Avira Free Antivirus

Manuel de l'utilisateur

AVIRA

Marques et copyright

Marques

Windows est une marque déposée de Microsoft Corporation aux États-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 ne signifie pas qu'elles peuvent être utilisées librement.

Remarques concernant le copyright

Des codes de fournisseurs tiers ont été utilisés pour Avira Free Antivirus. 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 Free Antivirus sous "Third Party Licenses".

Sommaire

1. Introduction

Avec votre produit Avira, protégez votre ordinateur contre les virus, vers, chevaux de Troie, logiciels publicitaires et espions, et de tout autre risque. Ce manuel aborde de manière simplifiée les virus ou logiciels malveillants (logiciels dommageables) ainsi que les programmes indésirables.

Le manuel décrit l'installation et l'utilisation du programme.

Sur notre page Web, vous pouvez utiliser les différentes options et autres solutions d'informations :

http://www.avira.com/fr

Sur le site Web d'Avira, vous pouvez :

- accéder aux informations concernant les autres programmes de bureau Avira
- télécharger les derniers programmes de bureau d'Avira
- télécharger les derniers manuels des produits au format PDF
- télécharger les outils de support et de réparation gratuits
- utiliser la vaste base de connaissances et les articles FAQ détaillés pour la résolution des problèmes
- accéder aux coordonnées du support en fonction des pays.

Votre équipe Avira

1.1 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 produit Avira.

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. zone de fenêtre ou message d'erreur).
Gras	Éléments de l'interface logicielle sur lesquels vous cliquez (par ex. option de menu, rubrique, champ d'option ou bouton).

2. Informations produit

Ce chapitre vous donne toutes les informations importantes pour l'acquisition et l'utilisation de votre produit Avira :

- voir le chapitre : Prestations
- voir le chapitre : Configuration minimale
- voir le chapitre : Attribution de licence et mise à niveau

Les produits Avira proposent des outils complets et flexibles pour protéger votre ordinateur de manière fiable contre les virus, logiciels malveillants, programmes indésirables et autres dangers.

▸ Attention :

Avertissement
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 100 % de la perte de données. Effectuez régulièrement des copies de sauvegarde (back-up) 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 à jour. Assurez-vous de l'actualité de votre produit Avira grâce à des mises à jour automatiques. Configurez le programme en conséquence.

2.1 Prestations

Votre produit Avira 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.
- Protection temps réel (On-Access Scan) pour la surveillance permanente de tous les accès aux données

- La barre d'outils SearchFree d'Avira, une barre de recherche intégrée au navigateur Web vous permettant de faire des recherches rapidement et confortablement sur Internet. Elle contient également des widgets pour les principales fonctions d'Internet.
- Protection Web (uniquement pour les utilisateurs d'Avira Free Antivirus disposant de la barre d'outils SearchFree d'Avira) pour la vérification des données et fichiers transmis depuis Internet par protocole HTTP (surveillance des ports 80, 8080, 3128)
- Avira Free Android Security est une application visant à protéger contre le vol et/ou la perte. L'application propose des fonctions permettant de retrouver l'appareil mobile si vous l'avez perdu ou pire, s'il a été volé. En outre, elle peut bloquer des appels entrants ou SMS. Avira Free Android Security protège les téléphones mobiles et smartphones fonctionnant avec le système d'exploitation Android.
- Gestion de quarantaine intégrée pour l'isolation et le traitement des fichiers suspects
- Protection Rootkits pour identifier les logiciels malveillants installés de façon dissimulée sur le système de l'ordinateur (Rootkits) (non 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 fichiers de 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
- Planificateur intégré pour la définition de 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)

2.2 Configuration minimale du système

La configuration minimale suivante s'applique :

- Processeur Pentium et plus, au moins 1 GHz
- Système d'exploitation
  - Windows XP, dernier SP (32 ou 64 bits) ou
  - Windows Vista, dernier SP (32 ou 64 bits) ou
  - Windows 7, dernier SP (32 ou 64 bits)

Remarque
Veuillez noter que notre logiciel n'est pas encore compatible avec Windows 8.

- 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)
- 512 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)

Barre d'outils SearchFree d'Avira

- Système d'exploitation
  - Windows XP, dernier SP (32 ou 64 bits) ou
  - Windows Vista, dernier SP (32 ou 64 bits) ou
  - Windows 7, dernier SP (32 ou 64 bits)
- Navigateur Web
  - Windows Internet Explorer 6.0 ou ultérieur
  - Mozilla Firefox 3.0 ou ultérieur
  - Google Chrome 18.0 ou ultérieur

Remarque
Veuillez désinstaller les barres de recherche éventuellement déjà installées avant l'installation de la barre d'outils Avira SearchFree. Autrement, il sera impossible d'installer la barre d'outils SearchFree d'Avira.

Consignes pour les utilisateurs de Windows Vista

Sous Windows XP, de nombreux utilisateurs travaillent avec des droits d'administrateur. Ceci n'est toutefois pas souhaitable pour des raisons de sécurité, car les virus et programmes indésirables peuvent plus facilement s'immiscer dans l'ordinateur.

Pour cette raison, Microsoft introduit avec Windows Vista le contrôle des comptes d'utilisateurs (User Account Control). Cette fonction offre plus de protection aux utilisateurs connectés en tant qu'administrateur : un administrateur sous Windows Vista dispose par défaut uniquement des privilèges d'un utilisateur normal. Les actions pour lesquelles des droits d'administrateur sont nécessaires sont repérées par une icône par Windows Vista. En outre, l'utilisateur doit confirmer l'action souhaitée. Ce n'est qu'après avoir donné son

accord que des privilèges plus importants sont octroyés et que le système d'exploitation exécute la tâche administrative en question.

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

2.3 Attribution de licence et mise à niveau

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

La licence est octroyée via une clé de licence numérique sous la forme d'un fichier *.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 e-mail si vous avez acheté votre produit Avira sur Internet ou se trouve sur le CD/DVD du programme.

3. Installation et désinstallation

Dans ce chapitre, vous trouverez des informations sur l'installation et la désinstallation de votre produit Avira :

- voir le chapitre : Avant l'installation : configuration requise, préparation de l'ordinateur à l'installation
- voir le chapitre : Installation express : installation standard selon le paramétrage par défaut
- voir le chapitre : Installation personnalisée : installation configurable
- voir le chapitre : Assistant de configuration
- voir le chapitre : Installation modifiée
- voir le chapitre : Modules d'installation
- voir le chapitre : Désinstallation : procéder à la désinstallation

3.1 Types d'installation

Pendant l'installation, vous pouvez choisir un type de configuration dans l'assistant d'installation :

Express

- Les fichiers de programme sont installés dans un répertoire par défaut sous *C:\Program Files*.
- Votre produit Avira 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 chapitre Installation et désinstallation > Module d'installation).
- Vous pouvez sélectionner un répertoire de destination pour les fichiers de programme à installer.
- Vous pouvez décider si un raccourci doit être créé sur votre Bureau et/ou un groupe de programmes doit être intégré dans le menu démarrer.
- À l'aide de l'assistant de configuration, vous pouvez procéder à des paramétrages personnalisés de votre produit Avira et effectuer un rapide contrôle du système directement après l'installation.

3.2 Avant l'installation

Remarque
Avant de procéder à l'installation, vérifiez si votre ordinateur affiche la configuration minimale requise. Si tel est le cas, vous pouvez installer le produit Avira.

Remarque
En cas d'installation sur un système d'exploitation de serveur, la protection temps réel et la protection des fichiers ne sont pas disponibles.

Initialisation avant l'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 entrer en conflit.
  - ↪ Le produit Avira va parcourir votre système pour détecter d'éventuels programmes incompatibles.
  - ↪ Si le produit identifie des logiciels incompatibles, il génère la liste de ces programmes.
  - ↪ Nous vous recommandons de désinstaller les programmes compromettant la sécurité de votre ordinateur.
- ▸ Dans cette liste, sélectionnez les programmes devant être supprimés automatiquement de votre ordinateur et cliquez sur **Suivant**.
- ▸ Certains programmes ne peuvent être supprimés que manuellement de votre ordinateur. Sélectionnez les programmes et cliquez sur **Suivant**.
  - ↪ La désinstallation d'un ou plusieurs programmes nécessite le redémarrage de l'ordinateur. L'installation se poursuit après le redémarrage.

Attention
Votre ordinateur est sans protection jusqu'à la finalisation de la procédure d'installation du produit Avira.

Installation

Le programme d'installation fonctionne en mode de dialogue auto-explicatif. Lors des nombreuses étapes d'installation, un simple clic suffit pour continuer.

.
Les principaux boutons disposent des fonctions suivantes :

- **OK** : confirmer l'action.
- **Annuler** : abandonner l'action.
- **Suivant** : passer à l'étape suivante.
- **Retour** : revenir à l'étape précédente.

▸ 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 définition des virus à jour par le biais du programme d'installation (en cas d'installation à partir d'Internet)
- Si nécessaire, exécution d'une mise à jour une fois l'installation terminée

Remarque
Installation à partir d'Internet :
pour une installation à partir d'Internet, vous disposez d'un programme d'installation qui charge les fichiers programme actuels à partir serveurs Web Avira avant l'exécution de l'installation. Cette procédure garantit que votre produit Avira est installé avec un fichier de définition des virus à jour.

Installation avec un pack d'installation :
le pack d'installation contient le programme d'installation et tous les fichiers programme nécessaires. Cependant, lors d'une installation à l'aide d'un pack d'installation, il n'y pas possibilité de sélection de la langue pour le produit Avira. Il est recommandé, à l'issue de l'installation, d'effectuer une mise à jour afin d'actualiser le fichier de définition des virus.

3.3 Installation express

Pour installer votre produit Avira, procédez de la façon suivante :

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

Installation à partir d'un téléchargement Internet

↪ La fenêtre de dialogue **Bienvenue** s'affiche.

▸ Cliquez sur **Suivant** 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 produit Avira 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 à partir des serveurs Web Avira. Une fois le téléchargement terminé, la fenêtre **Téléchargement** se referme.

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

↳ La fenêtre **Installation en cours de préparation** s'affiche.

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

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

Remarque
L'**installation express**, avec laquelle les composants standard sont installés sans possibilités de configuration, est activée par défaut. Si vous souhaitez effectuer une **Installation personnalisée**, consultez la section : Installation > Installation personnalisée.

- Confirmez que vous acceptez **l'accord de licence utilisateur final**. Pour consulter les détails de l'accord de licence, cliquez sur le lien correspondant.
- Cliquez sur **Suivant**.

  ↳ La fenêtre **Rejoignez les millions d'utilisateurs qui utilisent déjà Avira SearchFree** s'affiche.
- Si vous ne souhaitez pas installer la barre d'outils SearchFree d'Avira, désactivez les cases de l'**accord de licence** de la barre d'outils SearchFree d'Avira et de l'Avira SearchFree Updater, puis désactivez **Avira SearchFree (search.avira.com)** comme page de démarrage.

Remarque
Veuillez désinstaller, si nécessaire, les barres de recherche avant l'installation de la barre d'outils Avira SearchFree. Dans le cas contraire, l'installation de la barre d'outils SearchFree d'Avira sera impossible.

- Cliquez sur **Suivant**.

  ↳ L'*assistant de licence* s'ouvre et vous aide lors de l'activation de votre programme.

  ↳ Ici, vous pouvez configurer un serveur proxy.

  ↳ La progression de l'installation est représentée par une barre verte.

  ↳ Cliquez sur **Terminer** pour finaliser l'installation et quitter le programme d'installation.

  ↳ L'icône programme Avira est intégrée dans la barre des tâches.

  ↳ Le module **Updater** recherche les mises à jour éventuelles pour optimiser la protection de votre ordinateur.

↳ La fenêtre d'état **Luke Filewalker** s'affiche pour lancer une première recherche directe du scanner, vous informe de l'état de la vérification et vous affiche les résultats.

- Si une fois le contrôle du système effectué, vous êtes invité à relancer l'ordinateur, procédez au redémarrage pour que votre système soit intégralement protégé.

3.4 Installation personnalisée

Pour installer votre produit Avira, procédez de la façon suivante :

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

Installation à partir d'un téléchargement Internet

↳ La fenêtre de dialogue **Bienvenue** s'affiche.

- Cliquez sur **Suivant** 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 produit Avira 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 à partir des serveurs Web Avira. Une fois le téléchargement terminé, la fenêtre **Téléchargement** se referme.

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

↳ La fenêtre **Installation en cours de préparation** s'affiche.

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

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

Remarque
Par défaut, l'**Installation express**, avec laquelle les composants standard sont installés sans possibilité de configuration, est définie par défaut. Si vous souhaitez procéder à cette installation, consultez la section : Installation > Installation express.

