Avira Premium Security Suite

Manuel de l'utilisateur

AVIRA®

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 Premium Security Suite. 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 Premium Security Suite sous Third Party Licenses.

Table des matières

1 Introduction

Avira Premium Security Suite 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 Premium Security Suite sous forme de PDF, actualiser Avira Premium Security Suite 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 Premium Security Suite.

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 Premium Security Suite :

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

Avira Premium Security Suite 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 Premium Security Suite grâce aux mises à jour automatiques. Configurez le programme en conséquence.

3.1 Prestations

Avira Premium Security Suite 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
- 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
- Guard (On-Access Scan) pour la surveillance permanente de tous les accès aux fichiers
- Composant ProActiv pour une surveillance en permanence d'actions de programme (uniquement pour systèmes 32 bits, non disponible sous Windows 2000)
- 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

- WebGuard pour la vérification des données et fichiers en provenance d'Internet via le protocole HTTP (vérification des ports Ports 80, 8080, 3128)
- Composants de contrôle parental pour un filtrage basé sur des rôles de sites Internet indésirables et pour la limitation de l'utilisation sur Internet.
- Sauvegarde composants pour la création de sauvegardes de vos données (sauvegardes miroirs)
- 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) (pas disponible sous Windows XP 64 bits)
- 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
- 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)
- Pare-feu AntiVir pour protéger l'ordinateur des accès non autorisés en provenance d'Internet ou d'un réseau ainsi que des accès non autorisés à Internet/à un réseau par des utilisateurs non autorisés.

3.2 Configuration minimale du système

Pour que Avira Premium Security Suite 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)
- Windows 7 (32 ou 64 bits)
- 150 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)
- 256 Mo minimum de mémoire vive sous Windows 2000/XP

- 1024 Mo minimum de mémoire vive sous Windows Vista, Windows 7
- Pour l'installation de Avira Premium Security Suite : droits d'administrateur
- Pour toutes les installations : Windows Internet Explorer 6.0 ou ultérieur
- évent. connexion Internet disponible (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 Premium Security Suite 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 et mise à niveau

Pour pouvoir utiliser Avira Premium Security Suite, il vous faut une licence. Vous acceptez ainsi les conditions de licence de Avira Premium Security Suite.

La licence est donnée sous forme d'une clé d'activation. La clé d'activation est un code alphanumérique que vous recevez à l'achat du Avira Premium Security Suite. Les données exactes de votre licence sont enregistrées par le biais de la clé d'activation, c'est-à-dire pour quels programmes et pour combien de temps la licence vous a été accordée.

La clé d'activation vous est transmise par email si vous avez acheté Premium Security Suite sur Internet ou se trouve sur l'emballage du produit.

Pour obtenir la licence de votre programme, entrez la clé d'activation lors de l'activation de Avira Premium Security Suite. L'activation du produit peut s'effectuer lors de l'installation. Vous pouvez toutefois aussi activer Avira Premium Security Suite après l'installation dans la gestion des licences sous Aide::Gestion des licences.

Dans la gestion des licences, vous avez la possibilité de lancer une mise à niveau pour un produit de la famille de produits AntiVir Desktop : De ce fait, il n'est pas nécessaire d'effectuer une désinstallation manuelle de l'ancien produit et une installation manuelle du nouveau produit. En cas de mise à niveau à partir de la gestion des licences, indiquez la clé d'activation du produit auquel vous voulez passer dans le champ de saisie de la gestion des licences. Il y a une installation automatique du nouveau produit.

La gestion des licences permet l'exécution automatique des mises à niveau de produit suivants :

- Mise à niveau de Avira AntiVir Personal vers Avira AntiVir Premium
- Mise à niveau de Avira AntiVir Personal vers Avira Premium Security Suite
- Mise à niveau de AntiVir Premium vers Avira Premium Security Suite

4 Installation et désinstallation

Dans ce chapitre, vous obtenez des informations sur l'installation et la désinstallation de votre Avira Premium Security Suite :

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

4.1 Installation

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

Remarque
A partir de Windows XP, Avira Premium Security Suite génère un point de restauration de votre ordinateur avant l'installation de Avira Premium Security Suite. Cela vous permet de supprimer Avira Premium Security Suite 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 Premium Security Suite vous indique le point de restauration généré par Avira Premium Security Suite.

Types d'installation

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

Express

- Le système n'installe pas tous les composants disponibles du programme. Les composants suivants ne sont pas installés :

AntiVir ProActiv

Pare-feu AntiVir

- Les fichiers de programme sont installés dans un répertoire par défaut sous `C:\Programme`.
- Premium Security Suite est installé avec les réglages par défaut. Vous n'avez pas la possibilité d'effectuer des préréglages dans l'assistant de configuration.

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.
- Dans l'assistant de configuration, vous pouvez effectuer des réglages de Premium Security Suite et lancer un bref contrôle système exécuté automatiquement. après l'installation.

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)
- Activation de Avira Premium Security Suite
- Si nécessaire, exécution d'une mise à jour de Premium Security Suite une fois l'installation terminée
- Conservez la clé de licence du programme Premium Security Suite à portée de main, si vous souhaitez activer Premium Security Suite.

Remarque
Installation basée sur Internet :
Pour l'installation basée sur Internet de Avira Premium Security Suite, 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 Premium Security Suite 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 Premium Security Suite, 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.

Remarque
Pour activer le produit, Avira Premium Security Suite communique avec les serveurs de la société Avira GmbH, via le protocole HTTP et le port 80 (communication Web) ainsi que via le protocole de cryptage SSL et le port 443. Si vous utilisez un pare-feu, assurez-vous que celui-ci ne bloque pas les connexions nécessaires ou les données entrées ou sortantes.

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 Premium Security Suite :

Remarque
Les actions décrites ci-après pour la désactivation du pare-feu Windows ne concernent que le système d'exploitation Windows XP.

▶ 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 Premium Security Suite 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 Premium Security Suite*.

▶ 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

→ 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 *Générer un numéro de série* apparaît.

▶ Confirmez le cas échéant la création d'un numéro de série au hasard et sa transmission lors de la mise à jour et cliquez sur **Continuer**.

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

▶ Décidez si vous voulez effectuer une installation express ou une installation personnalisée.

▶ Activez l'option **Express** 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**.

→ Si le pare-feu Windows est installé, un message vous demande de le désactiver pour éviter les conflits avec le pare-feu Avira.

▶ Confirmez avec **Oui**.

→ Le pare-feu Windows est désactivé.

→ 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**.

▶ Ignorez la section suivante "Installation express".

Installation express

→ Si le pare-feu Windows est installé, un message vous demande de le désactiver pour éviter les conflits avec le pare-feu Avira.

▶ Confirmez avec **Oui**.

→ Le pare-feu Windows est désactivé.

Suite : Installation express et installation personnalisée

→ L'assistant de licence s'ouvre.

Vous pouvez sélectionner les options suivantes pour activer Premium Security Suite

– Entrée d'une clé d'activation

En saisissant votre clé d'activation, vous activez Avira Premium Security Suite avec votre licence.

– Sélection de l'option **Tester le produit**

Si vous sélectionnez **Tester le produit**, une licence d'évaluation est générée lors du processus d'activation, grâce à laquelle Avira Premium Security Suite est activé. Vous pouvez tester l'intégralité des fonctions de Avira Premium Security Suite pendant une période définie.

Remarque
L'option **Fichier de licence hbedv.key valide présent** vous permet de lire un fichier de licence valide. Le fichier de licence est généré avec une clé d'activation valide lors du processus d'activation du produit et enregistré dans le répertoire du programme Avira Premium Security Suite. Utilisez cette option, si vous avez déjà effectué une activation du produit et que vous souhaitez réinstaller Avira Premium Security Suite.

Remarque
Dans certaines versions en vente de Avira Premium Security Suite, une clé d'activation est déjà présente dans le produit. Il n'est donc pas nécessaire d'indiquer une clé d'activation. La clé d'activation enregistrée s'affiche dans l'assistant de licence, le cas échéant.

Remarque
Une connexion aux serveurs de la société Avira GmbH est établie pour activer Premium Security Suite. Sous **Réglages proxy**, vous pouvez configurer la connexion Internet via un serveur proxy.

▶ Sélectionnez un processus d'activation et confirmez en cliquant sur **Suivant**

Activation de produit

→ Une fenêtre de dialogue s'ouvre dans laquelle vous pouvez entrer vos données personnelles.

▶ Saisissez vos données et cliquez sur **Suivant**

→ Vos données sont transférées vers les serveurs Avira GmbH , puis vérifiées. Avira Premium Security Suite est activé avec votre licence.

→ Vos données de licence s'affichent dans la fenêtre de dialogue suivante.

▶ Cliquez sur **Suivant**.

▶ Ignorez la section suivante "Activation par la sélection de l'option **hbedv.key valide présent** ".

Sélection de l'option "hbedv.key valide présent"

→ Une fenêtre de dialogue s'ouvre pour lire le fichier de licence.

▶ Choisissez le fichier de licence hbedv.key avec vos données de licence pour Premium Security Suite et cliquez sur **Ouvrir**

→ Vos données de licence s'affichent dans la fenêtre de dialogue suivante.

▶ Cliquez sur **Suivant**

Suite, une fois l'activation terminée ou le fichier de licence chargé

→ Les composants du programme sont installés. La progression de l'installation s'affiche dans la fenêtre de dialogue.

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

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

→ L'assistant d'installation se referme.

Suite : Installation personnalisée
Assistant de configuration

→ En cas d'installation personnalisée, l'étape suivante ouvre l'assistant de configuration. Vous pouvez effectuer d'importants préréglages pour Premium Security Suite dans l'assistant de configuration.

▶ Dans la fenêtre de bienvenue de l'assistant de configuration, cliquez sur**Continuer**, pour commencer la configuration de Premium Security Suite.

→ 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 de 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 Premium Security Suite grâce à la sélection de catégories de dangers.

▶ Activez d'autres catégories de danger le cas échéant et poursuivez la configuration avec *Continuer*.

→ Si vous avez choisi le module d'installation pare-feu AntiVir pour l'installation, la fenêtre de dialogue *Niveau de sécurité pare-feu* s'affiche. Vous pouvez définir si le pare-feu Avira autorise les accès externes aux ressources partagées ainsi que les accès réseau des applications d'entreprises dignes de confiance.

▶ Activez les options souhaitées et poursuivez la configuration avec *Continuer*.

→ Si vous avez choisi le module d'installation AntiVir Guard pour l'installation, la fenêtre de dialogue *Mode de démarrage de Guard* s'affiche. Vous pouvez définir le point de démarrage de Guard. Le Guard démarre dans le mode de démarrage indiqué, à chaque redémarrage de l'ordinateur.

Remarque
Le mode de démarrage de Guard indiqué est consigné dans le registre et ne peut pas être modifié par la configuration.

▶ Activez l'option souhaitée et poursuivez la configuration avec *Continuer*.

→ Si vous avez choisi le module d'installation AntiVir WebGuard pour l'installation, la fenêtre de dialogue *Activer le contrôle parental* s'affiche. Vous pouvez définir le point de démarrage de Guard. Le Guard démarre dans le mode de démarrage indiqué, à chaque redémarrage de l'ordinateur. Vous avez la possibilité d'attribuer à l'utilisateur de l'ordinateur plusieurs rôle pour l'utilisation d'Internet : enfant, jeune et adulte. Vous pouvez également désactiver le contrôle parental.

▶ Procédez aux réglages souhaités concernant le contrôle parental et poursuivez la configuration avec Continuer.

→ La fenêtre de dialogue suivante *Attribuer un mot de passe*, vous permet de protéger l'accès à la configuration de Premium Security Suite avec un mot de passe. Ceci est particulièrement recommandé en cas de contrôle parental activé.

→ 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 parcourt 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.

Suite : Installation express et installation personnalisée

→ Si vous avez sélectionné l'option **Redémarrer l'ordinateur** dans le dernier assistant d'installation, le système redémarre l'ordinateur.

→ Après le redémarrage de l'ordinateur, le fichier lisez-moi de Premium Security Suite s'affiche si vous avez sélectionné l'option **Afficher lisez-moi.txt** dans l'assistant d'installation.

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

- Effectuez le cas échéant une mise à jour de Premium Security Suite 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 Premium Security Suite (voir chapitre Installation et désinstallation::Modules d'installation)

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

Sélectionnez Avira Premium Security Suite et cliquez sur **Modifier**. Dans le dialogue de bienvenue de Avira Premium Security Suite, 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 :

- **Premium Security Suite**
  Ce module contient tous les composants nécessaires pour l'installation correcte de Avira Premium Security Suite.
- **AntiVir Guard**
  AntiVir Guard fonctionne en arrière-plan. Il surveille et répare si possible les fichiers lors d'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 Premium Security Suite parcourt automatiquement le fichier. Lors de l'opération Renommer, aucune recherche de AntiVir Guard n'est effectuée.
- **AntiVir ProActiv**
  Le composant ProActiv surveille les actions des applications et signale si elles présentent un comportement suspect typique pour un logiciel malveillant. Avec cette détection basée sur la détection, vous pouvez vous protéger contre des logiciels malveillants inconnus. Le composant ProActiv est intégré dans AntiVir Guard.

- **AntiVir MailGuard**
  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. 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. En outre, MailGuard peut vous protéger efficacement contre les spams.
- **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. 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.
- **Pare-feu Avira**
  le pare-feu Avira contrôle les voies de communication de et vers votre ordinateur. Il autorise ou refuse la communication sur la base des consignes de sécurité.
- ***Protection Rootkit AntiVir***
  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 Premium Security Suite 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.
- **Sauvegarde**

Le composant Sauvegarde vous permet de créer manuellement et de manière automatisée des sauvegardes miroir de vos données.

4.4 désinstallation

Si vous souhaitez supprimer Avira Premium Security Suite 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 Premium Security Suite (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 Premium Security Suite** et cliquez sur **Supprimer**.

→ Le système vous demande si vous souhaitez réellement supprimer le programme.

- Confirmez avec **Oui**.

→ Le système vous demande si le pare-feu Windows doit être réactivé (car le pare-feu Avira va être désactivé).

- 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 Premium Security Suite 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 Premium Security Suite sont supprimés.

5 Aperçu de Premium Security Suite

Dans ce chapitre vous obtenez une vue d'ensemble des fonctionnalités et de la commande de Premium Security Suite.

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

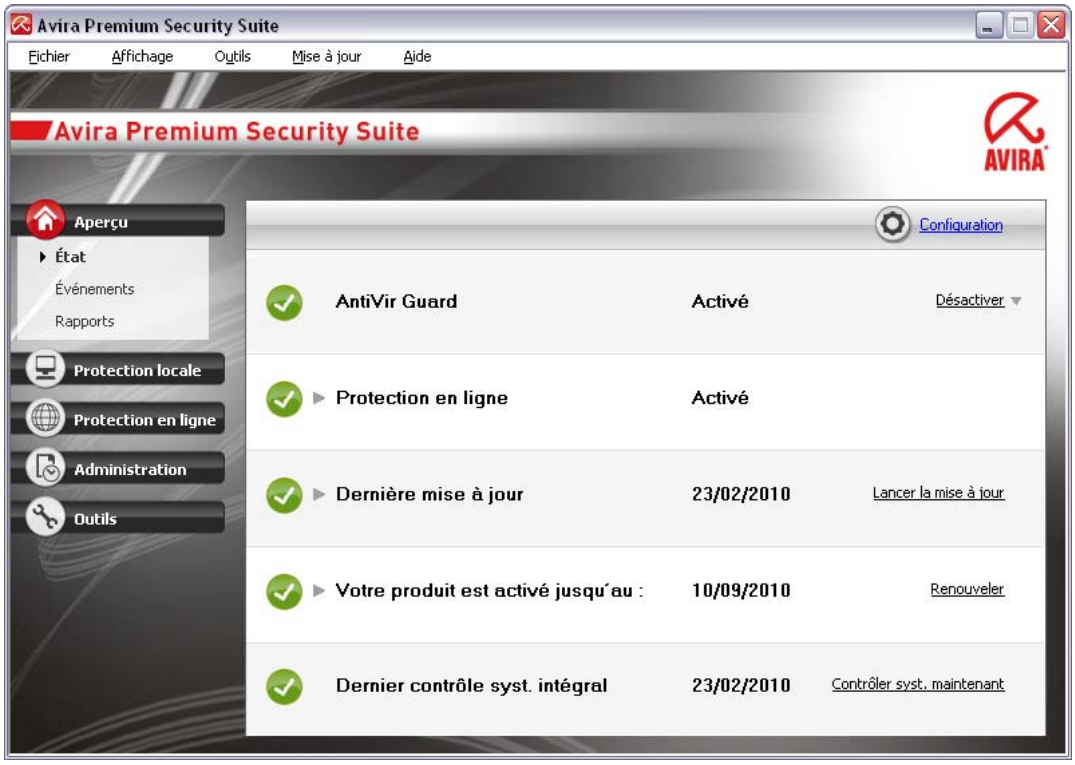
5.1 Interface et commande

La commande de Premium Security Suite se fait via trois éléments d'interface du programme :

- Control Center: surveillance et commande de Premium Security Suite
- Configuration: configuration de Premium Security Suite
- 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 l'état de protection de votre ordinateur et à commander et utiliser les composants de protection et les fonctions de Premium Security Suite.



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 Premium Security Suite.

- **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 Premium Security Suite 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 Premium Security Suite dans le menu Démarrer | Programmes.
- Via Avira Premium Security Suite l'icône de programme.

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.

Utilisation du 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.

