Avira AntiVir Professional

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

Table des matières

1 Introduction

Avec votre programme AntiVir, vous protégez votre ordinateur des virus, vers, chevaux de Troie, logiciels publicitaires et espions et autres dangers. Ce manuel aborde de manière simplifiée les virus ou logiciels malveillants et autres programmes indésirables.

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

Vous trouverez de nombreuses options et possibilités d'information sur notre site Web :

http://www.avira.com/fr

Sur le site Web Avira, vous pouvez...

- accéder à des informations sur d'autres programmes de bureau AntiVir
- télécharger les derniers programmes de bureau AntiVir
- télécharger les derniers manuels au format PDF
- télécharger des outils gratuits de support et de réparation
- utiliser la base de connaissances complètes et les articles de FAQ lors de la résolution des problèmes
- accéder aux adresses de support en fonction des pays.

Votre équipe Avira

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 de votre programme AntiVir.

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 votre produit AntiVir :

- voir le chapitre : Prestations
- voir le chapitre : Configuration système minimale
- voir le chapitre : Attribution de licence

Les programmes AntiVir offrent des outils complets et flexibles 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 votre programme AntiVir grâce aux mises à jour automatiques. Configurez le programme en conséquence.

3.1 Prestations

Votre programme AntiVir dispose des 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)
- 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 ou Intranet
- Attribution de licence intuitive dans la gestion des licences
- Le planificateur intégré pour la planification des tâches uniques ou répétées comme les mises à jour et les contrôles
- Identification extrêmement efficace des virus et logiciels malveillants grâce à des technologies de recherche innovantes (moteur de recherche) comprenant des procédés de recherche heuristique
- Identification de tous les types d'archives courants, y compris des extensions d'archives imbriquées et des extensions intelligentes
- Grande performance grâce à la capacité de multithreading (scannage simultané de nombreux fichiers à vitesse élevée)
- Pare-feu Avira 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 système minimale

Configurations minimales du système::

- Processeur Pentium et plus, au moins 266 MHz
- Système d’exploitation
- Windows XP, SP2 (32 ou 64 bits) ou
- Windows Vista (32 ou 64 bits, SP1)
- 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 XP
- 1024 Mo minimum de mémoire vive sous Windows Vista, Windows 7
- Pour l'installation du programme : droits d'administrateur
- Pour toutes les installations : Windows Internet Explorer 6.0 ou ultérieur
- Connexion Internet, le cas échéant (voir Installation)

3.3 Attribution de licence et mise à niveau

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

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

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

3.3.1 Gestion de licence

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

Gestion des licences Avira AntiVir Professional

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

Remarque
La gestion des licences Avira AntiVir Professional copie la licence correspondante automatiquement dans le dossier de produit correspondant. Si une licence est déjà disponible, un message s'affiche demandant si le fichier de licence doit être remplacé. Dans ce cas, le fichier de licence existant est écrasé par le fichier de licence actuel.

4 Installation et désinstallation

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

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

4.1 Installation

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

Remarque
Vous avez la possibilité de créer un point de restauration pendant le processus d'installation. Un point de restauration sert à réinitialiser le système d'exploitation à un état précédant l'installation. Si vous souhaitez utiliser cette option, assurez-vous que le système d'exploitation autorise la création de points de restauration :
Windows XP : Propriétés système -> Restauration du système : Désactivez l'option **Désactiver la restauration du système**.
Windows Vista / Windows 7 : Propriétés système -> Protection du système : Dans la zone **Points de restauration automatiques** sélectionnez le disque sur lequel est installé le système et cliquez sur le bouton **Créer**. Dans la fenêtre **Protection du système**, activez l'option **Restaurer les paramètres système et les versions de fichiers antérieurs**.

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 :

  Avira AntiVir ProActiv

  Pare-feu Avira

- Les fichiers de programme sont installés dans un répertoire par défaut sous `C:\Programme`.
- Votre programme AntiVir 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 votre programme AntiVir 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)
- Si nécessaire, exécution d'une mise à jour une fois l'installation terminée
- Enregistrez le fichier de licence hbedv.key sur votre système informatique, si vous souhaitez activer votre programme AntiVir.

Remarque
Installation basée sur Internet :
Pour l'installation basée sur Internet du programme, il existe un programme d'installation qui charge les fichiers programme actuels des serveurs Web de la société Avira GmbH, avant l'exécution de l'installation. Cette procédure garantit que le programme AntiVir 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 votre programme AntiVir lors d'une installation à l'aide d'un pack d'installation. Il est recommandé, à l'issue de l'installation, d'effectuer une mise à jour afin d'actualiser le fichier de définitions des virus.

Exécuter l'installation

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

Les principaux boutons disposent des fonctions suivantes :

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

– **Précédent :** retourner à l'étape précédente.

Procédure d'installation de votre programme AntiVir :

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 votre programme AntiVir et validez votre sélection de langue avec **Suivant**.

↪ 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. Une fois le téléchargement terminé, la fenêtre *Téléchargement* se referme.

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

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

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

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

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

▶ Cliquez sur **Suivant**.

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

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

▶ Confirmez que vous acceptez l'accord de licence et cliquez sur **Suivant**.

↪ 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 **Suivant**.

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

▶ Activez l'option **Express** ou **Personnalisée.** Si vous souhaitez créer un point de restauration, activez l'option **Créer un point de restauration du système**. Validez vos indications avec **Suivant**.

Installation personnalisée

↪ La fenêtre de dialogue *Sélectionner le répertoire d'installation* s'affiche.

▶ Confirmez le répertoire cible indiqué avec **Suivant**.

- OU -

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

↪ La fenêtre de dialogue *Choisir les composants à installer* s'affiche :

▶ Activez ou désactivez les composants souhaités et confirmez avec **Suivant**.

↪ Si vous avez choisi les composants ProActiv pour l'installation, la fenêtre *AntiVir ProActiv Community* s'affiche. Vous avez la possibilité de valider une participation à l'AntiVir ProActiv Community : Si l'option est activée, Avira AntiVir ProActiv envoie à l'Avira Malware Research Center les données sur les programmes suspects indiqués par le

composant ProActiv. Les données sont utilisées uniquement pour un contrôle en ligne étendu et pour étendre et affiner la technologie de détection. Le lien **Autres informations** vous permet d'avoir des détails sur le contrôle en ligne étendu.

▶ Activez ou désactivez la participation à l'AntiVir ProActiv Community et confirmez avec **Suivant**.

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

▶ Cliquez sur **Suivant**.

Suite : Installation express et installation personnalisée

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

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

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

→ Dans la fenêtre de dialogue suivante, vous pouvez décider si le fichier Lisez-moi doit être ouvert, une fois l'installation terminée 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 votre programme AntiVir dans l'assistant de configuration.

▶ Dans la fenêtre de bienvenue de l'assistant de configuration, cliquez sur **Suivant**, pour commencer la configuration du programme.

→ 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 votre programme AntiVir 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 Avira 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*.

→ Dans la fenêtre de dialogue suivante *Sélectionner les paramètres email*, vous pouvez procéder à des réglages de serveur pour l'envoi d'emails. Votre programme AntiVir utilise l'envoi d'emails par SMTP lors de l'envoi de notifications par email.

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

→ La fenêtre de dialogue suivante *Contrôle du système* permet d'activer ou de désactiver l'exécution d'un bref contrôle du système. Le bref contrôle du système est exécuté une fois la configuration terminée et avant le redémarrage de l'ordinateur. Il 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 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 le programme est à jour.

- Effectuez le cas échéant une mise à jour 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 programme de l'installation actuelle du programme AntiVir (voir chapitre Installation et désinstallation::Modules d'installation)

Si vous souhaitez ajouter ou supprimer des composants de programme de l'installation actuelle, vous pouvez utiliser l'option **Programmes** pour **ajouter/désinstaller** des programmes dans le **panneau de configuration Windows**.

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

4.3 Modules d'installation

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

- **AntiVir Professional**
  Ce module contient tous les composants nécessaires à l'installation réussie de votre programme AntiVir.
- **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), le programme AntiVir 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. 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.
- **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 génèrent dans le menu contextuel de l'explorateur Windows (bouton droit de la souris) une entrée Contrôler les fichiers sélectionnés avec AntiVir. Avec cette entrée, vous pouvez scanner directement certains fichiers ou répertoires.

4.4 Désinstallation

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

Voici comment désinstaller votre programme AntiVir (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 votre programme AntiVir dans la liste et cliquez sur **Désinstaller**.

→ 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**.

→ Le programme AntiVir est désinstallé, votre ordinateur est redémarré si besoin est, ce faisant, tous les répertoires, tous les fichiers et toutes les entrées de registre du programme sont supprimés.

4.5 Installation et désinstallation dans le réseau

Pour simplifier l'installation des programmes AntiVir dans un réseau à plusieurs ordinateurs clients pour l'administrateur du système, votre programme AntiVir propose une procédure spéciale pour l'installation initiale et l'installation modifiée.

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

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

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

Avec un script de connexion du serveur ou par SMS, les programmes AntiVir peuvent être répartis de manière confortable dans le réseau.

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

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

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

4.5.1 Installation dans le réseau

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

Le set-up est adapté aux installations suivantes :

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

▶ Installation modifiée ou mise à jour

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

Voici comment installer les programmes AntiVir automatiquement dans le réseau :

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

▶ Configurez les paramètres du fichier *setup.inf* et mémorisez le fichier.

▶ Démarrez l'installation avec le paramètre /inf ou liez le paramètre au script de connexion du serveur.

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

➔ L'installation se fait automatiquement.

4.5.2 Désinstallation dans le réseau

Voici comment désinstaller les programmes AntiVir automatiquement dans le réseau :

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

▶ Démarrez la désinstallation avec le paramètre `/remsilent` ou `/remsilentaskreboot` ou intégrez le paramètre dans le script de connexion du serveur.

En outre, vous pouvez indiquer le paramètre pour la documentation de la désinstallation.

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

➔ La désinstallation se fait automatiquement.

Remarque
Ne lancez pas le programme Setup pour la désinstallation sur un lecteur réseau autorisé, mais au niveau local, sur l'ordinateur où doit être désinstallé le programme AntiVir.

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

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

Pour l'installation, le paramètre suivant est possible :

– `/inf`

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

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

Pour la désinstallation, les paramètres suivants sont possibles :

– `/remove`

Le programme d'installation désinstalle le programme AntiVir.

Exemple : `presetup.exe /remove`

– `/remsilent`

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

Exemple : `presetup.exe /remsilent`

– `/remsilentaskreboot`

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

Exemple : `presetup.exe /remsilentaskreboot`

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

– `/unsetuplog`

Toutes les actions sont enregistrées à la désinstallation.

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

4.5.4 Paramètres du fichier setup.inf

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

– `DestinationPath`

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

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

– `ProgramGroup`

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

`1`: créer un groupe de programmes

`0`: ne pas créer de groupe de programmes

Exemple : `ProgramGroup=1`

– `DesktopIcon`

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

`1`: créer une icône de bureau

`0`: ne pas créer d'icône de bureau

Exemple : `DesktopIcon=1`

– `ShellExtension`

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

`1`: enregistrer l’extension du shell

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

Exemple : `ShellExtension=1`

– `Guard`

Installe AntiVir Guard (On-Access-Scanner).

`1`: Installer AntiVir Guard

`0`: Ne pas installer AntiVir Guard

Exemple : `Guard=1`

– `MailScanner`

Installe AntiVir MailGuard.

`1`: Installer AntiVir MailGuard

`0`: Ne pas installer AntiVir MailGuard

Exemple : `MailScanner=1`

– `KeyFile`

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

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

– `ShowReadMe`

Affiche le fichier readme.txt après l'installation.

`1`: afficher le fichier

`0`: ne pas afficher le fichier

Exemple : `ShowReadMe=1`

– `RestartWindows`

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

`1`: redémarrer l'ordinateur

`0`: ne pas redémarrer l'ordinateur

Exemple : `RestartWindows=1`

– `ShowRestartMessage`

Affiche une information pendant le setup avant un redémarrage automatique

`0`: ne pas afficher l'information

`1`: afficher l'information

Exemple : `ShowRestartMessage=1`

– SetupMode

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

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

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

Exemple : SetupMode=Update

– AVWinIni (option)

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

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

– Mot de passe

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

Exemple : Mot de passe=Mot de passe123

– WebGuard

Installe AntiVir WebGuard.

