sur Internet) à partir de PC qui se compose de bots communiquant entre eux. Ce contrôle est obtenu par des virus ou chevaux de Troie qui infectent l'ordinateur puis attendent des instructions sans faire de dégâts sur l'ordinateur infecté. Ces réseaux peuvent être utilisés pour répandre des spams, des attaques DDoS, etc., parfois sans que les utilisateurs des PC touchés ne le remarquent. Le principal potentiel des Bot-Nets est de pouvoir atteindre une taille de plusieurs milliers d'ordinateurs dont la somme des bandes passantes dépasse largement la plupart des accès à Internet traditionnels.

Exploit

Un Exploit (lacune de sécurité) est un programme informatique ou script qui exploite les faiblesses spécifiques ou dysfonctionnements d'un système d'exploitation ou d'un programme. Comme exemple d'Exploit on peut citer les attaques en provenance d'Internet à l'aide de paquets de données manipulés qui exploitent les faiblesses dans le logiciel de réseau. Ici, des programmes peuvent être infiltrés, permettant d'obtenir un accès plus grand.

Canulars (angl. hoax)

Depuis quelques années, les utilisateurs d'Internet et d'autres réseaux reçoivent des alertes aux virus qui se répandent par email. Ces avertissements sont transmis par email avec la consigne de les envoyer au plus grand nombre de collègues et d'utilisateurs possible pour les prévenir du "danger".

Pot de miel

Un pot de miel (angl. : honeypot) est un service installé dans un réseau (programme ou serveur). Il a la tâche de surveiller un réseau et de documenter les attaques. Ce service est inconnu de l'utilisateur légitime et n'est donc jamais sollicité. Si un agresseur examine les points faibles d'un réseau et sollicite les services proposés par un pot de miel, il est documenté et une alarme est déclenchée.

Macrovirus

Les macrovirus sont des petits programmes écrits dans le macrolangage d'une application (par ex. WordBasic sous WinWord 6.0) et peuvent se répandre normalement dans les documents de cette application seulement. On les appelle donc également des virus documents. Pour être activés, ils nécessitent le démarrage de l'application correspondante et l'exécution de l'une des macros infectées. Contrairement aux virus "normaux", les macrovirus n'infectent donc pas les fichiers exécutables mais les documents de l'application hôte.

Pharming

Le pharming est une manipulation du fichier hôte des navigateurs Web pour dévier les requêtes sur des sites web falsifiés. Il s'agit d'une variante d'hameçonnage. Les escrocs au pharming entretiennent de grandes fermes de serveurs sur lesquelles des sites Web sont archivés. Le pharming s'est établi comme terme générique pour plusieurs types d'attaques DNS. En cas de manipulation du fichier hôte, une manipulation ciblée du système est entreprise, à l'aide d'un cheval de Troie ou d'un virus. La conséquence est que seuls les sites Web falsifiés par ce système sont encore accessibles, même quand l'adresse Web a été correctement saisie.

Hameçonnage

L'hameçonnage est la "pêche" aux données personnelles de l'utilisateur d'Internet. Le pêcheur envoie à sa victime des courriers de facture officielle, comme par exemple des emails, qui doivent l'inciter à communiquer sans méfiance des informations, surtout pseudonymes et mots de passe ou PIN et TAN pour les transactions bancaires. Avec les données d'accès volées, le pêcheur peut prendre l'identité de sa victime et agir en son nom. Une chose est claire : les banques et assurances ne demandent jamais d'envoyer les numéros de cartes de crédit, PIN, TAN ou autres données d'accès par email, SMS ou téléphone.

Virus polymorphes

Les virus polymorphes sont de véritables maîtres du camouflage et du déguisement. Ils modifient leurs propres codes de programmation et sont donc particulièrement difficiles à identifier.

Virus programmes

Un virus informatique est un programme capable de se lier à d'autres programmes quand on l'ouvre et de les infecter. Les virus se multiplient donc seuls, contrairement aux bombes logiques et aux chevaux de Troie. Contrairement à un ver, le virus nécessite toujours un programme tiers pour hôte, dans lequel il dépose son code virulent. Normalement toutefois, le déroulement du programme lui-même de l'hôte n'est pas modifié.

Rootkit

Un rootkit est un ensemble d'outils logiciels qui s'installent après l'entrée dans un système informatique, pour masquer les identifiants de l'envahisseur, cacher des processus et couper des données - en résumé : pour se rendre invisible. Il essaie d'actualiser les programmes d'espionnage déjà installés et de réinstaller les logiciels espions supprimés.

Virus script et vers

Ces virus sont extrêmement simples à programmer et se répandent - quand les conditions techniques sont réunies - en quelques heures par email et partout dans le monde.

Les virus et vers de script utilisent l'un des langages du script, par ex. Javascript, VBScript etc., pour entrer dans de nouveaux scripts ou se répandre en accédant à des fonctions du système d'exploitation. Cela a lieu souvent par email ou lors de l'échange de fichiers (documents).

On appelle ver un programme qui se multiplie sans infecter d'hôte. Les vers ne peuvent pas devenir partie intégrante d'autres programmes. Les vers sont souvent la seule possibilité de faire entrer des programmes nuisibles sur les systèmes à mesures de sécurité restrictives.

Logiciels espions

Les logiciels espions sont des programmes qui envoient les données personnelles de l'utilisateur à son insu et sans son accord au fabricant du logiciel ou à un tiers. La plupart du temps, les programmes espions servent à analyser le type de navigation sur Internet et à afficher des bannières ou fenêtres intempestives publicitaires ciblées.

Chevaux de Troie

Les chevaux de Troie sont devenus fréquents ces derniers temps. C'est ainsi que l'on appelle les programmes qui semblent avoir une fonction spéciale mais montrent leur vrai visage après leur démarrage et exécutent une autre fonction souvent néfaste. Les chevaux de Troie ne peuvent pas se multiplier seuls, ce qui les différencie des virus et vers. La plupart portent un nom intéressant (SEX.EXE ou STARTME.EXE) pour inciter l'utilisateur à exécuter le cheval de Troie. Aussitôt après l'exécution, ils sont actifs et formatent le disque dur par exemple. Les droppers, qui 'déposent' des virus ou l'inséminent dans un système informatique, sont un type particulier de cheval de Troie.

Zombie

Un PC zombie est un ordinateur infecté par des programmes malveillants et qui permet aux pirates informatiques d'utiliser l'ordinateur à distance dans un but criminel. Le PC infecté démarre sur demande par exemple des attaques de type Denial-of-Service- (DoS) ou envoie des spams et des emails d'hameçonnage.

10 Info et service

Dans ce chapitre, vous obtenez des informations sur les moyens d'entrer en contact avec nous.

voir le chapitre Adresse de contact

voir le chapitre Support technique

voir le chapitre Fichier suspect

voir le chapitre Signaler une fausse alerte

voir le chapitre Vos réactions pour plus de sécurité

10.1 Adresse de contact

Nous serons heureux de vous assistez si vous avez des questions et suggestions concernant les produits Avira AntiVir Professional. Vous trouverez nos adresses de contact dans le Control Center sous Aide :: A propos de Avira AntiVir Professional.

10.2 Support technique

Le support de Avira AntiVir Professional est à vos côtés lorsqu'il s'agit de répondre à vos questions ou de résoudre un problème technique.

Sur notre site Web http://www.avira.de/fr/support, vous obtiendrez toutes les informations nécessaires à notre service étendu de support.

Pour nous permettre de vous aider rapidement et de manière fiable, préparez les informations suivantes :

- **Données de licence**. Vous les trouverez dans le Control Center Avira AntiVir Professional sous la rubrique Aide :: À propos de AntiVir Professional :: Informations de licence.
- **Informations de version**. Vous les trouverez dans le Control Center Avira AntiVir Professional du sous la rubrique Aide :: À propos de AntiVir Professional :: Informations de version.
- **Version du système d'exploitation** et packs de service éventuellement installés.
- **Packs logiciels installés**, par ex. logiciels antivirus d'autres fabricants.
- **Messages précis** du programme ou du fichier rapport.

10.3 Fichier suspect

Vous pouvez nous envoyer les virus qui ne peuvent pas encore être détectés ou supprimés par nos produits ou les fichiers suspects. Nous mettons à votre disposition plusieurs moyens.

- Sélectionnez le fichier dans le gestionnaire de quarantaine du Control Center, puis la rubrique Envoyer fichier à l'aide du menu contextuel ou du bouton correspondant.
- Envoyez le fichier souhaité compressé (WinZIP, PKZip, Arj etc.) en pièce jointe d'un email à virus-prof-fr@avira.com. Comme certaines passerelles de courrier électronique fonctionnent avec un logiciel antivirus, dotez le ou les fichier(s) d'un mot de passe (n'oubliez pas de nous communiquer ce mot de passe).

Alternativement, vous avez la possibilité de nous envoyer le fichier via notre site Web.

10.4 Signaler une fausse alerte

Si vous pensez que Avira AntiVir Professional indique un résultat positif dans un fichier qui est pourtant très probablement "propre", envoyez ce fichier compressé (WinZIP, PKZIP, Arj, etc.) en pièce jointe dans un email, à virus-prof-fr@avira.com. Comme certaines passerelles de courrier électronique fonctionnent avec un logiciel antivirus, dotez le ou les fichier(s) d'un mot de passe (n'oubliez pas de nous communiquer ce mot de passe).

10.5 Vos réactions pour plus de sécurité

Chez Avira, la sécurité de nos clients en première place. Pour cette raison, non seulement une équipe interne d'experts fait subir à chaque solution Avira et à chaque mise à jour des tests de qualité et de sécurité avant publication. Mais, pour nous, il s'agit aussi de prendre au sérieux les remarques sur d'éventuelles faiblesses de sécurité et de les traiter ouvertement.

Si vous croyez avoir trouvé une faiblesse de sécurité dans l'un de nos produits, veuillez envoyer un email à vulnerabilities-prof-fr@avira.com.

11 Référence : options de configuration

La référence de la configuration documente toutes les options de configuration disponibles dans Avira AntiVir Professional.

11.1 Scanner

La rubrique Scanner de la Configuration Avira AntiVir Professional est en charge de la configuration de la recherche directe, c'est-à-dire de la recherche à la demande.

11.1.1 Recherche

C'est ici que vous établissez le comportement de base de la routine de recherche lors d'une recherche directe. Si vous choisissez certains répertoires pour contrôle lors de la recherche directe, le Scanner contrôle, en fonction de la configuration :

- avec une puissance de recherche définie (priorité),
- plus les secteurs d'amorçage et la mémoire principale,
- certains ou tous les secteurs d'amorçage et la mémoire principale,
- tous ou certains fichiers dans le répertoire.

Fichiers

Le Scanner peut utiliser un filtre pour ne contrôler que les fichiers avec une certaine extension (type).

Tous les fichiers

Si cette option est activée, tous les fichiers sont parcourus à la recherche de virus et programmes indésirables, indépendamment de leur contenu et de leur extension. Le filtre n'est pas utilisé.

Remarque
Si l'option Tous les fichiers est activée, le bouton **Extensions de fichiers** n'est pas fonctionnel.

Sélection intelligente des fichiers

Si cette option est activée, la sélection des fichiers à contrôler est effectuée automatiquement par Avira AntiVir Professional. Cela signifie que le programme Avira AntiVir Professional décide en fonction du contenu d'un fichier si celui-ci doit être contrôlé quant à l'absence de virus et programmes indésirables. Ce processus est un peu plus lent que Utiliser la liste d'extensions de fichiers, mais beaucoup plus sûr, car le contrôle n'est pas seulement basé sur l'extension des fichiers. Ce réglage est activé par défaut et recommandé.

Remarque
Si l'option Sélection intelligente des fichiers est activée, le bouton **Extensions de fichiers** n'est pas fonctionnel.

Utiliser la liste d'extensions des fichiers

Si cette option est activée, seuls les fichiers dont l'extension a été présélectionnée sont parcourus. Sont présélectionnés par défaut tous les types de fichiers pouvant contenir des virus et programmes indésirables. Cette liste peut être modifiée manuellement avec le bouton Extension de fichier.

Remarque
Si cette option est activée et que vous avez supprimé toutes les entrées de la liste des extensions de fichiers, ceci s'affiche avec le texte "Aucune extension de fichier", sous le bouton Extensions de fichiers.

Extensions de fichiers

Ce bouton permet d'ouvrir une fenêtre de dialogue contenant toutes les extensions de fichiers examinées lors d'une recherche en mode **Utiliser la liste des extensions de fichiers**. Pour les extensions, des entrées sont indiquées par défaut, mais il est possible d'ajouter et de supprimer des entrées.

Remarque
Notez que la liste standard peut changer d'une version à l'autre.

Autres réglages

Secteur d'amorçage des lecteurs de recherche

Si cette option est activée, le Scanner contrôle les secteurs d'amorçage des lecteurs sélectionnés pour la recherche directe. Ce réglage est activé par défaut.

Contrôler les secteurs d'amorçage maîtres

Si cette option est activée, le Scanner contrôle les secteurs d'amorçage maîtres du ou des disques durs utilisés par le système.

Ignorer les fichiers hors ligne

Si cette option est activée, la recherche directe ignore complètement les fichiers hors ligne lors d'une recherche. Cela signifie que la présence de virus et programmes indésirables n'est pas contrôlée sur les fichiers. Les fichiers hors ligne sont des fichiers qui ont été déplacés physiquement par un système de gestion hiérarchique de la mémoire (HSMS) du disque dur vers une bande, par exemple. Ce réglage est activé par défaut.

Contrôle intégral de fichiers système

Si l'option est activée, les fichiers système Windows les plus importants sont soumis à un contrôle particulièrement sûr concernant d'éventuelles modifications opérées par des logiciels malveillants, et ce à chaque recherche directe. Si un fichier modifié est trouvé, celui-ci est signalé comme résultat positif suspect. Cette fonction utilise beaucoup de ressources de l'ordinateur. C'est pourquoi l'option est désactivée par défaut.

Recherche optimisée

Si l'option est activée, la capacité du processeur est utilisée de façon optimale lors d'une recherche du Scanner. Pour des raisons liées à la performance, la documentation lors d'une recherche optimisée est effectuée au plus à un niveau par défaut.

Remarque
L'option n'est disponible que sur des ordinateurs à processeurs multiples. Si AntiVir Professional est administré via le SMC, l'option s'affiche dans chaque cas et peut être activée : si l'ordinateur administré n'est pas équipé de plusieurs processeurs, le Scanner n'utilise pas l'option.

Suivre les liens symboliques

Si l'option est désactivée, le Scanner suit lors de la recherche, tous les liens symboliques du profil de recherche ou du répertoire sélectionné pour contrôler l'absence de virus et de logiciels malveillants dans les fichiers liés. Cette option n'est pas prise en charge sous Windows 2000 et est désactivée par défaut.

Important
L'option n'inclut aucun lien de fichiers (shortcuts) mais se réfère exclusivement aux liens symboliques (créés avec mklink.exe) ou aux Junction Points (créés avec junction.exe) qui sont présents de manière transparente dans le système de fichiers.

Recherche de rootkits lors du démarrage de la recherche

Si l'option est activée, le Scanner vérifie au démarrage le répertoire système Windows à la recherche de rootkits actifs, au moyen d'un processus dit accéléré. Ce processus contrôle l'absence de rootkits sur votre ordinateur de manière moins détaillée que le profil de recherche **Recherche de rootkits**, il est toutefois exécuté beaucoup plus rapidement.