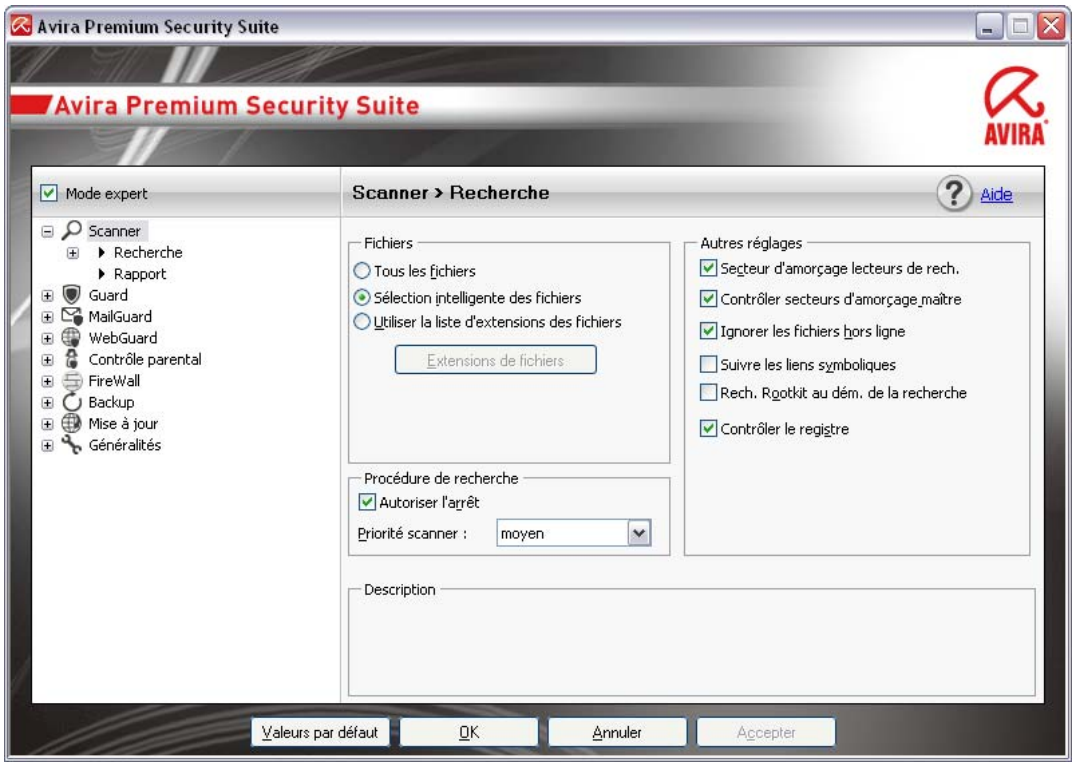
Aperçu du Control Center

- **Aperçu** : vous trouverez sous **Aperçu** toutes les rubriques vous permettant de surveiller le fonctionnement de Avira Premium Security Suite.
- La rubrique **État** offre la possibilité de voir d'un seul coup d'œil quels modules Avira Premium Security Suite sont actifs et fournit des informations sur la dernière mise à jour effectuée. En outre, vous voyez si vous disposez d'une licence valide.
- La rubrique Événements vous donne la possibilité de vous informer sur les événements générés par les modules du Avira Premium Security Suite.
- La rubrique Rapports vous permet de visualiser les résultats des actions effectuées par Avira Premium Security Suite.
- **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 MailGuard, leurs propriétés ainsi que d'autres données statistiques. En outre, vous avez la possibilité d'entraîner le filtre AntiSpam et d'exclure à l'avenir des adresses email de la vérification anti logiciels malveillants et antispam. Les emails peuvent aussi être supprimés de la mémoire tampon de MailGuard.
- La rubrique WebGuard vous fournit des informations sur les URL contrôlées et les virus détectés, ainsi que des données statistiques, pouvant être réinitialisées à tout moment et vous permet d'accéder au fichier de rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles quasiment "par pression d'un bouton".
- La rubrique pare-feu vous donne la possibilité de configurer les paramètres de base du pare-feu Avira. En outre, les débits actuels et toutes les applications actives utilisant une connexion réseau s'affichent.
- **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 rubriquePlanificateur vous donne la possibilité de créer des tâches de contrôle et de mise à jour programmées ainsi que des tâches de sauvegarde et d'ajuster ou de supprimer les tâches existantes.
- **Outils** : vous trouverez sous **Outils** d'autres outils concernant la sécurité des données.
- La rubrique Sauvegarde vous permet d'effectuer simplement et rapidement des sauvegardes de vos données et de créer des tâches de sauvegarde.

5.1.2 Configuration

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



La configuration 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 Premium Security Suite configuration

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 Avira Premium Security Suite l'icône de programme .

– Dans le Avira Premium Security Suite Control Center via la rubrique Outils | Configuration.
– Dans le Avira Premium Security Suite Control Center 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.

Commande de la configuration

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, 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 validés. 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.

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 de 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 de MailGuard

Fonction AntiBot : serveurs SMTP autorisés, expéditeurs d'emails autorisés

Exceptions de la recherche de MailGuard

Configuration de la mémoire tampon, vider la mémoire tampon

Configuration de la banque de données de formation AntiSpam, vider la banque de données de formation

Configuration d'un bas de page dans des emails envoyés

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

Fonction de contrôle parental : Filtre basé sur des rôles et limitation dans le temps basé sur des rôles de l'utilisation Internet

Réglage de la fonction de rapport

– **Pare-feu**: Configuration du pare-feu

Réglages des règles d'adaptateur

Réglage personnalisé des règles d'application

Liste des éditeurs dignes de confiance (exceptions lors de l'accès réseau par des applications)

Réglages étendus : timeout pour les règles, bloquer le fichier hôte Windows, arrêter le pare-feu Windows, notifications

Paramètres popup (messages d'avertissement lors de l'accès réseau par des applications)

– **Sauvegarde**:

Réglage du composant de sauvegarde (sauvegarde incrémentielle, recherche de virus lors de la sauvegarde)

Exceptions : réglage des fichiers à sauvegarder

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 réel

Protection par mot de passe pour l'accès au Control Center et à la configuration

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, réglage des mises à jour produits

Configuration des avertissements acoustiques en cas de détection de logiciel malveillant

5.1.3 Icône de programme

Après l'installation, l'icône de Premium Security Suite s'affiche dans la zone de notification de la barre des tâches :

Symbole	Description
	AntiVir Guard est activé et le pare-feu est activé
	AntiVir Guard est désactivé ou le pare-feu est désactivé

L'icône de programme indique l'état du service AntiVir Guard.

Via le menu contextuel de l'icône de programme, les fonctions centrales de Avira Premium Security Suite 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.

- **Pare-feu**:
- Activer le pare-feu : active ou désactive le pare-feu
- Bloquer tout le trafic : activé : bloque tout transfert de données à l'exception des transferts vers le système de l'ordinateur en question (Local Host / IP 127.0.0.1).
- Activer le mode jeu : active et désactive le mode :
  activé : toutes les règles définies pour l'adaptateur et l'application sont appliquées. Les applications pour lesquelles aucune règle n'est définie peuvent accéder au réseau et aucune fenêtre intempestive ne s'ouvre.
- **Démarrer AntiVir**: Ouvre le Avira Premium Security Suite Control Center.
- **Configurer AntiVir**: Ouvre la Configuration.
- **Démarrer 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 Premium Security Suite sur Internet. La condition est de disposer d'un accès actif à Internet.

5.2 Comment procéder

5.2.1 Activer le produit

Pour activer Avira Premium Security Suite, vous disposez des options suivantes :

- Activation avec une licence complète valide

  Pour activer le Avira Premium Security Suite avec une licence complète, vous avez besoin d'une clé d'activation valide, par le biais de laquelle les données de votre licence sont enregistrées. Soit nous vous avons envoyé la clé d'activation par email ou celle-ci est indiquée sur l'emballage du produit.

- Activation avec une licence d'évaluation

  Avira Premium Security Suite est activé par une licence d'évaluation générée automatiquement, grâce à laquelle vous pouvez tester l'intégralité des fonctions de Avira Premium Security Suite pendant une période limitée.

Remarque
Vous avez besoin d'une connexion Internet active pour activer le produit ou demander une licence test.
Si vous ne pouvez vous connecter aux serveurs de la société Avira GmbH, vérifiez les réglages du pare-feu utilisé, le cas échéant : Lors de l'activation du produit, des connexions sont utilisées via le protocole HTTP et le port 80 (communication Web) ainsi que via le protocole de cryptage SSL et le port 443. Assurez-vous que votre pare-feu ne bloque pas les données entrantes et sortantes. Vérifiez ensuite que vous pouvez accéder à des sites Internet par le biais de votre navigateur Web.

Voici comment activer Premium Security Suite :

Si vous n'avez pas encore installé Avira Premium Security Suite :

▶ installez Avira Premium Security Suite.

→ Au cours de l'installation, il vous est demandé de choisir une option d'activation

- *Activer le produit*

= Activation avec une licence complète valide

– *Tester le produit*

= Activation avec une licence d'évaluation

- Indiquez la clé d'activation dans le cas d'une activation avec licence complète.
- Confirmez la sélection du processus d'activation en cliquant sur **Suivant**.
- Entrez vos données personnelles pour une inscription, le cas échéant et confirmez votre saisie en cliquant sur **Suivant**.

→ Vos données de licence s'affichent dans la fenêtre de dialogue suivante. Avira Premium Security Suite a été activé.

- Poursuivez l'installation.

Si vous avez déjà installé Avira Premium Security Suite :

- Dans le Control Center de Avira Premium Security Suite, cliquez sur la rubrique **Aide :: Gestion de licence**.

→ L'assistant de licence s'affiche, dans lequel vous pouvez choisir l'option d'activation. Les étapes suivantes de l'activation du produit sont identiques à celles de la procédure présentée ci-avant.

5.2.2 Actualiser Avira Premium Security Suite de manière automatisée

Voici comment créer une tâche d'actualisation automatisée de Avira Premium Security Suite avec le planificateur AntiVir :

- Dans le Control Center, choisissez 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 d'actualiser Avira Premium Security Suite régulièrement et souvent. L'intervalle de mise à jour recommandé est : 2 heures.

- 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 de représentation* apparaît.

- Sélectionnez le mode de représentation de la fenêtre des tâches :
  - **Réduit** : uniquement la barre de progression
  - **Agrandi** : fenêtre des tâches intégrale
  - **Invisible** : pas de fenêtre des tâches
- 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 Premium Security Suite : 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 Premium Security Suite :

- Cliquez avec le bouton droit de la souris sur l'icône de programme Avira Premium Security Suite dans la barre des tâches.

→ Un menu contextuel s'affiche.

- Sélectionnez **Démarrer la mise à jour**.

→ La fenêtre de dialogue *Updater* apparaît.

- OU -

▶ Dans le Control Center, choisissez la rubrique **Aperçu :: Etat**.

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

→ La fenêtre de dialogue Updater apparaît.

- OU -

▶ Dans Control Center sélectionnez dans le menu **Mise à jour** la commande de menu *Lancer la mise à jour*.

→ La fenêtre de dialogue Updater apparaît.

Remarque
Nous conseillons vivement d'actualiser Avira Premium Security Suite régulièrement de manière automatisée. L'intervalle de mise à jour recommandé est : 2 heures.

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, choisissez 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 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 de Avira Premium Security Suite 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.

▶ Sélection dans le menu contextuel **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

Remarque
Après l'installation, le système crée la tâche de contrôle *Contrôle syst. intégral* dans le planificateur. Un contrôle de système intégral est exécuté automatiquement à l'intervalle recommandé.

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

▶ Dans le Control Center, choisissez 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 parcouru.
- ▶ 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 de représentation* apparaît.
- ▶ Sélectionnez le mode de représentation de la fenêtre des tâches :
  - **Réduit** : uniquement la barre de progression
  - **Agrandi** : fenêtre des tâches intégrale
  - **Invisible** : pas de fenêtre des tâches
- ▶ Sélectionnez l'option *Arrêter l'ordinateur*, si vous souhaitez que l'ordinateur s'arrête automatiquement dès que la tâche est exécutée et terminée. L'option est disponible uniquement en mode de représentation agrandi ou réduit.
- ▶ 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, choisissez la rubrique **Protection locale :: contrôler**.
- → Les profils de recherche prédéfinis apparaissent.
- ▶ Sélectionnez le profil de recherche prédéfini **Recherche de logiciel malveillant**.
- ▶ 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 Premium Security Suite, vous pouvez régler sous la rubrique *Action en cas de résultat positif* de la configuration, comment Premium Security Suite doit réagir en cas de détection d'un virus ou d'un programme indésirable :

Pour le composant ProActiv de Guard, il n'y a aucune option d'action configurable. Une résultat positif est toujours signalé dans la fenêtre *Guard: comportement suspect d'une application*.

Options d'action pour 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 du scanner**, vous recevez à l'issue de la recherche de fichiers, un message d'avertissement comportant une liste des fichiers concernés qui ont été trouvés. Vous avez la possibilité de sélectionner une action à exécuter pour les différents fichiers concernés, via le menu contextuel. Vous pouvez exécuter les actions choisies pour tous les fichiers concernés ou quitter le scanner .

- – **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.

Options d'action pour Guard :

- – **Interactif**

  En mode d'action interactif, l'accès au données est refusé et une notification s'affiche au bureau. Dans la notification affichée au bureau, vous avez la possibilité de retirer le logiciel malveillant trouvé, ou de le transmettre au composant scanner via le bouton Détails pour un traitement du virus. Le scanner signale le résultat positif dans une fenêtre où vous avez différentes options pour traiter le fichier concerné via un menu contextuel (voir résultat positif :: Scanner).

- – **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.

Options d'action pour 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 concerné. 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.

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 concernés et en exécutant l'action choisie par votre validation.

Les actions suivantes de traitement des objets concernés 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 de Guard (sans résultat positif de ProActiv):

– **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 va être supprimé. 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.

– **Écraser 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 Premium Security Suite n'effectue aucune autre action. Le fichier concerné 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 de Guard : l'accès au fichier concerné 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.

- **Réparer le secteur d'amorçage | télécharger l'outil de réparation**

  Options d'action en cas de résultat positif provenant de secteurs d'amorçage concernés : En cas de lecteurs de disquettes concernés, des options pour la réparation avec Premium Security Suite sont disponibles. Si aucune réparation n'est possible avec Premium Security Suite, vous pouvez télécharger un outil spécial pour la détection et la suppression de virus de secteur d'amorçage.

Remarque
Si vous appliquez des actions sur des processus en cours, les processus concernés sont arrêtés avant l'exécution de l'action.

Actions de Guard en cas de résultats positifs du composant ProActiv (message d'actions d'une application typiques pour un logiciel malveillant) :

- **Programme fiable**

  L'exécution de l'application se poursuit. Le programme est ajouté à la liste des applications autorisées, et il est exclu de la surveillance du composant ProActiv. En cas d'ajout à la liste des applications autorisées, il y a activation du type de surveillance *Contenu*. Cela signifie que l'application n'est exclue d'une surveillance par le composant ProActiv que si le contenu reste inchangé (voir Configuration :: Guard :: ProActiv :: filtre d'application : Applications autorisées).

- **Bloquer le programme une fois**

  L'application est bloquée, c'est-à-dire que l'exécution de l'application est arrêtée. Le composant ProActiv continue à surveiller les actions de l'application.

- **Bloquer toujours ce programme**

  L'application est bloquée, c'est-à-dire que l'exécution de l'application est arrêtée. Le programme est ajouté à la liste des applications à bloquer et ne peut plus être exécuté (voir Configuration :: Guard :: ProActiv :: Filtre d'application. Applications à bloquer).

- **Ignorer**

  L'exécution de l'application se poursuit. Le composant ProActiv continue à surveiller les actions de l'application.

Actions de MailGuard : Emails entrants

- **Déplacer en quarantaine**

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

- **Supprimer**

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

– **Supprimer la pièce jointe**

La pièce jointe concernée est remplacée par un texte standard. Si le corps de l'email est concerné, il 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 concernée 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. Choisissez 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 de 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 concerné 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 WebGuard.

Avertissement
Ce faisant, il est possible que des virus et programmes indésirables arrivent sur votre ordinateur. Choisissez 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://www.avira.com/fr/sample-upload
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, choisissez la rubrique **Gestion de 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 Premium Security Suite 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 Avira Malware Research Center en vue d'une analyse :

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

→ Une dialogue s'ouvre, contenant un formulaire pour la saisie de vos coordonnées.

▶ Indiquez les données au complet.

▶ Sélectionnez un type : **Fichier suspect** ou **Fausse alerte**.

▶ Appuyez sur **OK.**

→ Le fichier est téléchargé sur un serveur Web de 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 Premium Security Suite 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 : Premium Security Suite signale un résultat positif dans un fichier qui toutefois, n'est très vraisemblablement pas concerné 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 ne pouvez télécharger qu'un seul fichier à la fois.

Si vous souhaitez copier un objet en quarantaine dans un autre répertoire en le sortant de la quarantaine :

▶ Sélectionnez l'objet en quarantaine et cliquez sur  .

→ Une fenêtre de dialogue de recherche s'ouvre dans laquelle vous pouvez sélectionner un répertoire.

▶ Sélectionnez un répertoire dans lequel une copie de l'objet en quarantaine doit être mémorisé et validez votre sélection.

→ L'objet de quarantaine sélectionné est mis en mémoire dans le répertoire sélectionné.

Remarque
L'objet de quarantaine n'est pas identique au fichier restauré. L'objet de quarantaine est codé et ne peut pas être exécuté ni lu dans le format d'origine.

Si vous souhaitez exporter les propriétés de l'objet de quarantaine dans un fichier texte :

▶ sélectionnez l'objet en quarantaine et cliquez sur  .

→ Un fichier texte s'ouvre avec les données relatives à l'objet de quarantaine sélectionné.

▶ Mémorisez le fichier texte.

Vous pouvez aussi restaurer les fichiers en quarantaine :

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

5.2.11 Quarantaine : restaurer les fichiers en 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, choisissez la rubrique **Gestion de 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, choisissez la rubrique **Gestion de 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) :

✓ Dans le Control Center, choisissez 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 de Avira Premium Security Suite .

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

✓ Dans le Control Center, choisissez 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 Événements : Filtrer les événements

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

- Updater
- Guard
- MailGuard
- Scanner
- Planificateur
- Pare-feu

Les types d'événements suivants s'affichent :

- Information
- Avertissement
- Erreur
- Résultat positif

Voici comment filtrer les événements affichés :

▶ Dans le Control Center, choisissez la rubrique **Aperçu :: Événements**.

▶ Activez la case à cocher 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.