1: Installer AntiVir WebGuard

0: Ne pas installer AntiVir WebGuard

Exemple : WebGuard=1

– RootKit

Installe le module de protection Rootkit AntiVir. Sans protection Rootkit AntiVir, le scanner ne peut pas rechercher de rootkits sur le système !

1: Installer la protection Rootkit AntiVir

0: Ne pas installer la protection Rootkit AntiVir

Exemple : RootKit=1

– HIPS

Installe les composants AntiVir ProActiv. AntiVir ProActiv est une technologie de détection basée sur le comportement permettant de détecter les logiciels malveillants encore inconnus.

`1`: Installer ProActiv

`0`: Ne pas installer ProActiv

Exemple : `HIPS=1`

– `Pare-feu`

Installe les composants Avira pare-feu. Le pare-feu Avira surveille et régule le trafic de données entrant et sortant sur votre système informatique et protège votre ordinateur de menaces provenant d'Internet ou d'autres environnements réseau.

`1`: Installer le pare-feu

`0`: Ne pas installer le pare-feu

Exemple : `Pare-feu=1`

5 Aperçu

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

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

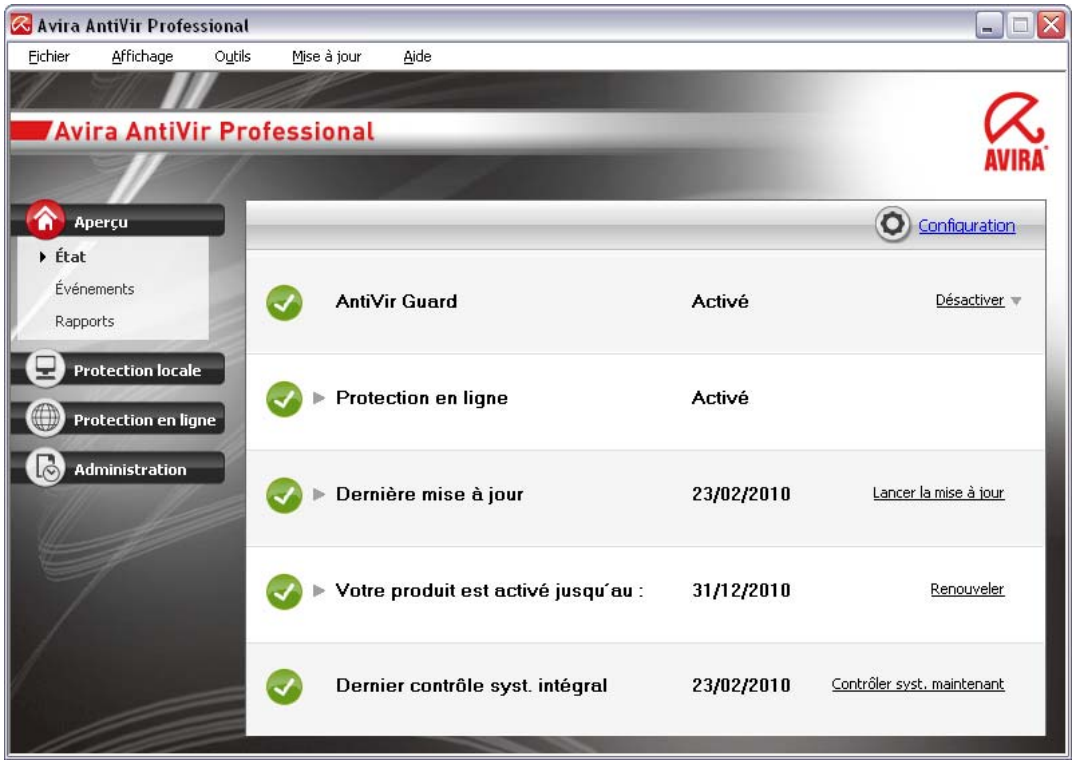
5.1 Interface et commande

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

- Control Center: la surveillance et la commande du programme AntiVir
- Configuration: Configuration de votre programme AntiVir
- 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 votre programme AntiVir.



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

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

- **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 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 dans le menu Démarrer | Programmes.
- Via l'icône de programme de votre programme AntiVir.

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 *Affichage*.

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.

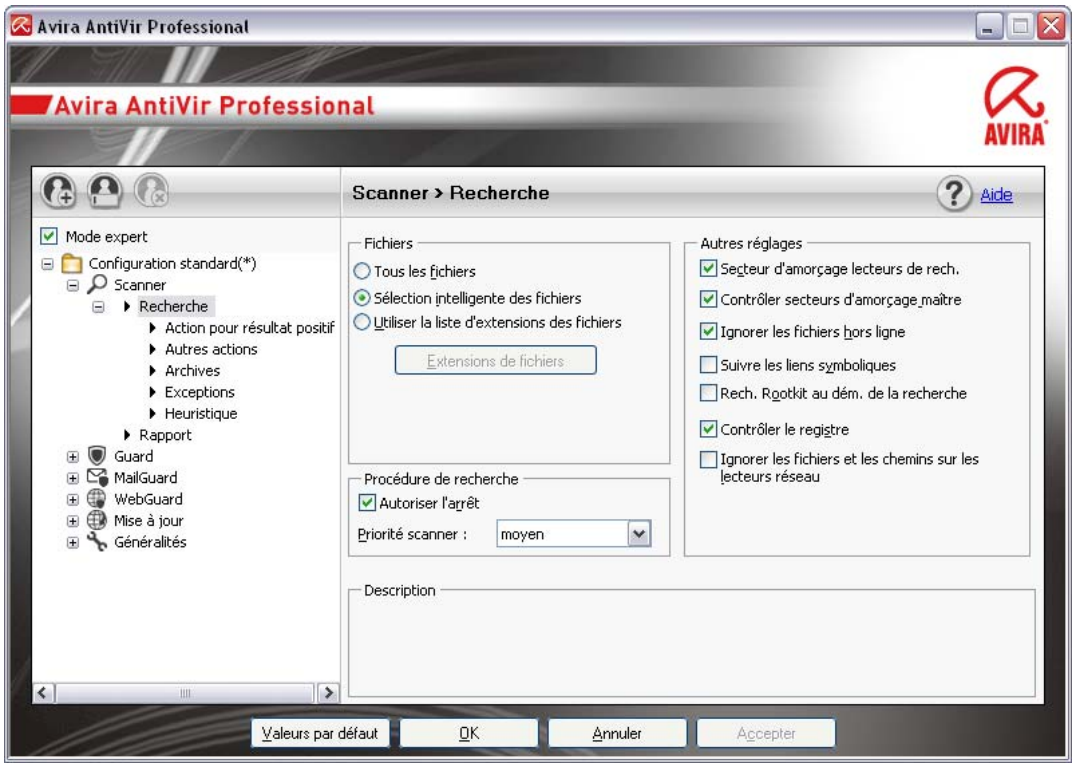
Aperçu du Control Center

- **Aperçu** : vous trouverez sous **Aperçu** toutes les rubriques vous permettant de surveiller le fonctionnement de votre programme AntiVir.

- La rubrique **État** offre la possibilité de voir d'un seul coup d'œil quels modules du programme sont actifs et fournit des informations sur la dernière mise à jour effectuée. De plus, elle vous permet de voir en si vous êtes détenteur d'une licence valable.
- La rubrique Evénements vous donne la possibilité de vous informer sur les événements générés par les modules du programme.
- La rubrique Rapports vous permet de visualiser les résultats des actions effectuées.
- **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 montre les informations sur les fichiers contrôlés, ainsi que d'autres données statistiques qui peuvent être réinitialisées à tout moment et permettent d'accéder au fichier rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles quasiment "par pression d'un bouton".
- **Protection en ligne** : Vous trouverez sous **protection en ligne** les composants vous permettant de protéger votre ordinateur contre les virus et logiciels malveillants provenant d'Internet ainsi que des accès réseau indésirables.
- La rubrique MailGuard vous indique les emails contrôlés par le MailGuard, leurs propriétés ainsi que d'autres données statistiques.
- La rubrique WebGuard vous donne des informations sur les URL contrôlées et les virus détectés, ainsi que d'autres données statistiques, pouvant être réinitialisées à tout moment et permet d'accéder au fichier 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 rubrique Planificateur vous donne la possibilité de créer des tâches de contrôle et de mise à jour programmées et d'ajuster ou de supprimer les tâches existantes.

5.1.2 Configuration

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



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 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 l'icône de programme de votre programme AntiVir.
- Dans le Control Center via la rubrique Extras | Configuration.
- Dans le 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.

Profils de configuration

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

- Utilisation dans le réseau de l'entreprise : mise à jour via le serveur Intranet, WebGuard désactivé

- Utilisation à domicile : mise à jour via le serveur Web par défaut de la société Avira GmbH, WebGuard activé

Si aucune règle de commutation n'a été définie, vous pouvez passer à une configuration dans le menu contextuel de l'icône de programme. Les boutons disponibles sur la barre de navigation ou les commandes du menu contextuel des rubriques de configuration vous permettent d'ajouter, de renommer, d'effacer, de copier, de réinitialiser des configurations ainsi que de définir des règles pour la commutation d'une configuration.

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

Aperçu des options de configuration

Vous disposez des options de configuration suivantes :

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

  Options de recherche

  Actions en cas de résultat positif

  Options pour la recherche dans les archives

  Exceptions de la recherche directe

  Heuristique de la recherche directe

  Réglage de la fonction de rapport

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

  Options de recherche

  Actions en cas de résultat positif

  Exceptions de la recherche en temps réel

  Heuristique de la recherche en temps réel

  Réglage de la fonction de rapport

- **MailGuard**: Configuration 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

  Exceptions de la recherche de MailGuard

  Configuration de la mémoire tampon, vider la mémoire tampon

  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

Réglage de la fonction de rapport

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

Réglages des règles d'adaptateurs

Réglage personnalisé des règles d'applications

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)

– **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 de 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, téléchargement via serveur Web ou serveur de fichiers, réglage des mises à jour produits

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

Configuration des avertissements acoustiques en cas de détection de logiciel malveillant

5.1.3 Icône de programme

Après l'installation, l'icône de votre programme AntiVir 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 Guard et du pare-feu .

Via le menu contextuel de l'icône de programme, les fonctions centrales de votre programme AntiVir 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 et désactive AntiVir Guard.
- **Activer MailGuard**: active et désactive AntiVir MailGuard.
- **Activer AntiVir WebGuard**: active et désactive AntiVir WebGuard.
- **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 les applications 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 Control Center.
- **Configurer AntiVir**: Ouvre la Configuration.
- **Démarrer la mise à jour**: démarre une mise à jour.
- **Sélectionner la configuration** : ouvre un sous-menu contenant les profils de configuration disponibles. Cliquez sur une configuration pour activer celle-ci. La commande de menu est désactivée si vous avez déjà défini des règles pour la commutation automatique de la configuration créée.
- **Aide**: ouvre l'aide en ligne.
- **À propos de AntiVir Professional :** Ouvre une fenêtre de dialogue comportant des informations sur votre programme AntiVir : Informations sur le produit, informations sur la version, informations sur la licence.
- **Avira sur Internet**: ouvre le portail Web Avira sur Internet. La condition est de disposer d'un accès actif à Internet.

5.2 Comment procéder

5.2.1 Activer la licence

Voici comment activer la licence de votre programme AntiVir :

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

Si vous n'avez pas encore installé votre programme AntiVir :

- Enregistrez le fichier de licence dans un répertoire local de votre ordinateur.
- Procédure d'installation de votre programme AntiVir.
- Lors de l'installation, indiquez où vous avez enregistré le fichier de licence.

Si vous avez déjà installé votre programme AntiVir :

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

  - OU -

- Dans le Control Center de votre programme AntiVir, cliquez sur la rubrique Aide/Charger le fichier de licence....

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

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

→ Un message apparaît.

- Validez avec **OK**.

→ La licence est activée.

- Redémarrez le système si nécessaire.

5.2.2 Exécution des mises à jour automatisées

Voici comment créer une tâche d'actualisation automatisée du programme AntiVir 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'effectuer des mises à jour régulières et fréquentes. L'intervalle de mise à jour recommandé est : 60 minutes.

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

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

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

→ La fenêtre de dialogue *Affichage du mode de représentation* apparaît.

- Sélectionnez le mode d'affichage 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 : 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 du produit n'a lieu que si, dans la configuration, sous Généralités :: Mise à jour vous avez activé l'option **Télécharger les mises à jour produit et installer automatiquement**.