Important
La recherche de rootkits n'est pas encore disponible sur les systèmes 64 bits !

Ne contrôler aucun fichier et chemin sur les lecteurs réseau

Si cette option est activée, les lecteurs réseau reliés à l'ordinateur sont exclus de la recherche directe. Cette option est recommandée quand les serveurs ou d'autres postes de travail sont protégés par un logiciel antivirus, par ex. d'autres installations du poste de travail par Avira AntiVir Professional. Cette option est désactivée par défaut.

Processus de recherche

Autoriser l'arrêt

Si cette option est activée, la recherche de virus et programmes indésirables peut être terminée à tout moment avec le bouton Stop dans la fenêtre du "Luke Filewalker". Si vous avez désactivé ce réglage, le bouton Stop de la fenêtre "Luke Filewalker" est en gris. L'interruption d'une recherche n'est pas possible ! Ce réglage est activé par défaut.

Priorité de scannage

Le Scanner distingue trois niveaux de priorité lors de la recherche directe. Cette distinction ne s'applique que si plusieurs processus sont actifs en même temps sur l'ordinateur. Le choix influe sur la vitesse de la recherche.

Bas

Le Scanner reçoit du système d'exploitation du temps de processeur uniquement si aucun autre processus ne nécessite de temps de calcul, c'est-à-dire tant que le Scanner tourne seul, la vitesse est maximale. Au total, le travail avec les autres programmes est ainsi facilité : l'ordinateur réagit plus vite si d'autres programmes ont besoin de temps de calcul, pendant que le Scanner continue de tourner en arrière-plan. Ce réglage est activé par défaut et recommandé.

Moyen

Le Scanner est exécuté avec le niveau de priorité normal. Tous les processus reçoivent du système d'exploitation autant de temps de processus. Dans certaines conditions, le travail avec d'autres applications peut être entravé.

Elevé

Le Scanner obtient la priorité. Le travail en parallèle avec d'autres applications n'est quasiment plus possible. Toutefois, le Scanner effectue sa recherche avec la vitesse maximale.

11.1.1.1. Action en cas de résultat positif

Action en cas de résultat positif

Vous pouvez établir des actions que le Scanner doit exécuter quand un virus ou programme indésirable a été détecté.

Interactif

Si l'option est activée, les résultats positifs de la recherche du Scanner sont signalés dans une fenêtre de dialogue. Lors de la recherche de rootkits, de virus de secteurs d'amorçage et du contrôle de processus actifs, une fenêtre de dialogue s'affiche vous permettant de sélectionner l'action à effectuer avec l'objet affecté. Lors de la recherche de fichiers, la notification et la possibilité de sélection du traitement des fichiers affectés dépendent du mode de notification choisi. Ce réglage est activé par défaut.

Actions autorisées

Dans cette zone d'affichage, vous pouvez choisir quelles actions peuvent être sélectionnées dans la fenêtre de dialogue du mode de notification individuel ou expert, en cas de détection d'un virus. Vous devez pour cela activer les options correspondantes.

réparer

Le Scanner répare le fichier touché si c'est possible.

renommer

Le Scanner renomme le fichier. Un accès direct à ces fichiers (en cliquant deux fois par ex.) n'est alors plus possible. Le fichier peut être réparé ultérieurement et à nouveau renommé.

Quarantaine

Le Scanner déplace le fichier en quarantaine. Le fichier peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou - si nécessaire - être envoyé à Avira Malware Research Center. Selon le fichier, d'autres possibilités de sélection sont disponibles dans le gestionnaire de quarantaines.

supprimer

Le fichier est supprimé mais peut être restauré avec les outils adéquats (par ex. Avira UnErase). Le modèle de détection des virus peut être retrouvé. Cette procédure est beaucoup plus rapide que "écraser et supprimer".

ignorer

Le fichier est conservé.

écraser et supprimer

Le Scanner écrase le fichier par un modèle standard et le supprime ensuite. Il ne peut plus être restauré.

Standard

Le bouton vous permet de définir une action par défaut du Scanner concernant le traitement des fichiers contaminés. Sélectionnez une action et cliquez sur le bouton **Standard**. Dans le mode de notification combiné, seule l'action par défaut sélectionnée peut être exécutée pour les fichiers contaminés. Dans le mode de notification individuel ou expert, l'action par défaut choisie est présélectionnée pour les fichiers contaminés.

Remarque
L'action **réparer** ne peut pas être sélectionnée comme action par défaut.

Remarque
Si vous avez sélectionné *supprimer* ou écraser et supprimer comme action par défaut et que vous souhaitez régler le mode de notification sur combiné, veuillez tenir compte du point suivant : en cas de résultats heuristiques, les fichiers affectés ne sont pas supprimés, mais placés en quarantaine.

Vous trouverez de plus amples informations ici.

Mode de notification

Le mode de notification vous permet de définir la forme sous laquelle les résultats positifs de virus sont signalés lors de la recherche de fichiers effectuée par le Scanner. Grâce au mode de notification, vous déterminez si des possibilités de sélection sont disponibles pour le traitement des fichiers affectés.

Combiné

En mode de notification combiné, vous recevez à l'issue de la recherche de fichiers, un message d'avertissement comportant une liste des fichiers contaminés qui ont été trouvés. Aucune possibilité de sélection n'est disponible pour le traitement des fichiers affectés. Vous pouvez exécuter l'action par défaut du Scanner pour tous les fichiers contaminés ou interrompre le Scanner. L'action par défaut du Scanner concernant le traitement des fichiers contaminés consiste à déplacer le fichier contaminé en quarantaine.

Combiné (expert)

En mode de notification expert, vous recevez à l'issue de la recherche de fichiers, un message d'avertissement comportant une liste des fichiers contaminés qui ont été trouvés. Vous avez la possibilité de sélectionner une action à exécuter pour les différents fichiers contaminés, via le menu contextuel. Vous pouvez exécuter les actions choisies pour tous les fichiers contaminés ou quitter le Scanner.

Individuel

En mode de notification individuel, chaque résultat positif de virus est signalé dans une fenêtre séparée lors de la recherche de fichiers. Vous pouvez sélectionner dans la fenêtre de dialogue ce qui doit advenir du fichier contaminé.

Automatique

Si l'option est activée, aucun dialogue permettant de sélectionner une action ne s'affiche en cas de détection d'un virus ou d'un programme indésirable. Le Scanner réagit en fonction de vos réglages effectués dans cette section.

Copier le fichier dans la quarantaine avant l'action

Si l'option est activée, le Scanner génère une copie de sécurité (backup) avant d'effectuer l'action principale ou secondaire souhaitée. La copie de sécurité est conservée en quarantaine où le fichier peut être restauré s'il a une valeur informative. En outre, vous pouvez envoyer la copie de sécurité à Avira Malware Research Center pour d'autres analyses.

Afficher les messages d'avertissement

Si l'option est activée, un message d'avertissement apparaît avec les actions à exécuter, en cas de détection d'un virus ou d'un programme indésirable.

Action principale

L'action principale est l'action effectuée lorsque le Scanner trouve un virus ou un programme indésirable. Si l'option **réparer** est sélectionnée, mais que la réparation du fichier touché est impossible, l'action sélectionnée sous **Action secondaire** est exécutée.

Remarque
L'option Action secondaire n'est sélectionnable que si sous Action principale le réglage **réparer** a été sélectionné.

réparer

Si l'option est activée, le Scanner répare les fichiers concernés automatiquement. Si le Scanner ne peut pas réparer un fichier touché, il exécute l'option choisie sous Action secondaire.

Remarque
Une réparation automatique est recommandée, mais cela signifie que le Scanner modifie les fichiers sur l'ordinateur.

supprimer

Si cette option est activée, le fichier est supprimé mais peut être restauré avec les outils adéquats (par ex. Avira UnErase). Le modèle de détection des virus peut ainsi être retrouvé. Cette procédure est beaucoup plus rapide que "écraser et supprimer".

écraser et supprimer

Si cette option est activée, le Scanner écrase le fichier par un modèle standard et le supprime ensuite. Il ne peut plus être restauré.

renommer

Si l'option est activée, le Scanner renomme le fichier. Un accès direct à ces fichiers (en cliquant deux fois par ex.) n'est alors plus possible. Les fichiers peuvent être réparés ultérieurement et à nouveau renommés.

ignorer

Si l'option est activée, l'accès au fichier est autorisé et le fichier est conservé.

Avertissement
Le fichier touché reste actif sur votre ordinateur! D'importants dégâts peuvent être causés sur votre ordinateur!

Quarantaine

Si l'option est activée, le Scanner déplace le fichier dans un répertoire de quarantaine. Les fichiers peuvent être réparés ultérieurement ou - si nécessaire - être envoyés à Avira Malware Research Center.

Action secondaire

L'option **Action secondaire** n'est sélectionnable que si sous **Action principale** l'option réparer a été sélectionnée. Cette option permet de décider ce qui doit être fait avec le fichier touché s'il n'est pas réparable.

supprimer

Si cette option est activée, le fichier est supprimé mais peut être restauré avec les outils adéquats (par ex. Avira UnErase). Le modèle de détection des virus peut ainsi être retrouvé. Cette procédure est beaucoup plus rapide que "écraser et supprimer".

écraser et supprimer

Si cette option est activée, le Scanner écrase le fichier par un modèle standard et le supprime ensuite (wipe). Il ne peut plus être restauré.

renommer

Si l'option est activée, le Scanner renomme le fichier. Un accès direct à ces fichiers (en cliquant deux fois par ex.) n'est alors plus possible. Les fichiers peuvent être réparés ultérieurement et à nouveau renommés.

ignorer

Si l'option est activée, l'accès au fichier est autorisé et le fichier est conservé.

Avertissement
Le fichier touché reste actif sur votre ordinateur! D'importants dégâts peuvent être causés sur votre ordinateur!

Quarantaine

Si l'option est activée, le Scanner déplace le fichier dans un répertoire de quarantaine. Les fichiers peuvent être réparés ultérieurement ou - si nécessaire - être envoyés à Avira Malware Research Center.

Remarque
Si vous avez sélectionné **supprimer** ou **écraser et supprimer** comme action primaire ou secondaire, veuillez tenir compte du point suivant : en cas de résultats heuristiques, les fichiers affectés ne sont pas supprimés, mais placés en quarantaine.

11.1.1.2. Autres actions

Lancer le programme après un résultat positif

Après la recherche directe, le Scanner peut ouvrir un fichier de votre choix (par ex. un programme), si au moins un virus ou un programme indésirable a été trouvé, par ex. un programme de messagerie électronique, pour vous permettre de prévenir d'autres utilisateurs ou l'administrateur.

Remarque
Pour des raisons de sécurité, il est possible de démarrer un programme après un résultat positif, uniquement si un utilisateur est connecté à l'ordinateur. Le fichier est alors démarré avec les droits qui s'appliquent à l'utilisateur connecté. Si aucun utilisateur n'est connecté, cette option n'est pas exécutée.

Nom du programme

Dans ce champ de saisie, vous pouvez saisir le nom et le chemin correspondant du programme que le Scanner doit démarrer après un résultat positif.

...

Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le programme à l'aide de l'explorateur de fichiers.

Arguments

Dans ce champ de saisie, vous pouvez éventuellement saisir les paramètres de lignes de commande du programme à démarrer.

Rapport d'événement

Utiliser le rapport d'événement

Si l'option est activée, un message d'événement avec les résultats de la recherche est transmis à la documentation des événements Windows, une fois la recherche du Scanner terminée. Les événements peuvent être consultés dans l'affichage des événements Windows. L'option est désactivée par défaut.

Lors de la recherche dans les archives, le Scanner peut utiliser une recherche récursive : les archives dans les archives sont décompressées et l'absence de virus et de programmes indésirables est contrôlée. Les fichiers sont contrôlés, décompressés et à nouveau contrôlés.

Contrôler les archives

Si cette option est activée, les archives présentes dans la liste d'archives sont contrôlées. Ce réglage est activé par défaut.

Tous les types d'archives

Si cette option est activée, toutes les archives présentes dans la liste d'archives sont sélectionnées et contrôlées.

Extensions intelligentes

Si cette option est activée, le Scanner détecte si un fichier présente un format compressé (archive), même quand l'extension diffère des extensions habituelles, et contrôle l'archive. Pour cela, chaque fichier doit être ouvert, ce qui réduit la vitesse de recherche. Exemple : si une archive *.zip est dotée de l'extension *.xyz, le Scanner décompresse également cette archive et la contrôle. Ce réglage est activé par défaut.

Remarque
Seuls les types d'archives repérés dans la liste des archives sont contrôlés.

Limiter la profondeur de récursivité

La décompression et le contrôle des archives à imbrication très profonde peut nécessiter beaucoup de temps de calcul et de ressources. Si cette option est activée, la profondeur de la recherche est limitée dans les archives multicompressées à un nombre défini sur les niveaux de paquets (profondeur de récursivité maximale). Vous économisez ainsi du temps et des ressources.

Remarque
Pour examiner un virus ou un programme indésirable au sein d'une archive, le Scanner doit scanner jusqu'au niveau de récursivité dans lequel le virus ou le programme indésirable se trouve.

Profondeur maximale de récursivité

Pour pouvoir saisir la profondeur de récursivité maximale, l'option Limiter la profondeur de récursivité doit être activée.
Vous pouvez soit saisir directement la profondeur de récursivité souhaitée, soit la modifier avec les touches flèches à droite du champ de saisie. Les valeurs autorisées vont de 1 à 99. La valeur par défaut recommandée est de 20.

Valeurs par défaut

Le bouton restaure les valeurs prédéfinies pour la recherche dans les archives.

Liste des archives

Dans cette zone d'affichage, vous pouvez définir quelles archives le Scanner doit parcourir. Pour cela, vous devez repérer les entrées correspondantes.

11.1.1.3. Exceptions

Objets de fichiers à exclure par le Scanner

La liste dans cette fenêtre contient les fichiers et chemins que le Scanner doit ignorer lors de la recherche de virus et programmes indésirables.

Entrez ici aussi peu d'exceptions que possible et uniquement les fichiers qui ne doivent vraiment pas être contrôlés lors d'une recherche normale, pour quelque motif que ce soit. Nous recommandons dans tous les cas d'examiner l'absence de virus et de programmes indésirables sur ces fichiers, avant de les mettre dans la liste !

Remarque
Les entrées de la liste ne doivent pas dépasser 6000 caractères au total.

Avertissement
Ces fichiers sont ignorés lors de la recherche !

Remarque
Les fichiers mémorisés dans cette liste sont mentionnés dans le fichier rapport. Contrôlez de temps en temps le fichier rapport concernant ces fichiers non contrôlés car la raison pour laquelle vous aviez exclu un fichier n'existe peut-être plus. Dans ce cas, retirez le nom de ce fichier de la liste.

Champ de saisie

Entrez dans ce champ le nom de l'objet fichier qui doit être ignoré par la recherche en temps réel. Aucun objet fichier n'est indiqué par défaut.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le fichier ou le chemin souhaité.
Si vous avez saisi un nom de fichier avec le chemin intégral, ce fichier uniquement n'est pas contrôlé. Si vous avez saisi un nom de fichier sans chemin, chaque fichier portant ce nom (quel que soit le chemin ou le lecteur) ne sera pas parcouru.

Ajouter

Ce bouton vous permet de reprendre dans la fenêtre d'affichage l'objet fichier entré dans le champ de saisie.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas fonctionnel si aucune entrée n'est sélectionnée.