▶ Activez la case à cocher 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 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 de MailGuard .
- ▶ Cliquez sur le symbole souhaité pour exclure l'email de la vérification par 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 sélectionnée ne sera plus contrôlée à l'avenir, quant à l'absence de spam.

→ 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 ou de spam .

Avertissement
N'excluez de la vérification par 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.

5.2.17 MailGuard : entraîner le module AntiSpam

Le module AntiSpam contient une base de données de formation. Cette base de données de formation recueille vos critères individuels de catégorisation. Avec le temps, les filtres internes, algorithmes et critères d'évaluation pour le spam s'ajustent à vos critères personnels.

Voici comment catégoriser les emails pour la base de données de formation :

- ▶ Dans le Control Center, choisissez la rubrique **Protection en ligne :: MailGuard** .
- → Dans la liste, vous voyez les emails entrants.
- ▶ Sélectionnez l'email à catégoriser.
- ▶ Cliquez sur le symbole souhaité pour repérer l'email par ex. comme spam  ou comme souhaité, c'est-à-dire comme "bon" email  .

→ L'email est pris dans la base de données de formation et sert à la détection de spam la prochaine fois.

Remarque
Vous pouvez supprimer la base de données de formation dans la configuration sous MailGuard :: Généralités :: Supprimer AntiSpam.

5.2.18 Pare-feu : choisir le niveau de sécurité du pare-feu

Vous avez le choix entre plusieurs niveaux de sécurité. En fonction de cela, vous avez diverses possibilités de configurations pour les règles d'adaptateurs.

Les niveaux de sécurité suivants sont disponibles :

- **Bas**
- Le flooding et le scannage des ports sont détectés.
- **Moyen**
- Les paquets TCP et UDP suspects sont rejetés.
- Le flooding et le scannage des ports sont empêchés.
- **Elevé**
- L'ordinateur est invisible dans le réseau.
- L'ordinateur est invisible dans le réseau.
- Le flooding et le scannage des ports sont empêchés.
- **Utilisateur**
- Règles définies par l'utilisateur : à ce niveau de sécurité, le programme commute automatiquement quand vous avez modifié les règles d'adaptateurs.

Remarque
Le réglage par défaut du niveau de sécurité pour toutes les règles prédéfinies du pare-feu Avira est **Élevé**.

Voici comment régler le niveau de sécurité pour le pare-feu :

▶ Dans le Control Center, choisissez la rubrique **Protection en ligne :: Pare-feu**.

▶ Placez la règle coulissante sur le niveau de sécurité souhaité.

→ Le niveau de sécurité sélectionné est aussitôt activé.

5.2.19 Sauvegarde : créer manuellement des sauvegardes

L'outil de sauvegarde du Control Center vous permet de créer rapidement et simplement une sauvegarde de vos données personnelles. La sauvegarde Avira vous permet de créer des sauvegardes dites miroir grâce auxquelles vous pouvez sauvegarder et conserver vos données à leur niveau le plus récent, sans trop utiliser de ressources. Lors de la sauvegarde à l'aide de la sauvegarde Avira, les fichiers à sauvegarder sont contrôlés quant à l'absence de virus et de logiciels malveillants. Les fichiers infectés ne sont pas sauvegardés.

Remarque
Lors d'une sauvegarde miroir, aucune version individuelle de sauvegarde n'est conservée à la différence de la sauvegarde de version. La sauvegarde miroir contient l'ensemble des données au moment de la dernière sauvegarde. Toutefois, si des fichiers sont effacés de l'ensemble des données à sauvegarder, aucun alignement n'est effectué à la sauvegarde suivante, c'est-à-dire que les fichiers supprimés se trouvent encore dans la sauvegarde.

Remarque
La sauvegarde Avira avec des réglages standard sauvegarde uniquement les fichiers modifiés et un contrôle est effectué concernant les virus et logiciels malveillants. Vous pouvez modifier ces réglages dans la configuration sous Sauvegarde::Réglages.

Voici comment sauvegarder vos données à l'aide de l'outil de sauvegarde :

- Dans le Control Center, choisissez la rubrique **Outils :: sauvegarde**.

→ Les profils de sauvegarde prédéfinis apparaissent à l'écran.

- Sélectionnez l'un des profils de sauvegarde prédéfinis.

  -OU-

- Réglez le profil de sauvegarde *Sélection manuelle* en fonction de vos besoins.

  -OU-

- Créez un nouveau profil de sauvegarde
- Indiquez un emplacement de sauvegarde dans le champ *Répertoire cible* pour le profil choisi.

  Vous pouvez choisir comme emplacement de sauvegarde un répertoire de votre ordinateur ou d'un lecteur réseau connecté ainsi qu'un support d'échanges de données tel qu'une clé USB ou une disquette.

- Cliquez sur le symbole 

→ La fenêtre *Sauvegarde Avira* s'affiche à l'écran et la sauvegarde démarre. L'état et les événements de la sauvegarde s'affichent dans la fenêtre de sauvegarde.

Si vous souhaitez adapter un profil de sauvegarde :

- Dans le profil de recherche *Sélection manuelle*, ouvrez l'arborescence de manière à ce que tous les lecteurs et répertoires devant être sauvegardés 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 sauvegarder 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)

Si vous souhaitez créer un nouveau profil de sauvegarde :

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

→ Le profil *Nouveau profil* apparaît sous les profils existants.

- Renommez le profil de sauvegarde si nécessaire, en cliquant sur le symbole  .
- Sélectionnez les nœuds et répertoires à sauvegarder 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)

5.2.20 Sauvegarde : créer des sauvegardes de données automatisées

Voici comment vous pouvez créer une tâche permettant d'effectuer des sauvegardes de données automatisées :

▶ Dans le Control Center, choisissez 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 l'entrée **Tâche de sauvegarde**.

▶ Cliquez sur **Suivant**.

→ La fenêtre de dialogue *Sélection du profil* apparaît.

▶ Choisissez le profil qui doit être parcouru.

Remarque
Seuls s'affichent les profils de sauvegarde pour lesquels un emplacement de sauvegarde a été indiqué.

▶ 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**
- **Plug&Play**

  Pour l'événement Plug&Play, la sauvegarde est créée dès que le support d'échanges de données indiqué comme lieu de sauvegarde pour le profil de sauvegarde est connecté à l'ordinateur. L'événement de sauvegarde Plug&Play implique qu'une clé USB a été indiquée comme lieu de sauvegarde.

▶ 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 de représentation* apparaît.

▶ Sélectionnez le mode de représentation de la fenêtre des tâches :

- **Réduit** : uniquement la barre de progression
- **Agrandi** : l'ensemble de la fenêtre de sauvegarde
- **Invisible** : pas de fenêtre de sauvegarde

▶ 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

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 concernés :

- **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 Avira Premium Security Suite Control Center 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 Avira Premium Security Suite Control Center, 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 logiciel malveillant*
- 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 Premium Security Suite pour l'exécution des mises à jour. L'Updater garantit que Avira Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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. Après une mise à jour de produit, il peut être nécessaire d'effectuer un redémarrage de votre système d'ordinateur. S'il n'y a qu'une mise à jour du fichier de définitions des virus et du moteur de recherche, il n'est pas nécessaire de redémarrer l'ordinateur.

Remarque
Pour des raisons de sécurité, l'Updater contrôle si le fichier hôte Windows de votre ordinateur a été modifié, si l'URL de mise à jour de Avira Premium Security Suite a été manipulée par un logiciel malveillant par exemple et si l'Updater 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 l'Updater.

Une mise à jour de Premium Security Suite est exécutée automatiquement à l'intervalle suivant : 2 heures. Vous pouvez modifier ou désactiver la mise à jour automatique via la configuration (Configuration :: Mise à jour).

Dans le Control Center, sous planificateur, vous pouvez configurer d'autres tâches de mise à jour qui seront exécutées par l'Updater aux intervalles indiqués. 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. Par défaut, la connexion réseau existante est utilisée comme connexion aux serveurs de téléchargement de la société Avira GmbH. Vous pouvez adapter ce réglage par défaut dans la configuration sous Généralités :: Mise à jour.

8 Pare-feu Avira :: Aperçu

Le pare-feu Avira surveille et régule le trafic de données entrant et sortant sur votre système informatique et vous protège de nombreuses attaques et menaces provenant d'Internet : Sur la base de directives de sécurité, le trafic de données entrant et sortant ou l'écoute de ports sont autorisés ou refusés. Vous recevez une notification sur le bureau si le pare-feu Avira refuse des activités réseau et bloque ainsi des connexions réseau. Vous avez les possibilités suivantes pour régler le pare-feu Avira :

– par le biais du réglage d'un niveau de sécurité dans Control Center

Dans le Control Center vous pouvez régler un niveau de sécurité. Les niveaux de sécurité *Bas*, *Moyen* et *Élevé* contiennent plusieurs règles de sécurité se complétant les unes les autres, basées sur des filtres de paquets. Ces règles de sécurité sont enregistrées comme règles d'adaptateurs prédéfinies dans la configuration sous Pare-feu :: Règles d'adaptateur.

– en enregistrant des actions dans la fenêtre Événement réseau

Si une application tente une connexion réseau ou Internet pour la première fois, la fenêtre popup *Événement réseau* s'ouvre. La fenêtre *Événement réseau* vous permet de déterminer si l'activité réseau de l'application est autorisée ou refusée. Si l'option **Mémoriser l'action pour cette application** est activée, l'action est créée comme règle d'application et enregistrée dans la configuration sous pare-feu :: Règles d'application. L'enregistrement d'actions dans la fenêtre Événement réseau vous permet d'obtenir un jeu de règles pour les activités réseau de l'application.

Remarque
Pour les applications de fournisseurs fiables, l'accès réseau est autorisé par défaut, à moins que la règle d'adaptateur n'interdise l'accès réseau. Vous avez la possibilité de supprimer le fournisseur de la liste de fournisseurs fiables.

– en créant des règles d'adaptateur et d'application dans la configuration

Dans la configuration, vous pouvez modifier les règles d'adaptateur prédéfinies ou créer de nouvelles règles. Le niveau de sécurité du pare-feu est automatiquement réglé sur la valeur *Utilisateur*, lorsque vous ajoutez ou modifiez des règles d'adaptateur.
Les règles d'application vous permettent de définir des règles de surveillance spécifiques aux applications :
Avec des règles d'application simples, vous pouvez définir si toutes les activités réseau d'une application logicielle doivent être autorisées ou refusées, traitées de manière interactive par le biais de la fenêtre popup *Événement réseau*.
Dans la configuration étendue de la rubrique *Règles d'application*, vous pouvez définir, pour une application, différents filtres de paquets à exécuter comme règles d'application spécifiées.

Remarque
Les règles d'application possèdent deux modes : *privilégié* et *filtré*. Pour les règles d'application en mode *filtré*, des priorités sont attribuées aux règles d'adaptateur applicables, c'est-à-dire que les règles d'adaptateur correspondantes s'appliquent selon la règle d'application. Il peut donc arriver que l'accès réseau d'applications autorisées soit refusé en raison d'un niveau de sécurité élevé ou de règles d'adaptateur correspondantes. Pour les règles d'application en mode *privilégié* les règles d'adaptateur sont ignorées. Si des applications sont autorisées en mode *privilégié*, l'accès réseau de l'application est toujours autorisé.

9 Sauvegarde

Vous avez différentes possibilités de créer une sauvegarde de vos données :

Sauvegarde via l'outil de sauvegarde

À l'aide de l'outil de sauvegarde, vous pouvez choisir ou créer des profils de sauvegarde et lancer manuellement une sauvegarde pour un profil sélectionné.

Sauvegarde via une tâche de sauvegarde dans le planificateur

Le planificateur vous donne la possibilité de créer des tâches de sauvegarde programmées ou commandées par événement. Le planificateur exécute automatiquement les tâches de sauvegarde. Ce procédé convient particulièrement si vous souhaitez sauvegarder régulièrement certaines données.

10 FAQ, astuces

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

voir le chapitre Aide en cas de problème

voir le chapitre Commandes clavier

Voir chapitre Centre de sécurité Windows

10.1 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.
- Aucune connexion réseau disponible dans les machines virtuelles, si le pare-feu Avira est installé sur le système d'exploitation hôte et le niveau de sécurité du pare-feu Avira est réglé sur moyen ou élevé.
- La connexion Virtual Private Network (VPN) est bloquée si le niveau de sécurité du pare-feu Avira est réglé sur moyen ou élevé.
- Un email envoyé via une connexion TSL a été bloqué par 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 Premium Security Suite.

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 Premium Security Suite 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 (mode expert) sous Généralités :: Mise à jour.

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

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

▶ Actualisez Avira Premium Security Suite.

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

▶ Démarrez l'ordinateur en mode sécurisé.

▶ Démarrez Avira Premium Security Suite et la configuration (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 : Le AntiVir Guard est désactivé.

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

Cause : AntiVirGuard 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.

▶ Dans la configuration (mode expert) sélectionnez Guard :: Recherche :: Exception et saisissez le nom du processus du logiciel de sauvegarde.

Mon pare-feu déclare les AntiVir Guard et AntiVir MailGuard, dès que ceux-ci sont activés.

Cause : la communication d'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 d'AntiVir MailGuard à l'aide des checklists suivantes, si des problèmes se produisent en combinaison avec AntiVir MailGuard.

Checkliste

▶ 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 ne prend pas en charge SSL et arrête donc les connexions codées SSL. Si vous utilisez les connexions codées SSL sans protection MailGuard, pour la connexion vous devez utiliser un autre port que les ports surveillés par MailGuard. Vous pouvez configurer les ports surveillés par MailGuard dans la configuration sous MailGuard:: Recherche.

▶ Le service AntiVir MailGuard (service) 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 Premium Security Suite via "Démarrer | Panneau de configuration | Performances et maintenance | Logiciel", redémarrez l'ordinateur et réinstallez Avira Premium Security Suite.

Généralités

▶ 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 Premium Security Suite 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.

Aucune connexion réseau disponible dans les machines virtuelles, si le pare-feu Avira est installé sur le système d'exploitation hôte et le niveau de sécurité du pare-feu Avira est réglé sur moyen ou élevé.

Si le pare-feu Avira est installé sur un ordinateur sur lequel une machine virtuelle est aussi installée (par ex. VMWare, Virtual PC, ex.), toutes les connexions réseau de la machine virtuelle sont bloquées si le niveau de sécurité du pare-feu Avira est réglé sur Moyen ou Élevé. Si le niveau de sécurité est Bas, le pare-feu Avira réagit comme attendu.

Cause : la machine virtuelle émule une carte réseau par logiciel. Par cette émulation, les paquets de données du système hôte sont englobés dans des paquets spéciaux (UDP) et redirigés vers le système hôte, via la passerelle externe. Dans le pare-feu Avira, à partir du niveau de sécurité Moyen, ils sont bloqués par les paquets venant de l'extérieur.

Pour contourner ce problème, procédez comme suit :

- Dans le Control Center, choisissez la rubrique **Protection en ligne :: Pare-feu**.
- Cliquez sur le lien **Configuration**.
- La fenêtre de dialogue *Configuration* s'affiche à l'écran. Vous vous trouvez dans la rubrique Configuration *Règles d'application*.
- Activez le **mode expert**.
- Sélectionnez la rubrique Configuration **Règles d'adaptateur**.
- Cliquez sur **Ajouter**.
- Sous *Règle entrante*, sélectionnez **UDP**.
- Donnez un **nom** à la règle dans la zone nom de la règle.
- Cliquez sur **OK**.
- Vérifiez si la règle obéit à un niveau de priorité supérieur avec la règle **Refuser tous les paquets IP**.

Avertissement
Cette règle porte des dangers potentiels en elle car elle autorise tous les paquets UDP ! Après l'utilisation de votre machine virtuelle, repassez au niveau de sécurité précédent.

La connexion Virtual Private Network (VPN) est bloquée si le niveau de sécurité du pare-feu Avira est réglé sur moyen ou élevé.

Cause : le problème est la dernière règle de la chaîne **Refuser tous les paquets IP** qui intervient toujours quand un paquet ne correspond à aucune des règles en amont. Les paquets envoyés par le logiciel VPN sont filtrés par cette règle, car ils n'entrent dans aucune autre catégorie en raison de leur type (paquets GRE).

Remplacez la règle **Refuser tous les paquets IP** par deux nouvelles règles qui refusent les paquets TCP et UDP. De cette manière il devient possible d'autoriser les paquets d'autres protocoles.

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

Cause : Transport Layer Security (TLS : protocole de cryptage pour la transmission de données par Internet) n'est actuellement pas pris en charge par 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 de 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 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 : 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;r;transfer-encoding= chunked' 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 : WebGuard :: Exceptions).

10.2 Commandes clavier

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

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

10.2.1 Dans les champs de dialogue

Commande clavier	Description
Ctrl + Tab Ctrl + PgDn	Navigation dans Control Center Passer à la rubrique suivante.
Ctrl + Shift + Tab Ctrl + PgUp	Navigation dans Control Center Passer à la rubrique précédente.
← ↑ → ↓	Navigation dans les rubriques de configuration Mettez d'abord l'accent avec la souris sur une rubrique de configuration.
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.

10.2.2 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.
PgUp PgDn	Parcourir un thème.

10.2.3 Dans le Control Center

Généralités

Commande clavier	**Description**
F1	Afficher l'aide
Alt + F4	Fermer Control Center
F5	Actualiser la vue
F8	Ouvrir la configuration
F9	Lancer m. 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 FireWall

Commande clavier	Description
Enter	Caractéristiques

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 Événements

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

10.3 Centre de sécurité Windows

- à partir de Windows XP Service Pack 2 -

10.3.1 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.