Voici comment démarrer manuellement une mise à jour de votre programme AntiVir :

- ▶ Cliquez avec le bouton droit de la souris sur l'icône de programme AntiVir 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 d'effectuer des mises à jour régulières. L'intervalle de mise à jour recommandé est : 60 minutes.

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

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

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

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

- Utiliser un profil de recherche prédéfini

  Si les profils de recherche prédéfinis répondent à vos besoins.

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

  Si vous souhaitez chercher avec un profil de recherche individualisé.

- Créer et utiliser un nouveau profil de recherche

  Si vous souhaitez créer votre propre profil de recherche.

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

- Sous Windows XP et 2000 :

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

- Sous Windows Vista :

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


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


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

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

- ▶ Dans le Control Center, 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 votre programme AntiVir est ouvert.

- ▶ Sélectionnez le fichier ou le répertoire qui doit être contrôlé par.
- ▶ 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 *Affichage du mode de représentation* apparaît.

- Sélectionnez le mode d'affichage 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 d'affichage de la fenêtre 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 et logiciels malveillants actifs*.

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 rootkits et logiciels malveillants actifs**.
- 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 votre programme AntiVir, vous pouvez régler sous la rubrique *Action si résultat positif* de la configuration, comment votre programme AntiVir 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. Un résultat positif s'affiche toujours 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 contaminés 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. Si vous activez l'option *Afficher le message d'avertissement*, vous recevez un message d'avertissement affichant l'action exécutée, en cas de détection d'un virus.

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. Si vous activez l'option *Afficher le message d'avertissement*, vous recevez une notification au bureau en cas de détection d'un virus.

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. Si vous activez l'option *Afficher le message d'avertissement*, vous recevez un message d'avertissement où vous pouvez confirmer l'action à exécuter.

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.

– **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.

– **Ecraser et supprimer**

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

– **Renommer**

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

– **Ignorer**

Aucune autre action n'est effectuée. 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.

– **Toujours ignorer**

Option d'action en cas de résultats positifs de Guard : Le Guard n'effectue aucune autre action. L'accès au fichier est autorisé. Tous les accès suivants à ce fichier sont autorisés et ne sont plus rapportés jusqu'au redémarrage de l'ordinateur ou jusqu'à la mise à jour du fichier de définitions des virus.

– **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 infectés, des options pour la réparation sont disponibles. Si aucune réparation n'est possible avec votre programme AntiVir, 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 (indication d'actions suspectes d'une application) :

– **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 des applications : 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 des applications. 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 contaminée est remplacée par un texte standard. Si le corps de l'email est touché, 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 touchée peut être délivrée plus tard par le gestionnaire de quarantaines.

– **Ignorer**

L'email concerné est livré.

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

Actions 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. Sélectionnez l'option **Ignorer** uniquement dans des cas exceptionnels le justifiant.

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

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

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

Voici comment manipuler les fichiers en quarantaine :

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

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

- Sélectionnez le fichier et cliquez sur  .

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

Si vous souhaitez à nouveau contrôler un fichier :

La vérification d'un fichier est recommandée quand le fichier de définitions des virus de votre programme AntiVir a été actualisé 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 votre programme AntiVir 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 : Votre programme AntiVir 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 pouvez télécharger simultanément plusieurs fichiers en sélectionnant tous les fichiers que vous souhaitez télécharger, puis en cliquant sur le bouton **Envoyer l'objet**.

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 dans la quarantaine

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

– Sous Windows XP et 2000 :

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

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

– Sous Windows Vista :

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

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

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

Voici comment restaurer les fichiers en quarantaine :

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

✓ Fichier recontrôlé par une recherche et réparé.

▶ Dans le Control Center, choisissez la rubrique **Administration :: Quarantaine**.

Remarque

Il n'est possible de restaurer que les emails et pièces jointes d'emails avec l'option  et 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

Il n'est possible de restaurer que les emails et pièces jointes d'emails avec l'option  et 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 **Administration :: Quarantaine**.

▶ Cliquez sur  .

➙ La fenêtre standard Windows pour sélectionner un fichier apparaît.

▶ Choisissez un fichier et validez.

→ Le fichier est déplacé en quarantaine.

Vous pouvez contrôler les fichiers en quarantaine avec AntiVir Scanner :

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

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

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

✓ 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 votre programme AntiVir.

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 :: Evénements** Les événements qui ont été créés par les composants de votre programme AntiVir (similaire à l'affichage des événements de votre système d'exploitation Windows). Les composants de programmes sont :

- Updater
- Guard
- MailGuard
- Scanner
- Planificateur
- Pare-feu
- WebGuard
- Service d'assistance
- ProActive

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 de l'expéditeur est ajoutée à la liste d'exceptions et n'est plus contrôlée quant à l'absence de virus et de logiciels malveillants .

Avertissement
N'excluez de la vérification par 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 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.
- Les connexions de l'extérieur sont bloquées.
- 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 :: Pare-feu**.

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

→ Le niveau de sécurité sélectionné est aussitôt activé.

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 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 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 **Extras**

7 Mises à jour

L'efficacité d'un logiciel antivirus 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 votre AntiVir pour l'exécution des mises à jour. L'Updater garantit que votre programme AntiVir 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 votre programme AntiVir 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 votre programme AntiVir 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 mise à jour 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 est exécutée automatiquement à l'intervalle suivant : 60 minutes. 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 ou bien via un serveur Web ou serveur de fichiers dans l'intranet qui télécharge des fichiers de mise à jour d'Internet et les met à disposition d'autres ordinateurs dans le réseau. Cette option est judicieuse si vous souhaitez mettre à jour des programmes AntiVir sur plusieurs ordinateurs dans un même réseau. Grâce à la configuration d'un serveur de téléchargement dans l'intranet, il est possible de garantir la mise à jour de programmes AntiVir sur tous les ordinateurs à protéger, sans utiliser trop de ressources. Pour configurer un serveur de téléchargement opérationnel dans l'Intranet, vous avez besoin d'un serveur offrant la structure de mise à jour de votre programme AntiVir.

Remarque
Vous pouvez utiliser le gestionnaire AntiVir de mise à jour Internet (serveur Web ou serveur de fichiers sous Windows) comme serveur Web ou serveur de fichiers dans l'Intranet. Le gestionnaire AntiVir de mise à jour Internet reflète le serveur de téléchargement des produits Avira AntiVir et peut être obtenu sur le site Internet Avira : http://www.avira.com/fr

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

8 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'applications 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'applications*, vous pouvez définir, pour une application, différents filtres de paquets à exécuter comme règles d'applications spécifiées.

Remarque
Les règles d'applications possèdent deux modes : *privilégié* et *filtré*. Pour les règles d'applications 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'applications. 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'applications 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 Résolution des problèmes, astuces

Dans ce chapitre, vous trouverez des conseils importants pour la résolution de problèmes et d'autres astuces pour l'utilisation de votre programme AntiVir.

voir le chapitre Aide en cas de problème

voir le chapitre Commandes clavier

voir chapitre Centre de sécurité Windows

9.1 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* s'affiche.

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. Voir également Gestion des licences.

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, il est impossible d'établir une connexion au 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 Vos réglages.

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

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

▶ Actualisez votre produit AntiVir.

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

▶ Démarrez l'ordinateur en mode sécurisé.

▶ Démarrez le programme AntiVir 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, à la 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.

▶ Choisissez dans la configuration (mode expert) Guard :: Recherche :: Exceptions et saisissez le nom du processus du logiciel de sauvegarde.

Mon pare-feu annonce AntiVir Guard et AntiVir MailGuard dès qu'ils 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 le programme AntiVir via "Démarrer | Panneau de configuration | Performances et maintenance | Logiciel" redémarrez l'ordinateur et réinstallez votre programme AntiVir.

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.

▶ Votre programme AntiVir 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. Cette émulation permet d'encapsuler les paquets de données du système invité dans des paquets spéciaux (UDP) et de les rediriger 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'applications*.
- 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).

9.2 Commandes clavier

Les commandes clavier - aussi appelées raccourcis clavier - permettent de naviguer dans le programme, d'accéder à divers modules et de démarrer des actions.

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

9.2.1 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.

9.2.2 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.

9.2.3 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	Démarrer la mise à jour

Rubrique Contrôler

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

Rubrique 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 à l'emplacement...
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 les événements
Enter	Afficher l'événement
Suppr	Supprimer les événements

9.3 Centre de sécurité Windows

- à partir de Windows XP Service Pack 2 -

9.3.1 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.

9.3.2 Le Centre de sécurité Windows et votre programme AntiVir

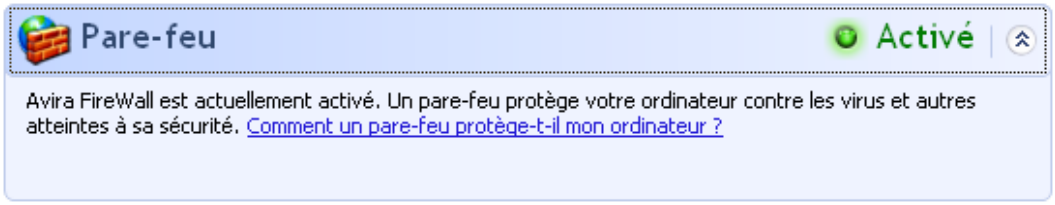
Pare-feu

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 vote programme AntiVir 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 État dans 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

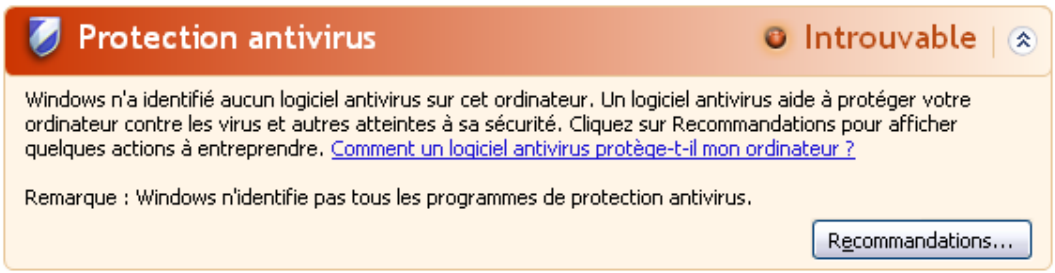
Protection antivirus ACTIVÉE

Protection antivirus DÉSACTIVÉE

Protection antivirus NON SURVEILLÉE

Protection antivirus NON TROUVÉE

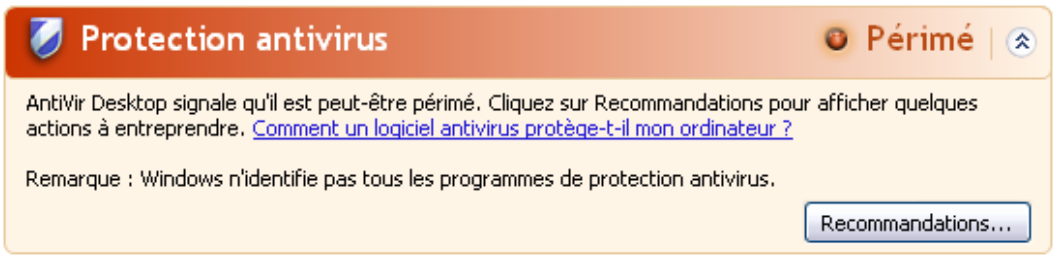
Cette remarque du Centre de sécurité Windows apparaît si le Centre de sécurité Windows n'a trouvé aucun logiciel antivirus sur votre ordinateur.