- Sélectionnez le type d'installation **Personnalisé**.
- Confirmez que vous acceptez **l'accord de licence utilisateur final**. Pour consulter les détails de l'accord de licence, cliquez sur le lien correspondant.
- Cliquez sur **Suivant**.

↳ La fenêtre **Rejoignez les millions d'utilisateurs qui utilisent déjà SearchFree d'Avira** s'affiche.

- Si vous ne souhaitez pas installer la barre d'outils SearchFree d'Avira, désactivez les cases de l'**accord de licence** de la barre d'outils SearchFree d'Avira et de l'Avira SearchFree Updater, puis désactivez **Avira SearchFree (search.avira.com)** comme page de démarrage.

> **Remarque**
> Le cas échéant, désinstallez les barres de recherche déjà installées avant l'installation de la barre d'outils SearchFree d'Avira. Dans le cas contraire, l'installation de la barre d'outils SearchFree d'Avira sera impossible.

- Cliquez sur **Suivant**.
  - ↪ La fenêtre **Sélectionner le répertoire d'installation** s'affiche.
  - ↪ Le répertoire *C:\Program Files\Avira\AntiVir Desktop* est paramétré par défaut
- Cliquez sur **Suivant** pour poursuivre l'installation.

  - OU -

  Avec **Parcourir**, choisissez un autre répertoire de destination et confirmez avec **Suivant**.
  - ↪ La boîte de dialogue **Installer les composants** s'affiche.
- Activez ou désactivez les composants souhaités et confirmez avec **Suivant**.
- Dans la boîte de dialogue suivante, vous pouvez décider si un raccourci doit être créé sur votre Bureau et/ou un groupe de programmes dans le menu démarrer.
- Cliquez sur **Suivant**.
- Une fois la procédure d'installation terminée, fermez l'installation en cliquant sur **Terminer**.
  - ↪ L'assistant d'installation se ferme et l'assistant de configuration s'ouvre.

3.5 Assistant de configuration

En cas d'installation personnalisée, l'assistant de configuration s'ouvre. Vous pouvez effectuer des réglages importants dans l'assistant de configuration pour votre produit Avira.

- Dans la fenêtre de bienvenue de l'assistant de configuration, cliquez sur **Suivant** pour commencer la configuration du programme.
  - ↪ Dans la fenêtre de dialogue **Configurer AHeAD**, vous pouvez choisir un degré d'identification pour la technologie AHeAD. Le degré d'identification choisi est repris pour le paramétrage de la technologie AHeAD du scanner (recherche directe) et de la protection temps réel (recherche en temps réel).
- Choisissez un degré d'identification et poursuivez la configuration avec **Suivant**.

↳ Dans la boîte de dialogue **Sélectionner des catégories de dangers étendues** suivante, vous pouvez adapter les fonctions de protection de votre produit Avira avec la sélection des catégories de dangers.

- Le cas échéant, sélectionnez des catégories de dangers supplémentaires et poursuivez la configuration en cliquant sur **Suivant**.

  ↳ Si vous avez choisi le module d'installation Protection temps réel Avira, la boîte de dialogue **Mode de démarrage de la protection temps réel** s'affiche. Vous pouvez définir le moment du démarrage de la protection temps réel. La protection temps réel démarre dans le mode de démarrage indiqué, à chaque redémarrage de l'ordinateur.

Remarque
Le mode de démarrage indiqué de la protection temps réel est consigné dans le Registre et ne peut pas être modifié par la configuration.

Remarque
Au démarrage de l'ordinateur, la sélection du mode de démarrage par défaut pour la protection temps réel (démarrage normal) et une connexion rapide au compte utilisateur évite, notamment, le scannage des programmes démarrant automatiquement, dans la mesure où ceux-ci sont démarrés avant le chargement complet de la protection temps réel.

- Activez l'option souhaitée et poursuivez la configuration avec **Suivant**.

  ↳ La boîte de dialogue suivante **Contrôle du système** permet d'activer ou de désactiver l'exécution d'un contrôle rapide du système. Ce rapide 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 **Contrôle rapide du système** et poursuivez la configuration avec **Continuer**.

  ↳ La boîte de dialogue suivante vous permet de finaliser la configuration avec **Terminer**.

  ↳ Les réglages indiqués et sélectionnés sont validés.

  ↳ Si vous avez activé l'option **Contrôle rapide du système**, la fenêtre **Luke Filewalker** s'ouvre. Le scanner effectue un contrôle rapide du système.

  ↳ Si, une fois le contrôle du système effectué, vous êtes invité à relancer l'ordinateur, procédez au redémarrage pour que votre système soit intégralement protégé.

Une fois l'installation réussie, il est recommandé de vérifier dans la zone **État** si le programme de protection est à jour.

- Si votre produit Avira vous indique que votre ordinateur n'est pas totalement protégé, cliquez sur **Résoudre le problème**.
  - ↪ La boîte de dialogue **Restaurer la protection** s'ouvre.
- Optimisez la sécurité de votre système en activant les options prescrites.
- Effectuez ensuite un contrôle intégral du système le cas échéant.

3.6 Installation modifiée

Vous avez la possibilité d'ajouter ou de supprimer certains composants de programmes de l'installation actuelle du produit Avira (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** dans le **Panneau de configuration Windows** pour **Modifier/Supprimer** des programmes.

Sélectionnez votre produit Avira et cliquez sur **Modifier**. Dans la boîte de dialogue *Bienvenue* du programme, sélectionnez l'option **Modifier le programme**. Le système vous guide pas à pas pour procéder à l'installation modifiée.

Remarque
Si vous désinstallez la barre d'outils SearchFree d'Avira, la protection Web est également désinstallée.

3.7 Modules d'installation

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

- **Avira Free Antivirus**
  Ce module contient tous les composants nécessaires à l'installation réussie de votre produit Avira.
- **Protection temps réel**
  La protection temps réel Avira fonctionne en arrière-plan. Elle surveille et répare si possible les fichiers lors d'opérations comme l'ouverture, l'écriture ou la copie en temps réel (On-Access = à l'accès). Si un utilisateur effectue une opération sur un fichier (chargement, exécution, copie), le produit Avira contrôle automatiquement le fichier. Lors de l'opération Renommer, la protection temps réel d'Avira n'effectue aucune recherche.
- **Protection Rootkits**
  La Protection Rootkits Avira contrôle si un logiciel, qui ne peut être détecté par les méthodes habituelles après infiltration dans votre système, s'est déjà installé sur votre ordinateur.

- **Protection Web** (pour les utilisateurs d'Avira Free Antivirus uniquement en association avec la barre d'outils SearchFree d'Avira)
  En navigant sur Internet, via votre navigateur Web, vous sollicitez des données à un serveur 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 la Protection temps réel le propose. De cette manière, des virus et programmes indésirables peuvent pénétrer dans votre système. La Protection Web 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 dans les données transférées. Selon la configuration, le programme traite les fichiers concernés automatiquement ou demande à l'utilisateur quelle action entreprendre.
- **Shell Extension**
  Shell Extension génère dans le menu contextuel de l'explorateur Windows (bouton droit de la souris) l'entrée *Contrôler les fichiers sélectionnés avec Avira*. Avec cette entrée, vous pouvez scanner directement certains fichiers ou répertoires.

3.8 Désinstallation

Pour supprimer votre produit Avira de votre ordinateur, vous pouvez utiliser l'option **Logiciel** pour **Modifier ou supprimer** des programmes dans le Panneau de configuration Windows.

Pour désinstaller votre produit Avira, procédez de la façon suivante (sur l'exemple de Windows 7) :

- Ouvrez le **Panneau de configuration** via le menu **Démarrer** de Windows.
- Double-cliquez sur **Programmes et fonctionnalités**.
- Sélectionnez votre produit Avira dans la liste et cliquez sur **Désinstaller**.
  - ↳ Le système vous demande si vous souhaitez réellement supprimer le programme.
- Confirmez avec **Oui**.
  - ↳ Tous les composants du programme sont supprimés.
- Cliquez sur **Terminer** pour terminer la désinstallation.
  - ↳ Une fenêtre de dialogue peut s'afficher vous conseillant de redémarrer l'ordinateur.
- Confirmez avec **Oui**.
  - ↳ Le produit Avira 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.

Remarque
La barre d'outils SearchFree d'Avira n'est pas intégrée dans la désinstallation du programme, mais doit être désinstallée de façon individuelle en reproduisant la procédure ci-dessus. Pour ce faire, la barre d'outils SearchFree d'Avira doit être désactivée dans le gestionnaire de modules complémentaires. Une fois la désinstallation achevée, la barre de recherche n'est plus intégrée dans votre navigateur.

Remarque
Si vous désinstallez la barre d'outils SearchFree d'Avira, la protection Web est également désinstallée.

4. Aperçu d'Avira Free Antivirus

Dans ce chapitre, vous obtenez une vue d'ensemble des fonctionnalités et de l'utilisation de votre produit Avira.

- voir le chapitre Interface et utilisation
- voir le chapitre Barre d'outils SearchFree d'Avira
- voir le chapitre Comment procéder

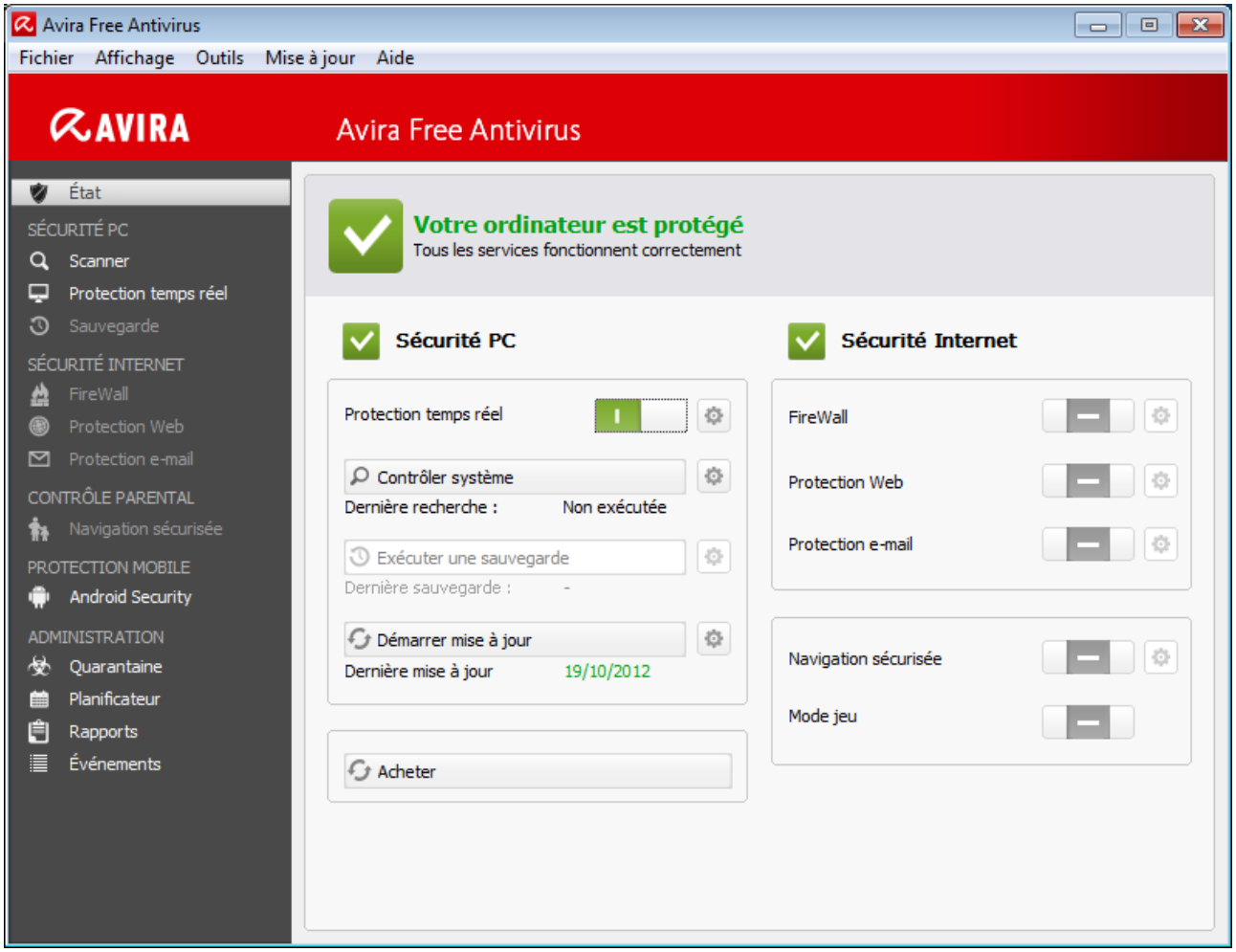
4.1 Interface et commande

L'utilisation de votre produit Avira se fait via trois éléments d'interface du programme :

- Control Center : surveillance et gestion du produit Avira
- Configuration : configuration du produit Avira
- Icône de programme dans la zone de notification de la barre des tâches : ouverture du Control Center et d'autres fonctions

4.1.1 Control Center

Le Control Center sert à vérifier l'état de protection de votre ordinateur, à gérer et utiliser les composants de protection et les fonctions de votre produit Avira.