10.3.2 Le Centre de sécurité Windows et Avira Premium Security Suite

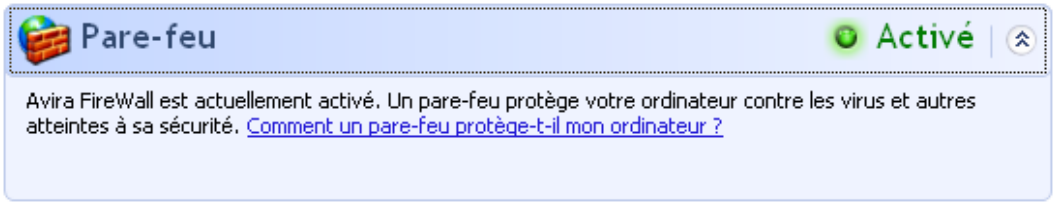
Pare-feu

Il est possible que vous receviez les informations suivantes du Centre de sécurité concernant le pare-feu :

- Pare-feu ACTIVÉ / Pare-feu en marche
- Pare-feu DÉSACTIVÉ / Pare-feu éteint

Pare-feu ACTIVÉ / Pare-feu éteint

Après l'installation de Avira Premium Security Suite et l'arrêt du pare-feu Windows, vous recevez le message suivant :



Pare-feu DÉSACTIVÉ / Pare-feu éteint

Vous recevez le message suivant dès que vous désactivez le pare-feu Avira :

Remarque
Vous pouvez activer et désactiver le pare-feu Avira via l'onglet État dans Avira Premium Security Suite Control Center.

Avertissement
Si vous désactivez le pare-feu Avira, votre ordinateur n'est plus protégé des accès non autorisés via le réseau ou Internet.

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

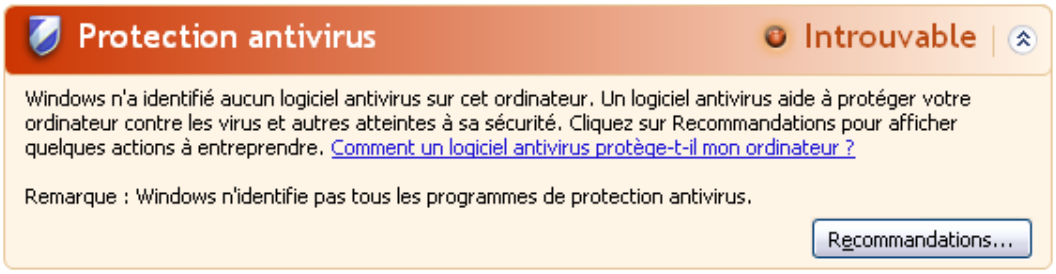
Protection antivirus ACTIVÉE

Protection antivirus DÉSACTIVÉE

Protection antivirus NON SURVEILLÉE

Protection antivirus NON TROUVÉE

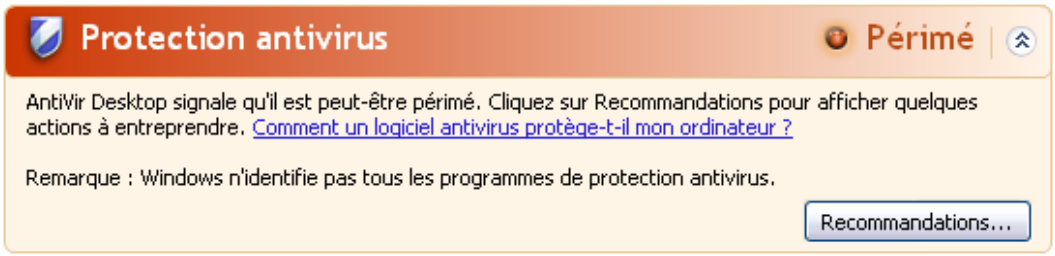
Cette remarque du Centre de sécurité Windows apparaît si le Centre de sécurité Windows n'a trouvé aucun logiciel antivirus sur votre ordinateur.



Remarque
Installez Avira Premium Security Suite sur votre ordinateur pour le protéger des virus et autres programmes indésirables !

Antivirus EXPIRÉ

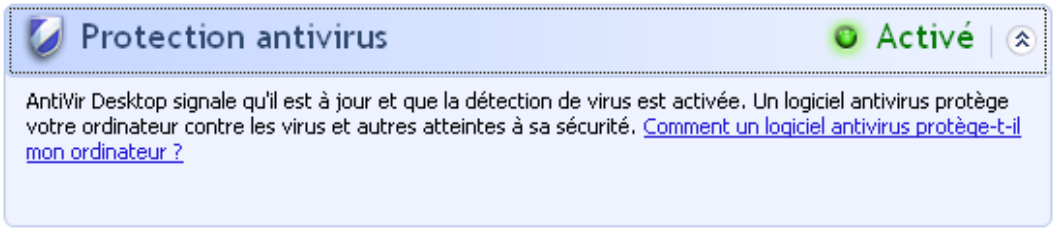
Si vous avez installé Windows XP Service Pack 2 ou Windows Vista puis Avira Premium Security Suite ou si vous avez installé Windows XP Service Pack 2 ou Windows Vista sur un système accueillant déjà Avira Premium Security Suite, vous recevez le message suivant :



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

Protection antivirus ACTIVÉE

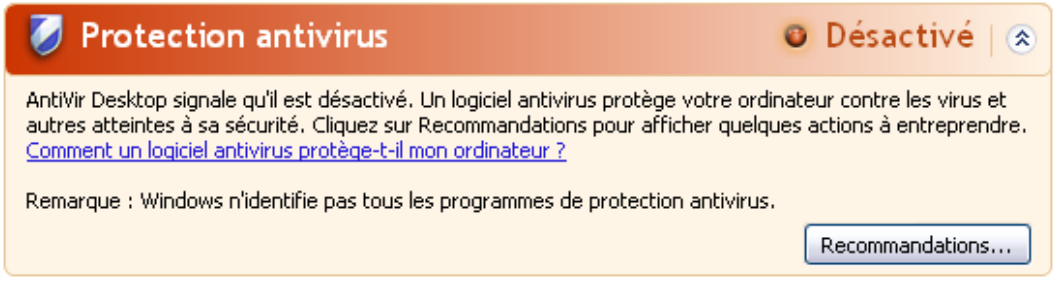
Après l'installation de Avira Premium Security Suite et une mise à jour immédiatement après, vous recevez le message suivant :



Avira Premium Security Suite 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 :: État du Avira Premium Security Suite 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 Premium Security Suite. 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 Premium Security Suite. 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 !

11 Virus et autres

11.1 Catégories étendues de dangers

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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite détecte les "logiciels publicitaires/espions". Si dans la configuration, l'option Logiciels publicitaires/logiciels espions est cochée sous **Catégories étendues de dangers**, vous recevez un avertissement si Avira Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite détecte l'"hameçonnage". Si dans la configuration, l'option Hameçonnage est cochée sous **Catégories étendues de dangers**, vous recevez un avertissement si Avira Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite détecte ce type de comportement.

11.2 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 contaminent 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 concernés 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. Dans ce cas, des programmes peuvent s' infiltrer, permettant d'obtenir un accès plus important.

Hoaxes (engl.: hoax - canulars)

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. Quand un agresseur examine alors 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 contaminées. 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 de l'hameçonnage. Les escrocs au pharming entretiennent leurs propres grandes fermes de serveurs sur lesquelles des sites Web falsifiés 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. L'hameçonneur 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 des identifiants et mots de passe ou PIN et TAN pour les transactions bancaires en ligne. Avec les données d'accès volées, l'hameçonneur 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. Toutefois, le déroulement même du programme de l'hôte n'est normalement 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 de 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 contaminer 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 disposant de 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.

12 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

12.1 Adresse de contact

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

12.2 Support technique

Le support de Avira Premium Security Suite 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.com/fr/premium-suite-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 la surface programme sous l'option de menu Aide :: concernant Premium Security Suite :: Informations de licence.
- **Informations de version**. Vous les trouverez dans la surface programme sous l'option de menu Aide :: concernant Premium Security Suite :: 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.

12.3 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 de Control Center et sélectionnez via le menu contextuel ou le bouton correspondant le point Envoyer fichier.
- Envoyez le fichier souhaité compressé (WinZIP, PKZip, Arj etc.) en pièce jointe d'un email à virus-premium-suite-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.

12.4 Indiquer une fausse alarme

Si vous pensez que Avira Premium Security Suite 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-premium-suite-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).

12.5 Vos réactions pour plus de sécurité

Chez Avira GmbH, la sécurité de nos clients est en première place. Pour cette raison, nous n'avons seulement recours à notre équipe interne d'experts qui fait subir à chaque solution Avira GmbH et à chaque mise à jour des tests de qualité et de sécurité avant publication. Nous prenons également au sérieux vos remarques sur d'éventuelles faiblesses de sécurité et nous les traitons ouvertement.

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

13 Référence : options de configuration

La référence de la configuration documente toutes les options de configuration disponibles dans Avira Premium Security Suite.

13.1 Scanner

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

13.1.1 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 contrôlés 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 Premium Security Suite. Cela signifie que le programme Avira Premium Security Suite 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 contrôlés. 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.

Important
Cette fonction n'est disponible qu'à partir de Windows Vista.

Remarque
Si vous utilisez des outils de fournisseurs-tiers, si vous modifiez les fichiers système et adaptez par exemple l'écran d'amorçage ou de démarrage à vos besoins, veuillez ne pas utiliser cette option. De tels outils sont constitués par exemple par les Skinpacks, TuneUp Utilities ou Vista Customization.

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.

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 Rootkit n'est pas disponible sous Windows XP 64 bits !

Contrôler le registre

Si l'option est activée, le système recherche la présence de renvois à des logiciels dommageables dans le registre.

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 Arrêt dans la fenêtre du "Luke Filewalker". Si vous avez désactivé ce réglage, le bouton Arrêt dans la fenêtre "Luke Filewalker" est en gris. L'interruption prématurée 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.

Élevé

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

13.1.1.1. 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 du scanner, 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.

Remarque
L'action « déplacer en quarantaine » est prédéfinie par défaut dans la boîte de dialogue pour le traitement des virus. Vous pouvez sélectionner d'autres actions via un menu contextuel.

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 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 (sauvegarde) avant d'exécuter l'action primaire 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.

Action primaire

L'action primaire 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 ne peut être sélectionnée que si sous Action primaire l'option **réparer** a été sélectionnée.

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 comme solution de rechange 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 l'option est activée, le fichier est supprimé. Ce processus est nettement 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 concerné 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. Ces fichiers peuvent être réparés ultérieurement ou - si nécessaire - être envoyés à Avira Malware Research Center.

Action secondaire

L'option **Action secondaire** ne peut être sélectionnée que si sous **Action primaire** 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 l'option est activée, le fichier est supprimé. Ce processus est nettement 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 (wipen). 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 concerné 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 en quarantaine. Ces 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.

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 récursion dans lequel le virus ou le programme indésirable se trouve.

Profondeur maximale de récursivité

Pour pouvoir saisir la profondeur de récursivité maximale, l'optionLimiter 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 contrôler. Pour cela, vous devez repérer les entrées correspondantes.

13.1.1.2. 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 contrôlé.

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.

13.1.1.3. Heuristique

Cette rubrique de configuration contient les réglages pour l'heuristique du moteur de recherche Avira Premium Security Suite.

Avira Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite détecte beaucoup plus de logiciels malveillants inconnus, mais vous devez vous attendre aussi à des messages erronés.

13.1.2 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

Désactivé

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 détenteur de la licence sont inscrits dans le fichier rapport.

Étendu

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 contrôlés. 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.

13.2 Guard

La rubrique Guard de la configuration est responsable de la configuration de la recherche en temps réel.

13.2.1 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 contrôler 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 contrôlés 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 Premium Security Suite. Cela signifie que Avira Premium Security Suite 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 lent 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 contrôlés. 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 contrôlés, décompressés et à nouveau contrôlés. 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.

13.2.1.1. 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 l'option est activée, une notification est affichée sur le bureau en cas de résultat positif du Guard. Vous avez la possibilité de retirer le logiciel malveillant trouvé ou d'appeler d'autres actions possibles pour le traitement du virus via le bouton « Détails ». Les actions sont affichées dans une fenêtre de dialogue. Cette option est activée 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 primaire 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.

Action primaire

L'action primaire 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 ne peut être sélectionnée que si sous Action primaire l'option réparer a été sélectionnée.

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 Guard modifie les fichiers sur l'ordinateur.

supprimer

Si l'option est activée, le fichier est supprimé. Ce processus est nettement plus rapide que "écraser et supprimer".

écraser et supprimer

Si cette option est activée, 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 concerné 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** ne peut être sélectionnée que si sous **Action primaire** 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 l'option est activée, le fichier est supprimé. Ce processus est nettement plus rapide que "écraser et supprimer".

écraser et supprimer

Si cette option est activée, 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 concerné 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.

13.2.1.2. Autres actions

Notifications

Rapport d'événement

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.

Autodémarrage

Bloquer la fonction d'autodémarrage

Si l'option est activée, l'exécution de la fonction d'autodémarrage Windows est bloquée sur tous les lecteurs intégrés comme les clés USB, les lecteurs CD et DVD, les lecteurs réseau. Avec la fonction d'autodémarrage Windows, les fichiers sur des supports de données ou sur des lecteurs réseau sont immédiatement lus lors de l'insertion ou de la connexion. Ainsi, les fichiers peuvent être démarrés et reproduits automatiquement. Toutefois, cette fonctionnalité présente un risque de sécurité élevé car elle permet le démarrage automatique de fichiers de logiciels malveillants et de programmes indésirables. La fonction d'autodémarrage est particulièrement critique pour les clés USB car les données sur une clé USB peuvent constamment changer.

Exclure des CD et DVD

Si l'option est activée, la fonction d'autodémarrage est autorisée sur les lecteurs de CD et DVD.

Avertissement
Ne désactivez la fonction d'autodémarrage pour les lecteurs de CD et de DVS que si vous êtes certain d'utiliser uniquement des supports de données dignes de confiance.

13.2.1.3. 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.

Remarque
Vous pouvez saisir 128 processus au maximum.

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

Avertissement :
Le chemin indiqué et le nom de fichier du processus peuvent contenir 255 signes au maximum.

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.

Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner un fichier exécutable.

Processus

Le bouton **Processus** ouvre la fenêtre *Sélection de processus*, dans laquelle les processus en cours sont affichés.

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.

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.

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

Remarque
Vous pouvez indiquer 20 exceptions au maximum par lecteur avec le chemin complet (commençant par la lettre du lecteur).
Ex. C:\Programmes\Application\Nom.log

Le nombre maximum d'exceptions sans chemin complet s'élève à 64.
Exemple : *.log

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.