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

Antivirus EXPIRÉ

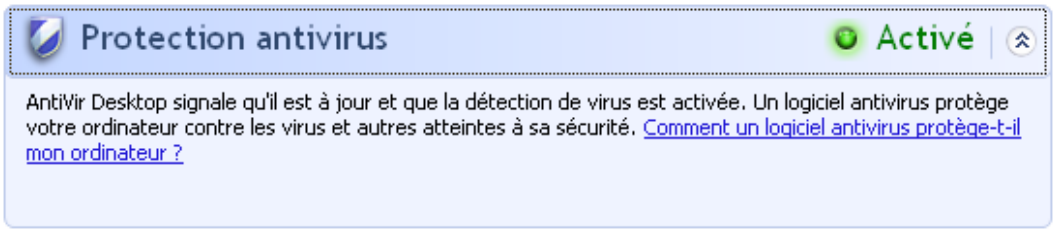
Si vous avez installé Windows XP Service Pack 2 ou Windows Vista puis votre programme AntiVir ou si vous avez installé Windows XP Service Pack 2 ou Windows Vista sur un système accueillant déjà le programme AntiVir, vous recevez le message suivant :



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

Protection antivirus ACTIVÉE

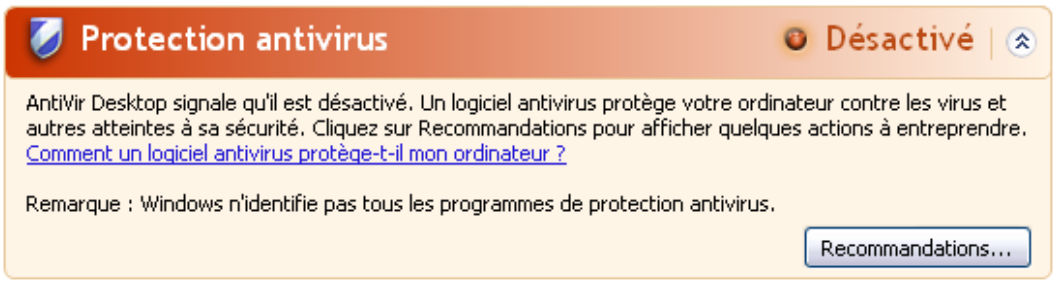
Après l'installation de votre programme AntiVir et une mise à jour immédiatement après, vous recevez le message suivant :



Votre programme AntiVir 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 AntiVirGuard dans la rubrique Aperçu :: état du 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 votre programme AntiVir. 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. 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 !

10 Virus et autres

10.1 Catégories 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, votre programme AntiVir identifie les programmes de numérotation payants qu'il connaît.

Si dans la configuration l'option **Programmes de numérotation payants (DIALER)** est cochée sous Catégories 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.

Votre programme AntiVir détecte les jeux vidéo. Si dans la configuration l'option **Jeux (GAMES)** est cochée sous Catégories de dangers, vous recevez un avertissement quand votre programme AntiVir 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.

Votre programme AntiVir 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.

Votre programme AntiVir détecte les logiciels "Security Privacy Risk". Si dans la configuration l'option **Security Privacy Risk (SPR)** est cochée sous Catégories de dangers, vous recevez un avertissement quand votre programme AntiVir a détecté un tel logiciel.

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.

Votre programme AntiVir détecte les "logiciels de commande Backdoor". Si dans la configuration l'option **Logiciel de commande Backdoor (BDC)** est cochée sous Catégories de dangers, vous recevez un avertissement quand votre programme AntiVir a détecté un tel logiciel.

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.

Votre programme AntiVir détecte les "logiciels publicitaires/espions". Si dans la configuration l'option **Logiciel publicitaire/logiciel espion (ADSPY)** est cochée sous Catégories de dangers, vous recevez un avertissement quand votre programme AntiVir a détecté un tel logiciel.

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.

Votre programme AntiVir détecte les "programmes de compression dans le temps d'exécution inhabituels". Si dans la configuration, l'option Programmes de décompression inhabituels est cochée sous **Catégories de dangers**, vous recevez un avertissement quand votre programme AntiVir 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.

Votre programme AntiVir 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 votre programme AntiVir 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.
Communiquer son adresse email sur Internet, remplir des formulaires en ligne, entrer dans des Newsgroups ou sur des sites Web présente le risque que vos données soient volées par des "Internet crawling spiders" et utilisées sans votre accord dans le but d'une escroquerie.

Votre programme AntiVir détecte le "hameçonnage". Si dans la configuration, l'option**Hameçonnage** est cochée sous Catégories de dangers, vous recevez un avertissement si votre programme AntiVir 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.

Votre programme AntiVir détecte les "applications (APPL)". Si dans la configuration, l'option**Applications** est cochée sous Catégories de dangers, vous recevez un avertissement si votre programme AntiVir détecte ce type de comportement.

10.2 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 programme de commande Backdoor (littéralement de porte arrière) 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.

Canulars (angl. hoax)

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

Pot de miel

Un pot de miel (angl. : honeypot) est un service installé dans un réseau (programme ou serveur). Il a la tâche de surveiller un réseau et de documenter les attaques. Ce service est inconnu de l'utilisateur légitime et n'est donc jamais sollicité. 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.

11 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

11.1 Adresse de contact

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

11.2 Support technique

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

Sur notre site Web, vous obtiendrez toutes les informations nécessaires concernant notre service étendu de support :

http://www.avira.de/fr/support

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

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

11.3 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 l'adresse suivante :.
  virus-prof-fr@avira.com
  Comme certaines passerelles de courrier électronique fonctionnent avec un logiciel antivirus, dotez le ou les fichier(s) d'un mot de passe (n'oubliez pas de nous communiquer ce mot de passe).

Alternativement, vous avez la possibilité de nous envoyer le fichier suspect via notre site Web : http://analysis.avira.com/samples/?lang=fr

11.4 Signaler une fausse alerte

Si vous pensez que votre programme AntiVir 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 l'adresse suivante :

- virus-prof-fr@avira.com

Comme certaines passerelles de courrier électronique fonctionnent avec un logiciel antivirus, dotez le ou les fichier(s) d'un mot de passe (n'oubliez pas de nous communiquer ce mot de passe).

11.5 Vos réactions pour plus de sécurité

Chez Avira, 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 d'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 l'adresse suivante :

vulnerabilities-prof-fr@avira.com

12 Référence : options de configuration

La référence de la configuration documente toutes les options de configuration disponibles.

12.1 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.

12.1.1 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 le programme. Cela signifie que le programme AntiVir 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. 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 plus fonctionnel.

Utiliser la liste d'extensions des fichiers

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

Remarque
Si cette option est activée et que vous avez supprimé toutes les entrées de la liste des extensions de fichiers, ceci s'affiche avec le texte **Extensions 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 standard peut changer d'une version à l'autre.

Autres réglages

Contrôler secteur d'amorçage des lecteurs

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 secteurs d'amorçage maître

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 les fichiers hors ligne. 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 migrés par un système de gestion de mémoire hiérarchique (HSMS) physiquement du disque dur sur un volume externe par exemple. Ce réglage est activé par défaut.

Contrôle d'intégrité 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. Si vous administrez le programme AntiVir sous SMS, l'option n'est pas disponible.

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. Si votre programme AntiVir est administré via le SMC, l'option s'affiche dans chaque cas et peut être activée : si l'ordinateur administré n'est pas équipé de plusieurs processeurs, le scanner n'utilise pas l'option.

Suivre les liens symboliques

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

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

Rech. les rootkits en début de contrôle

Si l'option est activée, le scanner contrôle la présence de Rootkits actifs sur le répertoire système de Windows lors du démarrage d'une recherche lors d'une procédure rapide. Ce processus contrôle l'absence de rootkits actifs 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.

Ne contrôler aucun fichier et chemin sur les lecteurs réseau

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

Processus de contrôle

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 du Scanner

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

Bas

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

Moyen

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

Elevé

Le scanner obtient la priorité 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.

12.1.1.1. Action si résultat positif

Action si 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 concernés, via le menu contextuel. Vous pouvez exécuter les actions choisies pour tous les fichiers contaminés ou quitter le scanner.

Remarque

Dans la boîte de dialogue du scanner, l'action « déplacer en quarantaine » est affichée comme action par défaut.

Actions autorisées

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

Réparer

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

Renommer

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

Quarantaine

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

Supprimer

Le fichier va être supprimé. Cette procédure est beaucoup plus rapide que "écraser et supprimer".

Ignorer

Le fichier est conservé.

écraser et supprimer

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

Standard

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

Remarque

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

Remarque

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

Vous trouverez de plus amples informations ici.

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.

Afficher les messages d'avertissement

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

Action principale

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

Réparer

Si l'option est activée, le scanner répare les fichiers concernés automatiquement. Si le scanner ne peut pas réparer un fichier concerné, 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. Cette procédure est beaucoup plus rapide que "écraser et supprimer".

écraser et supprimer

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

Renommer

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

Ignorer

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

Avertissement
Le fichier 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"** n'est sélectionnable que si sous "**Action primaire"** le réglage **réparer** a été sélectionné. 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. Cette procédure est beaucoup plus rapide que "écraser et supprimer".

écraser et supprimer

Si cette option est activée, le scanner écrase le fichier par un modèle standard et le supprime ensuite (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.

12.1.1.2. Autres actions

Démarrer le programme si résultat positif

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

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

Nom du programme

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

...

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

Arguments

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

Protocole d'événement

Utiliser le rapport d'événement

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

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

Contrôler les archives

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

Tous les types d'archives

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

Extensions intelligentes

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

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

Limiter la profondeur de récursivité

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

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

Profondeur maximale de récursivité

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

Valeur par défaut

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

Liste d'archives

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

12.1.1.3. Exceptions

Objets de fichiers à exclure par le Scanner

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

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

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

Avertissement
Ces fichiers sont ignorés lors de la recherche !

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

Champ de saisie

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

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

Ajouter

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

Supprimer

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

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

Remarque
Si vous administrez le programme AntiVir sous SMC, vous pouvez utiliser les variables dans les indications de chemins pour les exclusions de fichiers. Une liste des variables que vous pouvez utiliser est disponible sous Variables : exceptions Guard et Scanner.

12.1.1.4. Heuristique

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

Les produits AntiVir contiennent 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 de macrovirus

Heuristique de macrovirus

Le produit AntiVir 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

Votre programme AntiVir 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, la détection de logiciels malveillants inconnus est moins performante, 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, un nombre beaucoup plus élevé de logiciels malveillants inconnus est détecté, mais vous devez vous attendre aussi à des messages erronés.

12.1.2 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 preneur de 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.

Intégral

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.

12.2 Guard

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

12.2.1 Recherche

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

Mode de recherche

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

Contrôler pendant la lecture

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

Contrôler pendant l'écriture

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

Contrôler pendant la lecture et l'écriture

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

Fichiers

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

Tous les fichiers

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

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

Sélection intelligente des fichiers

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

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

Utiliser la liste d'extensions des fichiers

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

Remarque
Si cette option est activée et que vous avez supprimé toutes les entrées de la liste des extensions de fichiers, ceci s'affiche 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 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 contrôlées.

Nombre maximum de fichiers

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

Taille maximale (Ko)

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

Lecteurs

Lecteurs réseau

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

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

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

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

Activer la gestion d'antémémoire

Si l'option est activée, les fichiers surveillés sont mis à disposition sur les lecteurs réseaux dans la gestion d'antémémoire du Guard. La surveillance des lecteurs de réseau sans fonction de gestion d'antémémoire offre plus de sécurité mais est moins performante que la surveillance de lecteurs de réseau avec la fonctions gestion d'antémémoire.

12.2.1.1. Action si résultat positif

Action si 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.

Actions autorisées

Dans cette zone d'affichage, vous pouvez choisir quelles actions s'afficheront dans la fenêtre de dialogue comme actions supplémentaires pour le traitement du virus. Vous devez pour cela activer les options correspondantes.

réparer

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

Renommer

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

Quarantaine

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

Supprimer

Le fichier va être supprimé. Cette procédure est beaucoup plus rapide que "écraser et supprimer".

Ignorer

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

écraser et supprimer

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

Standard

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

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

Vous trouverez de plus amples informations ici.

Automatique

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

Copier le fichier dans la quarantaine avant l'action

Si l'option est activée, le Guard génère une copie de sécurité (backup) avant d'effectuer l'action 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.

Afficher les messages d'avertissement

Si l'option est activée, un message d'avertissement en cas de détection d'un virus ou d'un programme indésirable.

Action principale

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

réparer

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

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

Supprimer

Si l'option est activée, le fichier est supprimé. Cette procédure est beaucoup 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 Rapport d'événement 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 concerné s'il n'est pas réparable.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette procédure est beaucoup 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 Rapport d'événement 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.

12.2.1.2. Autres actions

Notifications

Protocole d'événement

Utiliser le rapport d'événement

Si cette option est activée, une entrée est inscrite dans le rapport d'événement Windows à chaque résultat positif. Les événements peuvent être consultés dans l'affichage des événements Windows. 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.

12.2.1.3. 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.
Lors de l'indication des processus et objets de fichiers à exclure, tenir compte des points suivants : La liste est traitée de haut en bas. Plus la liste est longue, plus le temps processeur nécessaire au traitement de la liste pour chaque accès augmente. Tenez les listes aussi courtes que possible.