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

- **Barre de menu :** dans les menus du Control Center, vous pouvez accéder aux fonctions générales du programme et à des informations sur le produit.
- **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 : champ d'action *Sécurité PC* - Rubrique **Protection temps réel**.
- **État :** l'écran de démarrage **État** vous indique immédiatement si votre ordinateur est suffisamment protégé, ainsi que les modules actifs, la date de la dernière sauvegarde et le dernier contrôle du système. La fenêtre **État** comprend tous les boutons de fonctions ou d'actions, comme l'activation ou la désactivation de la **Protection temps réel**.

Démarrage et arrêt du Control Center

Vous disposez des options 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 commande de votre produit Avira.

Vous quittez le Control Center via la commande de menu **Quitter** dans le menu **Fichier**, avec la commande clavier **Alt+F4** ou en cliquant sur la croix de fermeture dans Control Center.

Utilisation du Control Center

Voici comment naviguer dans le Control Center :

- Cliquez dans la barre de navigation sur un champ d'action sous une rubrique.
  - ↪ Le champ d'action apparaît avec les autres options de fonctions et de configuration dans la fenêtre de détail.
- Cliquez, le cas échéant, sur un autre champ pour les afficher dans la fenêtre de détail.

> **Remarque**
> La navigation au clavier dans la barre des menus s'active avec la touche [**Alt**]. La touche **Entrée** vous permet d'activer la rubrique sélectionnée.
> Pour ouvrir, fermer des menus dans le Control Center, ou naviguer dans les menus, vous pouvez également utiliser des raccourcis clavier : [**Alt**] + 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 :

- Sélectionnez les données ou objets que vous souhaitez traiter.

  Pour sélectionner plusieurs éléments, maintenez la touche **Ctrl** ou **Shift** (sélection d'éléments situés les uns sous les autres) enfoncée 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

- **État** : l'écran de démarrage **État** présente toutes les rubriques vous permettant de surveiller les fonctionnalités du programme (voir État).
  - La fenêtre **État** permet de visualiser rapidement les modules actifs et d'avoir des informations sur la dernière mise à jour effectuée.
- *SÉCURITÉ PC* : vous trouverez les composants vous permettant de contrôler l'absence de virus et de logiciels malveillants dans les fichiers de votre système informatique.
  - La rubrique **Contrôler** vous permet de configurer et de démarrer simplement la recherche directe (voir Scanner). Les profils prédéfinis permettent d'effectuer une

recherche avec des options par défaut adaptées. À l'aide de la sélection manuelle (qui est enregistrée) , vous pouvez également adapter la recherche de virus et de programmes indésirables à vos besoins personnels.

- *SÉCURITÉ INTERNET* : vous trouverez ici les composants vous permettant de protéger votre ordinateur contre les virus et logiciels malveillants provenant d'Internet et les accès réseau indésirables.

  - La rubrique Protection Web vous fournit des informations sur les URL contrôlées et les virus trouvés, ainsi que d'autres données statistiques qu'il est possible de réinitialiser à tout moment et vous permet d'afficher le fichier de rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles en un clic.

- *CONTRÔLE PARENTAL* : présente les outils permettant une utilisation d'Internet sécurisée pour vos enfants.

- *Administration* : vous trouvez ici des outils vous permettant d'isoler et de gérer les fichiers suspects ou infectés par des virus ainsi que de planifier des tâches récurrentes.

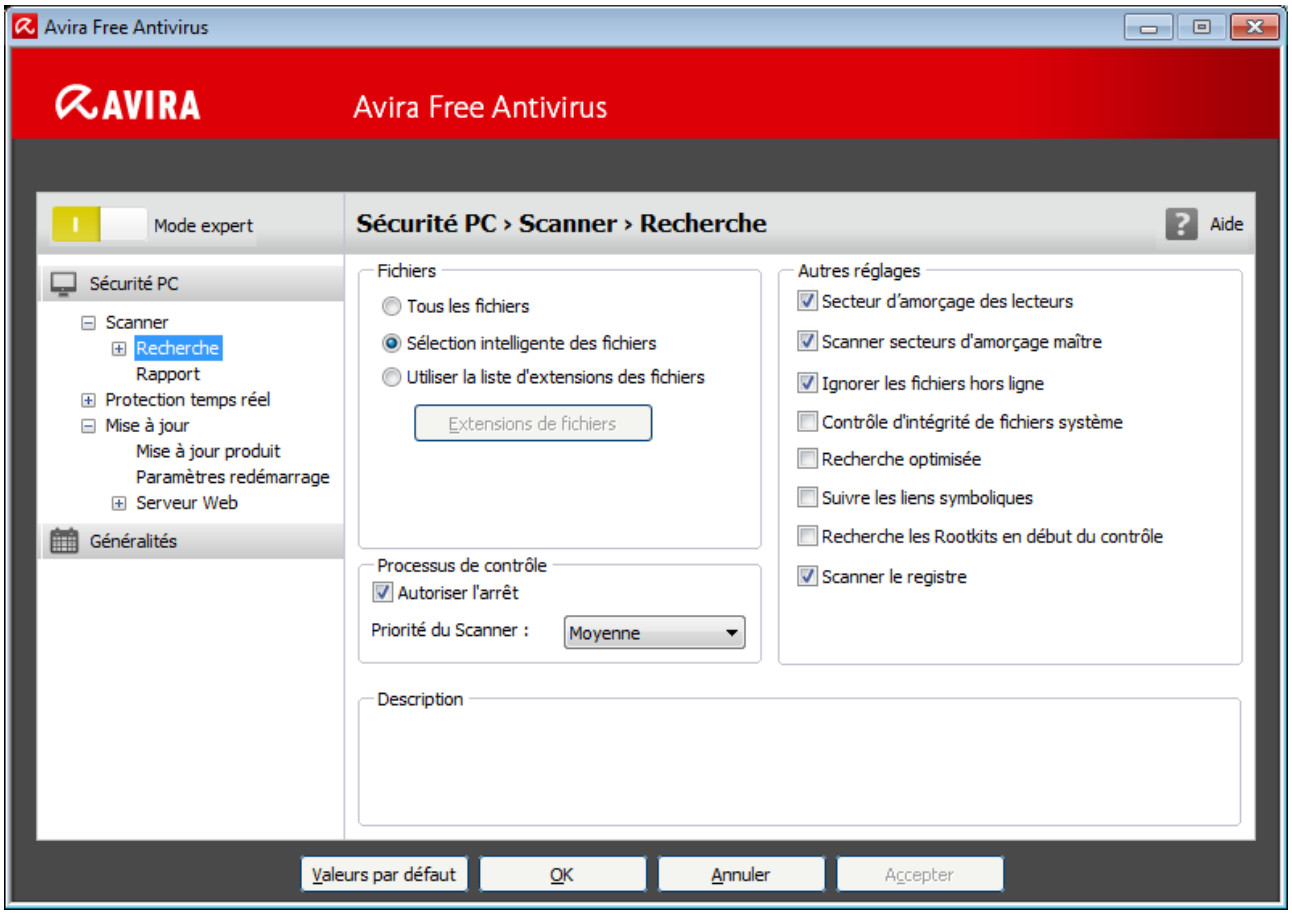
  - Sous la rubrique **Quarantaine** se trouve le gestionnaire de quarantaine. c'est l'emplacement central pour les fichiers déjà en quarantaine ou suspects que vous souhaitez mettre en quarantaine (voir Quarantaine). En outre, vous avez la possibilité d'envoyer un fichier par e-mail à l'Avira Malware Research Center.
  - La rubrique **Planificateur** vous permet de créer des tâches de contrôle et de mise à jour programmées ainsi que des tâches de sauvegarde et d'ajuster ou de supprimer les tâches existantes (voir Planificateur).
  - La rubrique **Rapports** vous permet de visualiser les résultats des actions effectuées (voir Rapports).
  - La rubrique **Événements** vous permet de vous informer sur les événements générés par les modules du programme (voir Résultats).

- *ANDROID* : à partir de cette section, vous serez redirigé vers l'accès en ligne pour les appareils Android.

  - Android Security gère tous vos appareils Android.

4.1.2 Configuration

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



La configuration se présente sous la forme d'une fenêtre de dialogue : les boutons **OK** ou **Valider** vous permettent d'enregistrer les réglages effectués dans la configuration, **Annuler** vous permet d'annuler vos réglages et le bouton **Valeurs par défaut** vous permet de réinitialiser les paramètres de la configuration aux valeurs par défaut. Dans la barre de navigation à 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 de Windows.
- Via le Centre de sécurité Windows - à partir de Windows XP Service Pack 2.
- Via l'icône de commande de votre programme Avira.
- Dans le Control Center via la rubrique Outils > Configuration.
- Dans le Control Center via le bouton Configuration.

Consigne
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, une boîte de dialogue s'affiche vous invitant à activer le **mode expert**.

Gestion 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 agrandir 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 agrandie.

Remarque
Pour activer ou désactiver des options dans la configuration et actionner des boutons, vous pouvez également utiliser les raccourcis clavier : touche [**Alt**] + lettre soulignée dans le nom de l'option ou de la désignation du bouton.

Consigne
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 paramètres dans la configuration :

- Cliquez sur le bouton **OK**.
  - ↪ La fenêtre de configuration se ferme et les paramètres sont validés.

  - OU -

  Cliquez sur le bouton **Valider**.
  - ↪ Les paramètres sont validés. La fenêtre de configuration reste ouverte.

Si vous souhaitez terminer la configuration sans valider vos paramètres :

- Cliquez sur le bouton **Annuler**.
  - ↪ La fenêtre de configuration se ferme et les paramètres sont rejetés.

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

- Cliquez sur **Valeurs par défaut**.

↪ Tous les paramètres de la configuration sont réinitialisés aux valeurs par défaut. Toutes les modifications et vos saisies sont perdues en cas de réinitialisation aux valeurs par défaut.

Aperçu des options de configuration

Vous disposez des options de configuration suivantes :

- **Scanner** : configuration de la recherche directe
  - Options de recherche
  - Action si 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
- **Protection temps réel** : configuration de la recherche en temps réel
  - Options de recherche
  - Action si résultat positif
  - Autres actions
  - Exceptions de la recherche en temps réel
  - Heuristique de la recherche en temps réel
  - Réglage de la fonction de rapport
- **Mise à jour** : configurations des paramètres de mise à jour
  - Réglage des mises à jour produit
  - Paramètres de redémarrage
- **Protection Web** : configuration de la Protection Web
  - Options de recherche, activation et désactivation de la Protection Web
  - Action si résultat positif
  - Accès bloqués : types de fichiers et types MIME indésirables
  - Exceptions de recherche de la protection Web : URL, types de fichiers, types MIME
  - Heuristique de la protection Web
  - Réglage de la fonction de rapport
- **Généralités** :
  - Catégories étendues de dangers pour la recherche directe et en temps réel
  - Filtre d'applications : bloquer ou autoriser des applications
  - Protection par mot de passe pour l'accès au Control Center et à la configuration
  - Sécurité : bloquer les fonctions Autorun, verrouiller les fichiers hôtes Windows, protection du produit
  - WMI : activer la prise en charge WMI
  - Configuration de la documentation des événements
  - Configuration des fonctions de rapport

- Réglage des répertoires utilisés
- Configuration des avertissements sonores en cas de détection de logiciel malveillant

4.1.3 Icône de programme

Après l'installation, l'icône de programme de votre produit Avira s'affiche dans la zone de notification de la barre des tâches :

Symbole	Description
	La Protection temps réel Avira activée
	La Protection temps réel Avira est désactivée

L'icône de programme affiche le statut de la Protection temps réel .

Les fonctions centrales de votre produit Avira sont rapidement accessibles via le menu contextuel de l'icône de programme.

- Pour accéder au menu contextuel, cliquez avec le bouton droit de la souris sur l'icône de programme.

Entrées dans le menu contextuel

- **Activer la Protection temps réel** : active ou désactive la Protection temps réel Avira.
- **Activer la Protection Web** : active ou désactive la Protection Web Avira.
- **Démarrer Avira Free Antivirus** : ouvre le Control Center.
- **Configurer Avira Free Antivirus** : ouvre la configuration.
- **Mes messages** : ouvre le message-bannière avec les derniers messages concernant le produit Avira.
- **Démarrer mise à jour** : démarre une mise à jour.
- **Aide** : ouvre l'aide en ligne.
- **À propos Avira Free Antivirus :** ouvre une boîte de dialogue avec des informations sur votre produit Avira : informations produit, version, licence.
- **Avira sur Internet** : ouvre le portail Web Avira sur Internet. Un accès Internet est nécessaire.