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
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 suit : Réglez la fonction de protocole du Guard sur **Intégral** dans la configuration sous Guard :: Rapport. Le Guard étant activé, accédez maintenant aux fichiers, répertoires, lecteurs intégrés . 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
```

13.2.1.4. Heuristique

Cette rubrique de configuration contient les réglages pour l'heuristique du moteur de recherche Avira Premium Security Suite.

Avira Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite détecte beaucoup plus de logiciels malveillants inconnus, mais vous devez vous attendre aussi à des messages erronés.

13.2.2 ProActive

En utilisant la fonction AntiVir ProActiv, vous vous protégez contre de nouvelles menaces et menaces inconnues pour lesquelles il n'existe encore aucune définition de virus ni d'heuristique. La technologie ProActiv est intégrée au composant Guard et observe et analyse les actions exécutées par des programmes. Le comportement de programmes est examiné à la recherche de modèles d'action typiques de logiciel malveillant : Type d'action et suites d'actions. Si un programme présente un comportement typique pour un logiciel malveillant, ceci est traité et signalé comme un virus détecté : Vous avez la possibilité de bloquer l'exécution du programme ou d'ignorer le message et de poursuivre l'exécution du programme. Vous pouvez classifier le programme comme étant digne de confiance et l'ajouter ainsi au filtre d'application des programmes autorisés. Vous avez également la possibilité d'ajouter le programme au filtre d'application des programmes à bloquer via l'instruction *Toujours bloquer*

Pour déterminer le comportement type d'un logiciel malveillant, le composant ProActiv utilise un ensemble de règles mises au point par le centre de recherche sur les logiciels malveillants Avira Malware Research Center. Avira Gmbh est alimentée en ensembles de règles par les banques de données. Pour la saisie d'information dans les banques de données, Avira, AntiVir ProActiv envoie des informations sur les programmes signalés comme suspects. Vous avez la possibilité de désactiver la transmission de données aux banques de données Avira.

Remarque
La technologie ProActiv n'est pas encore disponible sur les systèmes 64 bits ! Sous Windows 2000, il n'existe aucune prise en charge pour les composants ProActiv.

Généralités

Activer la fonction AntiVir ProActiv

Lorsque l'option est activée, les programmes sont surveillés sur votre système d'ordinateur et sont examinés pour savoir s'ils exécutent des actions typiques pour des logiciels malveillants. En cas de comportement typique pour des logiciels malveillants, vous êtes averti par un message. Vous avez la possibilité de bloquer l'exécution du programme ou de poursuivre le programme avec *Ignorer* . Sont exclus de la surveillance : tous les programmes classifiés comme étant dignes de confiance ainsi que les programmes signés qui sont contenus par défaut dans le filtre d'application des applications autorisées, tous les programmes que vous avez ajoutés au filtre d'application des programmes autorisés.

Participer à la communauté Avira ProActiv

Si l'option est activée, AntiVir ProActiv envoie aux banques de données Avira des données concernant les actions de programme exécutées. Après leur exploitation, les données sont intégrées aux ensembles de règles de l'analyse de comportement ProActiv. Ainsi, vous participez à la communauté Avira ProActiv et contribuez au perfectionnement constant de la technologie de sécurité ProActiv. Si l'option est désactivée, aucune donnée n'est envoyée. Ceci n'a aucune influence sur la fonctionnalité de ProActiv.

13.2.2.1. Filtre d'application : Applications à bloquer

Sous *filtre d'application : Applications à bloquer* vous pouvez ajouter les applications que vous classifiez comme nuisibles et qui doivent être bloquées par défaut par AntiVir ProActiv. Les applications ajoutées ne peuvent pas être exécutées sur votre système d'ordinateur. Vous pouvez également ajouter des programmes comme ayant un comportement suspect au filtre d'application pour les applications à bloquer via les messages du Guard à l'aide de l'option *Toujours bloquer ce programme* .

Applications à bloquer

Applications

La liste reprend toutes les applications que vous avez classifiées comme étant nuisibles et que vous avez ajoutées via la configuration ou via les messages des composants ProActiv. Les applications de la liste sont bloquées par ProActiv et ne peuvent pas être exécutées sur votre système d'ordinateur. Lors du démarrage d'un programme à bloquer, un message du système d'exploitation s'affiche. ProActiv identifie les applications à bloquer à l'aide du chemin indiqué et du nom de fichier et les bloque indépendamment de leur contenu.

Champ de saisie

Saisissez dans ce champ l'application qui doit être bloquée. Pour l'identification de l'application, il faut indiquer le chemin complet et le nom de fichier avec son extension. L'indication de chemin doit contenir le lecteur où est l'application, ou bien commencer avec une variable d'environnement.

Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner l'application à bloquer.

Ajouter

Le bouton **Ajouter** vous permet de reprendre dans la liste des applications à bloquer l'application indiquée dans le champ de saisie.

Remarque
les applications nécessaires à la fonctionnalité du système d'exploitation ne peuvent être ajoutées à la liste.

Supprimer

Le bouton **Supprimer** vous permet de supprimer une application sélectionnée de la liste des applications à bloquer.

13.2.2.2. Filtre d'application : applications autorisées

Sous *filtre d'application : applications autorisées* , les applications exclues de la surveillance du composant ProActiv sont regroupées dans une liste : les programmes signés classifiés comme étant dignes de confiance et qui sont contenus par défaut dans la liste, toutes les applications que vous avez classifiées comme étant dignes de confiance et ajoutés au filtre d'application . Dans la configuration vous pouvez ajouter des application à la liste des applications autorisées. Vous avez également la possibilité d'ajouter des applications comme ayant un comportement suspect via les messages du Guard en utilisant dans le message Guard l'option **Programme digne de confiance**.

Applications à exclure

Applications

La liste contient les applications exclues de la surveillance du composant ProActiv. Dans les paramètres par défaut après l'installation, la liste contient les applications signées de fabricants dignes de confiance. Vous avez la possibilité d'ajouter les applications que vous avez classifiées comme étant dignes de confiance via la configuration ou via les messages du Guard. Le composant ProActiv identifie les applications à l'aide du chemin indiqué, du nom de fichier et du contenu. Un contrôle de contenu est adapté car il est possible d'ajouter ultérieurement à un programme un code dommageable via des modifications comme des mises à jour. Vous pouvez déterminer via le type indiqué si un contrôle de contenu doit être effectué : Pour le type *Contenu* les applications indiquées avec le chemin et le nom de fichier sont examinées pour voir si le contenu du fichier ne présente pas des modifications, avant d'être exclues de la surveillance par le composant ProActiv. En cas de modification du contenu du fichier, l'application est à nouveau surveillée par le composant ProActiv. Pour le type *Chemin* il n'y a pas de contrôle de contenu avant que l'application soit exclue de la surveillance par Guard. Pour changer le type d'exclusion, cliquez sur le type affiché.

Avertissement
Utilisez le type *Chemin* uniquement dans des cas exceptionnels. Une mise à jour permet d'ajouter un code dommageable à une application. L'application a l'origine inoffensive devient alors un logiciel malveillant.

Remarque
Quelques applications dignes de confiance comme p. ex. tous les composants d'application de Premium Security Suite, sont exclus par défaut d'une surveillance par le composant ProActiv, mais ne figurent pas sur la liste.

Champ de saisie

Dans ce champ, vous indiquez l'application devant être exclue de la surveillances par le composant ProActiv. Pour l'identification de l'application, il faut indiquer le chemin complet et le nom de fichier avec son extension. L'indication de chemin doit contenir le lecteur où est l'application, ou bien commencer avec une variable d'environnement.

Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner l'application à exclure.

Ajouter

Le bouton **Ajouter** vous permet de reprendre dans la liste des applications à exclure l'application indiquée dans le champ de saisie.

Supprimer

Le bouton **Supprimer** vous permet de supprimer une application sélectionnée de la liste des applications à exclure.

13.2.3 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. En cas de limitation du fichier de rapport, 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.

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.

13.3 MailGuard

La rubrique MailGuard de la configuration est en charge de la configuration du MailGuard.

13.3.1 Recherche

Vous utilisez le MailGuard pour contrôler les emails entrants quant à l'absence de virus et de logiciels malveillants et de spam. Il est possible de faire contrôler les emails sortants par le MailGuard, quant à l'absence de virus et de logiciels malveillants. Le MailGuard peut bloquer les emails sortants qui sont envoyés de votre ordinateur par un bot inconnu pour diffuser des spams.

Recherche

Contrôler les emails entrants

Si l'option est activée, les emails sortants sont contrôlés quant à l'absence de virus, de logiciels malveillant et de spam . MailGuard prend en charge les protocoles POP3 et IMAP. Activez le compte de la boîte de réception utilisée 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. Les emails envoyés par un bot inconnu pour diffuser des spams, sont bloqués.

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.

13.3.1.1. Action en cas de résultat positif

Cette rubrique de configuration contient les réglages concernant les actions effectuées lorsque 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.

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 primaire

L'action primaire est l'action exécutée lorsque 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** ne peut être sélectionnée que si sous **Action primaire** l'option **Ignorer l'email** a été sélectionnée. 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 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 !

13.3.1.2. Autres actions

Cette rubrique de configuration contient d'autres réglages concernant les actions effectuées lorsque 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.

13.3.1.3. Heuristique

Cette rubrique de configuration contient les réglages pour l'heuristique du moteur de recherche Avira Premium Security Suite.

Avira Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite détecte beaucoup plus de logiciels malveillants inconnus, mais vous devez vous attendre aussi à des messages erronés.

13.3.1.4. AntiBot

La fonction AntiBot du MailGuard vous permet d'empêcher que votre ordinateur ne soit utilisé comme partie d'un réseau bot pour diffuser des emails spam : lors de la diffusion de spam par un réseau bot, l'agresseur infecte en règle générale plusieurs ordinateurs avec un bot qui se connecte ensuite à un serveur IRC, entre dans un certain canal et de là, attend de recevoir l'ordre d'envoyer des emails à spam. Pour différencier les emails à spam d'un bot inconnu des emails de l'utilisateur de l'ordinateur, MailGuard vérifie si le serveur SMTP utilisé et l'expéditeur d'un email sortant sont bien mentionnés dans les listes des serveurs et expéditeurs autorisés. Si ce n'est pas le cas, l'email sortant est bloqué, c'est-à-dire l'email n'est pas envoyé. L'email bloqué est signalé dans une fenêtre de dialogue.

Remarque
La fonction AntiBot ne peut être utilisée que si la recherche du MailGuard est active pour les emails sortants (voir option **contrôler les emails sortants** sous MailGuard :: Recherche).

Serveurs autorisés

Tous les serveurs apparaissant dans cette liste sont autorisés par le MailGuard pour l'envoi de emails : les emails envoyés à ces serveurs ne sont **pas** bloqués par le MailGuard. Si aucun serveur n'est indiqué dans la liste, aucune vérification du serveur SMTP utilisé n'est effectuée pour les emails sortants. Si la liste contient des entrées, MailGuard bloque les emails qui sont envoyés à un serveur SMTP ne figurant pas dans la liste.

Champ de saisie

Vous saisissez dans ce champ le nom d'hôte ou l'adresse IP du serveur SMTP que vous utilisez pour envoyer des emails.

Remarque
Vous trouverez les informations concernant les serveurs SMTP utilisés par votre programme email pour l'envoi d'emails, dans les données de votre programme sur les comptes utilisateurs créés.

Ajouter

Ce bouton vous permet d'accepter les serveurs indiqués dans le champ de saisie dans la liste des serveurs autorisés.

Supprimer

Ce bouton efface une entrée sélectionnée dans la liste des serveurs autorisés. Ce bouton n'est pas fonctionnel si aucune entrée n'est sélectionnée.

Supprimer tous

Ce bouton efface toutes les entrées de la liste des serveurs autorisés.

Expéditeurs autorisés

Tous les expéditeurs apparaissant dans cette liste sont autorisés par le MailGuard pour l'envoi de emails : les emails envoyés par cette adresse email ne sont **pas** bloqués par le MailGuard. Si aucun expéditeur n'est indiqué dans la liste, aucune vérification de l'adresse email utilisé par l'expéditeur n'est effectuée pour les emails sortants. Si la liste contient des entrées, MailGuard bloque les emails des expéditeurs ne figurant pas dans la liste.

Champ de saisie

Vous saisissez dans ce champ votre/vos adresse(s) email d'expéditeur.

Ajouter

Ce bouton vous permet d'accepter les expéditeurs indiqués dans le champ de saisie dans la liste des expéditeurs autorisés.

Supprimer

Ce bouton efface une entrée sélectionnée dans la liste des expéditeurs autorisés. Ce bouton n'est pas fonctionnel si aucune entrée n'est sélectionnée.

Supprimer tous

Ce bouton efface toutes les entrées de la liste des expéditeurs autorisés.

13.3.2 Généralités

13.3.2.1. 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 MailGuard exclusivement pour les emails entrants.

État

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

Adresse email

Adresse email qui ne doit plus être contrôlée.

Logiciel malveillant

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

Spam

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

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 MailGuard, quels que soient vos réglages.

Remarque
Lors de la saisie d'adresses email, vous pouvez utiliser des caractères de remplacement : caractère de remplacement * pour un nombre illimité de caractères et **?** pour un seul caractère. Les caractères de remplacement ne peuvent toutefois être utilisés que pour les adresses email qui ne doivent pas être contrôlées quant à l'absence de spam. Vous recevez donc un message d'erreur quand vous tentez d'exclure une adresse contenant des caractères de remplacement du contrôle concernant l'absence de logiciels malveillants, en activant la case à cocher **Logiciels malveillants** dans la liste d'exclusions. Lors de la saisie d'adresses avec des caractères de remplacement, tenez compte du fait que la série de caractères indiquée doit correspondre à la structure d'une adresse email (*@*.*).

Avertissement
Tenez compte des exemples donnés lors de l'utilisation de caractères de remplacement. N'utilisez les caractères de remplacement que de manière ciblée et contrôlez précisément les adresses email que vous acceptez dans la liste blanche de spam en saisissant des caractères de remplacement.

Exemples : utilisation de caractères de remplacement dans les adresses email (liste blanche de spam)

- `virus@avira.* /` = comprend tous les emails avec cette adresse et un nombre au choix de domaines de premier niveau : virus@avira.de, virus@avira.com, virus@avira.net,...
- `*@avira.com` = comprend tous les emails envoyés à partir du domaine **avira.com** : info@avira.com, virus@avira.com, contact@avira.com, employé@avira.com
- `info@*.com` = comprend toutes les adresses email avec le domaine de premier niveau **com** et l'adresse **info** : le domaine de second niveau est au choix : info@name1.com, info@name2.com,...

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.

Importer le carnet d'adresses Outlook

Ce bouton vous permet d'importer les adresses email du carnet d'adresses du programme email MS Outlook dans la liste des exceptions. Les adresses email importées ne sont pas contrôlées quant à l'absence de spam.

Importer le carnet d'adresses Outlook Express

Ce bouton vous permet d'importer les adresses email du carnet d'adresses du programme email MS Outlook Express dans la liste des exceptions. Les adresses email importées ne sont pas contrôlées quant à l'absence de spam.

13.3.2.2. Mémoire tampon

Mémoire tampon

La mémoire tampon de MailGuard contient les données sur les emails contrôlés qui sont affichés dans les statistiques du Control Center sous MailGuard. En outre, des copies des emails entrants sont stockées dans la mémoire tampon. Les emails sont utilisés pour les fonctions de formation (email bon &endash; utiliser pour la formation, Spam &endash; utiliser pour la formation) du module AntiSpam.

Remarque
Pour que les emails entrants soient mémorisés dans la mémoire tampon, le module AntiSpam doit être activé.

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.

13.3.2.3. MailGuard

AntiSpam

La fonction AntiVir MailGuard contrôle l'absence de virus et de programmes indésirables sur les emails. En outre, il peut vous protéger efficacement contre les spams.

AntiSpam

Activer le module AntiSpam

Si l'option est activée, la fonction AntiSpam du MailGuard est activée.

Repérer l'objet de l'email

Si l'option est activée, une mention est ajoutée à l'objet d'origine si l'email est identifié comme spam.

Simple

Une mention supplémentaire [SPAM] ou [Phishing] est ajoutée à l'objet si l'email est un spam ou une opération de hameçonnage. Cette option est activée par défaut.

Détaillé

Une mention étendue indiquant la probabilité qu'il s'agisse d'un spam est ajoutée à l'objet de l'email de spam ou de hameçonnage.

Documenter

Si cette option est activée, le MailGuard génère un fichier rapport spécial AntiSpam.

Utiliser les listes noires en temps réel

Si cette option est activée, une "liste noire" est interrogée en temps réel. Elle contient des informations supplémentaires pour classer les emails d'origine douteuse comme spams.

Timeout : n seconde(s)

Si les informations d'une liste noire ne sont pas disponibles au bout de n secondes, la tentative d'accès à la liste noire est interrompue.

Supprimer la base de données d'apprentissage

La base de données d'apprentissage est effacée si l'on clique sur ce bouton.

Ajouter automatiquement les destinataires des emails sortants à la liste blanche

Si l'option est activée, les adresses des destinataires d'emails sortants sont reprises automatiquement dans la liste blanche de spam (liste des emails qui ne doivent pas être contrôlés quant à l'absence de spam sous **MailGuard :: Généralités :: Exceptions**). Les emails entrants qui sont envoyés à partir des adresses de la liste blanche de spam, ne sont pas contrôlés quant à l'absence de spam. Le contrôle concernant les virus et logiciels malveillants continue d'être effectué. Cette option est désactivée par défaut.

Remarque
Cette option ne peut être activée que si la recherche du MailGuard est active pour les emails sortants (voir option **contrôler les emails sortants** sous MailGuard :: Recherche).

13.3.2.4. Pied de page

Sous *Pied de page* vous pouvez configurer un bas de page email qui sera affiché dans les emails que vous envoyez. Pour cette fonction, il est indispensable d'activer le contrôle MailGuard pour les emails sortants (voir option *contrôler les emails sortants (SMTP)* sous Configuration :: MailGuard :: Recherche) . Vous pouvez utiliser le bas de page défini AntiVir MailGuard avec lequel vous confirmez que l'email envoyé a été contrôlé par un programme de protection anti-virus. Vous avez également la possibilité d'entrer un texte pour un bas de page personnalisé. Si vous utilisez les deux options pour le bas de page, le texte personnalisé précède le bas de page AntiVir MailGuard.

Bas de page pour les emails à envoyer

Joindre bas de page AntiVir MailGuard

Si l'option est activée, le bas de page AntiVir MailGuard est affiché sous le texte de message de l'email envoyé. Avec le bas de page AntiVir MailGuard vous confirmez que l'email envoyé a été contrôlé par AntiVir MailGuard à la recherche de virus et de programmes indésirables et qu'il ne provient pas d'un bot inconnu. Le bas de page AntiVir MailGuard contient le texte suivant : "Contrôlé avec AntiVir MailGuard [version de produit] [abréviation de nom et numéro de version du moteur de recherche] [abréviation de nom et numéro de version du fichier]".

Joindre ce bas de page

Si l'option est activée, le texte que vous indiquez dans le champ de saisie s'affiche en bas de page dans les emails envoyés.

Champ de saisie

Dans ce champ de saisie vous pouvez saisir un texte qui sera affiché en bas de page dans les emails envoyés.

13.3.3 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 l'option est activée, le MailGuard consigne également les informations secondaires dans le fichier de 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. En cas de limitation du fichier de rapport, 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.

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.

13.4 Pare-feu

La rubrique Pare-feu de la configuration permet de configurer le pare-feu Avira.

13.4.1 Règles d'adaptateur

On appelle adaptateur dans le pare-feu Avira chacune des unités matérielles simulées par un logiciel (par ex. miniport, montage en pont, etc.) ou chaque unité matérielle (par ex. une carte réseau).

Le pare-feu Avira indique les règles d'adaptateur pour tous les adaptateurs existants sur votre ordinateur et pour lesquels un pilote est installé.

Une règle d'adaptateur prédéfinie dépend du niveau de sécurité. Vous pouvez modifier le niveau de sécurité via la rubrique Protection en ligne :: Pare-feu du Avira Premium Security Suite Control Center ou adapter les règles d'adaptateur à vos besoins. Si vous avez adapté les règles d'adaptateur à vos besoins, sous la rubrique Pare-feu du Avira Premium Security Suite Control Center, le régulateur est placé sur Utilisateur dans la zone Niveau de sécurité.

Remarque
Le réglage par défaut du niveau de sécurité pour toutes les règles prédéfinies du pare-feu Avira est **Élevé**.