Remarque
Si vous ajoutez toute une partition à la liste des objets de fichiers à exclure, seuls les fichiers enregistrés directement sous la partition sont exclus de la recherche, mais pas les fichiers présents dans les répertoires de la partition correspondante :
Exemple : objet de fichier à exclure : `D:\` = `D:\file.txt` est exclu de la recherche du Scanner, `D:\folder\file.txt` n'est pas exclu de la recherche.

11.1.1.4. Heuristique

Cette rubrique de configuration contient les réglages pour l'heuristique du moteur de recherche Avira AntiVir Professional.

Avira AntiVir Professional contient des heuristiques très performantes qui permettent de détecter dynamiquement des logiciels malveillants inconnus, c'est-à-dire avant même qu'une signature de virus spéciale n'ait été créée contre le parasite et qu'une mise à jour de protection antivirus correspondante n'ait été envoyée. La détection des virus s'effectue par une analyse et un examen complet du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés sont aussi possibles. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code annoncé est digne de confiance.

Heuristique macrovirus

Heuristique macrovirus

Avira AntiVir Professional contient une heuristique de macrovirus très performante. Si cette option est activée, toutes les macros du document affecté sont supprimées si une réparation est possible ; alternativement, les documents suspects sont seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce réglage est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

Avira AntiVir Professional contient une heuristique très performante grâce à la technologie AHeAD, lui permettant de détecter aussi les (nouveaux) logiciels malveillants inconnus. Si cette option est activée, vous pouvez régler ici la "sensibilité" de cette heuristique. Ce réglage est activé par défaut.

Degré d'identification bas

Si cette option est activée, Avira AntiVir Professional détecte un peu moins de logiciels malveillants inconnus, le risque de messages erronés est faible dans ce cas.

Degré d'identification moyen

C'est le réglage par défaut quand vous avez choisi l'utilisation de cette heuristique.

Degré d'identification élevé

Si l'option est activée, Avira AntiVir Professional détecte beaucoup plus de logiciels malveillants inconnus, mais vous devez vous attendre aussi à des messages erronés.

11.1.2 Rapport

Le Scanner dispose d'une fonction de documentation étendue. Vous obtenez ainsi des informations exactes sur les résultats d'une recherche directe. Le fichier rapport contient toutes les données du système, ainsi que les avertissements et messages de la recherche directe.

Remarque
Pour vous permettre de suivre quelles actions le Scanner a effectuées lors de la détection de virus ou de programmes indésirables, un fichier rapport doit toujours être généré.

Documentation

Désactivée

Si cette option est activée, le Scanner ne documente pas les actions et résultats de la recherche directe.

Standard

Si cette option est activée, le Scanner documente les noms des fichiers touchés en indiquant leur chemin. En outre, la configuration pour la recherche actuelle, les informations sur la version et sur le preneur de licence sont inscrits dans le fichier rapport.

Étendue

Si cette option est activée, le Scanner documente en plus des informations standard les avertissements et remarques.

Intégrale

Si cette option est activée, le Scanner documente en outre tous les fichiers parcourus. En outre, tous les fichiers touchés, ainsi que les avertissements et remarques sont repris aussi dans le fichier rapport.

Remarque
Si vous devez nous envoyer un fichier rapport (pour la recherche d'erreur), merci de générer ce fichier rapport dans ce mode.

11.2 Guard

La rubrique Guard de la Configuration Avira AntiVir Professional est responsable de la configuration de la recherche en temps réel.

11.2.1 Recherche

En règle générale, vous voudrez surveiller votre système en continu. Pour cela, utilisez le Guard (recherche en temps réel = On-Access-Scanner). Avec, vous pouvez faire parcourir tous les fichiers copiés ou ouverts sur l'ordinateur à la recherche de virus et de programmes indésirables, "tout en faisant autre chose".

Mode de recherche

Définissez ici le moment où le contrôle d'un fichier doit avoir lieu.

Contrôler pendant la lecture

Si cette option est activée, le Guard contrôle les fichiers avant qu'ils ne soient lus ou exécutés par le système d'exploitation.

Contrôler pendant l'écriture

Si cette option est activée, le Guard contrôle un fichier lors de l'écriture. Ce n'est qu'après cette procédure que vous pouvez accéder à nouveau au fichier.

Contrôler pendant la lecture et l'écriture

Si cette option est activée, le Guard contrôle les fichiers avant l'ouverture, la lecture et l'exécution, et après l'écriture. Ce réglage est activé par défaut et recommandé.

Fichiers

Le Guard peut utiliser un filtre pour ne contrôler que les fichiers avec une certaine extension (type).

Tous les fichiers

Si cette option est activée, tous les fichiers sont parcourus à la recherche de virus et programmes indésirables, indépendamment de leur contenu et de leur extension.

Remarque
Si l'option Tous les fichiers est activée, le bouton Extensions de fichiers n'est pas fonctionnel.

Sélection intelligente des fichiers

Si cette option est activée, la sélection des fichiers à contrôler est effectuée automatiquement par Avira AntiVir Professional. Cela signifie que Avira AntiVir Professional décide en fonction du contenu d'un fichier si celui-ci doit être contrôlé pour l'absence de virus et programmes indésirables. Ce processus est un peu plus long que l'option Utiliser la liste des extensions de fichiers, mais beaucoup plus sûr, car le contrôle n'a pas lieu uniquement sur la base des extensions de fichiers.

Remarque
Si l'option Sélection intelligente des fichiers est activée, le bouton Extensions de fichiers n'est pas fonctionnel.

Utiliser la liste d'extensions des fichiers

Si cette option est activée, seuls les fichiers dont l'extension a été présélectionnée sont parcourus. Sont présélectionnés par défaut tous les types de fichiers pouvant contenir des virus et programmes indésirables. Cette liste peut être modifiée manuellement avec le bouton Extension de fichier. Ce réglage est activé par défaut et recommandé.

Remarque
Si cette option est activée et que vous avez supprimé toutes les entrées de la liste des extensions de fichiers, ceci s'affiche sous le bouton Extensions de fichiers avec le texte "Aucune extension de fichier".

Extensions de fichiers

Ce bouton permet d'ouvrir une fenêtre de dialogue contenant toutes les extensions de fichiers examinées lors d'une recherche en mode **Utiliser la liste des extensions de fichiers**. Pour les extensions, des entrées sont indiquées par défaut, mais il est possible d'ajouter et de supprimer des entrées.

Remarque
Notez que la liste d'extensions de fichiers peut changer d'une version à l'autre.

Archives

Contrôler les archives

Si l'option est activée, les archives sont contrôlées. Les fichiers compressés sont parcourus, décompressés et à nouveau parcourus. Cette option est désactivée par défaut. La recherche dans les archives est limitée par le biais de la profondeur de récursivité, du nombre de fichiers à analyser et de la taille des archives. Vous pouvez régler la profondeur maximale de récursivité, le nombre de fichiers à contrôler et la taille maximale des archives.

Remarque
Cette option est désactivée par défaut car le processus utilise beaucoup de ressources de l'ordinateur. Généralement, il est conseillé de contrôler les archives avec la recherche directe.

Profondeur maximale de récursivité

Lors de la recherche dans les archives, le Guard utilise une recherche récursive : les archives dans les archives sont décompressées et l'absence de virus et de programmes indésirables est contrôlée. Vous pouvez définir la profondeur de récursivité. La valeur par défaut est de 1 pour la profondeur de récursivité et est celle recommandée : toutes les archives situées directement dans l'archive principale sont décompressées et contrôlées.

Nombre maximum de fichiers

Lors de la recherche dans les archives, celle-ci est limitée à un nombre maximal de fichiers dans l'archive. La valeur par défaut pour le nombre maximal de fichiers à contrôler est de 10 et est celle recommandée.

Taille maximale (Ko)

Lors de la recherche dans les archives, celle-ci est limitée à une taille maximale d'archive à décompresser. La valeur par défaut est 1000 Ko et est recommandée.

Lecteurs

Lecteurs réseau

Si l'option est activée, les fichiers se trouvant sur les lecteurs du réseau (lecteurs mappés), comme les volumes de serveur, les lecteurs clients, etc., sont surveillés.

Remarque
Pour ne pas trop restreindre les performances de votre ordinateur, activez l'option **Lecteurs réseau** uniquement dans des cas exceptionnels.

Avertissement
Quand l'option est désactivée, les lecteurs du réseau **ne sont pas** surveillés. Vous n'êtes plus protégé des virus et programmes indésirables !

Remarque
Quand des fichiers sont exécutés sur des lecteurs réseau, ceux-ci sont contrôlés par le Guard - indépendamment du réglage de l'option *Lecteurs réseau*. Dans certains cas, les fichiers sur des lecteurs réseau sont contrôlés à leur ouverture, bien que l'option *Lecteurs réseau* soit désactivée. Motif : l'accès à ces fichiers s'effectue avec le droit 'Exécuter le fichier'. Si vous souhaitez exclure ces fichiers, ou bien aussi des fichiers exécutés sur les lecteurs réseau, de la surveillance opérée par le Guard, veuillez inscrire les fichiers dans la liste des objets de fichiers à exclure (voir Guard::Recherche::Exceptions).

11.2.1.1. Action en cas de résultat positif

Action en cas de résultat positif

Vous pouvez établir des actions que le Guard doit exécuter quand un virus ou programme indésirable a été détecté.

Interactif

Si cette option est activée, une fenêtre de dialogue s'affiche pour sélectionner l'action à effectuer avec le fichier touché en cas de détection d'un virus ou d'un programme indésirable pendant la recherche en temps réel. Cette option est activée par défaut.

Actions autorisées

Dans cette zone d'affichage, vous pouvez choisir quelles actions s'afficheront dans la fenêtre de dialogue en cas de détection d'un virus ou d'un programme indésirable. Vous devez pour cela activer les options correspondantes.

réparer

Le Guard répare le fichier touché si c'est possible.

renommer

Le Guard renomme le fichier. Un accès direct à ces fichiers (en cliquant deux fois par ex.) n'est alors plus possible. Le fichier peut être réparé ultérieurement et à nouveau renommé.

Quarantaine

Le Guard déplace le fichier en quarantaine. Le fichier peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou - si nécessaire - être envoyé à Avira Malware Research Center. Selon le fichier, d'autres possibilités de sélection sont disponibles dans le gestionnaire de quarantaines.

supprimer

Le fichier est supprimé mais peut être restauré avec les outils adéquats (par ex. Avira UnErase). Le modèle de détection des virus peut être retrouvé. Cette procédure est beaucoup plus rapide que "écraser et supprimer".

ignorer

L'accès au fichier est autorisé et le fichier est conservé.

écraser et supprimer

Le Guard écrase le fichier par un modèle standard et le supprime ensuite. Il ne peut plus être restauré.

Refuser l'accès

L'accès au fichier est refusé. Le Guard inscrit le résultat dans le fichier rapport à condition que la fonction de rapport soit activée. En outre, le Guard écrit une entrée dans le protocole d'événements si cette option est activée.

Standard

A l'aide de ce bouton, vous pouvez sélectionner l'action activée par défaut dans la fenêtre de dialogue en cas de détection d'un virus. Sélectionnez l'action activée par défaut et cliquez sur le bouton **Standard**.

Remarque
L'action **réparer** ne peut pas être sélectionnée comme action par défaut.

Vous trouverez de plus amples informations ici.

Automatique

Si l'option est activée, aucun dialogue permettant de sélectionner une action ne s'affiche en cas de détection d'un virus ou d'un programme indésirable. Le Guard réagit en fonction de vos réglages effectués dans cette section.

Copier le fichier dans la quarantaine avant l'action

Si l'option est activée, le Guard génère une copie de sécurité (backup) avant d'effectuer l'action principale ou secondaire souhaitée. La copie de sécurité est conservée en quarantaine. Le fichier peut être restauré à partir du gestionnaire de quarantaines s'il a une valeur informative. En outre, vous pouvez envoyer la copie de sécurité à Avira Malware Research Center. En fonction de l'objet, d'autres possibilités de sélection sont disponibles dans le gestionnaire de quarantaines.

Afficher les messages d'avertissement

Si l'option est activée, un message d'avertissement apparaît avec les actions à exécuter, en cas de détection d'un virus ou d'un programme indésirable.

Action principale

L'action principale est l'action effectuée quand le Guard trouve un virus ou un programme indésirable. Si l'option **réparer** est sélectionnée, mais que la réparation du fichier touché est impossible, l'action sélectionnée sous **Action secondaire** est exécutée.

Remarque
L'option Action secondaire n'est sélectionnable que si sous Action principale le réglage réparer a été sélectionné.

réparer

Si l'option est activée, le Guard répare les fichiers concernés automatiquement. Si le Guard ne peut pas réparer un fichier touché, il exécute l'option choisie sous Action secondaire.

Remarque
Une réparation automatique est recommandée, mais cela signifie que le Guard modifie les fichiers sur l'ordinateur.

supprimer

Si cette option est activée, le fichier est supprimé mais peut être restauré avec les outils adéquats (par ex. Avira UnErase). Le modèle de détection des virus peut ainsi être retrouvé. Cette procédure est beaucoup plus rapide que "écraser et supprimer".

écraser et supprimer

Si cette option est activée, le Guard écrase le fichier par un modèle standard et le supprime ensuite. Il ne peut plus être restauré.

renommer

Si l'option est activée, le Guard renomme le fichier. Un accès direct à ces fichiers (en cliquant deux fois par ex.) n'est alors plus possible. Les fichiers peuvent être réparés ultérieurement et à nouveau renommés.

ignorer

Si l'option est activée, l'accès au fichier est autorisé et le fichier est conservé.

Avertissement
Le fichier touché reste actif sur votre ordinateur! D'importants dégâts peuvent être causés sur votre ordinateur!

Refuser l'accès

Si l'option est activée, le Guard inscrit le résultat positif dans le fichier rapport uniquement si la fonction de rapport est activée. En outre, le Guard écrit une entrée dans le protocole d'événements si cette option est activée.

Quarantaine

Si l'option est activée, le Guard déplace le fichier dans un répertoire de quarantaine. Les fichiers de ce répertoire peuvent être réparés ultérieurement ou - si nécessaire - être envoyés à Avira Malware Research Center.

Action secondaire

L'option **Action secondaire** n'est sélectionnable que si sous **Action principale** l'option **réparer** a été sélectionnée. Cette option permet de décider ce qui doit être fait avec le fichier touché s'il n'est pas réparable.

supprimer

Si cette option est activée, le fichier est supprimé mais peut être restauré avec les outils adéquats (par ex. Avira UnErase). Le modèle de détection des virus peut ainsi être retrouvé. Cette procédure est beaucoup plus rapide que "écraser et supprimer".

écraser et supprimer

Si cette option est activée, le Guard écrase le fichier par un modèle standard et le supprime ensuite. Il ne peut plus être restauré.

renommer

Si l'option est activée, le Guard renomme le fichier. Un accès direct à ces fichiers (en cliquant deux fois par ex.) n'est alors plus possible. Les fichiers peuvent être réparés ultérieurement et à nouveau renommés.

ignorer

Si l'option est activée, l'accès au fichier est autorisé et le fichier est conservé.

Avertissement
Le fichier touché reste actif sur votre ordinateur! D'importants dégâts peuvent être causés sur votre ordinateur!