4.2 Barre d'outils SearchFree d'Avira Toolbar

La barre d'outils SearchFree d'Avira comprend deux principaux composants : Avira SearchFree et la barre d'outils.

La nouvelle barre d'outils SearchFree d'Avira s'installe sous la forme de module complémentaire. Lorsque vous accédez la première fois au navigateur (Internet Explorer ou Firefox), un message vous demande si vous acceptez que le programme de barre d'outils SearchFree d'Avira modifie votre navigateur. Vous devez accepter afin de garantir le succès de l'installation de la barre d'outils SearchFree d'Avira.

Avira SearchFree est le nouveau moteur de recherche d'Avira et contient un logo Avira cliquable qui redirige vers le site Web d'Avira, ainsi que des canaux Web, d'images et de vidéos. Il permet aux utilisateurs d'Avira d'effectuer une recherche complète et plus sûre.

La barre d'outils est intégrée à votre navigateur Web et comprend un champ de recherche, un logo Avira redirigeant vers le site Web d'Avira, deux affichages d'état, deux widgets et le menu **Options**.

- Barre de recherche
  Utilisez la barre de recherche pour naviguer sur Internet rapidement et gratuitement à l'aide du moteur de recherche SearchFree d'Avira.
- Affichage d'état
  Les affichages d'état décrivent l'état de protection du navigateur et le statut de mise à jour actuel de votre produit Avira et vous permettent d'identifier les actions à entreprendre pour protéger votre PC.
- Widgets
  Avira vous permet d'accéder directement aux fonctions importantes sur Internet, par exemple vos messages Facebook ou votre messagerie. Vous pouvez également définir la protection de votre système grâce au widget Protection Web (uniquement sur Firefox et Internet Explorer).
- Options
  Le menu Options vous permet d'accéder aux options de barre d'outils, d'effacer l'historique de recherche, de consulter l'aide et les informations concernant la barre d'outils et de désinstaller la barre d'outils SearchFree d'Avira directement à partir du navigateur Web (Firefox et Internet Explorer uniquement).

4.2.1 Utilisation

Barre de recherche

La barre de recherche vous permet de rechercher un ou plusieurs termes sur Internet.

Saisissez à cet effet le terme dans le champ de recherche et cliquez sur la touche **Entrée** ou cliquez sur **Recherche**. L'outil de recherche SearchFree d'Avira parcourt Internet pour vous et affiche tous les résultats dans la fenêtre du navigateur.

Vous pouvez configurer Avira SearchFree à votre guise dans **Options** sur Internet Explorer, Firefox et Chrome.

Affichage d'état

Protection Web

Un message d'état sur la gauche indique les informations concernant la Protection Web d'Avira.

Protection Web

Si vous déplacez le curseur de la souris sur le symbole, le message suivant apparaît : *La Protection Web Avira est active. Votre PC est protégé.*

Aucune action n'est donc requise.

Protection Web

Si vous déplacez le curseur de la souris sur le symbole, le message suivant apparaît : *La Protection Web Avira est désactivée. Contrôler le logiciel Avira pour activer la Protection Web.*

Aucune Protection Web

Si vous déplacez le curseur de la souris sur le symbole, le message suivant apparaît : *Vous n'avez pas installé l'antivirus Avira. Votre ordinateur est exposé à des risques.*

Cela signifie que vous avez désinstallé le produit Avira ou qu'il n'est pas installé correctement.

↪ Vous êtes redirigé sur la page Web d'Avira sur laquelle vous pouvez télécharger le produit Avira.

Non disponible

Si vous vous déplacez sur le symbole avec le curseur de la souris, le message suivant apparaît : *La Protection Web Avira n'est pas disponible. Vérifiez si le logiciel Avira est installé et exécuté sur votre PC afin de vous assurer que votre PC est protégé.*

- Cliquez sur le symbole gris ou sur le texte pour accéder à la page d'aide Avira. Les instructions sur la procédure à suivre y figurent.

Erreur

Si vous vous déplacez sur le symbole avec le curseur de la souris, le message suivant apparaît : *Avira a signalé une erreur.*

- Cliquez sur le symbole gris ou sur le texte pour accéder à la page de Support Avira.

Widgets

La barre d'outils SearchFree d'Avira dispose de 3 widgets avec les principales fonctions d'Internet : Facebook, e-mail et Protection Web.

Facebook

Cette fonction vous permet de recevoir directement les messages Facebook et donc de rester toujours au courant.

E-mail

Si vous cliquez sur le symbole e-mail, une liste déroulante apparaît et vous permet de sélectionner parmi les principales messageries.

Protection Web

Ce widget a été développé par Avira et permet d'accéder très simplement à toutes les options de sécurité Internet. Pour le moment, il n'est disponible qu'avec Firefox et Internet Explorer. Différentes options sont proposées, elles peuvent porter des noms différents selon le navigateur :

- *Blocage des pop-up*

Si cette option est activée, toutes les fenêtres pop-up sont bloquées lorsque vous naviguez sur Internet.

- *Blocage des cookies*

Si cette option est activée, aucun cookie n'est enregistré pendant la navigation.

- *Mode privé (Firefox) / Navigation privée (Internet Explorer)*

Si cette option est activée, vous ne laissez aucune trace lorsque vous naviguez sur Internet. Cette option n'est pas disponible pour Internet Explorer 7 et 8.

- *Supprimer l'historique récent (Firefox) / Supprimer l'historique de navigation (Internet Explorer)*

Cette option vous permet de supprimer toutes les activités Internet actuelles.

Conseiller en sécurité des sites Internet

Le conseiller en sécurité des sites Internet vous propose des niveaux de sécurité pendant que vous naviguez sur Internet.
Vous pouvez ainsi évaluer si le site que vous consultez présente un risque élevé ou faible pour votre sécurité.
Ce widget vous fournit des informations concernant le site Internet, comme le propriétaire du domaine, ou la raison du niveau de sécurité.
On compte trois niveaux de sécurité : sûr, peu risqué et très risqué.

Les niveaux de sécurité apparaissent dans la barre d'outils et dans les résultats de recherche sous la forme d'une icône de programme Avira avec différents symboles :

 *Sûr*

Une coche verte pour les sites Internet les plus sûrs.

 *Peu risqué*

Un point d'exclamation jaune pour les sites Internet qui présentent un risque faible.

 *Très risqué*

Un panneau stop rouge pour les sites Internet présentant un risque élevé pour votre sécurité.

 *Échec*

Un point d'interrogation pour les sites Internet dont le risque ne peut être évalué.

 *Vérification en cours*

Ce symbole apparaît pendant la vérification de l'état.

Bloqueur de suivi du navigateur

Le bloqueur de suivi du navigateur vous permet d'interrompre le suivi et d'empêcher toute collecte d'informations lorsque vous naviguez sur Internet.
Le widget vous permet de sélectionner le suivi à bloquer et à autoriser.

Les entreprises se divisent en trois catégories :

- Réseaux sociaux
- Réseaux publicitaires
- Autres entreprises

4.2.2 Options

La barre d'outils SearchFree d'Avira est compatible avec Internet Explorer, Firefox et Google Chrome, et peut être configurée à votre gré dans les navigateurs Web :

- Options de configuration Internet Explorer
- Options de configuration Firefox
- Options de configuration Chrome

Internet Explorer

Dans le navigateur Internet Explorer, vous disposez des options de configuration ci-dessous pour la barre d'outils SearchFree d'Avira dans le menu **Options** :

Options de barre d'outils

Recherche

Moteur de recherche Avira

Dans le menu **Moteur de recherche Avira**, vous pouvez sélectionner le moteur de recherche à utiliser pour les recherches. Vous avez le choix entre des moteurs de recherche de différents pays : États-Unis, Brésil, Allemagne, Espagne, Europe, France, Italie, Pays-Bas, Russie et Grande-Bretagne.

Ouvrir la recherche dans

Dans le menu de l'option **Ouvrir la recherche dans**, vous pouvez sélectionner où afficher le résultat de la recherche, dans la **Fenêtre actuelle**, dans une **Nouvelle fenêtre** ou dans un **Nouvel onglet**.

Afficher les dernières recherches

Si l'option **Afficher les dernières recherches** est activée, vous pouvez demander l'affichage des termes saisis jusqu'alors sous le champ de saisie de la barre de recherche.

Supprimer l'historique de recherche du navigateur

Activez l'option **Supprimer l'historique de recherche lors de la fermeture du navigateur** si vous ne souhaitez pas enregistrer l'historique des recherches déjà effectuées mais si vous préférez les effacer lors de la fermeture du navigateur Web.

Autres options

Langue de la barre d'outils

Sous **Langue de la barre d'outils**, vous pouvez sélectionner la langue d'affichage de la barre d'outils SearchFree d'Avira. Vous avez le choix entre l'anglais, l'allemand, l'espagnol, le français, l'italien, le portugais et le néerlandais.

Remarque
La langue prédéfinie de la barre d'outils SearchFree d'Avira correspond à celle de votre programme, si disponible. Si la barre d'outils n'est pas disponible dans votre langue, l'anglais est défini par défaut.

Afficher les noms des touches

Désactivez l'option **Afficher les noms des touches** si vous souhaitez masquer le texte à côté des icônes de la barre d'outils SearchFree d'Avira.

Supprimer l'historique de recherche

Activez l'option **Supprimer l'historique de recherche**, si vous ne souhaitez pas enregistrer la/les recherche(s) déjà effectué(es) mais préférez la/les supprimer immédiatement.

Aide

Cliquez sur **Aide** pour accéder au site Web et aux questions fréquentes (FAQ) sur la barre d'outils.

Désinstaller

Vous pouvez également désinstaller directement la barre d'outils SearchFree d'Avira sur Internet Explorer : Désinstallation via le navigateur Web.

Info

Cliquez sur **Info** pour afficher la version de la barre d'outils SearchFree d'Avira installée.

Firefox

Dans le navigateur Firefox, vous disposez des options de configuration ci-dessous pour la barre d'outils SearchFree d'Avira dans le menu **Options** :

Options de barre d'outils

Recherche

Moteur de recherche Avira

Dans le menu **Moteur de recherche Avira**, vous pouvez sélectionner le moteur de recherche à utiliser pour les recherches. Vous avez le choix entre des moteurs de recherche de différents pays : États-Unis, Brésil, Allemagne, Espagne, Europe, France, Italie, Pays-Bas, Russie et Grande-Bretagne.

Afficher les dernières recherches

Si l'option **Afficher les dernières recherches** est activée, vous pouvez demander l'affichage des termes saisis jusqu'alors en cliquant sur la flèche dans la barre de recherche. Sélectionnez l'un des termes si vous souhaitez afficher de nouveau les résultats de recherche.

Supprimer l'historique de recherche du navigateur

Activez l'option **Supprimer l'historique de recherche lors de la fermeture du navigateur** si vous ne souhaitez pas enregistrer l'historique des recherches déjà effectuées mais si vous préférez les effacer lors de la fermeture du navigateur Web.

Afficher les résultats de recherches d'Ask lorsque je saisis des mots-clés ou des adresses URL non valides dans le champ d'adresse du navigateur

Si cette option est activée, chaque fois que vous saisissez des mots-clés ou une adresse URL non valide dans le champ d'adresse du navigateur Web, une recherche est lancée et les résultats s'affichent.

Autres options

Langue de la barre d'outils

Sous **Langue de la barre d'outils**, vous pouvez sélectionner la langue d'affichage de la barre d'outils SearchFree d'Avira. Vous avez le choix entre l'anglais, l'allemand, l'espagnol, le français, l'italien, le portugais et le néerlandais.

Remarque
La langue prédéfinie de la barre d'outils SearchFree d'Avira correspond à celle de votre programme, si disponible. Si la barre d'outils n'est pas disponible dans votre langue, l'anglais est défini par défaut.

Afficher les noms des touches

Désactivez l'option **Afficher les noms des touches** si vous souhaitez masquer le texte à côté des icônes de la barre d'outils SearchFree d'Avira.

Supprimer l'historique de recherche

Activez l'option **Supprimer l'historique de recherche**, si vous ne souhaitez pas enregistrer la/les recherche(s) déjà effectué(es) mais préférez la/les supprimer immédiatement.

Aide

Cliquez sur **Aide** pour accéder au site Web et aux questions fréquentes (FAQ) sur la barre d'outils.

Désinstaller

Vous pouvez également désinstaller directement la barre d'outils SearchFree d'Avira sur Internet Explorer : Désinstallation via le navigateur Web.