Protocole ICMP

L'Internet Control Message Protocol (ICMP) sert à l'échange de messages d'erreur et d'information dans les réseaux. Le protocole est aussi utilisé pour les messages d'état par ping ou tracert.
Cette règle vous permet de définir les types d'ICMP entrants et sortants qui doivent être bloqués, de fixer les paramètres de flooding et de définir le comportement en cas de paquets ICMP fragmentés. Cette règle sert à empêcher les attaques par inondation ICPM qui peuvent conduire à la surcharge du processeur de l'ordinateur attaqué car une réponse est donnée à chaque paquet.

Règles prédéfinies pour le protocole ICMP

Réglage : Bas	Réglage : Moyen	Réglage : Élevé
Bloque les types entrants : **Aucun type**. Bloque les types sortants : **Aucun type**. Suspecter un flooding si le délai entre les paquets est inférieur à **50** millisecondes. **Refuser** les paquets ICMP fragmentés.	Même règle que pour le réglage Bas.	Bloque les types entrants : **Différents types**. Bloque les types sortants : **Différents types**. Suspecter un flooding si le délai entre les paquets est inférieur à **50** millisecondes. **Refuser** les paquets ICMP fragmentés.

Types entrants bloqués : Aucun type/Différents types

Cliquez sur le lien pour ouvrir une liste avec les types de paquets ICMP. Dans cette liste, vous pouvez sélectionner les types de messages ICMP entrants que vous souhaitez bloquer.

Types sortants bloqués : Aucun type/Différents types

Cliquez sur le lien pour ouvrir une liste avec les types de paquets ICMP. Dans cette liste, vous pouvez sélectionner les types de messages ICMP sortants que vous souhaitez bloquer.

Flooding

Cliquez sur le lien pour ouvrir une fenêtre de dialogue dans laquelle vous pouvez saisir la valeur maximale autorisée pour le délai ICMP.

Paquets ICMP fragmentés

En cliquant sur le lien, vous avez la possibilité de choisir entre l'acceptation et le refus de paquets ICMP fragmentés.

Port-Scan TCP

Cette règle vous permet de définir quand le pare-feu doit suspecter un scannage de ports TCP et comment il doit se comporter dans ce cas. Cette règle sert à empêcher les attaques par scannage de ports TCP qui peuvent être constatées via les ports ouverts sur votre ordinateur. Les attaques de ce type sont surtout utilisées pour exploiter les faiblesses de votre ordinateur qui permettent d'opérer des attaques beaucoup plus dangereuses.

Règles prédéfinies pour le scannage de ports TCP

Réglage : Bas	Réglage : Moyen	Réglage : Élevé
Suspecter un scannage de ports TCP si **50** ports au moins ont été scannés en **5000** millisecondes. Lors de la détection d'un scannage de ports TCP, noter l'adresse IP de l'agresseur **dans le fichier rapport** et **ne pas ajouter** aux règles pour bloquer l'attaque.	Suspecter un scannage de ports TCP si **50** ports au moins ont été scannés en **5000** millisecondes. Si un scannage de ports TCP est constaté, noter l'adresse IP de l'agresseur **dans le fichier rapport** et **ajouter** aux règles pour bloquer l'attaque.	Même règle que pour le réglage Moyen.

Ports

Cliquez sur le lien pour ouvrir une fenêtre de dialogue dans laquelle vous pouvez saisir le nombre de ports qui doivent avoir été scannés pour qu'un scannage de ports TCP soit suspecté.

Intervalle scannage de ports

Cliquez sur le lien pour ouvrir une fenêtre de dialogue dans laquelle vous pouvez saisir l'intervalle pendant lequel un nombre défini de ports doit avoir été scanné pour que le système suspecte un scannage de ports TCP.

Fichier rapport

Cliquez sur ce lien pour avoir la possibilité de choisir si l'adresse IP de l'agresseur doit être inscrite ou non dans le fichier rapport.

Règle

Cliquez sur ce lien pour avoir la possibilité de choisir si la règle de blocage de l'attaque par scannage de ports TCP doit être ajoutée ou non.

Port-Scan UDP

Cette règle vous permet de définir quand le pare-feu doit suspecter un scannage des ports UDP et quel doit être son comportement dans ce cas. Cette règle sert à empêcher les attaques par scannage de ports UDP qui peuvent être constatées via les ports ouverts sur votre ordinateur. Les attaques de ce type sont surtout utilisées pour exploiter les faiblesses de votre ordinateur qui permettent d'opérer des attaques beaucoup plus dangereuses.

Règles prédéfinies pour le scannage de ports UDP

Réglage : Bas	Réglage : Moyen	Réglage : Élevé
Suspecter un scannage de ports UDP si **50** ports au moins ont été scannés en **5000** millisecondes. Si un scannage de ports UDP est détecté, noter l'adresse IP de l'agresseur **dans le fichier rapport** et **ne pas ajouter aux règles** pour bloquer l'attaque.	Suspecter un scannage de ports UDP si **50** ports au moins ont été scannés en **5000** millisecondes. Si un scannage de ports TCP est constaté, noter l'adresse IP de l'agresseur **dans le fichier rapport** et **ajouter** aux règles pour bloquer l'attaque.	Même règle que pour le réglage Moyen.

Ports

Cliquez sur le lien pour ouvrir une fenêtre de dialogue dans laquelle vous pouvez saisir le nombre de ports qui ont dû être scannés pour qu'un scannage de ports UDP soit suspecté.

Intervalle scannage de ports

Cliquez sur le lien pour ouvrir une fenêtre de dialogue dans laquelle vous pouvez saisir l'intervalle pendant lequel un nombre défini de ports doit avoir été scanné pour que le système suspecte un scannage de ports UDP.

Fichier rapport

Cliquez sur ce lien pour avoir la possibilité de choisir si l'adresse IP de l'agresseur doit être inscrite ou non dans le fichier rapport.

Règle

Cliquez sur ce lien pour avoir la possibilité de choisir si la règle de blocage de l'attaque par scannage de ports UDP doit être ajoutée ou non.

13.4.1.1. Règles entrantes

Les règles entrantes servent au contrôle du trafic de données entrant par le pare-feu Avira.

Remarque
Comme lors du filtrage d'un paquet les règles correspondantes sont appliquées les unes après les autres, leur ordre est important. Ne modifiez l'ordre des règles que si vous êtes certain du résultat que vous souhaitez obtenir.

Règles prédéfinies pour la surveillance du trafic de données TCP

Réglage : Bas	Réglage : Moyen	Réglage : Élevé
Le trafic de données entrantes n'est pas bloqué par le pare-feu Avira.	– Autoriser la connexion TCP existante sur le port 135 **Autoriser** les paquets TCP, de l'adresse **0.0.0.0** avec le masque	– Surveiller le trafic de données TCP autorisé **Autoriser** les paquets TCP de l'adresse **0.0.0.0** avec le masque **0.0.0.0**, quand le

	0.0.0.0, lorsque le port local se trouve sur **{135}** et le port distant sur **{0-65535}**. Appliquer sur les **paquets de connexions existantes**. **Ne pas écrire dans le fichier rapport** si le paquet correspond à la règle. Etendu : refuser les paquets avec les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**. – Rejeter les paquets TCP sur le port 135 **Rejeter** les paquets TCP, de l'adresse **0.0.0.0** avec le masque **0.0.0.0**, quand le port local est sur **{135}** et le port distant sur **{0-65535}**. Appliquer sur **tous les paquets**. **Ne pas écrire dans le fichier rapport** si le paquet correspond à la règle. Etendu : refuser les paquets avec les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**. – Surveillance du trafic des données conforme au TCP	port local est sur **{0-65535}** et le port distant sur **{0-65535}**. Appliquer sur les **paquets de connexions existantes**. **Ne pas écrire dans le fichier rapport** si le paquet correspond à la règle. Etendu : refuser les paquets avec les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**.

	Autoriser les paquets TCP de l'adresse **0.0.0.0** avec le masque **0.0.0.0**, quand le port local est sur **{0-65535}** et le port distant sur **{0-65535}**. Appliquer au **début de l'établissement de la connexion et sur les paquets des connexions existantes.** **Ne pas écrire dans le fichier rapport** si le paquet correspond à la règle. Etendu : refuser les paquets avec les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**. – Refuser tous les paquets TCP **Rejeter** les paquets TCP, de l'adresse **0.0.0.0** avec le masque **0.0.0.0**, quand le port local est sur **{0-65535}** et le port distant sur **{0-65535}**. Appliquer sur **tous les paquets**. **Ne pas écrire dans le fichier rapport** si le paquet correspond à la règle. Etendu : refuser les paquets avec	

	les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**.	

Autoriser/Refuser les paquets TCP

En cliquant sur le lien, vous avez la possibilité d'autoriser ou de rejeter les paquets TCP spécialement définis.

Adresse IP

Cliquez sur ce lien pour ouvrir une fenêtre de dialogue dans laquelle vous pouvez saisir l'adresse IP souhaitée.

Masque IP

En cliquant sur ce lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez saisir le masque IP souhaité.

Ports locaux

En cliquant sur ce lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez saisir un ou plusieurs ports locaux et des zones entières de ports.

Ports distants

En cliquant sur ce lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez saisir un ou plusieurs ports distants et des zones entières de ports.

Méthode d'application

En cliquant sur le lien, vous avez la possibilité de choisir si la règle doit être appliquée aux paquets de connexions existantes, au début de l'établissement de la connexion et aux paquets de connexions existantes ou à toutes les connexions.

Fichier rapport

En cliquant sur le lien, vous avez la possibilité de choisir d'écrire ou non dans le fichier rapport si le paquet correspond à la règle.

L'option **Etendu** autorise un filtrage sur la base du contenu. Ainsi, vous pouvez refuser des paquets qui contiennent des données spécifiques avec un décalage défini. Si vous ne souhaitez pas utiliser cette option, ne sélectionnez aucun fichier ou sélectionnez un fichier vide.

Filtrage en fonction du contenu : données

En cliquant sur le lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez sélectionner le fichier contenant la mémoire tampon spéciale.

Filtrage en fonction du contenu : masque

En cliquant sur le lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez sélectionner le masque spécial.

Filtrage en fonction du contenu : décalage

En cliquant sur le lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez indiquer le décalage pour un filtrage du contenu. Le décalage est calculé à partir de la fin de l'en-tête de TCP.

Règles prédéfinies pour la surveillance du trafic de données UDP

Réglage : Bas	Réglage : Moyen	Réglage : Élevé

-	– Surveillance du trafic de données conforme UDP **Autoriser** les paquets UDP de l'adresse **0.0.0.0** avec le masque **0.0.0.0**, quand le port local se trouve sur **{0-65535}** et le port distant sur **{0-65535}**. Appliquer la règle sur les **ports ouverts**. **Ne pas écrire dans le fichier rapport** si le paquet correspond à la règle. Etendu : refuser les paquets avec les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**. – Refuser tous les paquets UDP **Rejeter** les paquets UDP, de l'adresse **0.0.0.0** avec le masque **0.0.0.0** quand le port local est sur **{0-65535}** et le port distant sur **{0-65535}**. Appliquer sur **tous les ports**. **Ne pas écrire dans le fichier rapport** si le paquet correspond à la règle. Etendu : refuser les paquets avec les octets suivants **<vide>** avec le	Surveiller le trafic de données UDP autorisé **Autoriser** les paquets UDP de l'adresse **0.0.0.0** avec le masque **0.0.0.0**, quand le port local est sur **{0-65535}** et le port distant sur **{53, 67, 68, 123}**. Appliquer la règle sur les **ports ouverts**. **Ne pas écrire dans le fichier rapport** si le paquet correspond à la règle. Etendu : refuser les paquets avec les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**.

	masque **<vide>** sur le décalage **0**.	

Autoriser/Rejeter les paquets UDP

En cliquant sur le lien, vous avez la possibilité d'autoriser ou de rejeter les paquets UDP spécialement définis.

Adresse IP

Cliquez sur ce lien pour ouvrir une fenêtre de dialogue dans laquelle vous pouvez saisir l'adresse IP souhaitée.

Masque IP

En cliquant sur ce lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez saisir le masque IP souhaité.

Ports locaux

En cliquant sur ce lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez saisir un ou plusieurs ports locaux et des zones entières de ports.

Ports distants

En cliquant sur ce lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez saisir un ou plusieurs ports distants et des zones entières de ports.

Méthode d'application

En cliquant sur ce lien, vous pouvez choisir si la règle doit s'appliquer à tous les ports ou uniquement à tous les ports ouverts.

Fichier rapport

En cliquant sur le lien, vous avez la possibilité de choisir d'écrire ou non dans le fichier rapport si le paquet correspond à la règle.

L'option **Etendu** autorise un filtrage sur la base du contenu. Ainsi, vous pouvez refuser des paquets qui contiennent des données spécifiques avec un décalage défini. Si vous ne souhaitez pas utiliser cette option, ne sélectionnez aucun fichier ou sélectionnez un fichier vide.

Filtrage en fonction du contenu : données

En cliquant sur le lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez sélectionner le fichier contenant la mémoire tampon spéciale.

Filtrage en fonction du contenu : masque

En cliquant sur le lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez sélectionner le masque spécial.

Filtrage en fonction du contenu : décalage

En cliquant sur le lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez indiquer le décalage pour un filtrage du contenu. Le décalage est calculé à partir de la fin de l'en-tête d'UDP.

Règles prédéfinies pour la surveillance du trafic de données ICMP

Réglage : Bas	Réglage : Moyen	Réglage : Élevé
-	– Ne pas rejeter de paquets ICMP sur la base de l'adresse IP	Même règle que pour le réglage Moyen.

	Paquets ICMP **autoriser** de l'adresse **0.0.0.0** avec le masque **0.0.0.0**. **Ne pas écrire dans le fichier rapport** si le paquet correspond à la règle. Etendu : refuser les paquets avec les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**.	

Autoriser/Refuser les paquets ICMP

En cliquant sur le lien, vous avez la possibilité d'autoriser ou de rejeter les paquets ICMP spécialement définis.

Adresse IP

Cliquez sur ce lien pour ouvrir une fenêtre de dialogue dans laquelle vous pouvez saisir l'adresse IP souhaitée.

Masque IP

En cliquant sur ce lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez saisir le masque IP souhaité.

Fichier rapport

En cliquant sur le lien, vous avez la possibilité de choisir d'écrire ou non dans le fichier rapport si le paquet correspond à la règle.

L'option **Etendu** autorise un filtrage sur la base du contenu. Ainsi, vous pouvez refuser des paquets qui contiennent des données spécifiques avec un décalage défini. Si vous ne souhaitez pas utiliser cette option, ne sélectionnez aucun fichier ou sélectionnez un fichier vide.

Filtrage en fonction du contenu : données

En cliquant sur le lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez sélectionner le fichier contenant la mémoire tampon spéciale.

Filtrage en fonction du contenu : masque

En cliquant sur le lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez sélectionner le masque spécial.

Filtrage en fonction du contenu : décalage

En cliquant sur le lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez indiquer le décalage pour un filtrage du contenu. Le décalage est calculé à partir de la fin de l'en-tête d'ICMP.

Règle prédéfinie pour les paquets IP

Réglage : Bas	Réglage : Moyen	Réglage : Élevé
-	-	Refuser tous les paquets IP Paquets IP **rejeter** de l'adresse **0.0.0.0** avec le masque **0.0.0.0**. **Ne pas écrire dans le fichier rapport** si le paquet correspond à la règle.

Autoriser/refuser les paquets IP

En cliquant sur le lien, vous avez la possibilité d'autoriser ou de rejeter les paquets IP spécialement définis.

Adresse IP

Cliquez sur ce lien pour ouvrir une fenêtre de dialogue dans laquelle vous pouvez saisir l'adresse IP souhaitée.

Masque IP

En cliquant sur ce lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez saisir le masque IP souhaité.

Fichier rapport

En cliquant sur le lien, vous avez la possibilité de choisir d'écrire ou non dans le fichier rapport si le paquet correspond à la règle.

Règle possible pour la surveillance des paquets IP sur la base de protocoles IP

Paquets IP

En cliquant sur le lien, vous avez la possibilité d'autoriser ou de rejeter les paquets IP spécialement définis.

Adresse IP

Cliquez sur ce lien pour ouvrir une fenêtre de dialogue dans laquelle vous pouvez saisir l'adresse IP souhaitée.

Masque IP

En cliquant sur ce lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez saisir le masque IP souhaité.

Protocole

En cliquant sur ce lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez sélectionner le protocole IP souhaité.

Fichier rapport

En cliquant sur le lien, vous avez la possibilité de choisir d'écrire ou non dans le fichier rapport si le paquet correspond à la règle.

13.4.1.2. Règles sortantes

Les règles sortantes servent au contrôle du trafic de données sortant par le pare-feu Avira. Vous pouvez définir une règle sortante pour les protocoles suivants : IP, ICMP, UDP et TCP.

Remarque
Comme lors du filtrage d'un paquet les règles correspondantes sont appliquées les unes après les autres, leur ordre est important. Ne modifiez l'ordre des règles que si vous êtes certain du résultat que vous souhaitez obtenir.

Boutons

Bouton	Description
Ajouter	Vous permet de créer une nouvelle règle. Quand vous cliquez sur ce bouton, la fenêtre de dialogue "Ajouter une nouvelle règle" apparaît. Vous pouvez sélectionner de nouvelles règles dans cette fenêtre de dialogue.
Supprimer	Suppression d'une règle sélectionnée.
Vers le bas	Déplacement d'une règle sélectionnée d'une position vers le bas, ce qui réduit la priorité de cette règle.
Vers le haut	Déplacement d'une règle sélectionnée d'une position vers le haut, ce qui accroît la priorité de cette règle.
Renommer	Renommage d'une règle sélectionnée.

Remarque
Vous pouvez ajouter de nouvelles règles pour divers adaptateurs ou pour tous les adaptateurs présents sur l'ordinateur. Pour ajouter une règle d'adaptateur à tous les adaptateurs, sélectionnez **Poste de travail** dans la structure affichée des adaptateurs et cliquez sur le bouton **Ajouter**.

Remarque
Pour modifier la position d'une règle, vous pouvez également déplacer la règle à la position souhaitée, à l'aide de la souris.

13.4.2 Règles d'application

Règles liées à l'application pour l'utilisateur

Cette liste contient tous les utilisateurs du système. Si vous êtes connecté en tant qu'administrateur, vous pouvez sélectionner l'utilisateur pour lequel vous souhaitez établir des règles. Si vous n'êtes pas un utilisateur avec des droits privilégiés, la liste ne vous indique que l'utilisateur actuellement connecté.

Liste des applications

Ce tableau vous montre la liste des applications pour lesquelles les règles sont définies. La liste indique les réglages pour chaque application exécutée depuis l'installation du pare-feu Avira et pour laquelle une règle a été enregistrée.

Vue standard

	Description
Application	Nom de l'application.
Mode	Indique le mode réglé pour la règle d'application : Dans le mode **filtré**, les règles d'adaptateur sont contrôlées et exécutées, une fois la règle d'application exécutée. Dans le mode *privilégié*, les règles d'adaptateur sont ignorées. Un clic de souris sur le lien vous permet de passer à un autre mode.
Action	Indique l'action que le pare-feu Avira exécute automatiquement au cas où l'application utilise le réseau quelle que soit cette utilisation. Un clic de souris sur le lien vous permet de passer à un autre type d'action. Les types d'actions **Demander**, **Autoriser** ou **Rejeter** sont disponibles au choix. Le réglage standard est **Demander**.

Configuration étendue

Si vous souhaitez régler individuellement les accès réseau d'une application, vous pouvez créer des règles d'application spécifiques basées sur les filtres de paquets, semblables aux règles d'adaptateurs. Pour passer à la configuration étendue des règles d'application, activez tout d'abord le mode expert. Modifiez maintenant le réglage des règles d'application dans la rubrique Pare-feu :: Réglages : Activez l'option **Réglages étendus** et enregistrez le réglage avec **Valider** ou **OK**. Dans la configuration pare-feu, passez à la rubrique **Pare-feu :: Règles d'application**: La liste des règles d'application affiche une colonne supplémentaire *Filtrage* avec l'entrée *Simple*. Vous avez maintenant l'option supplémentaire **Filtrage :** *Avancées - action : Règles* permettant de passer à la configuration étendue.

	Description
Application	Nom de l'application.
Mode	Indique le mode réglé pour la règle d'application : Dans le mode **filtré**, les règles d'adaptateur sont contrôlées et exécutées, une fois la règle d'application exécutée. Dans le mode *privilégié*, les règles d'adaptateur sont ignorées. Un clic de souris sur le lien vous permet de passer à un autre mode.
Action	Indique l'action que le pare-feu Avira exécute automatiquement au cas où l'application utilise le réseau quelle que soit cette utilisation. Lors du réglage *Filtrage - simple* un clic de souris sur le lien vous permet de passer à un autre type d'action. Les types d'actions **Demander**, **Autoriser,** **Rejeter** ou *Étendu* sont disponibles au choix. En cas de réglage *Filtrage - avancé* le type d'action *Règles* est affiché. Le lien **Règles** ouvre la fenêtre **Règles d'application**, dans laquelle il est possible de mémoriser des règles spécifiques pour l'application.
Filtrage	Affiche le type de filtrage. Un clic de souris sur le lien vous permet de passer à un autre filtrage. *Simple*: En cas de filtrage simple, l'action indiquée est exécutée pour toutes les activités réseau de l'application logiciel. *Avancées*: Lors du filtrage, le système exécute les règles mémorisées dans la configuration étendue.

Si vous souhaitez créer des règles d'application spécifiques pour une application, sous *Filtrage* passez à l'entrée **Avancé**. Dans la colonne **Action** l'entrée *Règles* est maintenant affichée. Cliquez sur **Règles**, pour accéder à la fenêtre de création de règles d'application spécifiques.

Règles d'application spécifiques de la configuration étendue

Les règles d'application spécifiques vous permettent d'autoriser ou de rejeter un trafic de données spécifique de l'application, ainsi que d'autoriser ou de refuser l'écoute passive de ports individuels. Vous disposez des options suivantes :

- Autoriser ou refuser l'injection de code