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
Lors de l'indication du processus, les caractères Unicode sont acceptés. Vous pouvez donc indiquer des noms de processus ou de répertoires contenant des caractères spéciaux.

Remarque
Vous avez la possibilité d'exclure des processus de la surveillance du Guard, sans indiquer le chemin complet :
application.exe
Cela s'applique toutefois uniquement aux processus dont les fichiers exécutables se trouvent sur les lecteurs du disque dur.
L'indication du chemin intégral est nécessaire pour les processus dont les fichiers exécutables se trouvent sur des lecteurs connectés, p. ex. lecteurs réseau. Tenez compte des remarques suivantes sur la notation des Exceptions sur les lecteurs réseau connectés.
N'indiquez aucune exception pour les processus dont les fichiers exécutables se trouvent sur des lecteurs dynamiques. Les lecteurs dynamiques sont utilisés pour les supports de données comme les CD, DVD ou clés USB.

Remarque
Les lecteurs doivent être indiqués comme suit : [lettre du lecteur]:\
Le caractère (:) ne doit servir qu'à désigner des lecteurs.

Remarque
Lorsque vous indiquez un processus, vous pouvez utiliser des caractères de remplacement * (nombre au choix de caractères) et ? (un seul caractère) :
C:\Programmes\Application\application.exe
C:\Programmes\Application\applicatio?.exe
C:\Programmes\Application\applic*.exe
C:\Programmes\Application*.exe
Pour éviter que les processus soient exclus globalement de la surveillance du Guard, les indications contenant les caractères suivants sont incorrectes : * (astérisque), ? (point d'interrogation), / (barre oblique), \ (barre oblique inverse), . (point), : (deux points).

Remarque
Le chemin indiqué et le nom de fichier du processus peuvent contenir 255 signes au maximum. Les entrées de la liste ne doivent pas dépasser 6000 caractères au total.

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
Lorsque vous indiquez des objets de fichiers à exclure, vous pouvez utiliser des caractères de remplacement * (nombre au choix de caractères) et ? (un seul caractère). Certaines extensions de fichiers peuvent aussi être exclues (y compris avec des caractères de remplacement) :
C:\Répertoire*.mdb
*.mdb
*.md?
.xls
C:\Répertoire*.log

Remarque
Les noms de répertoires doivent se terminer par un antislash \, sous peine d'être pris pour un nom de fichier.

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

Remarque
Lorsqu'un répertoire est exclu, tous ses sous-répertoires sont automatiquement ignorés.

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

Le nombre maximum d'exceptions sans chemin complet s'élève à 64.
Exemple : *.log
\Ordinateur1\C\Répertoire1

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.

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.

Lors de l'indication d'exceptions, tenez compte des remarques suivantes :

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

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 documentation du Guard dans la configuration sous Guard :: Rapport sur **Intégral**. Le Guard étant activé, accédez maintenant aux fichiers, répertoires, lecteurs intégrés ou lecteurs réseau connectés . Vous pouvez maintenant lire le chemin à utiliser à partir du fichier de rapport du Guard. Vous accédez au fichier de rapport dans le Control Center sous Protection locale :: Guard.

Remarque
Si vous administrez le programme AntiVir sous SMC, vous pouvez utiliser les variables dans les indications de chemins pour les exclusions de processus et de fichiers. Une liste des variables que vous pouvez utiliser est disponible sous Variables : exceptions Guard et Scanner.

Exemples de processus à exclure :

- application.exe

Le processus du fichier application.exe est exclu de la recherche du Guard, quel que soit le lecteur du disque dur et le répertoire dans lequel le fichier application.exe se trouve.

– C:\Programmes1\application.exe

Le processus du fichier application.exe se trouvant à l'emplacement C:\Programmes1 est exclu de la recherche du Guard.

– C:\Programmes1*.exe

Tous les processus des fichiers exécutables se trouvant à l'emplacement C:\Programmes1 sont exclus de la recherche du Guard.

Exemples de fichiers à exclure :

– *.mdb

Tous les fichiers avec l'extension 'mdb' sont exclus de la recherche du Guard.

– *.xls*

Tous les fichiers dont l'extension commence par 'xls' sont exclus de la recherche Guard, p. ex. fichiers avec fichiers les extensions .xls et xlsx.

– C:\Répertoire*.log

Tous les fichiers journaux avec une extension 'log' se trouvant à l'emplacement C:\Répertoire sont exclus de la recherche du Guard.

– \\Nom de l'ordinateur1\Partage1\

Tous les fichiers auxquels on accède avec une connexion '\\Nom de l'ordinateur1\Partage1' sont exclus de la recherche du Guard. Il s'agit souvent d'un lecteur réseau connecté qui accède à un ordinateur avec un répertoire autorisé avec le nom d'ordinateur 'Nom d'ordinateur1' et le nom de partage 'Partage1'.

– \\1.0.0.0\Partage1*.mdb

Tous les fichiers avec l'extension 'mdb' auxquels on accède avec une connexion '\\1.0.0.0\Partage1' sont exclus de la recherche du Guard. Il s'agit souvent d'un lecteur réseau connecté qui accède à un autre ordinateur avec un répertoire autorisé avec l'adresse IP '1.0.0.0' et le nom de partage 'Partage1'.

12.2.1.4. Heuristique

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

Les produits AntiVir contiennent 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 de macrovirus

Heuristique de macrovirus

Le produit AntiVir 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

Votre programme AntiVir 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, la détection de logiciels malveillants inconnus est moins performante, 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, détecte beaucoup plus de logiciels malveillants inconnus, mais vous devez vous attendre aussi à des messages erronés.

12.2.2 ProActive

En utilisant la fonction AntiVir ProActiv d'Avira, 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 des applications des programmes autorisés. Vous avez également la possibilité d’ajouter le programme au filtre des applications des programmes à bloquer via l’instruction *Toujours bloquer*

Pour déterminer le comportement suspect, 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 d'Avira

Lorsque l'option est activée, les programmes sont surveillés sur votre système d'ordinateur et sont examinés pour savoir s'ils exécutent des actions suspectes typiques. 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 des applications des applications autorisées, tous les programmes que vous avez ajoutés au filtre d'application des programmes autorisés.

Améliorer la sécurité de votre ordinateur en participant à la communauté AntiVir ProActiv.

Si l'option est activée, Avira AntiVir ProActiv envoie à l'Avira Malware Research Center les données sur les programmes suspects et, dans certains cas, les fichiers de programmes suspects (fichiers exécutables). 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.

Cliquez ici pour obtenir de plus amples informations.

Le lien vous permet d'avoir des détails sur le contrôle en ligne étendu sur une page Internet. Les données transmises lors du contrôle en ligne étendu sont indiquées dans leur intégralité sur la page Internet.

12.2.2.1. Filtre des applications : Applications à bloquer

Sous *Filtre des applications : Applications à bloquer* vous pouvez ajouter les applications que vous classifiez comme nuisibles et qui doivent être bloquées par défaut par Avira 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 des applications 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 Avira AntiVir 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. Avira AntVir 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.

12.2.2.2. Filtre des applications : Applications autorisées

Sous *Filtre des applications : les applications autorisées* sont 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 des applications. 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 votre programme AntiVir, sont exclues 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.

12.2.3 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.

Intégral

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.

Restreindre 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. Emplacement de sauvegarde, voir Configuration :: Généralités :: Répertoires :: Répertoire de rapport.

Ecrire 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.

Remarque
Si vous n'avez indiqué aucune restriction du fichier de rapport, un nouveau fichier de rapport est automatiquement créé quand le fichier de rapport atteint une taille de 100 Mo. Une sauvegarde de l'ancien fichier de rapport est créée. Jusqu'à trois sauvegardes d'anciens fichiers de rapport sont conservées. Les sauvegardes les plus anciennes sont supprimées en premier.

12.3 MailGuard

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

12.3.1 Recherche

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

Recherche

Activer MailGuard

Si l'option est activée, le trafic email est contrôlé par le MailGuard. Le MailGuard est un serveur proxy qui contrôle sur le système d'ordinateur le trafic de données entre le serveur d'email que vous utilisez et le programme de client email. Dans les réglages par défaut, l'absence de logiciels malveillants est contrôlée sur les emails entrants. Si l'option est désactivée, le service MailGuard reste actif, mais la surveillance par le MailGuard est désactivée.

Contrôler les emails entrants

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

Contrôler les emails sortants (SMTP)

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

Ports surveillés

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

Standard

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

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

12.3.1.1. Action si 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 si résultat positif

Interactif

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

Actions autorisées

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

Déplacer en quarantaine

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

Supprimer

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

Supprimer la pièce jointe

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

Déplacer la pièce jointe en quarantaine

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

Ignorer

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

Standard

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

Afficher la barre de progression

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

Automatique

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

Action 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 concernées

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 !

12.3.1.2. 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.

12.3.1.3. Heuristique

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

Les produits AntiVir contiennent 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

Le produit AntiVir 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

Votre programme AntiVir 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, la détection de logiciels malveillants inconnus est moins performante, 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, un nombre beaucoup plus élevé de logiciels malveillants inconnus est détecté, mais vous devez vous attendre aussi à des messages erronés.

12.3.2 Généralités

12.3.2.1. 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.

Etat

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

Adresse email

Adresse email qui ne doit plus être contrôlée.

Logiciels malveillants

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

vers le haut

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

vers le bas

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

Champ de saisie

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

Ajouter

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

Supprimer

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

12.3.2.2. 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.

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.

12.3.2.3. 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 . 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.

12.3.3 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.

Intégral

Si l'option est activée, le MailGuard consigne également toutes les informations secondaires dans le fichier de rapport.

Restreindre 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. Emplacement de sauvegarde, voir Configuration :: Généralités :: Répertoires :: Répertoire de rapport.

Ecrire 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.

Remarque
Si vous n'avez indiqué aucune restriction du fichier de rapport, un nouveau fichier de rapport est automatiquement créé quand le fichier de rapport atteint une taille de 100 Mo. Une sauvegarde de l'ancien fichier de rapport est créée. Jusqu'à trois sauvegardes d'anciens fichiers de rapport sont conservées. Les sauvegardes les plus anciennes sont supprimées en premier.

12.4 Firewall

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

12.4.1 Règles d’adaptateurs

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 :: Modifier le pare-feu du 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 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 **Moyen**.

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 : Elevé
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 : Elevé
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 : Elevé
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.

12.4.1.1. 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 : Elevé

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 **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	– 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 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**.

	les paquets avec les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**. – Surveillance du trafic de données conforme au TCP **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**. – Rejeter 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 : Elevé
-	– Surveillance du trafic de données conforme à l'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**. – Rejeter 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**	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**.

	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/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 : Elevé
-	– Ne pas rejeter de paquets ICMP sur la base de l'adresse IP Autoriser les paquets ICMP 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**.	Même règle que pour le réglage Moyen.

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 : Elevé
-	-	Rejeter 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.

Rapport

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.

12.4.1.2. 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.
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.

12.4.2 Règles d'applications

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
Applicatioin	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'applications spécifiques basées sur les filtres de paquets, semblables aux règles d'adaptateurs. Pour passer à la configuration étendue des règles d'applications, activez tout d'abord le mode expert. Dans la rubrique Pare-feu:: Réglages, modifiez maintenant le réglage pour les règles d'application : 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'applications 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
Applicatioin	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'applications 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'applications spécifiques.

Règles d'applications spécifiques de la configuration étendue

Les règles d'applications 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'applications à volonté, pour chaque application. Les règles d'applications 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'applications 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'applications.

12.4.3 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 autom. 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'applications 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.

12.4.4 Réglages

Paramètres étendus

Activer FireWall

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 lors du 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 d'une 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.

Port Scan

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.

Les 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’applications

Les options de la zone Règles d'applications vous permettent de régler les possibilités de configuration des règles d’applications sous la rubrique Parefeu :: Règles d'applications.

Paramètres 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.

12.4.5 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 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'applications 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 dernière version

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 dernière version

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 dernière version

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.

12.5 Pare-feu sous SMC

La configuration pare-feu est adaptée aux exigences spécifiques d'une administration via le Avira Security Management Center. Il existe des options et limitations étendues de chacune des différentes options de configuration :

- Les paramètres pour le pare-feu s'appliquent à tous les utilisateurs des ordinateurs clients
- Règles d'adaptateur : Des niveaux de sécurité peuvent être réglés via des menus contextuels pour les différents adaptateurs
- Règles d'applications : L'accès au réseau d'applications peut être autorisé ou bloqué. Il n'existe aucune possibilité de créer des règles d'applications spécifiques.