Info

Cliquez sur **Info** pour afficher la version de la barre d'outils SearchFree d'Avira installée.

Chrome

Toutes les options de configuration sous le parapluie rouge Avira se trouvent dans le navigateur Web Google Chrome. Vous disposez des options suivantes pour la barre d'outils SearchFree d'Avira :

Aide

Cliquez sur **Aide** pour accéder au site Web et aux questions fréquentes (FAQ) sur la barre d'outils.

Instructions de désinstallation

Des liens vers les instructions de désinstallation pour la barre d'outils SearchFree d'Avira sont disponibles ici.

Info

Cliquez sur **Info** pour afficher la version de la barre d'outils SearchFree d'Avira installée.

Afficher et masquer la barre d'outils SearchFree d'Avira

Cette option de menu permet de masquer et d'afficher la barre d'outils SearchFree d'Avira qui se trouve dans la partie supérieure de la fenêtre.

4.2.3 Désinstallation

Voici la procédure à suivre pour désinstaller votre barre d'outils SearchFree d'Avira (sur l'exemple de Windows 7) :

- Ouvrez le **panneau de configuration** via le menu **Démarrer** de Windows.
- Double-cliquez sur **Programmes et fonctionnalités**.
- Sélectionnez **Barre d'outils SearchFree d'Avira et Protection Web** dans la liste et cliquez sur **Désinstaller**.
  - ↪ Un message vous demande alors si vous souhaitez vraiment désinstaller ce produit.
- Confirmez avec **Oui**.
  - ↪ La barre d'outils SearchFree d'Avira et la Protection Web sont désinstallées, votre ordinateur est redémarré si besoin est, et tous les répertoires, fichiers ainsi que toutes les entrées de registre de la barre d'outils SearchFree d'Avira et la Protection Web sont supprimés.

Désinstallation via le navigateur Web

Vous avez également la possibilité de désinstaller la barre d'outils SearchFree d'Avira directement dans le navigateur avec **Firefox et Internet Explorer** :

- Ouvrez le menu **Options** à droite dans la barre de recherche.
- Cliquez sur **Désinstaller**.
  - ↪ Si votre navigateur Web est encore ouvert, un message vous demandera de le fermer.

- Fermez le navigateur et cliquez sur **OK**.
  - ↪ La barre d'outils SearchFree d'Avira et la Protection Web sont désinstallées, votre ordinateur est redémarré si besoin est, et tous les répertoires, fichiers ainsi que toutes les entrées de registre de la barre d'outils SearchFree d'Avira et la Protection Web sont supprimés.

Remarque
Si vous désinstallez la barre d'outils SearchFree d'Avira, la Protection Web est également désinstallée.

Remarque
Notez que pour la désinstallation de la barre d'outils SearchFree d'Avira, la barre d'outils doit être activée dans le gestionnaire des modules complémentaires.

Désinstallation en tant que module complémentaire

Étant donné que la dernière version de la barre d'outils SearchFree d'Avira est installée sous forme de module complémentaire, il également possible de gérer l'outil avec différents gestionnaires de modules complémentaires.

Firefox

Cliquez sur **Outils > Modules complémentaires > Extensions**. Vous pouvez y gérer le module complémentaire d'Avira, c'est-à-dire l'activer, le désactiver ou le désinstaller.

Internet Explorer

Cliquez sur **Gérer les modules complémentaires > Barres d'outils et extensions**. Vous pouvez alors activer, désactiver et désinstaller le module complémentaire d'Avira.

Google Chrome

Outils > Extensions vous permet de gérer le module complémentaire Avira, et donc de l'activer, le désactiver ou le désinstaller.

4.3 Comment procéder

Les chapitres « Comment procéder » vous fournissent une rapide description de la procédure d'activation de la licence et du produit ainsi que des principales fonctions de votre produit Avira. Les courts descriptifs sélectionnés vous permettent d'obtenir rapidement un aperçu des fonctionnalités de votre produit Avira. Ils ne remplacent toutefois pas les explications détaillées fournies dans les différents chapitres de cette Aide.

4.3.1 Effectuer des mises à jour automatiques

Pour créer une tâche de mise à jour automatique de votre produit Avira avec le planificateur Avira, procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Planificateur**.
- Cliquez sur l'icône **Créer une nouvelle tâche avec l'assistant**.
  - ↪ La boîte de dialogue **Nom et description de la tâche** apparaît.
- Nommez la tâche et décrivez-la si besoin est.
- Cliquez sur **Suivant**.
  - ↪ La boîte de dialogue **Type de tâche** s'affiche.
- Sélectionnez **Tâche de mise à jour** dans la liste de sélection.
- Cliquez sur **Suivant**.
  - ↪ La boîte de dialogue **Heure 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**

> **Remarque**
> Nous vous recommandons d'effectuer des mises à jour régulières. L'intervalle de mise à jour recommandé est : 6 heures.

- Le cas échéant, saisissez la date selon votre sélection.
- Le cas échéant, sélectionnez des options supplémentaires (disponibles en fonction du type de tâche) :

- **Rattraper la tâche quand la date est déjà passée**
  Le programme effectue les tâches antérieures qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.

- Cliquez sur **Suivant**.
  - ↪ La boîte de dialogue **Affichage de la fenêtre** apparaît.
- Sélectionnez le mode d'affichage de la fenêtre des tâches :

- **Invisible** : pas de fenêtre des tâches
- **Réduit** : uniquement la barre de progression
- **Agrandi** : fenêtre des tâches complète

- 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 icônes suivantes 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

4.3.2 Démarrer manuellement une mise à jour

Vous avez différentes possibilités de démarrer manuellement une mise à jour : une mise à jour du fichier de définitions des virus et du moteur de recherche est effectuée systématiquement dans le cas d'une mise à jour lancée manuellement. Une mise à jour du produit n'est effectuée que si, dans la configuration, sous Sécurité PC > Mise à jour > Mise à jour produit, vous avez activé l'option **Télécharger et installer automatiquement les mises à jour produit**.

Pour démarrer manuellement la mise à jour de votre produit Avira, procédez de la façon suivante :

- Avec le bouton droit de la souris, cliquez sur l'icône de programme Avira dans la barre des tâches et sélectionnez **Démarrer mise à jour**.

  - OU -

- Dans le Control Center, sélectionnez la rubrique **État**, puis cliquez dans la zone **Dernière mise à jour** sur le lien **Démarrer mise à jour**.

  - OU -

  Dans le menu **Mise à jour** du Control Center, sélectionnez la commande de menu **Démarrer mise à jour**.

  ↪ La boîte de dialogue **Mise à jour** s'affiche.

Remarque
Nous vous recommandons d'effectuer des mises à jour régulières. L'intervalle de mise à jour recommandé est : 6 heures.

Remarque
Vous pouvez également effectuer une mise à jour manuelle directement à partir du centre de sécurité Windows.

4.3.3 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.

Pour rechercher via un profil de recherche, vous disposez des possibilités suivantes :

- Utiliser un profil de recherche prédéfini

  Si les profils de recherche prédéfinis répondent à vos besoins.
- Adapter et utiliser un profil de recherche (sélection manuelle)

  Si vous souhaitez chercher avec un profil de recherche individualisé.

Selon le système d'exploitation, différentes icônes sont disponibles pour le démarrage d'un profil de recherche :

- Sous Windows XP :

   Cette icône vous permet de lancer la recherche via un profil de recherche.
- Sous Windows Vista :

  Sous Microsoft Windows Vista, le Control Center n'a d'abord que des droits restreints, par ex. pour l'accès aux répertoires et fichiers. Le Control Center ne peut exécuter certaines actions et accéder 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 cette icône, vous démarrez une recherche limitée via 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 cette icône, 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.

Pour chercher des virus et logiciels malveillants avec un profil de recherche, procédez de la façon suivante :

- Dans le Control Center, choisissez la rubrique *SÉCURITÉ PC* **> Scanner**.

  ↪ Les profils de recherche prédéfinis apparaissent.
- Sélectionnez l'un des profils de recherche prédéfinis.

  - OU -

Adaptez le profil de recherche **Sélection manuelle**.

- Cliquez sur l'icône (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 adapter un profil de recherche :

- Dans le profil de recherche **Sélection manuelle**, déployez l'arborescence des fichiers de façon à ce que tous les lecteurs devant être parcourus soient ouverts:
- Sélectionnez les nœuds devant être parcourus, en cliquant sur chaque :

4.3.4 Recherche directe : chercher des virus et logiciels malveillants par glisser-déplacer

Pour chercher des virus et logiciels malveillants de manière ciblée par glisser-déplacer, procédez de la manière suivante :

- ✓ Ouvrez le Control Center de votre programme Avira.
- Sélectionnez le fichier, qui doit être contrôlé.
- Avec le bouton gauche de la souris, faites glisser le fichier dans le Control Center.
  - ↪ La fenêtre **Luke Filewalker** apparaît et la recherche directe démarre.
  - ↪ À la fin du processus de recherche, les résultats s'affichent.

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

Pour rechercher des virus et des logiciels malveillants de manière ciblée via le menu contextuel, procédez de la façon suivante :

- 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, contrôler.
  - ↪ Le menu contextuel de l'Explorateur Windows apparaît.
- Dans le menu contextuel, sélectionnez **Contrôler les fichiers sélectionnés avec Avira**.
  - ↪ La fenêtre **Luke Filewalker** apparaît et la recherche directe démarre.
  - ↪ A la fin du processus de recherche, les résultats s'affichent.

4.3.6 Recherche directe : recherche automatisée de virus et logiciels malveillants

Remarque
Après l'installation, la tâche de contrôle *Contrôle intégral du système* est créée

dans le planificateur : un contrôle intégral du système est effectué dans l'intervalle recommandé.

Pour créer une tâche de recherche automatisée des virus et logiciels malveillants, procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Planificateur**.
- Cliquez sur l'icône **Créer une nouvelle tâche avec l'assistant**.
  - ↪ La boîte de dialogue **Nom et description de la tâche** apparaît.
- Nommez la tâche et décrivez-la si besoin est.
- Cliquez sur **Suivant**.
  - ↪ La boîte de dialogue **Type de tâche** apparaît.
- Sélectionnez la **tâche de contrôle**.
- Cliquez sur **Suivant**.
  - ↪ La boîte de dialogue **Sélection du profil** apparaît.
- Choisissez le profil qui doit être parcouru.
- Cliquez sur **Suivant**.
  - ↪ La boîte 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**

- Le cas échéant, saisissez la date selon votre sélection.
- Sélectionnez l'option complémentaire le cas échéant (uniquement disponible en fonction du type de tâche) : **Rattraper la tâche quand la date est déjà passée**
  - ↪ Le programme effectue les tâches antérieures qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.
- Cliquez sur **Suivant**.
  - ↪ La boîte de dialogue **Affichage de la fenêtre** apparaît.
- Sélectionnez le mode d'affichage de la fenêtre des tâches :

- **Invisible** : pas de fenêtre des tâches
- **Réduit** : uniquement la barre de progression
- **Agrandi** : fenêtre des tâches complète

- Sélectionnez l'option **Arrêter l'ordinateur quand la tâche a été exécutée**, 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 l'écran principal de la rubrique *ADMINISTRATION* **> Planificateur**.

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

Les icônes suivantes 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

4.3.7 Recherche directe : chercher les rootkits actifs de manière ciblée

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

Pour rechercher les rootkits actifs de manière ciblée, procédez de la façon suivante :

- Dans le Control Center, choisissez la rubrique *SÉCURITÉ PC* **> Scanner**.

  ↪ Les profils de recherche prédéfinis apparaissent.

- Sélectionnez le profil de recherche prédéfini **Recherche des rootkits et des logiciels malveillants actifs**.

- Sélectionnez les éventuels autres nœuds et répertoires à contrôler en cliquant dans la case du niveau de répertoire concerné.

- Cliquez sur l'icône (Windows XP :  ou Windows Vista : ).

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

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

4.3.8 Réagir aux virus et logiciels malveillants détectés

Pour les différents composants de protection de votre produit Avira, vous pouvez régler sous la rubrique **Action si résultat positif** la façon dont votre produit Avira doit réagir en cas de détection d'un virus ou d'un programme indésirable.

Pour le composant Protection temps réel, il n'y a aucune option d'action configurable.Une notification est affichée sur le Bureau en cas de résultat positif. Dans la notification affichée sur le Bureau, vous avez la possibilité de supprimer 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 un menu contextuel vous propose différentes options pour traiter le fichier concerné (voir Résultat positif > Scanner).