  L'injection de code est une technique par laquelle on fait exécuter un code dans l'espace d'adressage d'un autre processus, en forçant ce processus à charger une Dynamic Link Library (DLL). La technique d'injection de code est utilisée entre autres par les logiciels malveillants pour exécuter un code sous le couvert d'un autre programme. Il se peut ainsi que le pare-feu ne détecte pas des accès à l'Internet, par exemple. L'injection de code est autorisée par défaut pour toutes les applications signées.

- Autoriser ou refuser l'écoute passive de l'application par des ports
- Autoriser ou refuser le trafic de données :

  Autoriser ou rejeter des paquets IP entrants et / ou sortants

  Autoriser ou rejeter des paquets TCP entrants et / ou sortants

  Autoriser ou rejeter des paquets UDP entrants et / ou sortants

Vous pouvez créer des règles d'application à volonté, pour chaque application. Les règles d'application sont exécutées dans l'ordre indiqué .

Remarque
Si vous modifiez le filtrage *Avancé* pour une règle d'application, les règles déjà créées dans la configuration étendue ne sont pas définitivement effacées, mais seulement désactivées. Si vous repassez au filtrage *Étendu*, les règles d'application déjà créées sont réactivées et s'affichent dans la fenêtre de la configuration étendue concernant les règles d'application.

Détails de l'application

Cette rubrique affiche les informations détaillées concernant l'application que vous avez sélectionnée dans la liste des applications.

	Description
Nom	Nom de l'application.
Chemin	Chemin complet vers le fichier exécutable.

Boutons

Bouton	Description
Ajouter une application	Vous permet la création d'une nouvelle règle d'application. Si vous cliquez sur ce bouton, une fenêtre de dialogue apparaît. Vous pouvez maintenant sélectionner une application pour laquelle vous souhaitez

	créer une règle.
Supprimer une règle	Suppression de la règle d'application sélectionnée.
Charger à nouveau	Nouveau chargement de la liste des applications avec rejet simultané de toutes les modifications qui viennent d'être effectuées sur les règles d'application.

13.4.3 Fournisseurs dignes de confiance

Une liste des éditeurs de logiciels dignes de confiance s'affiche sous *Fournisseurs dignes de confiance*. Vous pouvez supprimer ou ajouter des éditeurs à la liste en utilisant pour cela l'option *Toujours faire confiance à ce fournisseur* dans la fenêtre popup *Événement réseau*. Vous pouvez autoriser par défaut l'accès réseau des applications signées par les fournisseurs figurant dans la liste, en activant l'option **Autoriser automatiquement les applications créées par des fournisseurs dignes de confiance**.

Fournisseurs dignes de confiance pour l'utilisateur

Cette liste contient tous les utilisateurs du système. Si vous êtes connecté en tant qu'administrateur, vous pouvez sélectionner l'utilisateur dont vous souhaitez visualiser ou mettre à jour la liste de fournisseurs dignes de confiance. Si vous n'êtes pas un utilisateur avec des droits privilégiés, la liste ne vous indique que l'utilisateur actuellement connecté.

Autoriser automatiquement les applications créées par des fournisseurs dignes de confiance

Si l'option est activée, les applications dont la signature provient de fournisseurs connus et fiables sont automatiquement autorisées à accéder au réseau. L'option est activée par défaut.

Fournisseurs

La liste indique tous les fournisseurs considérés comme dignes de confiance.

Boutons

Bouton	Description
Supprimer	L'entrée sélectionnée est supprimée de la liste des fournisseurs dignes de confiance. Pour supprimer le fournisseur sélectionné définitivement de la liste, appuyez sur **Valider** ou **OK** dans la fenêtre de la configuration.
Charger à nouveau	Les modifications effectuées sont annulées : la dernière liste enregistrée est chargée.

Remarque
Si vous supprimez des fournisseurs de la liste, puis appuyez sur le bouton **Appliquer**, les fournisseurs sont définitivement effacés de la liste. La modification peut être annulée avec l'option *Charger de nouveau*. Vous avez toutefois la possibilité d'ajouter un éditeur de nouveau à la liste des fournisseurs dignes de confiance via l'option *Toujours faire confiance à ce fournisseur* dans la fenêtre popup *Événement réseau*.

Remarque
Le pare-feu donne la priorité aux règles d'application par rapport aux entrées de la liste des fournisseurs dignes de confiance : Si vous avez créé une règle d'application et que le fournisseur de l'application figure dans la liste des fournisseurs dignes de confiance, la règle d'application est exécutée.

13.4.4 Réglages

Réglages étendus

Activer le pare-feu

En cas d'option activée, le pare-feu Avira est actif et protège votre ordinateur de dangers provenant d'Internet et d'autres réseaux.

Désactiver le pare-feu Windows au démarrage

Si cette option est activée, le pare-feu Windows est désactivé au démarrage de l'ordinateur. Cette option est activée par défaut.

Fichier hôte Windows NON BLOQUE/BLOQUE

Si cette option est sur BLOQUE, le fichier hôte Windows est protégé en écriture. Il n'est plus possible de manipuler le fichier. Les logiciels malveillants ne sont plus capables par exemple de vous rediriger sur des pages Internet non souhaitées. Cette option est réglée sur NON BLOQUE par défaut.

Dépassement de délai de la règle

Toujours bloquer

Si l'option est activée, une règle générée automatiquement par exemple lors d'un scannage des ports, est conservée.

Supprimer la règle après n secondes

Si l'option est activée, une règle générée automatiquement lors du scannage des ports par exemple est supprimée après le délai que vous indiquez. Cette option est activée par défaut.

Notifications

L'option Notifications vous permet de définir les événements pour lesquels vous souhaitez recevoir un message du pare-feu affiché sur le bureau.

Scannage de ports

Si l'option est activée, vous recevez un message affiché sur le bureau lorsque le pare-feu a détecté un scannage de ports.

Flooding

Si l'option est activée, vous recevez un message affiché sur le bureau lorsque le pare-feu a détecté une attaque par flooding.

Des applications ont été bloquées.

Si l'option est activée, vous recevez un message affiché sur le bureau lorsque le pare-feu a rejeté, c'est-à-dire bloqué, une activité réseau d'une application.

IP bloquée

Si l'option est activée, vous recevez un message affiché sur le bureau lorsque le pare-feu a refusé le trafic de données d'une adresse IP.

Règles d'application

Les options de la zone Règles d'application vous permettent de régler les possibilités de configuration des règles d'application sous la rubrique Pare-feu :: Règles d'application.

Réglages étendus

Si l'option est activée, vous avez la possibilité de régler individuellement les différents accès réseau d'une application.

Réglages de base

Si l'option est activée, vous ne pouvez régler qu'une seule action pour les différents accès réseau de l'application.

Mode préféré

Les utilisateurs qui ne sont pas des administrateurs peuvent modifier les droits pour les applications.

Si l'option est activée, tous les utilisateurs peuvent modifier les règles d'application ou créer de nouvelles règles d'application. Si l'option est désactivée, seuls les utilisateurs disposant de droits d'administrateur peuvent modifier les règles d'application ou créer de nouvelles règles d'application. Les règles d'application sont affichées dans la configuration sous Pare-feu :: Règles d'application, et peuvent y être modifiées ou ajoutées. Dans le Control Center sous Protection en ligne :: Pare-feu, ainsi que dans la fenêtre événements réseau, il est possible de modifier les règles d'application.

13.4.5 Paramètres popup

Paramètres popup

Inspecter la pile de lancement du processus

Si l'option est activée, une vérification plus précise de la pile de processus a lieu. Le pare-feu part du principe que chaque processus suspect dans la pile est celui par lequel le processus enfant permet au système d'accéder au réseau. C'est pourquoi dans ce cas, une fenêtre popup s'ouvre pour chacun des processus suspects de la pile. Cette option est désactivée par défaut.

Afficher plusieurs fenêtres de dialogue par processus

Si l'option est activée, une fenêtre popup s'ouvre à chaque fois qu'une application essaie d'établir une connexion au réseau. Alternativement, l'information est donnée uniquement à la première tentative de connexion. Cette option est désactivée par défaut.

Bloquer automatiquement la notification par popup en mode jeu

Si cette option est activée, le pare-feu Avira passe automatiquement en mode jeu, lorsqu'une application est exécutée en mode plein écran sur votre ordinateur. Toutes les règles d'adaptateur et d'application définies sont appliquées en mode jeu. L'accès réseau autorisera temporairement les applications pour lesquelles aucune règle n'est définie avec les actions *Autoriser* ou *Rejeter*, de sorte qu'aucune fenêtre popup ne s'ouvre avec des demandes concernant l'événement réseau.

Mémoriser l'action pour cette application

Toujours activé

Si l'option est activée, l'option "Enregistrer l'action pour cette application" de la fenêtre de dialogue "Événement réseau" est activée par défaut. Cette option est activée par défaut.

Toujours désactivé

Si l'option est activée, l'option "Enregistrer l'action pour cette application" de la fenêtre de dialogue "Événement réseau" est désactivée par défaut.

Autoriser les applications signées

Si l'option est activée, l'option "Enregistrer l'action pour cette application" de la fenêtre de dialogue "Événement réseau" est activée automatiquement lors de l'accès au réseau d'applications signées de certains fabricants. Les fabricants sont : Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

Mémoriser la dernière version utilisée

Si l'option est activée, l'activation de l'option "Enregistrer l'action pour cette application" de la fenêtre de dialogue "Événement réseau" est la même que lors du dernier événement réseau. Si l'option "Enregistrer l'action pour cette application" a été activée lors du dernier événement réseau, l'option est active pour l'événement réseau suivant. Si l'option "Enregistrer l'action pour cette application" a été désactivée lors du dernier événement réseau, l'option est désactivée pour l'événement réseau suivant.

Afficher les détails

Dans ce groupe d'options de configuration, vous pouvez régler l'affichage des informations détaillées dans la fenêtre **Événement réseau**.

Afficher les détails sur demande

Si l'option est activée, les informations détaillées ne sont affichées dans la fenêtre *Événement réseau* que sur demande, c'est-à-dire que l'affichage des informations détaillées se fait en cliquant sur le bouton **Afficher les détails** dans la fenêtre *Événement réseau*.

Toujours afficher les détails

Si l'option est activée, les informations détaillées sont toujours affichées dans la fenêtre *Événement réseau*.

Mémoriser la dernière version utilisée

Si l'option est activée, l'affichage des informations détaillées est activé de la même manière que lors du précédent événement réseau. Si les informations détaillées ont été affichées lors du dernier événement réseau, elles le seront aussi lors de l'événement réseau suivant. Si les informations détaillées n'ont pas été affichées ou ont été masquées lors du dernier événement réseau, elles ne seront pas affichées lors de l'événement réseau suivant.

Autoriser de manière privilégiée

Dans ce groupe d'options de configuration, vous pouvez régler le statut de l'option *Autoriser de manière privilégiée* dans la fenêtre **Événement réseau**.

Toujours activé

Si l'option est activée, l'option *Autoriser de manière privilégiée* est activée par défaut dans la fenêtre *Événement réseau*.

Toujours désactivé

Si l'option est activée, l'option *Autoriser de manière privilégiée* est désactivée par défaut dans la fenêtre *Événement réseau*.

Mémoriser la dernière version utilisée

Si l'option est activée, le statut de l'option *Autoriser de manière privilégiée* dans la fenêtre *Événement réseau* est le même que lors du précédent événement réseau : Si l'option *Autoriser de manière privilégiée* était activée lors de l'exécution du dernier événement réseau, l'option est activée par défaut pour l'événement réseau suivant. Si l'option *Autoriser de manière privilégiée* était désactivée lors de l'exécution du dernier événement réseau, l'option est désactivée par défaut pour l'événement réseau suivant.

13.5 WebGuard

La rubrique WebGuard de la configuration est en charge de la configuration du WebGuard.

13.5.1 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 via le protocole HTTP aux ports 80, 8080, 3128. Pour les sites Web concernés, le chargement du site Web est bloqué. Si l'option est désactivée, le service WebGuard reste actif, mais la recherche de virus et de logiciels malveillants est désactivée.

Remarque
La fonction de contrôle parental ne dépend pas de l'activation ou de la désactivation du WebGuard.

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.

13.5.1.1. 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.

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.

Action primaire

L'action primaire 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, WebGuard écrit 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 concerné 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 WebGuard. L'accès au fichier est autorisé et le fichier est conservé.

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

13.5.1.2. 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 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 (personnalisés) à bloquer par 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.

13.5.1.3. 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 URL indiqués sont ignorés par WebGuard, ce qui signifie que ces données ne sont pas contrôlées à la recherche 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 (personnalisés)

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.com 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

13.5.1.4. Heuristique

Cette rubrique de configuration contient les réglages pour l'heuristique du moteur de recherche Avira Premium Security Suite.

Avira Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite 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 Premium Security Suite détecte beaucoup plus de logiciels malveillants inconnus, mais vous devez vous attendre aussi à des messages erronés.

13.5.2 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 de rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce réglage est activé par défaut.

Étendu

Si l'option est activée, le WebGuard consigne également les informations secondaires dans le fichier de 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. En cas de limitation du fichier de rapport, 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.

Premium Security Suite possède une fonction de contrôle parental permettant de filtrer les offres Internet indésirables ou illégales et de limiter la durée d'utilisation sur Internet. La fonction de contrôle parental fait partie des composants WebGuard. Des rôles d'usager peuvent être attribués aux utilisateurs de l'ordinateur. Une rôle d'usager peut être configuré et comprend un ensemble de règles avec les critères suivants :

- URL interdits ou autorisés (adresses Internet)
- Catégories de contenus interdites
- Durée d'utilisation d'Internet et horaires d'utilisation autorisées pour les jours de la semaine.

Des listes de filtres URL performantes sont employées pour le blocage des contenus Internet selon certaines catégories, dans lesquelles les URL sont classifiées dans des groupes en fonction des contenus des sites Internet. Les listes de filtres URL sont actualisées, adaptées et étendues plusieurs fois par heure. Les rôles enfant, adolescent, adulte sont préconfigurés avec les catégories interdites correspondantes.

Le système saisit la durée d'utilisation d'Internet après des demandes sur Internet qui ont lieu à un intervalle minimum de 5 minutes.

Si le contrôle parental est actif, tous les sites Web appelés dans le navigateur sont contrôlés pendant la navigation Internet, en fonction du rôle d'usager. Le site Web est bloqué s'il s'agit d'un site interdit et un message s'affiche dans le navigateur. En cas de dépassement de la durée d'utilisation autorisée, ou en cas d'utilisation en dehors des horaires autorisés, les sites Internet demandés sont bloqués. Un message s'affiche dans le navigateur.

Avertissement
Veuillez noter que vous devez activer le service WebGuard pour pouvoir utiliser la fonction de contrôle parental.

Avertissement
Protégez la configuration du programme Premium Security Suite par mot de passe, lorsque vous activez le contrôle parental. Si la configuration n'est pas protégée par mot de passe, tous les utilisateurs de l'ordinateur peuvent modifier ou désactiver les réglages du contrôle parental. Vous activez la protection par mot de passe sous Généralités::Mot de passe.

Si vous avez attribué un mot de passe pour le contrôle parental, la configuration contrôle parental est masquée et le bouton *Protégé par mot de passe* s'affiche.

Protégé par mot de passe

Appuyez sur le bouton **Protégé par mot de passe** et donnez un mot de passe pour le contrôle parental dans la fenêtre *Saisir mot de passe* pour activer la configuration contrôle parental.

Activer le contrôle parental

Si l'option est activée, tous les sites Web appelés lors de la navigation sur Internet sont contrôlés en fonction du rôle attribué dans le contrôle parental à l'utilisateur connecté. Les sites web sont bloqués s'ils ont été classés comme interdits pour le rôle attribué.

Remarque
Les utilisateurs de l'ordinateur auxquels n'a été attribué aucun rôle dans la configuration du contrôle parental se voient attribuer par défaut par le programme la qualité d'utilisateur *standard* avec le rôle *enfant*, lorsque le contrôle parental est activé. Vous pouvez modifier le rôle de l'utilisateur standard.
Après l'installation, les rôles d'utilisateur enfant, jeunes et adultes sont crées. Pour les rôles pré-configurés, la limitation dans le temps de l'utilisation Internet est désactivée.

Sélection de l'utilisateur

Liste utilisateurs - rôle

Cette liste affiche tous les utilisateurs ajoutés avec le rôle qui leur a été attribué. Le programme attribue par défaut le rôle *enfant* lors de l'ajout d'un utilisateur. Un clic de souris sur le rôle affiché vous permet de passer à un autre rôle.

Utilisateur

La liste contient tous les utilisateurs du système.

Ajouter

Ce bouton vous permet d'ajouter l'utilisateur sélectionné à la liste des utilisateurs protégés.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste.

Remarque
L'utilisateur standard ne peut pas être effacé.

Rôles

Liste

La liste affiche tous les rôles gérés. Un double-clic de souris sur le rôle affiché vous permet d'ouvrir le dialogue pour la définition du rôle.

Champ de saisie

Dans ce champ, saisissez le nom du rôle que vous souhaitez ajouter aux rôles d'usager.

Modifier

Le bouton *Modifier* vous permet de configurer le rôle sélectionné. Une fenêtre de dialogue apparaît à l'écran, dans laquelle vous pouvez définir des URL interdites et autorisées pour le rôle et sélectionner des contenus Internet interdits selon des catégories.

Ajouter

Ce bouton vous permet d'ajouter à la liste des rôles disponibles, le rôle entré dans le champ de saisie.

Supprimer

Le bouton supprime le rôle sélectionné de la liste.

Remarque
Les rôles déjà attribués à un utilisateur ne peuvent pas être effacés.

Propriétés du rôle

Le bouton *Modifier* vous permet d'accéder au dialogue *Propriétés du rôle*, dans laquelle vous pouvez définir des URL interdites et autorisées pour le rôle d'usager ainsi que des contenus Internet interdits. Vous disposez des options suivantes :

- Interdire l'accès aux URL
- Autoriser l'accès aux URL
- Bloquer les contenus Internet : vous pouvez sélectionner des catégories de contenus Internet qui doivent être bloqués.
- Limiter l'utilisation d'Internet dans le temps : Vous pouvez régler une durée d'utilisation autorisée (par jour, par semaine, par mois). Des périodes d'utilisation précises peuvent être autorisées pour chaque jour.

13.6 Sauvegarde

La rubrique Sauvegarde de la configuration permet de configurer la sauvegarde des composants Avira.

13.6.1 Réglages

Vous pouvez configurer le comportement de la sauvegarde composant sous la rubrique **Réglages**.

Réglages

Sauvegarder uniquement les fichiers modifiés

Si l'option est activée, une sauvegarde incrémentielle est créée : seuls sont sauvegardés les fichiers du profil de sauvegarde qui ont été modifiés depuis la dernière sauvegarde de données. Si l'option est désactivée, une sauvegarde complète est effectuée à chaque sauvegarde d'un profil de sauvegarde : tous les fichiers correspondant au profil de sauvegarde sont sauvegardés. Cette option est activée par défaut et est recommandée, car les sauvegardes incrémentielles sont créées plus rapidement et en utilisant moins de ressources que les sauvegardes complètes.

Contrôler l'absence de logiciel malveillant avant la sauvegarde

Si l'option est activée, les fichiers à sauvegarder sont contrôlés lors de la sauvegarde quant à l'absence de virus et de logiciels malveillants. Les fichiers infectés ne sont pas sauvegardés. Cette option activée par défaut est recommandée.

13.6.2 Exceptions

Vous pouvez déterminer sous Exceptions quels objets et types de fichiers doivent être sauvegardés ou non lors d'une sauvegarde.

Objets de fichiers à exclure par le Backup

La liste affichée dans cette fenêtre contient des fichiers et chemins qui ne doivent pas être sauvegardés lors d'une sauvegarde.

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

Remarque
Les fichiers mémorisés dans cette liste sont mentionnés dans le fichier rapport.

Champ de saisie

Vous saisissez dans ce champ le nom de l'objet de fichier qui ne doit pas être sauvegardé. Le chemin allant vers le répertoire temporaire des paramètres locaux pour l'utilisateur connecté 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 saisissez un nom de fichier avec son chemin complet, c'est exactement ce fichier qui n'est pas sauvegardé. Si vous avez inscrit le nom d'un fichier sans son chemin, chaque fichier de ce nom (quel que soit son chemin ou le lecteur sur lequel il se situe) n'est pas sauvegardé.

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.

Réinitialiser la liste

Ce bouton restaure les valeurs prédéfinies par défaut.

Tenez compte des points suivants :

- Les caractères de remplacement * (nombre illimité) et ? (un seul) ne sont autorisés que dans les noms de fichiers.
- La liste est traitée de haut en bas.
- Lorsqu'un répertoire est exclu, tous ses sous-répertoires sont automatiquement ignorés.
- Certaines extensions de fichiers peuvent aussi être exclues (y compris avec des caractères de remplacement).
- 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.

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 !

Exemples :