Refuser l'accès

Si l'option est activée, le Guard inscrit le résultat positif dans le fichier rapport uniquement si la fonction de rapport est activée. En outre, le Guard écrit une entrée dans le protocole d'événements si cette option est activée.

Quarantaine

Si l'option est activée, le Guard déplace le fichier dans un répertoire de quarantaine. Les fichiers peuvent être réparés ultérieurement ou - si nécessaire - être envoyés à Avira Malware Research Center.

Remarque
Si vous avez sélectionné **supprimer** ou écraser et supprimer comme action primaire ou secondaire, veuillez tenir compte du point suivant : en cas de résultats heuristiques, les fichiers affectés ne sont pas supprimés, mais placés en quarantaine.

11.2.1.2. Autres actions

Notifications

Utiliser le rapport d'événement

Si cette option est activée, une entrée est inscrite dans le protocole d'événement à chaque résultat positif. L'administrateur peut détecter les résultats positifs et réagir en conséquence. Ce réglage est activé par défaut.

11.2.1.3. Exceptions

Avec ces options, vous pouvez configurer les objets pour le Guard (recherche en temps réel). Les objets correspondants sont alors ignorés lors de la recherche en temps réel. Le Guard peut ignorer via la liste des processus à exclure leurs accès aux fichiers lors de la recherche en temps réel. Ceci est utile par exemple sur les bases de données ou solutions de sauvegarde.

Processus à exclure par le Guard

Tous les accès aux fichiers par les processus de cette liste sont exclus de la surveillance par le Guard.

Champ de saisie

Dans ce champ, saisissez le nom du processus qui doit être ignoré lors de la recherche en temps réel. Aucun processus n'est indiqué par défaut. Les noms des processus en question sont indiqués dans le gestionnaire des tâches. Dans l'onglet "Processus" (englisch: "Processes") du gestionnaire de tâches, vous voyez les noms de tous les processus actifs. Recherchez "votre" processus et saisissez son nom sous "Nom de l'image" (englisch: "Image Name").

Remarque
Vous pouvez saisir 20 processus au maximum.

Avertissement :
Seuls les 15 premiers caractères du nom du processus (extension incluse) sont pris en compte. S'il existe 2 processus dont les 15 premiers caractères sont similaires, les deux processus sont exclus de la surveillance par le Guard.

Avertissement
Notez que tous les accès aux fichiers par les processus inclus dans la liste sont exclus de la recherche de virus et de programmes indésirables ! L'explorateur Windows et le système d'exploitation eux-mêmes ne peuvent être exclus. Une telle saisie dans la liste serait ignorée.

Ajouter

Avec ce bouton, vous pouvez valider le processus entré dans le champ de saisie dans la fenêtre d'affichage.

Supprimer

Le bouton vous permet de supprimer un processus sélectionné de la fenêtre d'affichage.

Objets de fichiers à exclure par le Guard

Tous les accès fichiers aux objets de cette liste sont exclus de la surveillance par le Guard.

Remarque
Les entrées de la liste ne doivent pas dépasser 6000 caractères au total.

Champ de saisie

Entrez dans ce champ le nom de l'objet fichier qui doit être ignoré par la recherche en temps réel. Aucun objet fichier n'est indiqué par défaut.



Ce bouton ouvre une fenêtre dans laquelle vous pouvez sélectionner l'objet fichier à exclure.

Ajouter

Ce bouton vous permet de reprendre dans la fenêtre d'affichage l'objet fichier entré dans le champ de saisie.

Supprimer

Le bouton Supprimer vous permet de supprimer un objet fichier sélectionné de la fenêtre d'affichage.

Tenez compte des points suivants :

- Les caractères de remplacement * (nombre illimité) et ? (un seul) ne sont autorisés que dans les noms de fichiers.
- Les noms de répertoires doivent se terminer par un antislash \, sous peine d'être pris pour un nom de fichier.
- La liste est traitée de haut en bas.
- Certaines extensions de fichiers peuvent aussi être exclues (y compris avec des caractères de remplacement).
- Lorsqu'un répertoire est exclu, tous ses sous-répertoires sont automatiquement ignorés.
- Plus la liste est longue, plus le temps processeur nécessaire au traitement de la liste pour chaque accès augmente. Tenez la liste aussi courte que possible.
- Pour exclure des objets également lors d'un accès avec un nom de fichier DOS court (convention de noms DOS 8.3), le nom de fichier court correspondant doit aussi être saisi dans la liste.
- Pour exclure des fichiers et répertoires sur des lecteurs réseau connectés, de la recherche effectuée par le Guard, notez dans la liste des exceptions le même chemin UNC que celui que vous utilisez pour connecter le lecteur réseau : \\<Nom de l'ordinateur>\<Partage>\ - OU- \\<Adresse IP>\<Partage>\

Remarque
Un nom de fichier contenant des caractères de remplacement ne doit pas se terminer par un antislash.

Exemple :

```
C:\Programmes\Application\applic*.exe\
```

Cette saisie n'est pas bonne et n'est pas traitée comme une exception !

Remarque
Pour les exceptions sur des lecteurs réseau connectés, tenez compte du point suivant : si vous utilisez la lettre du lecteur connecté, les fichiers et répertoires indiqués ne sont PAS exclus de la recherche effectuée par le Guard. Si le chemin UNC figurant dans la liste des exceptions est différent de celui utilisé pour connecter le lecteur réseau (indication de l'adresse IP dans la liste des exceptions – indication du nom de l'ordinateur pour la connexion avec le lecteur réseau), les fichiers et répertoires indiqués ne sont PAS exclus de la recherche effectuée par le Guard. Déterminez le chemin UNC à utiliser, à l'aide du fichier de rapport du Guard.

Remarque
Sur les lecteurs dynamiques qui sont intégrés (montés) en tant que répertoire sur un autre lecteur, vous devez utiliser dans la liste des exceptions, l'alias du système d'exploitation pour le lecteur intégré :
par ex. \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
Si vous utilisez le point de mise à disposition (mount point) lui-même, par ex. C:\DynDrive, le lecteur dynamique sera malgré tout contrôlé. Vous pouvez déterminer l'alias du système d'exploitation à utiliser, à partir du fichier de rapport du Guard.

Remarque
Vous pouvez déterminer les chemins utilisés par le Guard lors de la recherche de fichiers contaminés, à partir du fichier de rapport du Guard. Utilisez systématiquement les mêmes chemins dans la liste des exceptions. Procédez comme : Réglez la fonction de protocole du Guard dans la configuration sous Guard :: Rapport sur **Intégral**. Le Guard étant activé, accédez maintenant aux fichiers, répertoires, lecteurs intégrés ou lecteurs réseau connectés. Vous pouvez maintenant lire le chemin à utiliser à partir du fichier de rapport du Guard. Vous accédez au fichier de rapport dans le Control Center sous Protection locale ::Guard.

Exemples :

```
C:
C:\
C:\*.*
C:\*
*.exe
*.xl?
*.*
C:\Programmes\Application\application.exe
C:\Programmes\Application\applic*.exe
C:\Programmes\Application\applic*
C:\Programmes\Application\applic?????.e*
C:\Programmes\
C:\Programmes
C:\Programmes\Application\*.mdb
\\Nom de l'ordinateur\Partage\
\\1.0.0.0\Partage\application.exe
```

11.2.1.4. Heuristique

Cette rubrique de configuration contient les réglages pour l'heuristique du moteur de recherche Avira AntiVir Professional.

Avira AntiVir Professional contient des heuristiques très performantes qui permettent de détecter dynamiquement des logiciels malveillants inconnus, c'est-à-dire avant même qu'une signature de virus spéciale n'ait été créée contre le parasite et qu'une mise à jour de protection antivirus correspondante n'ait été envoyée. La détection des virus s'effectue par une analyse et un examen complet du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés sont aussi possibles. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code annoncé est digne de confiance.

Heuristique macrovirus

Heuristique macrovirus

Avira AntiVir Professional contient une heuristique de macrovirus très performante. Si cette option est activée, toutes les macros du document affecté sont supprimées si une réparation est possible ; alternativement, les documents suspects sont seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce réglage est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

Avira AntiVir Professional contient une heuristique très performante grâce à la technologie AHeAD, lui permettant de détecter aussi les (nouveaux) logiciels malveillants inconnus. Si cette option est activée, vous pouvez régler ici la "sensibilité" de cette heuristique. Ce réglage est activé par défaut.

Degré d'identification bas

Si cette option est activée, Avira AntiVir Professional détecte un peu moins de logiciels malveillants inconnus, le risque de messages erronés est faible dans ce cas.

Degré d'identification moyen

C'est le réglage par défaut quand vous avez choisi l'utilisation de cette heuristique.

Degré d'identification élevé

Si l'option est activée, Avira AntiVir Professional détecte beaucoup plus de logiciels malveillants inconnus, mais vous devez vous attendre aussi à des messages erronés.

11.2.2 Rapport

Le Guard dispose d'une fonction étendue de documentation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif.

Documentation

Ce groupe permet de définir le contenu du fichier de rapport.

Désactivé

Si cette option est activée, le Guard ne génère pas de rapport.
Ne renoncez à la documentation que dans des cas exceptionnels, par ex. uniquement lorsque vous effectuez des tests avec de nombreux virus ou programmes indésirables.

Standard

Si cette option est activée, le Guard consigne les informations importantes (sur le résultat positif, les avertissements et les erreurs) dans le fichier de rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce réglage est activé par défaut.

Étendu

Si cette option est activée, le Guard consigne également les informations secondaires dans le fichier rapport.

Intégrale

Si cette option est activée, le Guard consigne toutes les informations - même celles sur la taille et le type des fichiers, la date, etc. - dans le fichier de rapport.

Limiter le fichier de rapport

Limiter la taille à n Mo

Si cette option est activée, le fichier rapport peut être limité à une taille définie ; valeurs possibles : 1 à 100 Mo. Ce réglage est activé par défaut avec une valeur de 1 Mo.

Sauvegarder le fichier de rapport avant de raccourcir

Si l'option est activée, le fichier de rapport est sauvegardé avant d'être raccourci. Emplacement de sauvegarde, voir Configuration :: Généralités :: Répertoires :: Répertoire de rapport.

Écrire la configuration dans le fichier de rapport

Si cette option est activée, la configuration de la recherche en temps réel utilisée est écrite dans le fichier rapport.

11.3 MailGuard

La rubrique MailGuard de la Configuration Avira AntiVir Professional est en charge de la configuration du MailGuard.

11.3.1 Recherche

Vous utilisez le MailGuard pour contrôler les emails entrants quant à l'absence de virus et de logiciels malveillants . Il est possible de faire contrôler les emails sortants par le MailGuard, quant à l'absence de virus et de logiciels malveillants.

Recherche

Contrôler les emails entrants

Si l'option est activée, les emails entrants sont contrôlés quant à l'absence de virus et de logiciels malveillants . MailGuard prend en charge les protocoles POP3 et IMAP. Activez le compte de la boîte de réception utilisé par votre client email pour la réception des emails, pour le faire surveiller par le MailGuard.

Surveiller les comptes POP3

Si l'option est activée, les comptes POP3 sont surveillés sur les ports indiqués.

Ports surveillés

Saisissez dans ce champ le port utilisé comme boîte de réception par le protocole POP3. Vous pouvez indiquer plusieurs ports en les séparant par des virgules.

Standard

Ce bouton permet de réinitialiser les ports indiqués au port par défaut de POP3.

Surveiller les comptes IMAP

Si l'option est activée, les comptes IMAP sont surveillés sur les ports indiqués.

Ports surveillés

Saisissez dans ce champ le port utilisé par le protocole IMAP. Vous pouvez indiquer plusieurs ports en les séparant par des virgules.

Standard

Ce bouton permet de réinitialiser les ports indiqués au port par défaut d'IMAP.

Contrôler les emails sortants (SMTP)

Si l'option est activée, les emails sortants sont contrôlés quant à l'absence de virus et de logiciels malveillants.

Ports surveillés

Saisissez dans ce champ le port utilisé comme boîte d'envoi par le protocole SMTP. Vous pouvez indiquer plusieurs ports en les séparant par des virgules.

Standard

Ce bouton permet de réinitialiser les ports indiqués au port par défaut de SMTP.

Remarque
Pour vérifier les protocoles et les ports utilisés, affichez les propriétés de vos comptes email dans le programme client de messagerie électronique. Les ports par défaut sont utilisés la plupart du temps.

11.3.1.1. Action en cas de résultat positif

Cette rubrique de configuration contient les réglages concernant les actions effectuées lorsque le MailGuard trouve un virus ou un programme indésirable dans un email ou une pièce jointe.

Remarque
Les actions réglées ici sont exécutées en cas de détection de virus dans des emails entrants, de même que dans des emails sortants.

Action en cas de résultat positif

Interactif

Si cette option est activée, une fenêtre de dialogue s'affiche pour sélectionner l'action à effectuer avec le fichier touché en cas de détection d'un virus ou d'un programme indésirable dans un email ou une pièce jointe. Cette option est activée par défaut.

Actions autorisées

Dans cette zone d'affichage, vous pouvez choisir quelles actions s'afficheront dans la fenêtre de dialogue en cas de détection d'un virus ou d'un programme indésirable. Vous devez pour cela activer les options correspondantes.

Déplacer en quarantaine

Si l'option est activée, l'email, y compris toutes les pièces jointes, est déplacé en quarantaine. Il peut être délivré ultérieurement par le gestionnaire de quarantaines. L'email touché est supprimé. Le corps et les pièces jointes éventuelles de l'email sont remplacés par un texte standard.

Supprimer

Si cette option est activée, l'email touché est automatiquement supprimé si un virus ou un programme indésirable a été détecté. Le corps et les pièces jointes éventuelles sont remplacés par un texte standard.

Supprimer la pièce jointe

Si cette option est activée, la pièce jointe touchée est remplacée par un texte standard. Si le corps de l'email est touché, celui-ci est supprimé et également remplacé par un texte standard. L'email lui-même est délivré.

Déplacer la pièce jointe en quarantaine

Si cette option est activée, la pièce jointe touchée est placée en quarantaine puis supprimée (remplacée par un texte standard). Le corps de l'email est délivré. La pièce jointe touchée peut être délivrée plus tard par le gestionnaire de quarantaines.

Ignorer

Si cette option est activée, un email touché est délivré même si un virus ou un programme indésirable a été détecté.

Standard

A l'aide de ce bouton, vous pouvez sélectionner l'action activée par défaut dans la fenêtre de dialogue en cas de détection d'un virus. Sélectionnez l'action activée par défaut et cliquez sur le bouton **Standard**.

Afficher la barre de progression

Si cette option est activée, le MailGuard affiche une barre de progression pendant le téléchargement des emails. L'activation de cette option n'est possible que si l'option **Interactif** a été sélectionnée.

Automatique

Si cette option est activée, vous n'êtes plus prévenu si un virus ou un programme indésirable est détecté. Le MailGuard réagit en fonction de vos réglages effectués dans cette section.

Action principale

L'action principale est l'action exécutée quand le MailGuard trouve un virus ou un programme indésirable dans un email. Si l'option **Ignorer l'email** est sélectionnée, vous pouvez choisir sous **Pièces jointes touchées** ce qui doit se passer quand un résultat positif est détecté dans une pièce jointe.

Supprimer l'email

Si cette option est activée, l'email touché est automatiquement supprimé si un virus ou un programme indésirable a été détecté. Le corps de l'email (body) est remplacé par le texte standard ci-dessous. La même chose s'applique à toutes les pièces jointes incluses (attachments) ; celles-ci sont également remplacées par un texte standard.