En cas d'administration de votre programme AntiVir via Avira Security Management Center, les possibilités de réglage suivantes du pare-feu dans le Control Center sur les ordinateurs clients sont désactivées :

- réglage des niveaux de sécurité du pare-feu
- Réglage des règles d'adaptateur et d'application

12.5.1 Paramètres généraux

Paramètres étendus

Bloquer le fichier hôte Windows

Si cette option est activée, 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.

Activer le 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'applications 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.

Désactiver le pare-feu Windows lors du démarrage

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

Activer FireWall

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

Dépassement de délai d'une 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.

12.5.2 Règles générales d'adaptateur

On désigne sous le terme d'adaptateur les connexions réseau réalisées. Des règles d'adaptateur peuvent être réalisées pour les connexions réseau client suivantes :

- Adaptateur par défaut : LAN ou Internet haute vitesse
- Sans fil
- Connexion télétransmission

Pour chaque adaptateur disponible, vous pouvez fixer des règles d'adaptateur pré-définies via le menu contextuel relatif à l'adaptateur :

- Niveau de sécurité élevé
- Niveau de sécurité moyen
- Niveau de sécurité bas

Vous avez également la possibilité d'adapter chacune des règles d'adaptateur et de les régler individuellement.

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

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 : Elevé
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 : Elevé

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 : Elevé**
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**	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.

l'attaque.		

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.

12.5.2.1. 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 : Elevé
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 **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**	– 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 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

		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 de données conforme au TCP **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	paquet correspond à la règle. Etendu : refuser les paquets avec les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**.

	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**. – Rejeter 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 : Elevé
-	– Surveillance du trafic de données conforme à l'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	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

	{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**. – Rejeter 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 masque **<vide>** sur le décalage **0**.	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**.

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

	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 : Elevé
-	-	Rejeter 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.

Rapport

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.

12.5.2.2. 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.

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.

12.5.3 Liste d'applications

Sous la liste d'applications, vous avez la possibilité de créer des règles pour les accès au réseau d'applications. Vous pouvez ajouter des applications à la liste et fixer via un menu contextuel les règles *Autoriser* et **Bloquer** pour l'application sélectionnée :

- Les accès au réseau d'applications avec la règle *Autoriser* sont autorisés.
- Les accès au réseau d'applications avec la règle *Bloquer* sont rejetés.

Lors de l'ajout d'applications, la règle *Autoriser* est définie.

Liste des applications

Ce tableau vous montre la liste des applications pour lesquelles les règles sont définies. Les symboles indiquent si les accès au réseau des applications sont permis ou bloqués. Vous pouvez modifier les règles relatives aux applications via un menu contextuel.

Boutons

Bouton	Description
Ajouter par chemin d'accès	Le bouton ouvre une boîte de dialogue dans laquelle vous pouvez sélectionner les applications. L'application est ajoutée à la liste d'applications avec la règle « **Autoriser accès au réseau** ». Si vous utilisez l'option « **Ajouter par chemin d'accès »**, l'application ajoutée est identifiée par le pare-feu au moyen du chemin et du nom du fichier. Les règles pour une application restent valables et sont appliquées par le pare-feu, même si le contenu d'un fichier exécutable a été modifié par une mise à jour par exemple.
Ajouter par md5	Le bouton ouvre une boîte de dialogue dans laquelle vous pouvez sélectionner les applications. L'application est ajoutée à la liste d'applications avec la règle « **Autoriser accès au réseau** ». Si vous utilisez l'option « **Ajouter par md5 »**, toutes les applications

	ajoutées sont clairement identifiées à l'aide de la somme de contrôle MD5. Cela permet au pare-feu d'identifier les modifications des contenus de fichiers. En cas de modification d'une application, par exemple en raison d'une actualisation, l'application avec la règle définie est automatiquement retirée de la liste d'applications. Après la modification, l'application doit à nouveau être ajoutée à la liste, la règle souhaitée doit être créée à nouveau.
Ajouter groupe	Le bouton ouvre une boîte de dialogue dans laquelle vous pouvez sélectionner un répertoire. Toutes les applications sous le chemin sélectionné sont ajoutées à la liste d'applications avec la règle « **Autoriser accès au réseau** ».
Supprimer	La règle d'application sélectionnée est retirée.
Tout supprimer	Toutes les règles d'applications sont retirées.

12.5.4 Fournisseurs dignes de confiance

Une liste des éditeurs de logiciels dignes de confiance s'affiche sous *Fournisseurs dignes de confiance*. Les accès au réseau des applications des éditeurs de logiciel sur la liste sont autorisés. Il est possible d'ajouter ou de supprimer des éditeurs de la liste.

Fournisseurs

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

Boutons

Bouton	Description
Ajouter	Le bouton ouvre une boîte de dialogue dans laquelle vous pouvez sélectionner les applications. L'éditeur de l'application est déterminé et ajouté à la liste des fournisseurs dignes de confiance.
Ajouter groupe	Le bouton ouvre une boîte de dialogue dans laquelle vous pouvez sélectionner un répertoire. Les éditeurs de toutes les applications sont déterminés sous le chemin sélectionné et ajoutés à la liste des fournisseurs dignes de confiance.
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.
Tout supprimer	Toutes les entrées sont retirées de la liste des fournisseurs dignes de confiance.
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*.

Remarque
Le pare-feu donne la priorité aux règles d'applications 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.

12.5.5 Autres réglages

Notifications

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

Port Scan

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.

Les 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.

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 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'applications 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.

12.5.6 Paramètres d'affichage

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 dernière version

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 dernière version

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 dernière version

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.

12.6 WebGuard

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

12.6.1 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.

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 suspects

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 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.

12.6.1.1. Action si résultat positif

Action si 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 concerné apparaît. Ce réglage est activé par défaut.

Actions autorisées

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

Refuser l'accès

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

Quarantaine

La page Web demandée par le serveur Web ou les données et fichiers transmis sont déplacés en quarantaine en cas de détection d'un virus ou d'un logiciel malveillant. Le fichier 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.

Standard

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

Vous trouverez de plus amples informations ici.

Afficher la barre de progression

Si l'option est activée, un message affiché sur le bureau apparaît avec une barre de progression de téléchargement, lorsque le téléchargement de contenus de sites Internet dépasse un délai d'attente de 20 secondes . Ce message affiché sur le bureau sert notamment à contrôler le téléchargement de sites Internet avec de gros volumes de données : lors de la navigation avec le WebGuard, les contenus des sites Internet ne sont pas chargés successivement dans le navigateur Internet, du fait qu'ils sont contrôlés quant à l'absence de virus et de logiciels malveillants avant d'être affichés dans le navigateur. Cette option est désactivée par défaut.

Automatique

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

Afficher les messages d'avertissement

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

Action principale

L'action 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.

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 !

12.6.1.2. 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.

12.6.1.3. 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

12.6.1.4. Heuristique

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

Les produits AntiVir contiennent 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 de macrovirus

Heuristique de macrovirus

Le produit AntiVir 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

Votre programme AntiVir 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, la détection de logiciels malveillants inconnus est moins performante, 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, un nombre beaucoup plus élevé de logiciels malveillants inconnus est détecté, mais vous devez vous attendre aussi à des messages erronés.

12.6.2 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.

Intégral

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.

Restreindre 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 20% soit atteinte.

Sauvegarder le fichier de rapport avant de raccourcir

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

Ecrire 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.

Remarque
Si vous n'avez indiqué aucune restriction du fichier de rapport, toutes les anciennes entrées sont supprimées automatiquement quand le fichier de rapport atteint une taille de 100 Mo. Les entrées sont supprimées jusqu'à ce que le fichier de rapport atteigne une taille de 80 Mo.

12.7 Mise à jour

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

Remarque
Si vous configurez votre programme AntiVir via l'AntiVir Security Management Center, la configuration des mises à jour automatiques n'est pas disponible.

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 également la tâche quand une connexion Internet est établie

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.

Télécharger

Par serveur Web

La mise à jour s'effectue via un serveur web par connexion HTTP. Vous pouvez utiliser un serveur Web du fabricant sur Internet, ou bien un serveur Web dans l'Intranet qui télécharge des fichiers de mise à jour à partir d'un serveur de téléchargement du fabricant sur Internet.

Remarque
Vous trouverez d'autres paramètres relatifs à la mise à jour via un serveur Web sous : Configuration :: Généralités :: Mise à jour :: Serveur web .

Par serveur de fichiers/répertoires partagés

La mise à jour s'effectue via un serveur de fichier dans l'Intranet qui télécharge des fichiers de mise à jour à partir d'un serveur de téléchargement du fabricant sur Internet.

Remarque
Vous trouverez d'autres paramètres relatifs à la mise à jour via un serveur de fichiers sous : Configuration :: Généralités :: Mise à jour :: Serveur de fichiers .

12.7.1 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 celui-ci, 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).

Remarque
Si vous avez activé une option pour une mise à jour de produit automatique, vous pouvez configurer d'autres options pour le message et les possibilités d'interruption du redémarrage sous Paramètres de redémarrage.

12.7.2 Paramètres de redémarrage

Si une mise à jour de votre programme AntiVir est exécutée, 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 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 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 au '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.

12.7.3 Serveur de fichiers

En présence de plusieurs ordinateurs dans un réseau, votre programme AntiVir peut télécharger une mise à jour d'un serveur de fichiers dans l'Intranet qui acquiert lui-même les fichiers de mise à jour à partir d'un serveur de téléchargement du fabricant sur Internet. Ceci permet de garantir l'actualité des programmes AntiVir sur tous les ordinateurs en préservant les ressources.

Remarque
La rubrique configuration n'est activée que si sous Configuration :: Mise à jour:: Mise à jour produit , l'option **Par serveur de fichiers/répertoires partagés** a été sélectionnée.

Télécharger

Indiquez le serveur de fichiers où se trouvent les fichiers d'actualisation de votre programme AntiVir ainsi que les répertoires '/release/update/' nécessaires. L'indication suivante est indispensable : file://<Adresse IP du serveur de fichiers>/release/update/. Le répertoire 'release' doit être un répertoire autorisé à tous les utilisateurs.

Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le répertoire de téléchargement souhaité.

Connexion au serveur

Identifiant de connexion

Saisissez un identifiant pour la connexion au serveur. Utilisez un compte d'utilisateur disposant de droits d'accès au répertoire utilisé autorisé sur le serveur.

Mot de passe de connexion

saisissez le mot de passe du compte d'utilisateur utilisé. Les caractère saisis sont masqués par des *.

Remarque
Si vous ne saisissez aucune donnée dans la zone de données de connexion au serveur, aucune identification sur le serveur de fichiers ne sera effectuée lors d'un accès au serveur de fichiers. Dans ce cas, des droits d'utilisateur suffisants doivent être disponibles sur le serveur de fichiers.

12.7.4 Serveur web

La mise à jour peut être effectuée directement via un serveur web sur Internet ou sur l'Intranet .

Connexion au serveur Web

Utiliser la connexion existante (réseau)

Ce réglage s'affiche lorsque votre connexion via un réseau est utilisée.

Utiliser la connexion suivante :

Ce réglage s'affiche quand vous définissez votre connexion individuellement.

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.

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.

Télécharger

Serveur standard

Saisissez ici les adresses (URL) du serveur web à partir desquels les mises à jour doivent être chargées, ainsi que le répertoire de mise à jour 'update' nécessaire. L'indication suivante d'un serveur Web est valable : http://<Adresse du serveur Web>[:Port]/update. Si vous n'indiquez aucun port, le port 80 est utilisé. Les serveurs Web accessibles d'Avira sont saisis par défaut pour la mise à jour. Toutefois, vous pouvez également utiliser votre propre serveur Web sur l'Intranet par exemple. En cas d'indication de plusieurs serveurs Web, les serveurs sont séparés par des virgules.

Standard

Le bouton permet de restaurer les adresses prédéfinies.

Serveur prioritaire

Indiquez dans ce champ l'adresse (URL) du serveur Web qui doit être interrogé en premier lors d'une mise à jour ainsi que le répertoire de mise à jour nécessaire. Si ce serveur n'est pas accessible, les serveurs standard indiqués sont interrogés. L'indication suivante du serveur Web est valable : http://<Adresse du serveur Web>[:Port]/update. Si vous n'indiquez aucun port, le port 80 est utilisé.