Options d'action pour le Scanner :

- **Interactif**

  En mode d'action interactif, les résultats positifs de la recherche du Scanner sont signalés dans une boîte de dialogue. Ce paramètre est activé par défaut.
  Lors de la **Recherche par le Scanner**, vous recevez à l'issue de la recherche un message d'avertissement avec une liste des fichiers contaminés qui ont été trouvés. Vous avez la possibilité de sélectionner une action à exécuter pour les différents fichiers contaminés, via le menu contextuel. Vous pouvez exécuter les actions choisies pour tous les fichiers concernés ou quitter le Scanner.

- **Automatique**

  En mode d'action automatique, l'action que vous avez choisie dans cette zone est exécutée automatiquement en cas de détection d'un virus ou d'un programme indésirable.

Options d'actions pour la Protection Web :

- **Interactif**

  En mode d'action interactif, une boîte 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 paramètre 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.

Mode d'action interactif

- En mode d'action interactif, vous réagissez aux virus et programmes indésirables détectés en sélectionnant dans le message une **Action pour les objets contaminés** et exécutez l'action en cliquant sur **Confirmer**.

Les actions de traitement des objets concernés suivantes sont disponibles :

Remarque
Les actions disponibles à la sélection dépendent du système d'exploitation, du composant de protection (Scanner Avira, Protection temps réel Avira, Protection Web Avira), qui signale le résultat positif et le logiciel malveillant détecté.

Actions du Scanner:

- **Réparer**

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

- **Renommer**

  Le fichier est renommé en **.vir*. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Les fichiers peuvent ensuite être réparés puis renommés avec leur désignation d'origine.

- **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 est supprimé.
  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.

- **Ignorer**

  Aucune action supplémentaire 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 résultat positif avec la Protection temps réel : aucune action supplémentaire n'est effectuée par la Protection temps réel. L'accès au fichier est autorisé. Tous les accès ultérieurs à ce fichier sont autorisés et ne sont plus signalés 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 programme trouvé est copié en quarantaine.

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

  Options d'action en cas de détection de secteurs d'amorçage infectés : des options d'action pour la réparation de lecteurs de disquettes sont disponibles. Si aucune réparation n'est possible avec votre produit Avira, 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.

Action de la protection Web :

- **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.

- **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 quarantaine s'il a une valeur informative ou - si nécessaire - être envoyé à l'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 la protection Web.

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

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

4.3.9 Quarantaine : traiter les fichiers (*.qua) en quarantaine

Pour traiter les fichiers en quarantaine, procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Quarantaine**.
- Vérifiez de quels fichiers il s'agit pour pouvoir recharger 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 boîte de dialogue **Caractéristiques** avec des informations supplémentaires sur le fichier apparaît.

Si vous souhaitez à nouveau contrôler un fichier :

La vérification d'un fichier est recommandée quand le fichier de définitions de virus de votre produit Avira a été actualisé et qu'il y a un doute de fausse alerte. De cette façon, vous pouvez 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 paramètres 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  .
- Confirmez votre sélection avec **Oui**.

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

- Sélectionnez le fichier que vous souhaitez télécharger.
- Cliquez sur  .
  - ↪ La boîte de dialogue *Chargement du fichier* s'ouvre, avec un formulaire pour la saisie de vos coordonnées.
- Indiquez les données complètes.
- Sélectionnez un type : **Fichier suspect** ou **Doute de fausse alerte**.
- Sélectionnez un format de réponse : **HTML**, **Texte**, **HTML & texte**.
- Cliquez sur **OK.**
  - ↪ Le fichier est chargé sur un serveur Web de l'Avira Malware Research Center.

Remarque
Dans les cas suivants, une analyse par l'Avira Malware Research Center est recommandée :
Résultat heuristique positif (fichier suspect) : lors d'une recherche, votre produit Avira a classé un fichier comme suspect et l'a placé en quarantaine :

dans la boîte de dialogue de détection de virus ou dans le fichier de rapport de la recherche, il a été recommandé de faire analyser le fichier par l'Avira Malware Research Center.

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

Remarque
Vous ne pouvez charger qu'un seul fichier à la fois.

Si vous souhaitez exporter les propriétés de l'objet en 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 en quarantaine sélectionné.
- Enregistrez le fichier texte.

Vous pouvez également restaurer les fichiers en quarantaine (voir chapitre : Quarantaine : Restaurer les fichiers en quarantaine).

4.3.10 Quarantaine : restaurer les fichiers en quarantaine

En fonction du système d'exploitation, diverses icônes sont disponibles pour la restauration :

- **Sous Windows XP et 2000** :

   Cette icône vous permet de restaurer les fichiers dans le répertoire d'origine.

   Cette icône vous permet de restaurer des fichiers dans un répertoire de votre choix.

- **Sous Windows Vista** :

  Sous Microsoft Windows Vista, le Control Center n'a d'abord que des droits restreints, par ex. pour l'accès aux répertoires et fichiers. Le Control Center ne peut exécuter certaines actions et accéder 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.

   Cette icône vous permet de restaurer des fichiers dans un répertoire de votre choix.

 Cette icône 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.

Pour restaurer des fichiers en quarantaine, procédez de la manière suivante :

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

✓ Fichier recontrôlé et réparé par une recherche.

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Quarantaine**.

Remarque
Il n'est possible de restaurer les e-mails et pièces jointes d'e-mails qu'avec l'option  et avec l'extension **.eml*.

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

- Sélectionnez le fichier et cliquez sur l'icône (Windows XP :  , Windows Vista ).

  Cette option n'est pas disponible pour les e-mails.

Remarque
Il n'est possible de restaurer les e-mails et pièces jointes d'e-mails qu'avec l'option  et avec l'extension **.eml*.

  ↳ Le système vous demande si vous souhaitez restaurer le fichier.

- Cliquez sur **Oui**.

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

Si vous souhaitez restaurer un fichier dans un répertoire particulier :

- Sélectionnez le fichier et cliquez sur  .

  ↳ Le système vous demande si vous souhaitez restaurer le fichier.

- Cliquez sur **Oui**.

↳ La fenêtre Windows par défaut pour sélectionner un répertoire s'affiche.

- Sélectionnez le répertoire dans lequel le fichier doit être restauré et validez.
  ↳ Le fichier est restauré dans le répertoire choisi.

4.3.11 Quarantaine : déplacer un fichier suspect en quarantaine

Vous pouvez déplacer manuellement un fichier suspect en quarantaine de la manière suivante :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Quarantaine**.
- Cliquez sur [+].
  ↳ La fenêtre standard Windows pour sélectionner un fichier s'affiche.
- Choisissez un fichier et validez avec **Ouvrir**.
  ↳ Le fichier est déplacé en quarantaine.

Vous pouvez vérifier les fichiers en quarantaine avec le Scanner Avira (voir chapitre : Quarantaine : Traiter les fichiers (*.qua) en quarantaine).

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

Voici comment établir pour un profil de recherche qui scanne des types de fichiers supplémentaires ou exclut certains types de fichiers lors de la recherche (possible uniquement en cas de sélection manuelle) :

✓ Dans le Control Center, accédez à la rubrique *SÉCURITÉ PC* **> 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 boîte 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.

4.3.13 Profil de recherche : créer un raccourci sur le Bureau pour le profil de recherche

Le raccourci 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 produit Avira.

Pour créer un raccourci vers le profil de recherche sur le Bureau, procédez de la manière suivante :

- ✓ Dans le Control Center, accédez à la rubrique *SÉCURITÉ PC* **> Contrôler**.
- Sélectionnez le profil de recherche vers lequel vous souhaitez créer un raccourci.
- Cliquez sur l'icône  .
  - ↪ Le raccourci sur le Bureau est créé.

4.3.14 Événements : filtrer les événements

Dans le Control Center, sous *ADMINISTRATION* **> Événements** sont affichés tous les événements générés par les composants programme de votre produit Avira (comme avec l'affichage des événements de votre système d'exploitation Windows). Les composants programme sont, par ordre alphabétique, les suivants :

- Protection Web
- Protection temps réel
- Service d'assistance
- Planificateur
- Scanner
- Mise à jour

Les types d'événements suivants s'affichent :

- *Information*
- *Avertissement*
- *Erreur*
- *Résultat positif*

Voici comment filtrer les événements affichés :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* > Événements.
- Activez les cases à cocher des composants programme pour afficher les événements des composants activés.

  - OU -

  Décochez les cases à cocher des composants programme pour masquer les événements des composants désactivés.
- Activez la case à cocher des types d'événements pour afficher ces événements.

  - OU -

  Décochez les cases des types d'événements pour masquer ces événements.

5. Scanner

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

- **Recherche directe via le menu contextuel**
  La recherche directe via le menu contextuel (bouton droit de la souris - entrée **Contrôler les fichiers sélectionnés avec Avira**) est recommandée si vous voulez contrôler des fichiers et répertoires séparément dans l'explorateur Windows par exemple. Autre avantage : il n'est pas nécessaire de démarrer le Control Center pour la recherche directe via le menu contextuel.
- **Recherche directe via 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 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. Voir Recherche directe via les profils.
- **Recherche via le planificateur**
  Le planificateur offre la possibilité de faire effectuer des tâches de contrôle programmées dans le temps. Voir Recherche directe via le planificateur.

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

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

6. Mises à jour

L'efficacité d'un logiciel antivirus dépend de la mise à jour du programme, et tout particulièrement de celle du fichier de définitions des virus et du moteur de recherche. Le composant de mise à jour ou Updater est intégré dans votre produit Avira pour l'exécution des mises à jour. Il garantit que votre produit Avira 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 le modèle de détection des programmes malveillants que votre produit Avira 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 produit Avira 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 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 produit, il peut être nécessaire d'effectuer un redémarrage de votre système. 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 a par ex. été manipulée par un logiciel malveillant et redirige l'Updater vers des pages de téléchargement indésirables. Si le fichier hôte Windows a été manipulé, l'opération est visible dans le fichier rapport de l'Updater.

Une mise à jour est exécutée automatiquement dans l'intervalle suivant : 6 heures.

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 sous la rubrique **État**
- Via le menu contextuel de l'icône de programme

Vous pouvez obtenir des mises à jour à partir d'Internet, via un serveur Web du fabricant. Par défaut, la connexion réseau existante est utilisée comme connexion aux serveurs de téléchargement Avira. Vous pouvez adapter ce réglage par défaut dans la configuration sous Généralités > Mise à jour.

7. Résolution des problèmes, astuces

Dans ce chapitre, vous trouverez des indications importantes pour résoudre des problèmes, ainsi que d'autres astuces pour utiliser votre produit Avira.

- voir le chapitre Aide en cas de problème
- voir le chapitre Commandes clavier
- voir le chapitre Centre de sécurité Windows (pour Windows XP et Vista) ou Centre de maintenance Windows (à partir de Windows 7)

7.1 Aide en cas de problème

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

- 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.
- Les virus et logiciels malveillants ne peuvent pas être déplacés ou supprimés.
- L'icône de programme indique un état de désactivation.
- L'ordinateur devient très lent quand j'enregistre des données.
- Mon pare-feu signale la Protection temps réel Avira , dès qu'elle est active.
- Le chat Internet ne fonctionne pas : les messages du chat ne s'affichent pas.

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 aucune connexion au serveur Web sur Internet ne peut être établie.

- 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 :

- Vérifiez dans la configuration (mode expert) sous Sécurité PC > Mise à jour.

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 Avira.
- Si vous utilisez le système d'exploitation Windows XP, désactivez la restauration du système.
- Démarrez l'ordinateur en mode sécurisé.
- Ouvrez la configuration de votre produit Avira (mode expert).
- Sélectionnez **Scanner > Recherche**, dans le champ *Fichier* sélectionnez l'option **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 : la Protection temps réel a été désactivée.

- Dans le Control Center, cliquez sur le point **État** et dans la zone *Sécurité PC*, activez la **Protection temps réel**.

- OU -

- Cliquez avec le bouton droit de la souris sur l'icône de programme. Le menu contextuel s'ouvre. Cliquez sur **Activer la Protection temps réel**.

Cause : la Protection temps réel est bloquée par un pare-feu.

- Dans la configuration de votre pare-feu, définissez une autorisation générale pour la Protection temps réel Avira. La Protection temps réel Avira fonctionne uniquement avec l'adresse 127.0.0.1 (localhost). Aucune connexion à Internet n'est établie.

Sinon :

- Vérifiez le type de démarrage du service Protection temps réel Avira. Le cas échéant, activez le service : dans la barre de démarrage, sélectionnez **Démarrer > Panneau de configuration**. Lancez la fenêtre de configuration **Services** par double clic (sous Windows XP, vous trouvez l'applet Services dans le sous-dossier *Administration*). Recherchez l'entrée *Protection temps réel Avira*. Comme type de démarrage, vous devez sélectionner `Automatique` et comme état `Démarré`. Le cas échéant, démarrez le service manuellement 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 : la Protection temps réel Avira parcourt tous les fichiers que la sauvegarde des données traite lors du processus de sauvegarde.