Isoler l'email

Si cette option est activée, l'email complet avec toutes ses pièces jointes est mis en Quarantaine si un virus ou un programme indésirable est détecté. Il pourra ensuite être restauré. L'email lui-même est supprimé. Le corps de l'email (body) est remplacé par le texte standard ci-dessous. La même chose s'applique à toutes les pièces jointes incluses (attachments) ; celles-ci sont également remplacées par un texte standard.

Ignorer l'email

Si cette option est activée, l'email touché est automatiquement ignoré si un virus ou un programme indésirable a été détecté. Vous avez toutefois la possibilité de décider ce qui doit arriver avec une pièce jointe touchée :

Pièces jointes touchées

L'option **Pièces jointes touchées** n'est sélectionnable que si sous **Action principale** le réglage **Ignorer l'email** a été sélectionné. Cette option permet de décider ce qui doit être fait en cas de pièce jointe touchée.

supprimer

Si cette option est activée, la pièce jointe touchée par un virus ou un programme indésirable est supprimée et remplacée par un texte standard.

isoler

Si cette option est activée, la pièce jointe touchée est placée en quarantaine puis supprimée (et remplacée par un texte standard). La pièce jointe touchée pourra ensuite être restaurée.

ignorer

Si cette option est activée, la pièce jointe touchée est automatiquement ignorée et délivrée même si un virus ou un programme indésirable a été détecté.

Avertissement
Si vous choisissez cette option, vous n'êtes pas du tout protégé des virus et programmes indésirables par le MailGuard. Ne choisissez cette rubrique que si vous savez exactement ce que vous faites. Désactivez l'aperçu dans votre programme de courrier électronique, n'ouvrez pas les pièces jointes par double-clic !

11.3.1.2. Autres actions

Cette rubrique de configuration contient d'autres réglages concernant les actions effectuées lorsque le MailGuard trouve un virus ou un programme indésirable dans un email ou une pièce jointe.

Remarque
Les actions réglées ici sont exécutées exclusivement en cas de détection de virus dans des emails entrants.

Texte standard pour les emails supprimés et déplacés

Le texte dans ce champ est ajouté comme message dans l'email, à la place de l'email concerné. Vous pouvez éditer ce message. Un texte ne doit pas contenir plus de 500 caractères.

Vous pouvez utiliser les combinaisons de touches suivantes pour le formatage:

Strg + Enter ajoute un saut de ligne.

Standard

Le bouton insère un texte standard prédéfini dans le champ d'édition.

Texte standard pour les pièces jointes supprimées et déplacées

Le texte dans ce champ est ajouté comme message dans l'email, à la place de la pièce jointe concernée. Vous pouvez éditer ce message. Un texte ne doit pas contenir plus de 500 caractères.

Vous pouvez utiliser les combinaisons de touches suivantes pour le formatage:

Strg + Enter ajoute un saut de ligne.

Standard

Le bouton insère un texte standard prédéfini dans le champ d'édition.

11.3.1.3. Heuristique

Cette rubrique de configuration contient les réglages pour l'heuristique du moteur de recherche Avira AntiVir Professional.

Avira AntiVir Professional contient des heuristiques très performantes qui permettent de détecter dynamiquement des logiciels malveillants inconnus, c'est-à-dire avant même qu'une signature de virus spéciale n'ait été créée contre le parasite et qu'une mise à jour de protection antivirus correspondante n'ait été envoyée. La détection des virus s'effectue par une analyse et un examen complet du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés sont aussi possibles. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code annoncé est digne de confiance.

Heuristique macrovirus

Activer l'heuristique de macrovirus

Avira AntiVir Professional contient une heuristique de macrovirus très performante. Si cette option est activée, toutes les macros du document affecté sont supprimées si une réparation est possible ; alternativement, les documents suspects sont seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce réglage est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

Avira AntiVir Professional contient une heuristique très performante grâce à la technologie AHeAD, lui permettant de détecter aussi les (nouveaux) logiciels malveillants inconnus. Si cette option est activée, vous pouvez régler ici la "sensibilité" de cette heuristique. Ce réglage est activé par défaut.

Degré d'identification bas

Si cette option est activée, Avira AntiVir Professional détecte un peu moins de logiciels malveillants inconnus, le risque de messages erronés est faible dans ce cas.

Degré d'identification moyen

C'est le réglage par défaut quand vous avez choisi l'utilisation de cette heuristique. Ce réglage est activé par défaut et recommandé.

Degré d'identification élevé

Si l'option est activée, Avira AntiVir Professional détecte beaucoup plus de logiciels malveillants inconnus, mais vous devez vous attendre aussi à des messages erronés.

11.3.2 Généralités

11.3.2.1. Exceptions

Adresses emails qui ne sont pas contrôlées

Ce tableau vous donne la liste des adresses emails qui ont été exclues de la surveillance par AntiVir MailGuard (liste blanche).

Remarque
La liste des exceptions est utilisée par le MailGuard exclusivement pour les emails entrants.

État

Symbole	Description
	Cette adresse email ne sera plus contrôlée à la recherche de logiciels malveillants.

Adresse email

Adresse email qui ne doit plus être parcourue.

Logiciel malveillant

Si l'option est activée, l'adresse email ne sera plus contrôlée à la recherche de logiciels malveillants.

vers le haut

Ce bouton vous permet de déplacer une adresse email sélectionnée d'une position vers le haut. Ce bouton n'est pas disponible si aucune entrée n'est sélectionnée ou si l'adresse sélectionnée figure en première position dans la liste.

vers le bas

Ce bouton vous permet de déplacer une adresse email sélectionnée d'une position vers le bas. Ce bouton n'est pas disponible si aucune entrée n'est sélectionnée ou si l'adresse sélectionnée figure en dernière position dans la liste.

Champ de saisie

Dans ce champ, saisissez l'adresse email que vous souhaitez ajouter à la liste des adresses emails à ne pas contrôler. L'adresse email ne sera plus contrôlée par le MailGuard, quels que soient vos réglages.

Ajouter

Ce bouton vous permet d'ajouter à la liste des adresses emails à ne pas contrôler l'adresse email entrée dans le champ de saisie.

Supprimer

Ce bouton efface l'adresse email sélectionnée dans la liste.

11.3.2.2. Mémoire tampon

Mémoire tampon

La mémoire tampon du MailGuard contient les données sur les emails parcourus qui sont affichés dans les statistiques du Control Center sous MailGuard.

Nombre maximum d'emails à mémoriser dans la mémoire tampon

Dans ce champ, saisissez le nombre maximum d'emails conservés dans la mémoire tampon du MailGuard. Les emails les plus anciens sont supprimés en premier.

Durée de mémorisation maximale d'un email en jours

Saisissez dans ce champ la durée de mémorisation maximale d'un email en jours. Après cet intervalle, l'email est supprimé de la mémoire tampon.

Vider la mémoire tampon

Cliquez sur ce bouton pour supprimer les emails conservés dans la mémoire tampon.

11.3.3 Rapport

Le MailGuard dispose d'une fonction étendue de documentation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif.

Documentation

Ce groupe permet de définir le contenu du fichier de rapport.

Désactivé

Si cette option est activée, le MailGuard ne génère pas de rapport.
Ne renoncez à la documentation que dans des cas exceptionnels, par ex. uniquement lorsque vous effectuez des tests avec de nombreux virus ou programmes indésirables.

Standard

Si cette option est activée, le MailGuard consigne les informations importantes (sur le résultat positif, les avertissements et les erreurs) dans le fichier de rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce réglage est activé par défaut.

Étendu

Si cette option est activée, le MailGuard consigne également les informations secondaires dans le fichier rapport.

Intégrale

Si cette option est activée, le MailGuard consigne toutes les informations - même celles sur la taille et le type des fichiers, la date, etc. - dans le fichier de rapport.

Limiter le fichier de rapport

Limiter la taille à n Mo

Si cette option est activée, le fichier rapport peut être limité à une taille définie ; valeurs possibles : 1 à 100 Mo. Ce réglage est activé par défaut avec une valeur de 1 Mo. Une tolérance de 50 kilo-octets environ est accordée pour maintenir la charge de l'ordinateur à un faible niveau. Si la taille du fichier de rapport dépasse la taille indiquée de 50 kilo-octets, les anciennes entrées sont supprimées automatiquement jusqu'à ce que la taille indiquée moins 50 kilo-octets soit atteinte.

Sauvegarder le fichier de rapport avant de raccourcir

Si l'option est activée, le fichier de rapport est sauvegardé avant d'être raccourci. Emplacement de sauvegarde, voir Configuration :: Généralités :: Répertoires :: Répertoire de rapport.

Écrire la configuration dans le fichier de rapport

Si l'option est activée, la configuration utilisée par le MailGuard est écrite dans le fichier de rapport.

11.4 WebGuard

La rubrique WebGuard de la Configuration Avira AntiVir Professional est en charge de la configuration du WebGuard.

11.4.1 Recherche

Le WebGuard vous protège des virus et logiciels malveillants qui parviennent sur votre ordinateur par le biais des sites Internet que vous chargez dans votre navigateur Internet. Vous pouvez configurer le comportement du WebGuard dans la rubrique *Recherche*.

Recherche

Activer le WebGuard

Si l'option est activée, les sites Internet auxquels vous accédez par un navigateur Internet sont contrôlés quant à l'absence de virus et de logiciels malveillants : Le WebGuard surveille les données en provenance d'Internet, transmises via le protocole HTTP sur les ports 80, 8080, 3128. Les sites Internet contaminés sont bloqués au chargement. Si l'option est désactivée, le service WebGuard reste actif, mais la recherche de virus et logiciels malveillants est désactivée.

Protection contre les téléchargements automatiques intempestifs

La protection contre les téléchargements automatiques intempestifs vous permet de procéder à des réglages visant à bloquer les I-Frames, appelées aussi Inline frames. Les I-Frames sont des éléments HTML, c'est-à-dire des éléments de sites Internet qui délimitent une zone d'une page Web. Grâce aux I-Frames, il est possible de charger et d'afficher d'autres contenus Web – le plus souvent d'autres URL – en tant que documents autonomes, dans une sous-fenêtre du navigateur. Les I-Frames sont la plupart du temps utilisées pour la publicité par bandeau publicitaire. Dans certains cas, les I-Frames servent à dissimuler des logiciels malveillants. La zone de l'I-Frame n'est alors le plus souvent peu ou pas visible dans le navigateur. L'option *Bloquer les I-Frames suspectes* vous donne la possibilité de contrôler et de bloquer le chargement des I-Frames.

Bloquer les I-Frames suspectes

Si l'option est activée, les I-Frames des sites Internet demandés sont contrôlées selon certains critères. Si des I-Frames suspectes sont présentes sur un site Internet demandé, l'I-Frame est bloquée. Un message d'erreur (code d'état HTTP 403) s'affiche dans la fenêtre de l'I-Frame.

Standard

Si l'option est activée, toutes les I-Frames avec des contenus suspects sont bloquées.

Étendu

Si l'option est activée, toutes les I-Frames avec des contenus suspects et/ou qui sont utilisées d'une manière suspecte sont bloquées. Il a y utilisation suspecte d'I-Frames quand l'I-Frame est très petite et qu'elle est de ce fait peu ou pas visible dans le navigateur ou lorsque l'I-Frame est placée dans une position inhabituelle sur la page Web.

11.4.1.1. Action en cas de résultat positif

Action en cas de résultat positif

Vous pouvez établir des actions que le WebGuard doit exécuter quand un virus ou programme indésirable a été détecté.

Interactif

Si l'option est activée, pendant la recherche directe, si un virus ou un programme indésirable est détecté, une fenêtre de dialogue dans laquelle vous sélectionnez quoi faire avec le fichier touché apparaît. Ce réglage est activé par défaut.

Actions autorisées

Dans cette zone d'affichage, vous pouvez choisir quelles actions s'afficheront dans la fenêtre de dialogue en cas de détection d'un virus ou d'un programme indésirable. Vous devez pour cela activer les options correspondantes.

Refuser l'accès

La page Web demandée par le serveur Web ou les données et fichiers transmis ne sont pas envoyés à votre navigateur Web. Dans le navigateur Web, un message d'erreur de refus d'accès s'affiche. Le WebGuard inscrit le résultat positif dans le fichier rapport, à condition que la fonction de rapport soit activée. En outre, le WebGuard inscrit une entrée dans le protocole d'événements, si cette option est activée.

Quarantaine

La page Web demandée par le serveur Web ou les données et fichiers transmis sont déplacés en quarantaine en cas de détection d'un virus ou d'un logiciel malveillant. Le fichier peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou - si nécessaire - être envoyé à Avira Malware Research Center.

ignorer

La page Web demandée par le serveur Web ou les données et fichiers transmis sont envoyés à votre navigateur Web par le WebGuard.

Standard

A l'aide de ce bouton, vous pouvez sélectionner l'action activée par défaut dans la fenêtre de dialogue en cas de détection d'un virus. Sélectionnez l'action activée par défaut et cliquez sur le bouton "Standard".

Vous trouverez de plus amples informations ici.

Afficher la barre de progression

Si l'option est activée, un message affiché sur le bureau apparaît avec une barre de progression de téléchargement, lorsque le téléchargement de contenus de sites Internet dépasse un délai d'attente de 20 secondes . Ce message affiché sur le bureau sert notamment à contrôler le téléchargement de sites Internet avec de gros volumes de données : lors de la navigation avec le WebGuard, les contenus des sites Internet ne sont pas chargés successivement dans le navigateur Internet, du fait qu'ils sont contrôlés quant à l'absence de virus et de logiciels malveillants avant d'être affichés dans le navigateur. Cette option est désactivée par défaut.

Automatique

Si l'option est activée, aucun dialogue permettant de sélectionner une action ne s'affiche en cas de détection d'un virus ou d'un programme indésirable. Le WebGuard réagit en fonction de vos réglages effectués dans cette section.

Afficher les messages d'avertissement

Si l'option est activée, un message d'avertissement apparaît avec les actions à exécuter, en cas de détection d'un virus ou d'un programme indésirable.

Action principale

L'action principale est l'action effectuée lorsque le WebGuard trouve un virus ou un programme indésirable.

Refuser l'accès

La page Web demandée par le serveur Web ou les données et fichiers transmis ne sont pas envoyés à votre navigateur Web. Dans le navigateur Web, un message d'erreur de refus d'accès s'affiche. Le WebGuard inscrit le résultat positif dans le fichier rapport, à condition que la fonction de rapport soit activée. En outre, le WebGuard inscrit une entrée dans le protocole d'événements, si cette option est activée.

isoler

La page Web demandée par le serveur Web ou les données et fichiers transmis sont déplacés en quarantaine en cas de détection d'un virus ou d'un logiciel malveillant. Le fichier peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou - si nécessaire - être envoyé à Avira Malware Research Center.

ignorer

La page Web demandée par le serveur Web ou les données et fichiers transmis sont envoyés à votre navigateur Web par le WebGuard. L'accès au fichier est autorisé et le fichier est conservé.

Avertissement
Le fichier touché reste actif sur votre ordinateur! D'importants dégâts peuvent être causés sur votre ordinateur!

11.4.1.2. Accès bloqués

Sous **Accès bloqués**, vous pouvez indiquer les types de fichiers et les types MIME (types de contenus des données transmises) qui doivent être bloqués par le WebGuard. Le filtre Web vous permet de bloquer les URL indésirables, comme par ex. des URL à hameçonnage et de logiciel malveillant. Le WebGuard empêche la transmission des données d'Internet vers votre ordinateur.