12.7.4.1. 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. Vous pouvez configurer les paramètres système de Windows pour l'utilisation d'un serveur proxy sous **Performances et maintenance:: Options Internet :: Connexions :: Réglages LAN**. Dans Internet Explorer, vous pouvez également accéder aux options Internet dans le menu Outils.

Avertissement

Si vous utilisez un serveur proxy nécessitant une identification, indiquez l'intégralité des données sous l'option *Connexion via ce serveur proxy* >. L'option *Utiliser les réglages système de Windows* ne peut servir que pour les serveurs proxy sans identification.

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 le nom de l'ordinateur 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 un identifiant pour la 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

12.8 Généralités

12.8.1 Email

Le programme AntiVir peut lors d'événements particuliers, envoyer des avertissements et messages par email à un ou plusieurs destinataire(s) . Pour ce faire, le Simple Message Transfer Protocol (SMTP) est utilisé.

Les messages peuvent ici être déclenchés par différents événements. Les composants suivants prennent en charge l'envoi de emails :

- Guard : Envoi de notifications
- Scanner : Envoi de notifications
- Updater : Envoi de notifications

Remarque
Attention, l'ESMTP n'est pas pris en charge. En outre, une transmission codée par TLS (Transport Layer Security) ou SSL (Secure Sockets Layer) n'est pas encore possible.

Messages emails

Serveur SMTP

Entrez ici le nom de l'hôte à utiliser - son adresse IP ou le nom de l'hôte direct.
Le nom de l'hôte ne doit pas dépasser 127 caractères.

Exemple :

192.168.1.100 ou mail.nom.de.

Adresse de l'expéditeur

Saisissez dans ce champ l'adresse email de l'expéditeur. L'adresse de l'expéditeur ne doit pas dépasser 127 caractères.

Identification

Certains serveurs mail attendent qu'un programme s'identifie (se connecte) auprès du serveur avant l'envoi d'un email. Les avertissements par email peuvent être transmis avec identification à un serveur SMTP.

Utiliser l'identification

Si cette option est activée, il est possible de saisir un identifiant et un mot de passe pour la connexion (identification) dans les champs de saisie prévus.

- **Identifiant** : Saisissez ici l'identifiant.
- **Mot de passe** : saisissez ici le mot de passe correspondant. Le mot de passe est mémorisé de manière cryptée. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Envoyer un email test

En cliquant sur ce bouton, le programme essaie d'envoyer un email test à l'adresse du destinataire pour contrôle des données saisies.

12.8.2 Catégories de dangers

Sélection des catégories de dangers

Votre produit AntiVir vous protège des virus informatiques.

En outre, vous avez la possibilité de rechercher les catégories 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 tout

Si cette option est activée, tous les types sont activés.

Valeur 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.

12.8.3 Mot de passe

Vous pouvez protéger votre programme AntiVir 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

Votre programme AntiVir 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, le mot de passe défini 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 FireWall	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.
Télécharger le CD de secours depuis Internet	Si l'option est activée, le mot de passe défini est nécessaire pour démarrer le téléchargement du CD de secours Avira.
Quarantaine	Si l'option est activée, toutes les zones possibles du gestionnaire de quarantaine 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, le mot de passe défini est nécessaire pour restaurer un objet.
Nouveau contrôle des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour recontrôler un objet.
Caractéristiques des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour l'affichage des caractéristiques d'un objet.
Suppression des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour supprimer un objet.
Envoyer un email à Avira	Si l'option est activée, le mot de passe défini est nécessaire pour l'envoi d'un objet pour contrôle à Avira Malware Research Center.
Copie des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour copier l’objet concerné.
Ajouter et modifier des tâches	Si l'option est activée, le mot de passe défini est nécessaire pour ajouter et modifier des tâches dans le planificateur.
Démarrer les mises à jour produit	Si l'option est activée, le mot de passe défini est nécessaire dans le menu Mise à jour pour démarrer la mise à jour produit.
Configuration	Si l'option est activée, la configuration du

	programme n'est possible qu'après la saisie du mot de passe défini.
Changer manuellement de configuration	Si l'option est activée, le mot de passe défini est nécessaire pour passer manuellement à un autre profil de configuration.
Activer le mode expert	Si l'option est activée, le mot de passe défini est nécessaire pour activer le mode expert.
Installation/Désinstallation	Si l'option est activée, le mot de passe défini est nécessaire pour l'installation et la désinstallation du programme.

12.8.4 Sécurité

Mise à jour

Avertissement si la dernière mise à jour date de plus de n jour(s)

Dans ce champ, vous pouvez saisir le nombre de jours qui doit s'écouler au maximum depuis la dernière mise à jour. Si cet âge est dépassé, une icône rouge s'affiche dans Control Center sous Etat pour l'état de mise à jour.

Afficher la remarque, 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

Remarque
Les options de protection du produit ne sont pas disponibles si le Guard n'a pas été installé sur une installation personnalisée.

Protéger les processus d'un arrêt non souhaité

Si l'option est activée, tous les processus du programme 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 étendue des processus

Si l'option est activée, tous les processus du programme 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. L'option est activée par défaut. Pour désactiver 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 entrées de registre de toute manipulation

Si l'option est activée, toutes les entrées de registre du programme, ainsi que tous les fichiers du programme (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.

Avertissement
Notez que si l'option est désactivée, la réparation d'ordinateurs infectés par certains types de logiciels malveillants peut échouer.

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 !

12.8.5 WMI

Prise en charge de Windows Management Instrumentation

Windows Management Instrumentation est une technologie de gestion Windows de base qui permet d'accéder en lecture et en écriture aux paramètres d'ordinateurs Windows, localement et à distance, au moyen de langages de script et de programmation. Votre programme AntiVir est compatible WMI et met à disposition les données (informations d'état, données statistiques, rapports, tâches planifiées, etc.) et méthodes (arrêter et démarrer les processus) sur une interface. WMI vous donne la possibilité d'interroger les données d'exploitation du programme et de commander le programme . Vous pouvez obtenir une référence complète de l'interface WMI auprès de l'éditeur. Vous recevez la référence au format PDF, après avoir signé un accord de confidentialité.

Activer la prise en charge de WMI

Si l'option est activée, vous avez la possibilité d'interroger les données d'exploitation du programme.

Autorise l'activation/désactivation de services

Si l'option est activée, vous avez la possibilité d'activer et de désactiver des services du programme via WMI.

12.8.6 Répertoires

Chemin temporaire

Saisissez dans ce champ le chemin où le programme 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.

Répertoire de rapport

Ce champ de saisie contient le chemin vers le répertoire de rapport.

...

Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le répertoire souhaité.

Standard

Ce bouton restaure le chemin prédéfini vers le répertoire de rapport.

Répertoire de quarantaine

Ce champ de saisie contient le chemin vers le répertoire de quarantaine.

...

Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le répertoire souhaité.

Standard

Ce bouton restaure le chemin prédéfini vers le répertoire de quarantaine.

12.8.7 Avertissements

12.8.7.1. Réseau

Vous pouvez envoyer des avertissements configurables individuellement du Scanner ou du Guard à n'importe quel ordinateur de votre réseau.

Remarque
Vérifiez si le service de messages a démarré. Vous trouverez ce service (exemple Windows XP) sous « Démarrer | Panneau de configuration| Performances et maintenance | Outils d'administration | Services ».

Remarque
Un avertissement est toujours envoyé à l'ordinateur, PAS à un utilisateur particulier.

Avertissement
Cette fonctionnalité n'est pas prise en charge par les systèmes d'exploitation suivants :
Microsoft Server 2008 et supérieur
Windows Vista et supérieur

Envoyer le message à

La liste dans cette fenêtre indique le nom des ordinateurs recevant un message en cas de résultat positif.

Remarque
Un ordinateur ne peut être saisi qu'une seule fois dans cette liste.

Insérer

Ce bouton vous permet d'ajouter un ordinateur. Une fenêtre s'ouvre dans laquelle vous pouvez saisir le nom du nouvel ordinateur. Un nom d'ordinateur ne peut pas contenir plus de 15 caractères.

Le bouton ouvre une fenêtre dans laquelle vous pouvez alternativement sélectionner un ordinateur dans votre environnement réseau.

Supprimer

Ce bouton vous permet de supprimer de la liste l'entrée actuellement sélectionnée.

Guard

Avertissements réseau

Si l'option est activée, des avertissements réseau sont envoyés. Cette option est désactivée par défaut.

Remarque
Pour pouvoir activer cette option, au moins un destinataire doit être saisi sous Généralités :: Avertissements :: Réseau.

Message à envoyer

La fenêtre montre le message envoyé à l'ordinateur choisi en cas de résultat positif. Vous pouvez éditer ce message. Un texte ne doit pas contenir plus de 500 caractères.

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

Strg + Tab	ajoute une tabulation. La ligne actuelle est repoussée à droite de quelques caractères.
Strg + Enter	ajoute un saut de ligne.

Le message peut aussi contenir des caractères de remplacement pour les informations trouvées pendant la recherche. Ces caractères de remplacement sont remplacés par le vrai texte à l'envoi.

Les caractères de remplacement suivants sont autorisés :

%VIRUS%	contient le nom du virus ou programme indésirable trouvé
%FILE%	contient le chemin et le nom du fichier concerné
%COMPUTER%	contient le nom de l'ordinateur sur lequel le Guard

	fonctionne
%NAME%	contient le nom de l'utilisateur qui a accédé au fichier concerné
%ACTION%	contient l'action exécutée après la découverte du virus
%MACADDR%	contient l'adresse MAC de l'ordinateur sur lequel Guard fonctionne

Standard

Ce bouton restaure le texte standard prédéfini pour l'avertissement.

Scanner

Activer les avertissements réseau

Si l'option est activée, des avertissements réseau sont envoyés. Cette option est désactivée par défaut.

Remarque
Pour pouvoir activer cette option, au moins un destinataire doit être saisi sous Généralités :: Avertissements :: Réseau.

Message à envoyer

La fenêtre montre le message envoyé à l'ordinateur choisi en cas de résultat positif. Vous pouvez éditer ce message. Un texte ne doit pas contenir plus de 500 caractères.

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

Strg + Tab	ajoute une tabulation. La ligne actuelle est repoussée à droite de quelques caractères.
Strg + Enter	ajoute un saut de ligne.

Le message peut aussi contenir des caractères de remplacement pour les informations trouvées pendant la recherche. Ces caractères de remplacement sont remplacés par le vrai texte à l'envoi.

Les caractères de remplacement suivants sont autorisés :

%VIRUS%	contient le nom du virus ou programme indésirable trouvé
%NAME%	contient le nom de l'utilisateur connecté qui exécute le scanner

Standard

Ce bouton restaure le texte standard prédéfini pour l'avertissement.

12.8.7.2. Email

Email

Le programme AntiVir peut lors d'événements particuliers, envoyer des avertissements et messages par email à un ou plusieurs destinataire(s) . Pour ce faire, le Simple Message Transfer Protocol (SMTP) est utilisé.

Les messages peuvent ici être déclenchés par différents événements. Les composants suivants prennent en charge l'envoi de emails :

- Guard : Envoi de notifications
- Scanner : Envoi de notifications
- Updater : Envoi de notifications

Remarque
Attention, l'ESMTP n'est pas pris en charge. En outre, une transmission codée par TLS (Transport Layer Security) ou SSL (Secure Sockets Layer) n'est pas encore possible.

Messages emails

Serveur SMTP

Entrez ici le nom de l'hôte à utiliser - son adresse IP ou le nom de l'hôte direct.
Le nom de l'hôte ne doit pas dépasser 127 caractères.

Exemple :

192.168.1.100 ou mail.nom.de.

Adresse de l'expéditeur

Saisissez dans ce champ l'adresse email de l'expéditeur. L'adresse de l'expéditeur ne doit pas dépasser 127 caractères.

Identification

Certains serveurs mail attendent qu'un programme s'identifie (se connecte) auprès du serveur avant l'envoi d'un email. Les avertissements par email peuvent être transmis avec identification à un serveur SMTP.

Utiliser l'identification

Si cette option est activée, il est possible de saisir un identifiant et un mot de passe pour la connexion (identification) dans les champs de saisie prévus.

- **Identifiant** : Saisissez ici l'identifiant.
- **Mot de passe** : saisissez ici le mot de passe correspondant. Le mot de passe est mémorisé de manière cryptée. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Envoyer un email test

En cliquant sur ce bouton, le programme essaie d'envoyer un email test à l'adresse du destinataire pour contrôle des données saisies.

Guard

AntiVir Guard peut envoyer des avertissements par email à un ou plusieurs destinataires lors de certains événements.