- Dans la configuration (mode expert), sélectionnez **Protection temps réel > Recherche > Exceptions** et saisissez le nom du processus du logiciel de sauvegarde.

Mon pare-feu signale la Protection temps réel Avira, dès qu'elle est activée.

Cause : la communication de la Protection temps réel Avira s'effectue via le protocole Internet TCP/IP. Un pare-feu surveille toutes les connexions via ce protocole.

- Définissez une autorisation générale pour la Protection temps réel . La Protection temps réel Avira fonctionne uniquement avec l'adresse 127.0.0.1 (localhost). Aucune connexion à Internet n'est établie.

> **Remarque**
> Nous vous recommandons d'effectuer régulièrement des mises à jour Microsoft pour combler d'éventuelles lacunes de sécurité.

Le chat Internet ne fonctionne pas : les messages du chat ne s'affichent pas.

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

Cause : la Protection Web 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 du transfert de données avec 'transfer-encoding: chunked', la Protection Web 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 : Protection Web > Recherche > Exceptions).

7.2 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 rapidement.

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

7.2.1 Dans les boîtes de dialogue

Commande clavier	Description
Ctrl + Tab **Ctrl + PgDn**	Navigation dans le Control Center Passer à la rubrique suivante.
Ctrl + Maj + Tab **Ctrl + PgDn**	Navigation dans le Control Center Passer à la rubrique précédente.
← ↑ → ↓	Navigation dans les rubriques de configuration Faites d'abord glisser la souris sur la rubrique de configuration que vous souhaitez consulter. Naviguer entre les options dans un champ de liste déroulante sélectionné ou entre les options dans un groupe d'options.
Tab	Passer à l'option suivante ou au groupe d'options suivant.
Maj + Tab	Passer à l'option précédente ou au groupe d'options précédent.
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.
Échap	Fermer le champ de liste déroulante sélectionné. Annuler la commande et fermer la boîte de dialogue.
Touche Entrée	Exécuter la commande pour l'option active ou le bouton actif.

7.2.2 Dans l'Aide

Commande clavier	Description
Alt + touche espace	Afficher le menu système.
Alt + Tab	Naviguer entre l'Aide et les autres fenêtres ouvertes.
Alt + F4	Fermer l'Aide.
Maj + F10	Afficher les menus contextuels de l'Aide.
Ctrl + Tab	Passer à la rubrique suivante dans la fenêtre de navigation.
Ctrl + Maj + 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.

7.2.3 Dans le Control Center

Généralités

Commande clavier	Description
F1	Afficher l'Aide
Alt + F4	Fermer le Control Center
F5	Actualiser la vue
F8	Ouvrir la configuration

F9	Démarrer mise à jour

Rubrique **Scanner**

Commande clavier	Description
F3	Démarrer la recherche avec le profil choisi
F4	Créer un raccourci sur le Bureau pour le profil sélectionné

Rubrique **Quarantaine**

Commande clavier	Description
F2	Contrôler à nouveau l'objet
F3	Restaurer l'objet
F4	Envoyer l'objet
F6	Restaurer l'objet à l'emplacement...
Entrée	Propriétés
Ins	Ajouter le fichier
Suppr	Supprimer l'objet

Rubrique **Planificateur**

Commande clavier	Description
F2	Modifier la tâche
Entrée	Propriétés
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
Entrée	Afficher le rapport
Suppr	Supprimer le(s) rapport(s)

Rubrique **Événements**

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

7.3 Centre de sécurité Windows

- à partir de Windows XP Service Pack 2 -

7.3.1 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 obsolète), le Centre de sécurité envoie un avertissement et émet des recommandations pour mieux protéger l'ordinateur.

7.3.2 Le Centre de sécurité Windows et votre produit Avira

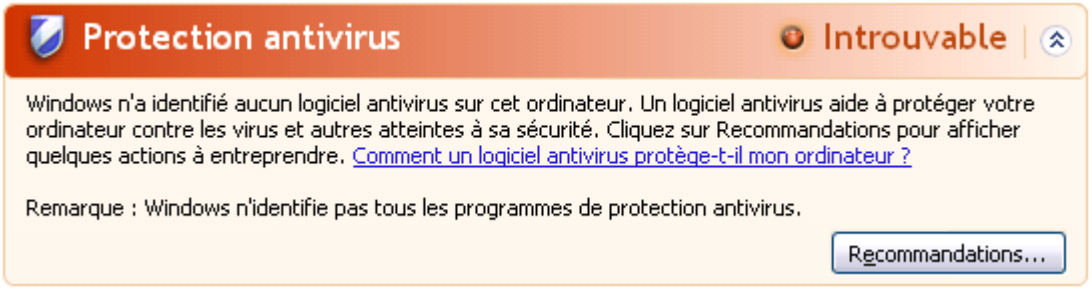
Logiciel antivirus / Protection contre les logiciels nuisibles

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

- Protection antivirus NON TROUVÉE
- Protection antivirus EXPIRÉE
- Protection antivirus ACTIVÉE
- Protection antivirus DÉSACTIVÉE
- Protection antivirus NON SURVEILLÉE

Protection antivirus NON TROUVÉE

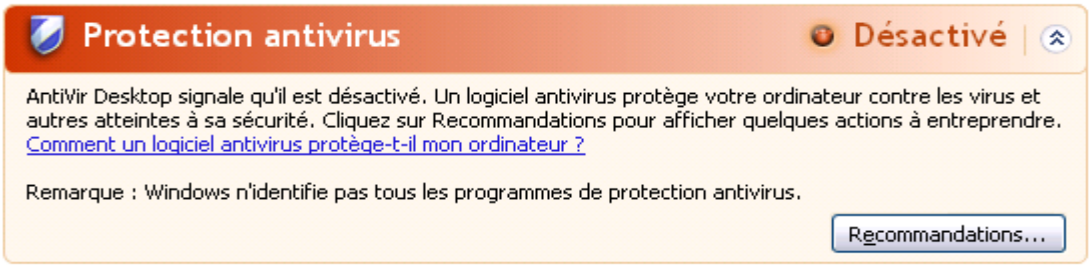
Cette notification du Centre de sécurité Windows apparaît si le Centre de sécurité Windows n'a trouvé aucun logiciel antivirus sur votre ordinateur.



> **Remarque**
> Installez votre produit Avira sur votre ordinateur pour le protéger des virus et autres programmes indésirables !

Protection antivirus EXPIRÉE

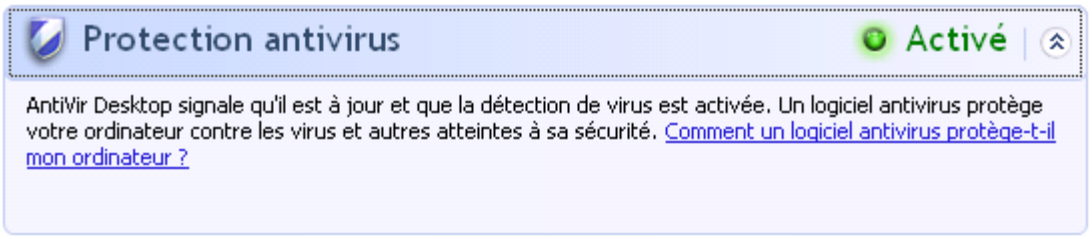
Si vous avez installé Windows XP Service Pack 2 ou Windows Vista et installez votre produit Avira ou si vous avez installé Windows XP Service Pack 2 ou Windows Vista sur un système accueillant déjà votre produit Avira, vous recevez le message suivant :



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

Protection antivirus ACTIVÉE

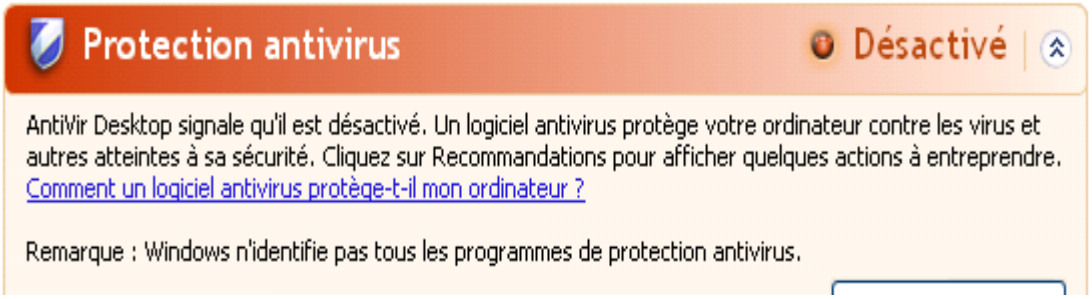
Après l'installation de votre produit Avira et une mise à jour immédiatement après, vous recevez le message suivant :



Votre produit Avira est maintenant à jour et la Protection temps réel Avira est activée.

Protection antivirus DÉSACTIVÉE

Vous recevez le message suivant si vous désactivez la Protection temps réel Avira ou si vous arrêtez le service Protection temps réel.



Remarque
Vous pouvez activer et désactiver la Protection temps réel Avira sous la rubrique **État** du **Control Center**. Vous voyez en outre que la Protection temps

réel Avira est activée lorsque 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
Cette fonction n'est pas prise en charge par Windows Vista.

Remarque
Le centre de sécurité Windows est pris en charge par votre produit Avira. 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 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 !

7.4 Centre de maintenance Windows

- Windows 7 -

7.4.1 Généralités

Remarque :
Dans Windows 7, le **Centre de sécurité Windows** a été renommé **Centre de maintenance Windows**. Dans cette section du programme, vous trouvez l'état de toutes les options de sécurité.

Le Centre de maintenance Windows vérifie l'état d'un ordinateur concernant les aspects importants de la sécurité. Vous pouvez accéder directement au Centre de maintenance en cliquant sur le petit drapeau dans la Barre des tâches ou sous **Panneau de configuration > Centre de maintenance**.

Si un problème est constaté sur l'un de ces points importants (par ex. un programme antivirus dépassé), le Centre de maintenance envoie un avertissement et émet des recommandations pour mieux protéger l'ordinateur. En d'autres termes, si tout fonctionne bien, vous ne recevez aucun message du Centre de maintenance. Cependant, il est possible de surveiller l'état de la sécurité de l'ordinateur dans le **Centre de maintenance** sous la rubrique **Sécurité**.
Vous avez également la possibilité de gérer et de sélectionner les logiciels que vous avez installés (par ex. *Afficher les programmes anti-espion installés*).

Vous pouvez désactiver les messages d'avertissement sous **Centre de maintenance > Modifier les paramètres**(par ex.*Désactiver les messages de sécurité pour la protection contre les logiciels espions et logiciels malveillants*).

7.4.2 Le Centre de maintenance Windows et votre produit Avira

Logiciel antivirus / Protection contre les logiciels nuisibles

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

- Avira Desktop indique être à jour et que la détection des virus est activée
- Avira Desktop indique que la détection des virus est provisoirement désactivée
- Avira Desktop n'est plus à jour
- Aucun programme antivirus n'a été trouvé sur l'ordinateur

Avira Desktop indique être à jour et que la détection des virus est activée

Après l'installation de votre produit Avira et après une mise à jour effectuée à la suite, vous ne recevez tout d'abord aucun message du Centre de maintenance Windows. Cependant sous **Centre de maintenance > Sécurité** , vous pouvez trouver les indications suivantes : *« Avira Desktop » indique être à jour et que la détection de virus est activée*. Cela signifie que votre produit Avira est maintenant à jour et que la Protection temps réel est activée.

Avira Desktop indique que la détection de virus est provisoirement désactivée

Vous recevez le message suivant si vous désactivez la Protection temps réel Avira ou si vous arrêtez le service Protection temps réel.

Remarque
Vous pouvez activer ou désactiver la **Protection temps réel Avira** sous la rubrique **État** de l'**Avira Control Center**. En outre, vous voyez que la **Protection temps réel Avira** est activée lorsque le parapluie rouge est ouvert dans votre barre des tâches. Il est également possible d'activer les différents composants Avira en cliquant sur la touche *Activer maintenant* du Centre de maintenance. Si vous obtenez un message où vous devez donner votre accord pour lancer le programme Avira, cliquez sur *Autoriser* et la Protection temps réel est activée.