Types de fichiers / types MIME (définis par l'utilisateur) à exclure par le WebGuard

Tous les types de fichiers et les types MIME (types de contenus des données transmises) figurant dans la liste sont bloqués par le WebGuard.

Champ de saisie

Saisissez dans ce champ les noms des types MIME et des types de fichiers qui doivent être bloqués par le WebGuard. Pour les types de fichiers, saisissez l'extension de fichier, par ex. **.htm**. Pour les types MIME, notez le type de support et éventuellement le sous-type. Les deux indications sont séparées par une barre oblique, par ex. **video/mpeg** ou **audio/x-wav**.

Remarque
Les fichiers qui ont déjà été enregistrés sur votre ordinateur comme fichiers Internet temporaires, sont certes bloqués par le WebGuard, mais peuvent être chargés localement par votre ordinateur à partir du navigateur Internet. Les fichiers Internet temporaires sont des fichiers sauvegardés sur votre ordinateur par le navigateur Internet, pour pouvoir afficher plus rapidement les sites Internet.

Remarque
La liste des types de fichiers et types MIME à bloquer est ignorée si des entrées figurent dans la liste des types de fichiers et types MIME à exclure sous WebGuard::Recherche::Exceptions.

Remarque
Lorsque vous indiquez des types de fichiers et des types MIME, vous ne pouvez pas utiliser de caractères de remplacement (caractère de remplacement * pour un nombre au choix de caractères ou ? pour un caractère exactement).

Types MIME : exemples de types de médias :

- `text` = pour fichiers texte
- `image` = pour fichiers graphiques
- `video` = pour fichiers vidéo
- `audio` = pour fichiers son
- `application` = pour les fichiers associés à un certain programme

Exemples : types de fichiers et types MIME à exclure

- `application/octet-stream` = les fichiers du type MIME application/octet-stream (fichiers exécutables *.bin, *.exe, *.com, *dll, *.class) sont bloqués par le WebGuard.
- `application/olescript` = les fichiers du type MIME application/olescript (fichiers script ActiveX *.axs) sont bloqués par le WebGuard.
- `.exe` = tous les fichiers avec l'extension .exe (fichiers exécutables) sont bloqués par le WebGuard.
- `.msi` = tous les fichiers avec l'extension .msi (fichiers Windows Installer) sont bloqués par le WebGuard.

Ajouter

Avec ce bouton, vous pouvez valider le type MIME ou de fichier entré dans le champ de saisie dans la fenêtre d'affichage.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas fonctionnel si aucune entrée n'est sélectionnée.

Filtre Web

Le filtre Web dispose d'une base de données interne mise à jour quotidiennement, dans laquelle les URL sont classées par critères de contenus.

Activer le filtre Web

Si l'option est activée, toutes les URL figurant parmi les catégories sélectionnées dans la liste du filtre Web sont bloquées.

Liste du filtre Web

La liste du filtre Web vous permet de choisir les catégories de contenus dont les URL doivent être bloquées par le WebGuard.

Remarque
Le filtre Web est ignoré si des entrées figurent dans la liste des URL à ignorer sous WebGuard::Recherche::Exceptions.

Remarque
Sous la rubrique URL de spam sont catégorisées les URL diffusées par des emails de spam. La catégorie Arnaque et fraude englobe les sites Internet comportant des 'pièges d'abonnement' et autres offres de services dont les coûts sont dissimulés par le fournisseur.

11.4.1.3. Exceptions

Ces options vous permettent d'exclure des types MIME (types de contenus des données transmises) et des URL (adresses Internet) de la recherche du WebGuard. Les types MIME et les URL indiqués sont ignorés par le WebGuard, ce qui signifie que ces données ne sont pas contrôlées quant à l'absence de virus et logiciels malveillants, lors de la transmission sur votre ordinateur.

Types de MIME à exclure par le WebGuard

Dans ce champ, vous pouvez sélectionner les types MIME (types de contenus des données transmises) à exclure de la recherche par WebGuard.

Types de fichiers à exclure par le WebGuard / types MIME (définis par l'utilisateur)

Tous les types de fichiers et types MIME (types de contenus des données transmises) de la liste sont exclus de la recherche par le WebGuard.

Champ de saisie

Dans ce champ, vous pouvez sélectionner les types MIME et types de fichiers à exclure de la recherche par le WebGuard. Pour les types de fichiers, saisissez l'extension de fichier, par ex. **.htm**. Pour les types MIME, notez le type de support et éventuellement le sous-type. Les deux indications sont séparées par une barre oblique, par ex. **video/mpeg** ou **audio/x-wav**.

Remarque
Lorsque vous indiquez des types de fichiers et des types MIME, vous ne pouvez pas utiliser de caractères de remplacement (caractère de remplacement * pour un nombre au choix de caractères ou ? pour un caractère exactement).

Avertissement
Tous les types de fichiers et types de contenus figurant dans la liste d'exception sont chargés dans le navigateur Internet sans autre contrôle des accès bloqués (liste des types de fichiers et types MIME à bloquer sous WebGuard::Recherche::Accès bloqués) ou du WebGuard : toutes les entrées de la liste d'exception concernant les types de fichiers et types MIME à bloquer sont ignorées. Aucune recherche n'est effectuée quant à l'absence de virus et de logiciels malveillants.

Types MIME : exemples de types de médias :

- `text` = pour fichiers texte
- `image` = pour fichiers graphiques
- `video` = pour fichiers vidéo
- `audio` = pour fichiers son
- `application` = pour les fichiers associés à un certain programme

Exemples : types de fichiers et MIME à exclure

- `audio/` = tous les fichiers de type de média audio sont exclus de la recherche du WebGuard
- `video/quicktime` = tous les fichiers vidéo du sous-type Quicktime (*.qt, *.mov) sont exclus de la recherche du WebGuard
- `.pdf` = tous les fichiers PDF Adobe sont exclus de la recherche du WebGuard.

Ajouter

Avec ce bouton, vous pouvez valider le type MIME ou de fichier entré dans le champ de saisie dans la fenêtre d'affichage.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas fonctionnel si aucune entrée n'est sélectionnée.

URL à exclure par le WebGuard

Toutes les URL de cette liste sont exclues de la recherche du WebGuard.

Champ de saisie

Saisissez dans ce champ les URL (adresses Internet) à exclure de la recherche du WebGuard, par ex. **www.domainname.com/**. Vous pouvez indiquer des parties de l'URL en marquant le niveau de domaine avec des points finaux ou de début : .nom de domaine.fr pour tous les sites et tous les sous-domaines du domaine. Notez un site Web avec un domaine de premier niveau quelconque (.com ou .net) avec un point final : **domainname.**. Si vous notez une suite de caractères sans point final ou point de début, celle-ci sera interprétée comme un domaine de niveau supérieur, par ex. **net** pour tous les domaines NET (www.domain.net).

Remarque
Lors de l'indication des URL, vous pouvez également utiliser le caractère de remplacement * pour un nombre au choix de caractères. Utilisez aussi des points finaux ou de début en combinaison avec les caractères de remplacement, pour repérer les niveaux de domaine :
.domainname.*
*.domainname.com
.*name*.com (valable mais n'est pas conseillé)
Les indications sans points comme *name* sont interprétées comme des parties d'un domaine de niveau supérieur et ne sont pas pertinentes.

Avertissement
Tous les sites Web figurant dans la liste des URL à exclure sont chargés dans le navigateur Internet sans autre contrôle par le filtre Web ou le WebGuard : toutes les entrées de la liste des URL à ignorer concernant le filtre Web sont ignorées (voir WebGuard::Recherche::Accès bloqués). Aucune recherche n'est effectuée quant à l'absence de virus et de logiciels malveillants. Par conséquent, n'excluez de la recherche du WebGuard que les URL dignes de confiance.

Ajouter

Avec ce bouton, vous pouvez valider l'URL (adresse Internet) entrée dans le champ de saisie de la fenêtre d'affichage.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas fonctionnel si aucune entrée n'est sélectionnée.

Exemples : URLs à exclure

- `www.avira.com` -OU- `www.avira.com/*`

  = Toutes les URL avec le domaine 'www.avira.com' sont exclues de la recherche du WebGuard : www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,.. Les URL avec le domaine www.avira.fr ne sont pas exclues de la recherche du WebGuard.

- `avira.com` -OU- `*.avira.com`

  = Toutes les URL avec le domaine de second niveau et de niveau supérieur 'avira.com' sont exclues de la recherche du WebGuard. L'indication implique tous les sous-domaines existants pour '.avira.com' : www.avira.com, forum.avira.com,...

- `avira.` -OU- `*.avira.*`

  = Toutes les URL avec le domaine de second niveau 'avira' sont exclues de la recherche du WebGuard. L'indication implique tous les domaines de niveau supérieur ou sous-domaines existants pour '.avira.' : www.avira.com, www.avira.de, forum.avira.com,...

- `.*domaine*.*`

  Toutes les URL contenant un domaine de second niveau avec la chaîne de caractères 'domaine' sont exclues de la recherche du WebGuard : www.domaine.com, www.new-domaine.fr, www.sample-domaine1.fr, ...

- `net` -OU- `*.net`

  = Toutes les URL avec le domaine de niveau supérieur 'net' sont exclues de la recherche du WebGuard : www.name1.net, www.name2.net, ...

Avertissement
Indiquez aussi précisément que possible les URL que vous souhaitez exclure de la recherche du WebGuard. Évitez d'indiquer des ensembles de domaines de niveau supérieur ou des parties d'un nom de domaine de second niveau, car il y a un risque que des pages Internet propageant des logiciels malveillants ou programmes indésirables soient exclues de la recherche du WebGuard par des indications globales définies sous la rubrique Exceptions. Il est recommandé d'indiquer au moins le domaine de second niveau dans son entier et le domaine de niveau supérieur : domainname.com

11.4.1.4. Heuristique

Cette rubrique de configuration contient les réglages pour l'heuristique du moteur de recherche Avira AntiVir Professional.

Avira AntiVir Professional contient des heuristiques très performantes qui permettent de détecter dynamiquement des logiciels malveillants inconnus, c'est-à-dire avant même qu'une signature de virus spéciale n'ait été créée contre le parasite et qu'une mise à jour de protection antivirus correspondante n'ait été envoyée. La détection des virus s'effectue par une analyse et un examen complet du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés sont aussi possibles. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code annoncé est digne de confiance.

Heuristique macrovirus

Heuristique macrovirus

Avira AntiVir Professional contient une heuristique de macrovirus très performante. Si cette option est activée, toutes les macros du document affecté sont supprimées si une réparation est possible ; alternativement, les documents suspects sont seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce réglage est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

Avira AntiVir Professional contient une heuristique très performante grâce à la technologie AHeAD, lui permettant de détecter aussi les (nouveaux) logiciels malveillants inconnus. Si cette option est activée, vous pouvez régler ici la "sensibilité" de cette heuristique. Ce réglage est activé par défaut.

Degré d'identification bas

Si cette option est activée, Avira AntiVir Professional détecte un peu moins de logiciels malveillants inconnus, le risque de messages erronés est faible dans ce cas.

Degré d'identification moyen

C'est le réglage par défaut quand vous avez choisi l'utilisation de cette heuristique.

Degré d'identification élevé

Si l'option est activée, Avira AntiVir Professional détecte beaucoup plus de logiciels malveillants inconnus, mais vous devez vous attendre aussi à des messages erronés.

11.4.2 Rapport

Le WebGuard dispose d'une fonction étendue de documentation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif.

Documentation

Ce groupe permet de définir le contenu du fichier de rapport.

Désactivé

Si cette option est activée, le WebGuard ne génère pas de rapport.
Ne renoncez à la documentation que dans des cas exceptionnels, par ex. uniquement lorsque vous effectuez des tests avec de nombreux virus ou programmes indésirables.

Standard

Si cette option est activée, le WebGuard consigne les informations importantes (sur le résultat positif, les avertissements et les erreurs) dans le fichier rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce réglage est activé par défaut.

Étendu

Si cette option est activée, le WebGuard consigne également les informations secondaires dans le fichier rapport.

Intégrale

Si cette option est activée, le WebGuard consigne toutes les informations - même celles sur la taille et le type des fichiers, la date, etc. - dans le fichier de rapport.

Limiter le fichier de rapport

Limiter la taille à n Mo

Si cette option est activée, le fichier rapport peut être limité à une taille définie ; valeurs possibles : 1 à 100 Mo. Ce réglage est activé par défaut avec une valeur de 1 Mo. Une tolérance de 50 kilo-octets environ est accordée pour maintenir la charge de l'ordinateur à un faible niveau. Si la taille du fichier de rapport dépasse la taille indiquée de 50 kilo-octets, les anciennes entrées sont supprimées automatiquement jusqu'à ce que la taille indiquée moins 50 kilo-octets soit atteinte.

Écrire la configuration dans le fichier de rapport

Si cette option est activée, la configuration de la recherche en temps réel utilisée est écrite dans le fichier rapport.

11.5 Généralités

11.5.1 Configuration :: Généralités

11.5.1.1. Email

Avira AntiVir Professional peut envoyer des messages et avertissements par email lors d'événements particuliers à un ou plusieurs destinataires. Pour ce faire, le Simple Message Transfer Protocol (SMTP) est utilisé.

Les messages peuvent ici être déclenchés par différents événements. L'envoi d'emails est soutenu par les modules suivants :

- Avertissements emails par le Guard
- Avertissements emails par le Scanner
- Demandes d'examen de fichiers suspects envoyées à Avira Malware Research Center

Remarque
Attention, l'ESMTP n'est pas pris en charge. En outre, une transmission codée par TLS (Transport Layer Security) ou SSL (Secure Sockets Layer) n'est pas encore possible.

Messages emails

Serveur SMTP

Entrez ici le nom de l'hôte à utiliser - son adresse IP ou le nom de l'hôte direct.
Le nom de l'hôte ne doit pas dépasser 127 caractères.

Exemple :

192.168.1.100 ou mail.nom.de.

Adresse de l'expéditeur

Saisissez dans ce champ l'adresse email de l'expéditeur. L'adresse de l'expéditeur ne doit pas dépasser 127 caractères.

Identification

Certains serveurs mail attendent qu'un programme s'identifie (se connecte) auprès du serveur avant l'envoi d'un email. Avira AntiVir Professional peut transmettre des avertissements par mail avec identification au serveur SMTP.

Utiliser l'identification

Si cette option est activée, il est possible de saisir un identifiant et un mot de passe pour la connexion (identification) dans les champs de saisie prévus.

- **Identifiant** : Saisissez ici l'identifiant.
- **Mot de passe** : saisissez ici le mot de passe correspondant. Le mot de passe est mémorisé de manière cryptée. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Envoyer un email test

En cliquant sur ce bouton, Avira AntiVir Professional essaie d'envoyer un email test à l'adresse du destinataire pour contrôle des données saisies.

11.5.2 Configuration :: Généralités

11.5.2.1. Catégories de dangers étendues

Sélection des catégories de dangers étendues

Avira AntiVir Professional vous protège des virus informatiques.

En outre, vous avez la possibilité de rechercher les catégories étendues de dangers suivantes.