Guard

Avertissements email

Si cette option est activée, AntiVir Guard envoie des messages email avec les principales données lorsqu'un événement défini se produit. Cette option est désactivée par défaut.

Notification par email lors des événements suivants

Lors de la recherche en temps réel, un résultat positif a été annoncé.

Si cette option est activée, vous recevez un email avec le nom du virus ou du programme indésirable du fichier concerné à chaque fois que la recherche en temps réelle trouve un virus ou un programme indésirable.

Éditer

Avec le bouton *Editer*, ouvrez la fenêtre *Modèle d'email*, où vous pouvez configurer le message pour l'événement « Détection lors de recherche en temps réel ». Vous avez la possibilité d'entrer du texte pour l'objet et le message de l'email. A cet effet, vous pouvez utiliser des variables (voir Configuration::Généralités::Email::Avertissements::Modèle d'email).

Une erreur critique s'est produite au sein du Guard.

Si cette option est activée, vous recevez un email si une erreur critique interne est constatée.

Remarque

Dans ce cas, veuillez informer notre support technique et envoyez-lui les données indiquées dans l'email. Le fichier concerné doit aussi être envoyé pour contrôle.

Éditer

Avec le bouton *Editer* ouvrez la fenêtre *Modèle d'email*, où vous pouvez configurer le message pour l'événement « Erreur critique dans Guard ». Vous avez la possibilité d'entrer du texte pour l'objet et le message de l'email. A cet effet, vous pouvez utiliser des variables (voir Configuration::Généralités::Avertissements::Email::Modèle d'email).

Destinataire(s)

Dans ce champ, saisissez l'adresse email du ou des destinataire(s). Les adresses sont séparées par des virgules. La longueur maximale de toutes les adresses (la totalité de la chaîne de caractères donc) est de 260 caractères.

Scanner

La recherche directe, c'est-à-dire à la demande, peut envoyer des avertissements par email à un ou plusieurs destinataires lors de certains événements.

Scanner

Activer les avertissements email

Si cette option est activée, le programme envoie des messages email avec les principales données lorsqu'un événement défini se produit. Cette option est désactivée par défaut.

Notification par email lors des événements suivants

Lors de la recherche, un résultat positif est annoncé.

Si cette option est activée, vous recevez un email avec le nom du virus ou du programme indésirable du fichier concerné à chaque fois que la recherche en temps réelle trouve un virus ou un programme indésirable.

Éditer

Avec le bouton *Editer*, ouvrez la fenêtre *Modèle d'email*, où vous pouvez configurer le message pour l'événement « Détection lors de recherche ». Vous avez la possibilité d'entrer du texte pour l'objet et le message de l'email. A cet effet, vous pouvez utiliser des variables (voir Configuration::Généralités::Avertissements::Email::Modèle d'email).

Fin d'une recherche planifiée.

Si l'option est activée, un email est envoyé lorsque la tâche de contrôle a été exécutée. L'email contient les données concernant l'heure et la durée de la recherche, les répertoires et fichiers contrôlés ainsi que les virus détectés et les avertissements.

Éditer

Avec le bouton *Editer*, ouvrez la fenêtre *Modèle d'email*, où vous pouvez configurer le message pour l'événement « Fin de recherche ». Vous avez la possibilité d'entrer du texte pour l'objet et le message de l'email. A cet effet, vous pouvez utiliser des variables (voir Configuration::Généralités::Avertissements::Email::Modèle d'email).

Ajouter le fichier de rapport en pièce jointe

Si l'option est activée, lors de l'envoi de notifications scanner, le fichier de rapport actuel du composant scanner est ajouté comme pièce jointe à l'email.

Adresse du ou des destinataire(s)

Dans ce champ, saisissez l'adresse email du ou des destinataire(s). Les adresses sont séparées par des virgules. La longueur maximale de toutes les adresses (la totalité de la chaîne de caractères donc) est de 260 caractères.

Updater

Le composant Updater peut envoyer des messages par email à un ou plusieurs destinataires lors de certains événements.

Updater

Avertissements email

Si l'option est activée, la mise à jour composant envoie des messages emails avec les principales données quand un événement particulier se produit. Cette option est désactivée par défaut.

Notifications par email lors des événements suivants

Aucune mise à jour nécessaire. Votre programme est à jour.

Si l'option est activée, un email est envoyé quand l'Updater a réussi à établir une connexion au serveur de téléchargement, mais qu'aucun nouveau fichier n'est disponible sur le serveur. Cela signifie que votre programme AntiVir est actuel.

Éditer

Avec le bouton *Editer*, ouvrez la fenêtre *Modèle d'email*, où vous pouvez configurer le message pour l'événement « Pas de mise à jour nécessaire ». Vous avez la possibilité d'entrer du texte pour l'objet et le message de l'email. A cet effet, vous pouvez utiliser des variables (voir Configuration::Généralités::Avertissements::Email::Modèle d'email).

La mise à jour a réussi. De nouveaux fichiers ont été installés.

Si l'option est activée, un email est envoyé au moment des mises à jour : il peut s'agir d'une mise à jour du produit ou d'une actualisation du fichier de définitions des virus ou du moteur de recherche.

Éditer

Avec le bouton *Editer*, ouvrez la fenêtre *Modèle d'email*, où vous pouvez configurer le message pour l'événement « Mise à jour installation de nouveaux fichiers réussie ». Vous avez la possibilité d'entrer du texte pour l'objet et le message de l'email. A cet effet, vous pouvez utiliser des variables (voir Configuration::Généralités::Avertissements::Email::Modèle d'email).

La mise à jour a réussi. Une nouvelle mise à jour du produit est disponible.

Si l'option est activée, un email est envoyé uniquement lorsqu'une actualisation du fichier de définitions des virus ou du moteur de recherche a été effectuée sans mise à jour du produit, mais qu'une mise à jour du produit est disponible.

Éditer

Avec le bouton *Editer*, ouvrez la fenêtre *Modèle d'email*, où vous pouvez configurer le message pour l'événement « Mise à jour réussie - mise à jour de produit disponible ». Vous avez la possibilité d'entrer du texte pour l'objet et le message de l'email. A cet effet, vous pouvez utiliser des variables (voir Configuration::Généralités::Avertissements::Email::Modèle d'email).

La mise à jour a échoué.

Si l'option est activée, un email est envoyé si la mise à jour a échoué en raison d'une erreur.

Éditer

Avec le bouton *Editer*, ouvrez la fenêtre *Modèle d'email*, où vous pouvez configurer le message pour l'événement « Echec de la mise à jour ». Vous avez la possibilité d'entrer du texte pour l'objet et le message de l'email. A cet effet, vous pouvez utiliser des variables (voir Configuration::Généralités::Avertissements::Email::Modèle d'email).

Ajouter le fichier de rapport en pièce jointe

Si l'option est activée, lors de l'envoi de notifications Updater, le fichier de rapport actuel du composant Updater est ajouté comme pièce jointe à l'email.

Destinataire(s)

Dans ce champ, saisissez l'adresse email du ou des destinataire(s). Les adresses sont séparées par des virgules. La longueur maximale de toutes les adresses (la totalité de la chaîne de caractères donc) est de 260 caractères.

Remarque

Lors des événements suivants, des messages d'avertissement sont toujours envoyés par email, si un serveur SMTP et une adresse destinataire ont été configurés pour des notifications Updater :
Une mise à jour du produit est nécessaire pour chacune des futures actualisations du programme.
Une actualisation du fichier de définitions des virus ou du moteur de recherche n'a pas pu être effectuée, car une mise à jour du produit est nécessaire.

L'envoi de ces messages d'avertissement est effectué indépendamment de vos réglages d'avertissements par email du composant de mise à jour.

Modèle d'email

Dans la fenêtre *Modèle d'email*, vous configurez les notifications par email des différents composants pour les événements activés. Vous pouvez entrer un texte de128 signes maximum dans la ligne d'objet et un texte de 1 024 signes maximum dans le champ de message.

Les variables suivantes peuvent être utilisées dans l'objet email et dans le message email.

Variables globalement valables

Variable	Valeur
Variables d'environnement Windows	Le composant des notifications par email prend en charge toutes les variables d'environnement Windows.
%SYSTEM_IP%	Adresse IP de l'ordinateur
%FQDN%	Nom de domaine au complet (fully qualified domain name)
%TIMESTAMP%	Horodatage de l'événement : Les formats de temps et de date correspondent aux réglages de langue du système d'exploitation
%COMPUTERNAME%	Nom de l'ordinateur NetBIOS
%USERNAME%	Nom de l'utilisateur qui accède au composant
%PRODUCTVER%	Version du produit
%PRODUCTNAME%	Nom du produit
%MODULENAME%	Nom du composant qui envoie l'email
%MODULEVER%	Version du composant qui envoie l'email

Variables spécifiques des composants

Variable	Valeur	Emails des composants
%ENGINEVER%	Version du moteur de recherche utilisé	Guard Scanner
%VDFVER%	Version du fichier de définition des virus utilisé	Guard Scanner
%SOURCE%	Nom de fichier entièrement qualifié	Guard
%VIRUSNAME%	Nom du virus ou du programme indésirable	Guard
%ACTION%	Action exécutée après la découverte	Guard
%MACADDR%	Adresse MAC de la première carte réseau enregistrée	Guard
%UPDFILESLIST%	Liste des fichiers actualisés	Updater
%UPDATETYPE%	Type de mise à jour : Mise à jour de moteur	Updater

	de recherche et de fichier de définitions des virus ou mise à jour du produit avec actualisation de moteur de recherche et fichier de définitions des virus.	
%UPDATEURL%	URL du serveur de téléchargement utilisé pour la mise à jour	Updater
%UPDATE_ERROR%	Erreur de mise à jour en mots	Updater
%DIRCOUNT%	Nombre de répertoires contrôlés	Scanner
%FILECOUNT%	Nombre de fichiers contrôlés	Scanner
%MALWARECOUNT%	Nombre de virus ou de programmes indésirables trouvés	Scanner
%REPAIREDCOUNT%	Nombre de fichiers réparés concernés	Scanner
%RENAMEDCOUNT%	Nombre de fichiers concernés renommés	Scanner
%DELETEDCOUNT%	Nombre de fichiers concernés supprimés	Scanner
%WIPECOUNT%	Nombre de fichiers concernés qui ont été écrasés et supprimés	Scanner
%MOVEDCOUNT%	Nombre de fichiers concernés qui ont été déplacés en quarantaine	Scanner
%WARNINGCOUNT%	Nombre d'avertissements	Scanner
%ENDTYPE%	Etat de la recherche : interrompue | terminée avec succès	Scanner
%START_TIME%	Heure de démarrage de la recherche Heure de début de la mise à jour	Scanner Updater
%END_TIME%	Fin de la recherche : Fin de la mise à jour	Scanner Updater
%TIME_TAKEN%	Durée d'exécution de la recherche en minutes Durée d'exécution de l'actualisation en	Scanner Updater

	minutes	
%LOGFILEPATH%	Chemin et nom de fichier du fichier de rapport	Scanner Updater

12.8.7.3. Avertissements acoustiques

Avertissement acoustique

En cas de détection d'un virus ou d'un logiciel malveillant par le scanner ou le Guard, un bip d'avertissement retentit dans le mode d'action interactif. Vous avez la possibilité de désactiver ou d'activer 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 si résultat positif. Le mode d'action du Guard se règle dans la configuration sous Guard::Recherche::Action si 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.

Prévenir via les enceintes 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 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.

Tester

Ce bouton sert à tester le fichier Wave sélectionné.

12.8.7.4. Avertissements

Votre programme AntiVir 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 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.

12.8.8 Événements

Limiter la taille de la base de données des 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 dépassée, les saisies les plus anciennes sont supprimées.

Supprimer tous les événements de plus de n jour(s)

Si cette option est activée, les événements sont supprimés de la base de données d'événements après un certain nombre de jours ; les valeurs autorisées sont : 1 à 90 jours. Cette option est activée par défaut avec une valeur de 30 jours.

Ne pas limiter la taille de la base de données (supprimer les événements manuellement)

Si l'option est activée, la taille de la base de données n'est pas limitée. Toutefois, 20 000 entrées au maximum sont affichées à la surface programme sous événements.

12.8.9 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 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.

Edition du 3er trimestre 2011.

AVIRA

live *free.*™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
L'Allemagne

Téléphone: +49 7542-500 0
Fax: +49 7542-500 3000
Internet: www.avira.com