```
application.exe
\Programmes\
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
```

Liste des extensions de fichiers

Prendre en compte toutes les extensions de fichiers

Si l'option est activée, tous les fichiers du profil de sauvegarde sont sauvegardés.

Activer les extensions de fichiers à exclure du Backup

Si l'option est activée, tous les fichiers du profil de sauvegarde sont sauvegardés, à l'exception des fichiers dont les extensions figurent dans la liste des extensions de fichiers à exclure.

Extensions de fichiers

Ce bouton permet de faire apparaître une fenêtre de dialogue dans laquelle s'affichent toutes les extensions de fichiers qui sont ignorées lors d'une sauvegarde si l'option "Extensions de fichiers à exclure" est activée. Pour les extensions, des entrées sont indiquées par défaut, mais il est possible d'ajouter et de supprimer des entrées.

Activer la liste des extensions de fichiers à inclure dans la sauvegarde

Si l'option est activée, seuls sont sauvegardés les fichiers dont les extensions figurent dans la liste des extensions de fichiers à inclure.

Extensions de fichiers

Ce bouton permet de faire apparaître une fenêtre de dialogue dans laquelle s'affichent toutes les extensions de fichiers qui sont sauvegardées lors d'une sauvegarde si l'option "Extensions de fichiers à inclure" est activée. Pour les extensions, des entrées sont indiquées par défaut, mais il est possible d'ajouter et de supprimer des entrées.

13.6.3 Rapport

Le composant sauvegarde dispose d'une fonction étendue de documentation.

Documentation

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

Désactivé

Si l'option est activée, le composant sauvegarde ne génère pas de rapport. Ne renoncez à la documentation que dans des cas exceptionnels.

Standard

Si cette option est activée, le composant sauvegarde consigne les informations importantes (sur la sauvegarde, sur les virus détectés, 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 l'option est activée, le composant sauvegarde consigne également les informations secondaires dans le fichier de rapport.

Intégrale

Si l'option est activée, la sauvegarde composant consigne toutes les informations concernant le déroulement de la sauvegarde et la recherche de virus dans le fichier de rapport.

13.7 Mise à jour

La rubrique *Mise à jour* vous permet de configurer l'exécution automatique de mises à jour. Vous avez la possibilité d'activer et de désactiver différents intervalles de mise à jour et la mise à jour automatique.

Mise à jour automatique

Activer

Si l'option est activée, des mises à jour automatiques sont exécutées aux intervalles de temps indiqués ainsi que pour les événements activés.

Mise à jour automatique tous les n jours / heures / minutes

Dans ce champ, vous pouvez indiquer l'intervalle auquel les mises à jour automatiques doivent être exécutées. Pour modifier l'intervalle de mise à jour, marquez l'une des indications de temps dans le champ et modifiez-la via les touches fléchées à droite du champ de saisie.

Démarrer la tâche en plus par connexion Internet (télétransmission de données)

Si l'option est activée, en plus de l'intervalle de mise à jour défini, la tâche de mise à jour est exécutée à chaque démarrage d'une connexion Internet.

Rattraper la tâche quand la date est déjà passée

Si l'option est activée, le programme effectue les tâches de mise à jour situées dans le passé qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.

13.7.1 Mise à jour produit

Sous **Mise à jour produit**, vous configurez l'exécution de mises à jour produit ou la notification des mises à jour produit disponibles.

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 le composant de mise à jour 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.

Télécharger les mises à jour produit. Si un redémarrage est nécessaire, installer la mise à jour après le prochain redémarrage du système, sinon l'installer aussitôt.

Si cette option est activée, des mises à jour du produit sont téléchargées dès que des mise à jour de produit sont disponibles. La mise à jour est installée automatiquement après le téléchargement des fichiers de mise à jour, au cas où aucun redémarrage n'est nécessaire. S'il s'agit d'une mise à jour de produit nécessitant un redémarrage de l'ordinateur, la mise à jour du produit n'est pas effectuée aussitôt après le téléchargement des fichiers de mise à jour, mais seulement après le redémarrage suivant du système commandé par l'utilisateur. Ceci présente l'avantage que le redémarrage n'est pas effectué au moment où un utilisateur travaille sur l'ordinateur. 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 :: Événements.

Informer de nouveau après n jour(s)

Indiquez dans ce champ après combien de jours une nouvelle notification doit s'afficher concernant les mises à jour produit disponibles, au cas où la mise à jour produit n'a pas été effectuée après la première notification.

Ne pas télécharger les mises à jour produit

Si cette option est activée, l'Updater n'effectue aucune mise à jour automatique du produit ni notification concernant les mises à jour du produit disponibles. 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).

13.7.2 Paramètres de redémarrage

Si une mise à jour de produit est exécutée par Premium Security Suite, il peut être nécessaire d'effectuer un redémarrage de votre système d'ordinateur. Si vous avez défini une exécution automatique de mises à jour de produit sous Généralités :: Mise à jour :: Actualisation de produit, vous pouvez choisir entre plusieurs options pour le message de redémarrage et pour l'interruption du redémarrage sous **Paramètres redémarrage**.

Remarque
Lors de vos réglages pour le redémarrage, veuillez noter que sous Généralités :: Mise à jour :: Actualisation de produit, vous pouvez choisir dans la configuration entre deux options pour l'exécution d'une mise à jour avec un redémarrage d'ordinateur nécessaire :

exécution automatique de la mise à jour de produit avec redémarrage d'ordinateur nécessaire en cas de mise à jour disponible : la mise à jour et le redémarrage sont exécutés pendant qu'un utilisateur travaille sur l'ordinateur. Si vous avez activé cette option, les routines de redémarrage avec possibilité d'interruption ou avec fonction de rappel peuvent être adaptées.

Exécution de la mise à jour de produit avec redémarrage d'ordinateur nécessaire après le prochain démarrage du système : La mise à jour et le redémarrage sont exécutés après le démarrage de l'ordinateur par un utilisateur et après sa connexion. Pour cette option, les routines de redémarrage automatiques sont conseillées.

Paramètres de redémarrage

Redémarrage de l'ordinateur après n secondes

Si l'option est activée, un redémarrage éventuellement nécessaire après l'exécution d'une mise à jour de produit est **automatiquement** exécuté aux intervalles de temps définis. Un message de compte à rebours s'affiche sans possibilité d'interrompre le redémarrage d'ordinateur.

Message de rappel pour le redémarrage toutes les n secondes

Si l'option est activée, un redémarrage éventuellement nécessaire après l'exécution d'une mise à jour de produit n'est **pas automatiquement** exécuté. Vous recevez des messages aux intervalles de temps indiqués sans possibilité d'interruption pour le redémarrage. Dans les messages, vous pouvez confirmer le redémarrage de l'ordinateur ou sélectionner l'option **Rappeler une autre fois**.

Demande si le redémarrage de l'ordinateur doit être effectué

Si l'option est activée, un redémarrage éventuellement nécessaire après l'exécution d'une mise à jour de produit n'est **pas automatiquement** exécuté. Vous recevez un message unique où vous pouvez confirmer le redémarrage ou interrompre la routine de redémarrage.

Redémarrage de l'ordinateur sans demande

Si l'option est activée, un redémarrage éventuellement nécessaire après l'exécution d'une mise à jour de produit est **automatiquement** exécuté. Vous ne recevez aucun message.

13.7.3 Serveur web

La mise à jour peut être effectuée directement via un serveur web sur Internet .

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.

L'Updater 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 Premium Security Suite.

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.

13.7.3.1. 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

13.8 Généralités

13.8.1 Catégories de dangers étendues

Sélection des catégories de dangers étendues

Avira Premium Security Suite 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.

13.8.2 Mot de passe

Vous pouvez protéger Avira Premium Security Suite 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.

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 Premium Security Suite 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 le démarrage du Control Center.
Activer/Désactiver Guard	Si l'option est activée, le mot de passe défini est nécessaire pour l'activation et la désactivation d'AntiVir Guard.
Activer/Désactiver MailGuard	Si l'option est activée, le mot de passe défini est nécessaire pour l'activation et la désactivation de MailGuard.
Activer/désactiver pare-feu	Si l'option est activée, le mot de passe défini est nécessaire pour l'activation et la désactivation du pare-feu.
Activer/Désactiver WebGuard	Si l'option est activée, le mot de passe défini est nécessaire pour l'activation et la désactivation de WebGuard.
Activer / désactiver le contrôle parental.	Si l'option est activée, le mot de passe défini est nécessaire pour l'activation et la désactivation du contrôle parental.
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.
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 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 Avira	Si l'option est activée, un mot de passe est nécessaire pour l'envoi d'un objet pour contrôle à Avira Malware Research Center.
Copie des objets concernés	Si l'option est activée, un mot de passe est nécessaire pour copier l’objet concerné.

Configuration	Si l'option est activée, la configuration de Avira Premium Security Suite 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 Premium Security Suite nécessitent un mot de passe.

13.8.3 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 Premium Security Suite. Si cet âge est dépassé, une icône rouge s'affiche dans Control Center sous Etat pour l'état de mise à jour.

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.

Protection du produit

Protéger les processus d'un arrêt non souhaité

Si l'option est activée, tous les processus du programme Premium Security Suite 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.

Protection de processus étendue

Si l'option est activée, tous les processus de Premium Security Suite sont protégés avec des méthodes étendues contre un arrêt non voulu. Cette protection de processus étendue nécessite beaucoup plus de ressources de l'ordinateur que la protection de processus simple. C'est pourquoi l'option est désactivée par défaut. Pour activer l'option, il est nécessaire de redémarrer l'ordinateur.

Important
La protection de processus n'est pas disponible sous Windows XP 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 Premium Security Suite, 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. Pour activer l'option, il est nécessaire de redémarrer l'ordinateur.

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 disponible sous Windows XP 64 bits !

13.8.4 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. Premium Security Suite 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 . WMI vous donne la possibilité d'interroger.

activer la prise en charge WMI

Si l'option est activée, vous avez la possibilité d'interroger les données d'exploitation du programme Premium Security Suite via WMI.

13.8.5 Répertoires

Chemin temporaire

Saisissez dans ce champ le chemin où Avira Premium Security Suite met ses fichiers temporaires en mémoire.

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.

13.8.6 Événements

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 limité à une taille définie ; les valeurs autorisées sont : 100 à 10 000 entrées. Si le nombre d'entrées saisies est dépassé, 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 à la surface programme sous événements.

13.8.7 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.

13.8.8 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 l'avertissement acoustique ainsi que de sélectionner un autre fichier Wave comme avertissement acoustique.

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 Wave 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 un 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 Premium Security Suite 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.

13.8.9 Avertissements

Premium Security Suite génère pour certains événements des notifications affichées sur le bureau appelées Slide-Ups, pour vous informer de dangers et de la réussite ou de l'échec de l'exécution de programmes, p. ex. l'exécution d'une mise à jour. Sous *Avertissements* vous pouvez activer ou désactiver la notification pour certains événements.

En cas de notifications affichées sur le bureau, vous avez la possibilité de désactiver directement la notification dans le Slide-Up. Vous pouvez annuler la désactivation de la notification sous *Avertissements*.

Avertissements

concernant les connexions Dial-Up utilisées

Si l’option est activée, une notification affichée sur le bureau vous avertit lorsqu'un programme de numérotation établit sur votre ordinateur une connexion par téléphone ou par réseau RNIS. Le programme de numérotation risque d’être un numéroteur inconnu et indésirable qui établit une connexion payante. (voir virus et autres catégories étendues de dangers : Numéroteurs).

concernant les fichiers actualisés avec succès

Si l'option est activée, vous recevez un message affiché sur le bureau lorsqu’une mise à jour a réussi et lorsque les fichiers ont été actualisés.

concernant un échec de la mise à jour

Si l'option est activée, vous recevez un message affiché sur le bureau lorsqu’une mise à jour a échoué. Le système n’a pas établi de connexion au serveur de téléchargement, ou les fichiers de mise à jour n'ont pas pu être installés.

sur le fait qu’aucune mise à jour n’est nécessaire

Si l'option est activée, vous recevez un message affiché sur le bureau lorsqu’une mise à jour a été lancée sans qu’il soit toutefois nécessaire d’installer des fichiers car votre programme est à jour.

connecté avec des droits d’administrateur

Si l'option est activée, après connexion à l’ordinateur, vous recevez un message d’avertissement au cas où votre compte utilisateur inclut des droits d’administrateur. Pour des raisons de sécurité, il est recommandé de travailler avec des droits d’utilisateur limités. Grâce à la limitation des droits d’utilisateur que vous utilisez pour travailler avec votre système d’ordinateur, vous évitez l’installation automatique de programmes indésirables et la modification par inadvertance des réglages système.

Avira Premium Security Suite

www.avira.com

Avira GmbH

Lindauer Str. 21
88069 Tettnang
L'Allemagne
Téléphone: +49 7542-500 0
Fax: +49 7542-525 10
Internet: www.avira.com

AVIRA®