- Logiciel de commande Backdoor (BDC)
- Programmes de numérotation payants (DIALER)
- Jeux (GAMES)
- Programmes de blagues (JOKES)
- Security Privacy Risk (SPR)
- Logiciels publicitaires/Logiciel espions (ADSPY)
- Programmes de compression d'exécutables (PCK) inhabituels
- Fichiers à extensions déguisées (HEUR-DBLEXT)
- Hameçonnage
- Application (APPL)

En cliquant sur la case, le type choisi est activé (coche) ou désactivé (pas de coche).

Activer tous

Si cette option est activée, tous les types sont activés.

Valeurs par défaut

Ce bouton restaure les valeurs prédéfinies par défaut.

Remarque
Si un type est désactivé, les fichiers identifiés comme type de programme correspondant, ne sont plus annoncés. Aucune entrée n'est effectuée dans le fichier rapport.

11.5.3 Configuration :: Généralités

11.5.3.1. Mot de passe

Vous pouvez protéger Avira AntiVir Professional dans diverses zones par un mot de passe. Si un mot de passe a été attribué, vous devrez saisir ce mot de passe à chaque fois que vous voulez ouvrir la zone protégée.

Remarque
Si vous administrez AntiVir Professional via le SMC, les champs de mot de passe sont désactivés. Il n'est possible de définir les mots de passe pour AntiVir Professional que localement.

Mot de passe

Saisir le mot de passe

Saisissez ici votre mot de passe. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*). Vous pouvez saisir 20 caractères au maximum. Si le mot de passe est indiqué une fois, le programme refuse l'accès en cas de saisie d'un mot de passe erroné. Un champ vide signifie "pas de mot de passe".

Confirmer le mot de passe

Saisissez ici le mot de passe saisi ci-dessus pour le confirmer. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Remarque
La différence est faite entre les majuscules et minuscules !

Mot de passe zones protégées

Avira AntiVir Professional peut protéger diverses zones par mot de passe. En cliquant sur la case correspondante, la demande de mot de passe pour les diverses zones peut être désactivée et activée à souhait.

Zone protégée par mot de passe	Fonction
Control Center	Si l'option est activée, un mot de passe est nécessaire pour démarrer le Control Center.
Activer/Désactiver le Guard	Si l'option est activée, le mot de passe défini est nécessaire pour l'activation et la désactivation de AntiVir Guard.
Activer/Désactiver le MailGuard	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver le MailGuard.
Activer/Désactiver le WebGuard	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver le WebGuard.
Ajouter et modifier des tâches	Si l'option est activée, un mot de passe est nécessaire pour ajouter et modifier des tâches dans le Planificateur.
Démarrer les mises à jour produit	Si l'option est activée, un mot de passe est nécessaire dans le menu Mise à jour pour démarrer la mise à jour produit.
Télécharger le CD de secours depuis Internet	Si l'option est activée, un mot de passe est nécessaire pour démarrer le téléchargement du CD de secours Avira.
Quarantaine	Si l'option est activée, toutes les zones possibles du gestionnaire de quarantaines protégées par mot de

	passe sont activées. En cliquant sur la case correspondante, la demande de mot de passe pour les diverses zones peut être désactivée et activée à souhait.
Restauration des objets concernés	Si l'option est activée, un mot de passe est nécessaire pour restaurer un objet.
Réparation des objets concernés	Si l'option est activée, un mot de passe est nécessaire pour réparer un objet.
caractéristiques des objets concernés	Si l'option est activée, un mot de passe est nécessaire pour l'affichage des caractéristiques d'un objet.
Suppression des objets concernés	Si l'option est activée, un mot de passe est nécessaire pour supprimer un objet.
Envoyer un email à AntiVir	Si l'option est activée, un mot de passe est nécessaire pour l'envoi d'un objet à Avira Malware Research Center pour contrôle.
Configuration	Si l'option est activée, la configuration de Avira AntiVir Professional n'est possible qu'après saisie du mot de passe défini.
Activer le mode expert	Si l'option est activée, un mot de passe est nécessaire pour l'activation du mode expert.
Installation/Désinstallation	Si cette option est activée, l'installation et la désinstallation de Avira AntiVir Professional nécessitent un mot de passe.

11.5.4 Sécurité

Mise à jour

Avertissement si la dernière mise à jour date de plus de n jour(s)

Dans ce champ, vous pouvez saisir le nombre de jours qui doit s'écouler au maximum depuis la dernière mise à jour de Avira AntiVir Professional. Si cette durée est dépassée, un message d'avertissement s'affiche dans le Planificateur.

Afficher un avertissement si le fichier de définitions des virus est obsolète

Si l'option est activée, vous recevez un message d'avertissement en cas de fichier de définitions des virus obsolète. A l'aide de l'option Avertissement, si la dernière mise à jour a plus de n jour(s), vous pouvez configurer l'intervalle avant l'avertissement.

Contrôle intégral du système

Cette zone vous permet de configurer l'affichage d'état pour le contrôle intégral du système dans le Control Center sous Aperçu:: État.

État 'jaune', si datant de plus de n jours

Indiquez dans ce champ un intervalle de temps en jours, selon lequel l'affichage d'état doit passer au jaune, une fois ce délai dépassé depuis le dernier contrôle intégral du système. L'intervalle indiqué doit être inférieur à celui défini pour l'état rouge. La valeur par défaut est de sept jours et est celle recommandée.

État 'rouge', si datant de plus de n jours

Indiquez dans ce champ un intervalle de temps en jours, selon lequel l'affichage d'état doit passer au rouge, une fois ce délai dépassé depuis le dernier contrôle intégral du système. L'intervalle indiqué doit être supérieur à celui défini pour l'état jaune. La valeur par défaut est de 30 jours et est celle recommandée.

Remarque
Lorsque vous indiquez 0 pour les deux intervalles de temps, la surveillance de l'état est désactivée pour le contrôle intégral du système. Un symbole vert s'affiche systématiquement. Ce réglage ne doit être utilisé que dans des cas exceptionnels justifiés. Si vous indiquez 0 pour un seul intervalle, l'entrée est rejetée comme non valide.

Protection du produit

Protéger les processus d'un arrêt non souhaité

Si l'option est activée, tous les processus du programme AntiVir sont protégés d'un arrêt non souhaité par des virus et des logiciels malveillants ou d'un arrêt 'incontrôlé' par un utilisateur, par ex. via le gestionnaire des tâches. Cette option est activée par défaut.

Important
La protection de processus n'est pas encore disponible pour les systèmes 64 bits !

Avertissement
Si la protection des processus est activée, des problèmes d'interaction peuvent survenir avec d'autres logiciels. Désactivez la protection des processus dans ces cas.

Protéger les fichiers et les entrées de registre de toute manipulation

Si l'option est activée, toutes les entrées de registre du programme AntiVir Professional, ainsi que tous les fichiers (fichiers binaires et de configuration) sont protégés contre toute manipulation. La protection contre la manipulation comprend la protection contre l'accès en écriture, en suppression et partiellement en lecture aux entrées de registre ou aux fichiers du programme, par l'utilisateur ou des programmes-tiers.

Remarque
Si l'option est activée, les modifications de la configuration ne sont possibles que via l'interface utilisateur, de même que la modification des tâches de contrôle ou de mise à jour.

Important
La protection des fichiers et des entrées de registre n'est pas encore disponible pour les systèmes 64 bits !

11.5.5 WMI

Prise en charge de Windows Management Instrumentation

Windows Management Instrumentation est une technologie de gestion Windows de base qui permet d'accéder en lecture et en écriture aux paramètres d'ordinateurs Windows, localement et à distance, au moyen de langages de script et de programmation. AntiVir Professional prend en charge WMI et met à disposition d'une interface, les données (informations sur l'état, données statistiques, rapports, tâches planifiées, etc.) ainsi que les événements et les méthodes (arrêt et démarrage de processus). WMI vous donne la possibilité d'interroger les données d'exploitation du programme AntiVir Professional et de commander AntiVir Professional. Vous pouvez obtenir une référence complète de l'interface WMI auprès de l'éditeur du programme AntiVir Professional. Vous recevez la référence au format PDF, après avoir signé un accord de confidentialité.

Activer la prise en charge WMI

Si l'option est activée, vous avez la possibilité d'interroger les données d'exploitation du programme AntiVir Professional via WMI.

Autoriser l'activation/la désactivation de services

Si l'option est activée, vous avez la possibilité d'activer et de désactiver des services du programme AntiVir Professional via WMI.

11.5.6 Répertoires

Chemin temporaire

Saisissez dans ce champ le chemin temporaire avec lequel Avira AntiVir Professional fonctionne.

Utiliser le réglage système

Si cette option est activée, les réglages du système sont utilisés pour la manipulation des fichiers temporaires.

Remarque

Pour savoir où votre système enregistre les fichiers temporaires sur Windows XP - allez à : Démarrer | Panneau de configuration | Performances et maintenance | Système | onglet "Avancé" | bouton "Variables d'environnement". Les variables temporaires (TEMP, TMP) pour l'utilisateur connecté et pour les variables du système (TEMP, TMP) sont visibles ici avec leurs valeurs respectives.

Utiliser le répertoire suivant

En cas d'option activée, c'est le chemin indiqué dans le champ de saisie qui est utilisé.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le chemin temporaire souhaité.

Standard

Ce bouton restaure le répertoire prédéfini pour le chemin temporaire.

Répertoire de rapport

Ce champ de saisie contient le chemin vers le répertoire de rapport de Avira AntiVir Professional.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le répertoire souhaité.

Standard

Ce bouton restaure le chemin prédéfini vers le répertoire de rapport.

Répertoire de quarantaine

Ce champ de saisie contient le chemin vers le répertoire de quarantaine de Avira AntiVir Professional.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le répertoire souhaité.

Standard

Ce bouton restaure le chemin prédéfini vers le répertoire de quarantaine.

11.5.7 Mise à jour

La rubrique **Mise à jour** de la Configuration Avira AntiVir Professional est en charge de la configuration du programme de mise à jour . Vous avez la possibilité d'effectuer une mise à jour via le serveur Web mais aussi via le serveur de fichiers / partage.

Téléchargement

via le serveur web

L'Avira AntiVir Professional Updaterr effectue une actualisation via un serveur central qui reçoit les mises à jour d'Internet ou de l'Intranet.

Remarque
Si l'option est activée, vous avez la possibilité d'adapter à vos besoins la mise à jour via un serveur Web sous Configuration :: Généralités :: Mise à jour :: Serveur Internet.

via serveur de fichiers/partage

La mise à jour est effectuée via un serveur de fichiers ou par partage.

Remarque
Si l'option est activée, vous avez la possibilité d'adapter à vos besoins la mise à jour via serveur de fichiers sous Configuration :: Généralités :: Mise à jour :: Serveur de fichiers.

Mises à jour produit

Télécharger les mises à jour produit et installer automatiquement

Si cette option est activée, les mises à jour produit sont téléchargées et installées automatiquement par l'Updater dès qu'elles sont disponibles. Les mises à jour du fichier de définitions des virus et du moteur de recherche sont toujours effectuées, indépendamment de ce réglage. Les conditions pour cette fonction sont : la configuration intégrale de la mise à jour et une connexion existante vers un serveur de téléchargement.

Informer lorsque des nouvelles mises à jour produit sont disponibles

Si cette option est activée, vous n'êtes prévenu que si de nouvelles mises à jour du produit sont disponibles. Les mises à jour du fichier de définitions des virus et du moteur de recherche sont toujours effectuées, indépendamment de ce réglage. Les conditions pour cette fonction sont : la configuration intégrale de la mise à jour et une connexion existante vers un serveur de téléchargement. Vous êtes prévenu par un message affiché sur le bureau, sous la forme d'une fenêtre popup et par un message d'avertissement de l'Updater dans le Control Center sous Aperçu ::Evénements.

Ne pas télécharger les mises à jour produit

Si cette option est activée, aucune mise à jour automatique du produit ni avertissement sur la disponibilité de mises à jour du produit ne sont effectués par l'Updater. Les mises à jour du fichier de définitions des virus et du moteur de recherche sont toujours effectuées, indépendamment de ce réglage.

Important
Le fichier de définitions des virus et le moteur de recherche sont mis à jour à chaque exécution d'une mise à jour, indépendamment des réglages concernant la mise à jour produit (voir à ce sujet le chap. Mises à jour).

11.5.7.1. Serveur de fichiers

En présence de plusieurs ordinateurs dans un réseau, Avira AntiVir Professional peut télécharger une mise à jour dans l'Intranet à partir d'un serveur qui acquiert lui-même les fichiers de mise à jour sur Internet. Ceci permet de garantir l'actualité de Avira AntiVir Professional sur tous les ordinateurs en préservant les ressources.

Remarque
La rubrique de configuration n'est activée que l'option **via serveur de fichiers / partage** a été sélectionnée sous Configuration :: Généralités :: Mise à jour .

Téléchargement

Saisissez le chemin sur lequel les fichiers actuels de Avira AntiVir Professional se trouvent sur le serveur.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le répertoire de téléchargement souhaité.

Connexion au serveur

Identifiant de connexion

Saisissez votre identifiant de connexion au serveur.

Mot de passe de connexion

Saisissez votre mot de passe dans le champ correspondant pour la connexion au serveur. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Remarque
Si vous ne saisissez aucune donnée dans la zone de données de connexion au serveur, aucune identification sur le serveur de fichiers ne sera effectuée lors d'un accès au serveur de fichiers. Dans ce cas, des droits d'utilisateur suffisants doivent être disponibles sur le serveur de fichiers.

11.5.7.2. Serveur web

La mise à jour peut être effectuée directement via un serveur web sur Internet ou sur l'Intranet .

Connexion au serveur web

Utiliser la connexion existante (réseau)

Ce réglage s'affiche lorsque votre connexion via un réseau est utilisée.

Utiliser la connexion suivante :

Ce réglage s'affiche quand vous définissez votre connexion individuellement.

Avira AntiVir Professional Updaterr détecte automatiquement quelles options de connexion sont disponibles. Les options de connexion indisponibles sont sur fond gris et ne peuvent pas être activées. Vous pouvez établir une connexion de télétransmission par ex. manuellement via une entrée de répertoire téléphonique dans Windows.

- **Utilisateur :** saisissez l'identifiant du compte sélectionné.
- **Mot de passe :** saisissez le mot de passe pour ce compte. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Remarque
Adressez-vous au fournisseur d'accès Internet si vous avez oublié l'identifiant ou le mot de passe d'un compte Internet existant.

Remarque
La composition automatique de l'updater via les outils Dial-Up (par ex. SmartSurfer, Oleco, ...) n'est pas encore disponible dans Avira AntiVir Professional.

Arrêter une connexion de télétransmission ouverte pour la mise à jour

Si cette option est activée, la connexion de télétransmission ouverte pour la mise à jour est interrompue automatiquement dès que le téléchargement a été effectué avec succès.

Remarque
L'option n'est pas disponible sous Vista. La connexion de télétransmission ouverte pour la mise à jour est systématiquement interrompue sous Vista, dès que le téléchargement a été effectué.

Téléchargement

Serveur standard

Saisissez ici l'adresse (URL) du serveur web à partir duquel les mises à jour doivent être chargées. Le serveur web peut être un serveur sur Internet ou sur l'Intranet. Vous pouvez saisir plusieurs adresses. Les serveurs Web accessibles sont saisis par défaut pour la mise à jour de AntiVir Professional.

Standard

Le bouton permet de restaurer les adresses prédéfinies.

Serveur prioritaire

Indiquez dans ce champ l'adresse (URL) du serveur Web qui doit être interrogé en premier lors d'une mise à jour. Si ce serveur n'est pas accessible, les serveurs standard indiqués sont interrogés.

Proxy

Serveur proxy

Ne pas utiliser de serveur proxy

Si cette option est activée, votre connexion au serveur web n'a pas lieu via un serveur proxy.

Utiliser les réglages système de Windows

Si cette option est activée, les réglages système actuels de Windows pour la connexion au serveur web via un serveur proxy sont utilisés.

Connexion via ce serveur proxy

Si l'option est activée, votre connexion au serveur web a lieu via un serveur proxy, mais les réglages que vous avez indiqués sont utilisés.

Adresse

Saisissez l'URL ou l'adresse IP du serveur proxy que vous souhaitez utiliser pour la connexion avec le serveur web.

Port

Saisissez le numéro de port du serveur proxy que vous souhaitez utiliser pour la connexion avec le serveur web.

Identifiant de connexion

Saisissez votre identifiant de connexion au serveur proxy.

Mot de passe de connexion

Saisissez le mot de passe correspondant pour la connexion au serveur proxy. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Exemples :

Adresse : proyx.domain.de Port : 8080

Adresse : 192.168.1.100 Port : 3128

11.5.8 Avertissements

11.5.8.1. Réseau

Vous pouvez envoyer des avertissements configurables individuellement du Scanner ou du Guard à n'importe quel ordinateur de votre réseau.

Remarque
Vérifiez si le "service de messages" a démarré. Vous trouverez ce service (exemple Windows XP) sous "Démarrer | Panneau de configuration| Performances et maintenance | Outils d'administration | Services".

Remarque
Un avertissement est toujours envoyé à l'ordinateur, PAS à un utilisateur particulier.

Avertissement
Cette fonctionnalité n'est pas prise en charge par les systèmes d'exploitation suivants :
Microsoft Server 2008 et supérieur
Windows Vista et supérieur

Envoyer le message à

La liste dans cette fenêtre indique le nom des ordinateurs recevant un message en cas de résultat positif.

Remarque
Un ordinateur ne peut être saisi qu'une seule fois dans cette liste.

Ajouter

Ce bouton vous permet d'ajouter un ordinateur. Une fenêtre s'ouvre dans laquelle vous pouvez saisir le nom de l'ordinateur. Un nom d'ordinateur ne peut pas contenir plus de 15 caractères.



Le bouton ouvre une fenêtre dans laquelle vous pouvez alternativement sélectionner un ordinateur dans votre environnement réseau.

Supprimer

Ce bouton vous permet de supprimer de la liste l'entrée actuellement sélectionnée.

Guard

Avertissements réseau

Si l'option est activée, des avertissements réseau sont envoyés. Cette option est désactivée par défaut.

Remarque
Pour pouvoir activer cette option, au moins un destinataire doit être saisi sous Généralités :: Avertissements :: Réseau.

Message à envoyer

La fenêtre montre le message envoyé à l'ordinateur choisi en cas de résultat positif. Vous pouvez éditer ce message. Un texte ne doit pas contenir plus de 500 caractères.

Vous pouvez utiliser les combinaisons de touches suivantes pour le formatage du message :

Strg + Tab	ajoute une tabulation. La ligne actuelle est repoussée à droite de quelques caractères.
Strg + Enter	ajoute un saut de ligne.

Le message peut aussi contenir des caractères de remplacement pour les informations trouvées pendant la recherche. Ces caractères de remplacement sont remplacés par le vrai texte à l'envoi.

Les caractères de remplacement suivants sont autorisés :

%VIRUS%	contient le nom du virus ou programme indésirable trouvé
%FILE%	contient le chemin et le nom du fichier touché
%COMPUTER%	contient le nom de l'ordinateur sur lequel le Guard fonctionne
%NAME%	contient le nom de l'utilisateur qui a accédé au fichier touché
%ACTION%	contient l'action exécutée après la découverte du virus
%MACADDR%	contient l'adresse MAC de l'ordinateur sur lequel le Guard fonctionne

Standard

Ce bouton restaure le texte standard prédéfini pour l'avertissement.

Scanner

Activer les avertissements réseau

Si l'option est activée, des avertissements réseau sont envoyés. Cette option est désactivée par défaut.

Remarque
Pour pouvoir activer cette option, au moins un destinataire doit être saisi sous Généralités :: Avertissements :: Réseau.

Message à envoyer

La fenêtre montre le message envoyé à l'ordinateur choisi en cas de résultat positif. Vous pouvez éditer ce message. Un texte ne doit pas contenir plus de 500 caractères.

Vous pouvez utiliser les combinaisons de touches suivantes pour le formatage du message :

Strg + Tab	ajoute une tabulation. La ligne actuelle est repoussée à droite de quelques caractères.
Strg + Enter	ajoute un saut de ligne.

Le message peut aussi contenir des caractères de remplacement pour les informations trouvées pendant la recherche. Ces caractères de remplacement sont remplacés par le vrai texte à l'envoi.

Les caractères de remplacement suivants sont autorisés :

%VIRUS%	contient le nom du virus ou programme indésirable trouvé
%NAME%	contient le nom de l'ordinateur connecté qui exécute le Scanner

Standard

Ce bouton restaure le texte standard prédéfini pour l'avertissement.

11.5.8.2. Email

Guard

AntiVir Guard peut envoyer des avertissements par email à un ou plusieurs destinataires lors de certains événements.

Guard

Avertissements email

Si cette option est activée, AntiVir Guard envoie des messages email avec les principales données lorsqu'un événement défini se produit. Cette option est désactivée par défaut.

Avertissement par email lors des événements suivants

- **Lors de la recherche en temps réel, un résultat positif a été annoncé**
  Si cette option est activée, vous recevez un email avec le nom du virus ou du programme indésirable du fichier concerné à chaque fois que la recherche en temps réel trouve un virus ou un programme indésirable.
- **Au sein du Guard, une erreur critique s'est produite**
  Si cette option est activée, vous recevez un email si Avira AntiVir Professional constate une erreur critique interne.

Remarque
Dans ce cas, veuillez informer notre support technique et envoyez-lui les données indiquées dans l'email. Le fichier concerné doit aussi être envoyé pour contrôle.

Destinataire

Dans ce champ, saisissez l'adresse email du ou des destinataire(s). Les adresses sont séparées par des virgules. La longueur maximale de toutes les adresses (la totalité de la chaîne de caractères donc) est de 260 caractères.

Scanner

La recherche directe, c'est-à-dire à la demande, peut envoyer des avertissements par email à un ou plusieurs destinataires lors de certains événements.

Scanner

Activer les avertissements email

Si cette option est activée, Avira AntiVir Professional envoie des messages email avec les principales données lorsqu'un événement défini se produit. Cette option est désactivée par défaut.

Avertissement par email lors des événements suivants

- **Lors de la recherche, un résultat positif a été annoncé**
  Si cette option est activée, vous recevez un email avec le nom du virus ou du programme indésirable du fichier concerné à chaque fois que la recherche directe trouve un virus ou un programme indésirable.
- **Fin d'une recherche planifiée**
  Si l'option est activée, un email est envoyé lorsque la tâche de contrôle a été exécutée. L'email contient les données concernant l'heure et la durée de la recherche, les répertoires et fichiers contrôlés ainsi que les virus détectés et les avertissements.

Adresse du ou des destinataire(s)

Dans ce champ, saisissez l'adresse email du ou des destinataire(s). Les adresses sont séparées par des virgules. La longueur maximale de toutes les adresses (la totalité de la chaîne de caractères donc) est de 260 caractères.

Updater

L'Updater peut envoyer des messages par email à un ou plusieurs destinataires lors de certains événements.

Updater

Avertissements email

Si l'option est activée, l'Updater envoie des messages emails avec les principales données quand un événement particulier se produit. Cette option est désactivée par défaut.

Avertissement par email lors des événements suivants

- **Mise à jour nécessaire. Votre programme est à jour.**
  Si l'option est activée, un email est envoyé quand l'Updater a pu établir une connexion au serveur de téléchargement, mais qu'aucun nouveau fichier n'est disponible sur le serveur. Cela signifie que AntiVir Professional est actuel.
- **La mise à jour a réussi. De nouveaux fichiers ont été installés.**
  Si l'option est activée, un email est envoyé au moment des mises à jour : il peut s'agir d'une mise à jour du produit ou d'une actualisation du fichier de définitions des virus ou du moteur de recherche.
- **La mise à jour a réussi. Une nouvelle mise à jour du produit est disponible.**
  Si l'option est activée, un email est envoyé uniquement lorsqu'une actualisation du fichier de définitions des virus ou du moteur de recherche a été effectuée sans mise à jour du produit, mais qu'une mise à jour du produit est disponible.

– **La mise à jour a échoué.**
Si l'option est activée, un email est envoyé si la mise à jour a échoué en raison d'une erreur.

Destinataire

Dans ce champ, saisissez l'adresse email du ou des destinataire(s). Les adresses sont séparées par des virgules. La longueur maximale de toutes les adresses (la totalité de la chaîne de caractères donc) est de 260 caractères.

Remarque
Lors des événements suivants, des messages d'avertissement sont envoyés par email, si une notification par email a été configurée sous Configuration::Généralités::Email :
Une mise à jour du produit est nécessaire pour chacune des futures actualisations de AntiVir Professional.
Une actualisation du fichier de définitions des virus ou du moteur de recherche n'a pas pu être effectuée, car une mise à jour du produit est nécessaire.

L'envoi de ces messages d'alerte est effectué indépendamment de vos réglages d'avertissements par email dans l'Updater.

11.5.8.3. Avertissements acoustiques

Avertissement acoustique

En cas de détection d'un virus ou d'un logiciel malveillant par le Scanner ou le Guard , un bip d'avertissement retentit dans le mode d'action interactif. Vous avez la possibilité de désactiver ou d'activer le bip d'avertissement ainsi que de sélectionner un fichier WAVE différent comme bip d'avertissement.

Remarque
Le mode d'action du Scanner se règle dans la configuration sous Scanner::Recherche::Action en cas de résultat positif. Le mode d'action du Guard se règle dans la configuration sous Guard::Recherche::Action en cas de résultat positif.

Pas d'avertissement

Si l'option est activée, aucun avertissement acoustique ne se produit lors de la détection d'un virus par le Scanner ou le Guard.

Diffuser par le haut-parleur du PC (uniquement en mode interactif)

Si l'option est activée, un avertissement acoustique se produit à l'aide d'un bip d'avertissement par défaut, lors de la détection d'un virus par le Scanner ou le Guard. Le bip d'avertissement est diffusé par le haut-parleur interne du PC.

Utiliser le fichier WAV suivant (uniquement en mode interactif)

Si l'option est activée, un avertissement acoustique se produit à l'aide du fichier WAVE sélectionné, en cas de détection d'un virus par le Scanner ou le Guard. Le fichier WAVE sélectionné est diffusé par le haut-parleur externe raccordé.

Fichier Wave

Dans ce champ de saisie, vous pouvez saisir le nom et le chemin correspondant d'un fichier audio de votre choix. Le bip d'avertissement par défaut du programme AntiVir Professional est inscrit par défaut.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le fichier à l'aide de l'explorateur de fichiers.

Test

Ce bouton sert à tester le fichier Wave sélectionné.

11.5.9 Evénements

Limiter la taille de la base de données d'événements

Limiter la taille à n entrées maximum

Si l'option est activée, le nombre maximum d'entrées dans la base de données d'événements peut être limitée à une taille définie ; les valeurs autorisées sont : 100 à 10 000 entrées. Si le nombre d'entrées saisies est dépassée, les saisies les plus anciennes sont supprimées.

Supprimer tous les événements de plus de n jour(s)

Si cette option est activée, les événements sont supprimés de la base de données d'événements après un certain nombre de jours ; les valeurs autorisées sont : 1 à 90 jours. Cette option est activée par défaut avec une valeur de 30 jours.

Ne pas limiter la taille de la base de données (supprimer les événements manuellement)

Si l'option est activée, la taille de la base de données n'est pas limitée. Toutefois, 20 000 entrées au maximum sont affichées dans le Control Center sous Evénements.

11.5.10 Limiter les rapports

Limiter le nombre des rapports

Limiter le nombre maximum à n pièces

Si l'option est activée, le nombre maximum de rapports peut être limité ; les valeurs autorisées sont : 1 à 300. Si le nombre indiqué est dépassé, les rapports les plus anciens sont supprimés.

Supprimer tous les rapports âgés de plus de n jour(s)

Si l'option est activée, les rapports sont supprimés automatiquement après un certain nombre de jours ; valeurs autorisées : 1 à 90 jours. Cette option est activée par défaut avec une valeur de 30 jours.

Ne pas limiter le nombre de rapports (supprimer les rapports manuellement)

Si cette option est activée, le nombre de rapports n'est pas limité.

11.5.11 Avertissements acoustiques

Avertissement acoustique

En cas de détection d'un virus ou d'un logiciel malveillant par le Scanner ou le Guard , un bip d'avertissement retentit dans le mode d'action interactif. Vous avez la possibilité de désactiver ou d'activer le bip d'avertissement ainsi que de sélectionner un fichier WAVE différent comme bip d'avertissement.

Remarque
Le mode d'action du Scanner se règle dans la configuration sous Scanner::Recherche::Action en cas de résultat positif. Le mode d'action du Guard se règle dans la configuration sous Guard::Recherche::Action en cas de résultat positif.

Pas d'avertissement

Si l'option est activée, aucun avertissement acoustique ne se produit lors de la détection d'un virus par le Scanner ou le Guard.

Diffuser par le haut-parleur du PC (uniquement en mode interactif)

Si l'option est activée, un avertissement acoustique se produit à l'aide d'un bip d'avertissement par défaut, lors de la détection d'un virus par le Scanner ou le Guard. Le bip d'avertissement est diffusé par le haut-parleur interne du PC.

Utiliser le fichier WAV suivant (uniquement en mode interactif)

Si l'option est activée, un avertissement acoustique se produit à l'aide du fichier WAVE sélectionné, en cas de détection d'un virus par le Scanner ou le Guard. Le fichier WAVE sélectionné est diffusé par le haut-parleur externe raccordé.

Fichier Wave

Dans ce champ de saisie, vous pouvez saisir le nom et le chemin correspondant d'un fichier audio de votre choix. Le bip d'avertissement par défaut du programme AntiVir Professional est inscrit par défaut.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le fichier à l'aide de l'explorateur de fichiers.

Test

Ce bouton sert à tester le fichier Wave sélectionné.

Avira AntiVir Professional

Avira GmbH

Lindauer Str. 21
88069 Tettnang
L'Allemagne
Téléphone: +49 7542-500 0
Fax: +49 7542-525 10
Internet: http://www.avira.com/fr

© Avira GmbH. Tous droits réservés.

Ce manuel a été élaboré avec le plus grand soin. Il n'est toutefois pas exclu que des erreurs s'y soient glissées dans la forme et/ou le contenu. Il est interdit de reproduire la présente publication dans sa totalité ou en partie, sous quelque forme que ce soit, sans l'accord préalable écrit d'Avira GmbH.

Sous réserve d'erreurs et de modifications techniques.

Edition du 1er trimestre 2009

AntiVir® est une marque déposée de la société Avira GmbH. Tous les autres noms de produits et de marques sont des marques ou marques déposées de leurs détenteurs respectifs. Les marques protégées ne sont pas identifiées dans le présent manuel. Cela ne signifie toutefois pas qu'elles peuvent être utilisées librement.