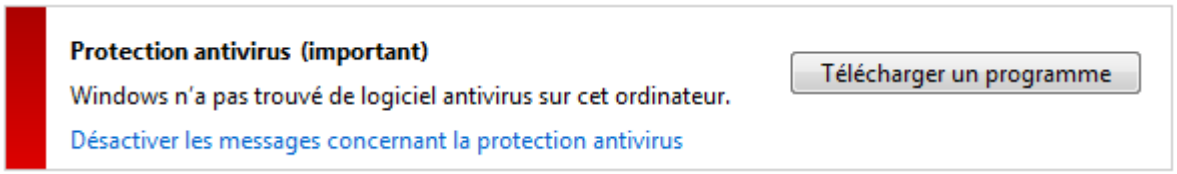
Avira Desktop n'est plus à jour

Si vous installez votre produit Avira sur un système Windows 7 ou si vous mettez à niveau vers Windows 7 un système d'exploitation antérieur sur lequel vous avez déjà installé votre produit Avira, vous obtenez le message suivant :

Remarque
Pour que le Centre de maintenance identifie votre produit Avira comme mis à jour, vous devez obligatoirement effectuer une mise à jour après l'installation. Vous actualisez votre système en exécutant une Mise à jour.

Aucun programme antivirus n'a été trouvé sur l'ordinateur

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



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

Protection contre les logiciels espions et logiciels indésirables

Vous pouvez recevoir les consignes suivantes du Centre de maintenance Windows, concernant votre protection contre les logiciels espions et les logiciels indésirables :

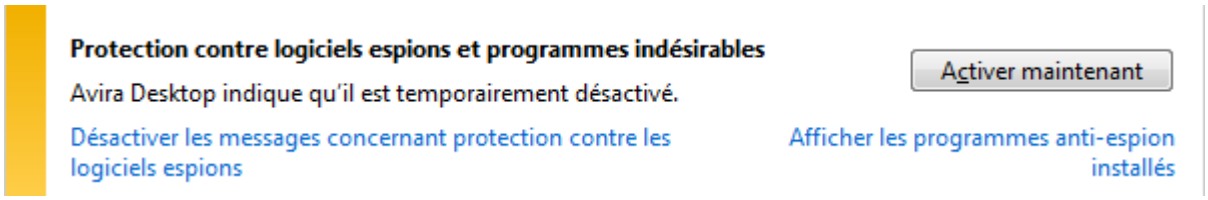
- Avira Desktop indique qu'il est activé
- Avira Desktop indique qu'il est provisoirement désactivé
- Windows Defender n'est plus à jour
- Windows Defender est désactivé

Avira Desktop indique qu'il est activé

Après l'installation de votre produit Avira et après une mise à jour effectuée à la suite, vous ne recevez tout d'abord aucun message du Centre de maintenance Windows. Cependant sous **Centre de maintenance > Sécurité** , vous pouvez trouver les indications suivantes : *« Avira Desktop » indique être à jour et que la Protection temps réel Avira est activée*. Cela signifie que votre produit Avira est mis à jour et que la Protection temps réel Avira est activée.

Avira Desktop indique qu'il est provisoirement désactivé

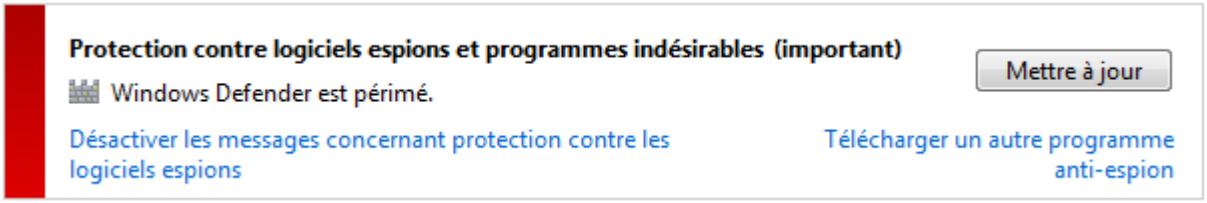
Vous recevez le message suivant si vous désactivez la Protection temps réel Avira ou si vous arrêtez le service Protection temps réel.



Remarque
Vous pouvez activer ou désactiver la **Protection temps réel Avira** sous la rubrique **État** de l'**Avira Control Center**. Vous voyez en outre que la **Protection temps réel Avira** est activée lorsque le parapluie rouge est ouvert dans votre barre des tâches. Il est également possible d'activer les différents composants Avira en cliquant sur *Activer maintenant* du Centre de maintenance. Si vous obtenez un message où vous devez donner votre accord pour lancer le programme Avira, cliquez sur *Autoriser* et la Protection temps réel est activée.

Windows Defender n'est plus à jour

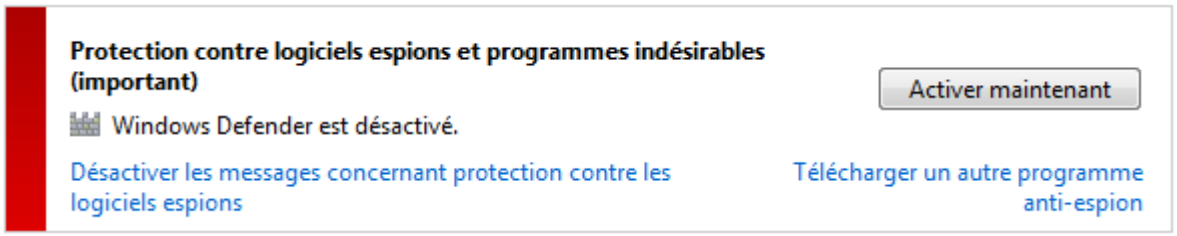
Vous recevez le message suivant lorsque Windows Defender est désactivé. Cela peut indiquer que votre produit Avira n'a pas été correctement installé. Veuillez vérifier l'installation.



Remarque
Windows Defender est la solution contre les logiciels espions de Windows. Il est inclus dans le pack Windows et activé par défaut sous Windows Vista et Windows 7.

Windows Defender est désactivé

Vous recevez le message du Centre de maintenance Windows *Windows Defender est désactivé* lorsqu'aucun logiciel de protection contre les logiciels espions n'a été trouvé sur votre ordinateur. Windows Defender est un logiciel intégré par défaut dans le système d'exploitation pour identifier les logiciels espions. Si vous avez installé un autre logiciel antivirus sur votre ordinateur, cette application est désactivée.
Si votre produit Avira a été correctement installé, vous ne recevez plus ce message, car le Centre de maintenance identifie automatiquement Avira. Vérifiez si Avira fonctionne correctement.



Remarque
Même si vous avez installé Windows 7, vous avez besoin d'une protection antivirus supplémentaire. Windows peut certes vérifier votre logiciel antivirus, mais lui-même ne contient que Windows Defender et le pare-feu Windows. Sans protection antivirus supplémentaire, vous ne seriez donc pas protégé des virus et autres logiciels malveillants !

8. Virus et autres

8.1 Virus et autres

Avira Free Antivirus identifie non seulement les virus et les logiciels malveillants, il peut également vous protéger contre d'autres dangers. Dansde ce chapitre, vous trouvez un aperçu des différents types de logiciels malveillants ainsi que des autres dangers encourus. Cette présentation décrit non seulement leur origine et leur comportement, mais également les mauvaises surprises qu'ils vous réservent.

Thèmes apparentés :

- Catégories de dangers
- Virus et autres logiciels malveillants

8.2 Catégories de dangers

Logiciels publicitaires

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

Votre produit Avira identifie les logiciels publicitaires. Si dans la configuration, sous Catégorie de dangers, l'option **Logiciels publicitaires** est activée, votre produit Avira vous avertit lorsqu'il détecte de tels logiciels.

Logiciels publicitaires/logiciels espions

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 produit Avira détecte les « logiciels publicitaires/logiciels espions ». Si dans la configuration, sous Catégories de dangers l'option **Logiciels publicitaires/logiciels espions** est activée, votre produit Avira vous avertit lorsqu'il détecte ce type de programmes.

Application

L'appellation Application désigne une application dont l'utilisation peut être associée à un risque ou dont l'origine est douteuse.
Votre produit Avira détecte les « applications » (APPL). Si dans la configuration, sous

Catégories de dangers, l'option **Application** est activée, votre produit Avira vous avertit lorsqu'il détecte ce type d'application.

Logiciels de commande Backdoor

Pour voler des données ou manipuler l'ordinateur, un programme de serveur backdoor passe par la « porte de derrière » sans que l'utilisateur le remarque. Par l'intermédiaire d'Internet ou du réseau, ce programme peut être commandé via un logiciel de commande backdoor (client) par des tiers.
Votre produit Avira détecte les logiciels de commande backdoor. Si dans la configuration, sous Catégories de dangers, l'option **Logiciels de commande Backdoor** est activée, votre produit Avira vous avertit lorsqu'il détecte ce type de programme.

Fichiers à extensions déguisées

Fichiers exécutables qui déguisent leur extension de manière suspecte. Cette méthode de dissimulation est souvent utilisée par les logiciels malveillants.
Votre produit Avira détecte les « fichiers à extensions déguisées ». Si dans la configuration, sous Catégories de dangers, l'option **Fichiers à extensions déguisées** est activée, votre produit vous avertit lorsqu'il détecte ce type de fichier.

Programme de numérotation payant

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 claires. L'établissement de la connexion via des programmes de numérotation sérieux s'affiche sans ambiguïté. En outre, les dialers sérieux indiquent clairement et avec précision les frais de connexion générés.

Malheureusement, il existe des dialers qui s'installent sur les ordinateurs de manière cachée et douteuse, voire à des fins frauduleuses. 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'après réception 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 faire bloquer ce type de numéros directement auprès de votre opérateur téléphonique.

En général, votre produit Avira identifie les programmes de numérotation payants qu'il connaît.

Si dans la configuration, sous Catégories de dangers, l'option **Programmes de numérotation payants** est activée, votre produit Avira vous avertit lorsqu'il détecte un programme de ce type. 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.

Hameçonnage

L'hameçonnage, également connu sous le nom de « phishing » ou « brand spoofing », est une forme élaborée de vol de données qui vise les clients ou clients potentiels des FAI, banques, services bancaires en lignes, autorités d'enregistrement.
En transmettant votre adresse e-mail, sur Internet, en remplissant des formulaires en ligne, en participant à des groupes d'information ou des pages Web, il est possible que vos données soient volées par des « Internet crawling spiders » (robots d'indexation ou araignées du Web) et utilisées sans votre accord pour une escroquerie ou d'autres forfaits.

Votre produit Avira détecte l'« hameçonnage ». Si dans la configuration, sous Catégories de dangers, l'option **Hameçonnage** est activée, votre produit Avira vous avertit qu'il a détecté un comportement de ce type.

Programmes portant atteinte à la vie privée

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 produit Avira détecte les logiciels de type « Security Privacy Risk ». Si dans la configuration, sous Catégories de dangers, l'option **Programmes portant atteinte à la vie privée** est activée, votre programme Avira vous avertit lorsqu'il détecte des logiciels de ce type.

Programmes de blagues

Les programmes de blagues sont uniquement conçus pour effrayer ou pour amuser, sans être nuisibles ni se multiplier. Souvent, l'ordinateur joue une mélodie à l'ouverture du programme de blague ou affiche quelque chose d'inhabituel à l'écran. On peut citer à titre d'exemples la machine à laver dans le lecteur de disquettes (DRAIN.COM) et le mangeur d'écran (BUGSRES.COM).

Mais prudence ! Tous les signes des programmes de blagues peuvent aussi provenir d'un virus ou d'un cheval de Troie. Au mieux, vous en êtes quitte pour une belle frayeur, au pire la panique peut générer de véritables dégâts sur votre machine.

Votre produit Avira est capable de détecter les programmes de blagues grâce à l'élargissement de ses routines de recherche et d'identification et le cas échéant, les éliminer comme programmes indésirables. Si dans la configuration, sous Catégories de

dangers, l'option **Programmes de blagues** est activée, votre produit Avira vous avertit lorsqu'il détecte ce type de programmes.

Jeux

Les jeux vidéo sont une activité délassante - mais n'ont pas obligatoirement leur place 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 e-mail aussi sont de plus en plus populaires : des simples échecs à la bataille navale, 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 produit Avira identifie les jeux vidéo. Si dans la configuration, sous Catégories de dangers, l'option **Jeux** est activée, votre produit Avira vous avertit lorsqu'il détecte des jeux. Fin du jeu, au sens propre, car vous avez la possibilité de le supprimer.

Logiciels frauduleux

Également appelés « scareware » (logiciel destiné à effrayer) ou « rogueware » (logiciels fripouilles), il s'agit de logiciels frauduleux simulant des attaques virales et se proposant comme un logiciel antivirus professionnel. Le scareware est conçu pour inquiéter ou intimider l'utilisateur. Si la victime tombe dans le panneau et se pense menacée, elle se voit proposer contre paiement l'élimination du danger inexistant. Dans certains cas, la victime pensant être la cible d'une attaque est amenée à effectuer des manipulations qui elles, permettent alors une véritable attaque.

Si dans la configuration, sous Catégories de dangers, l'option **Logiciels frauduleux** est activée, votre produit Avira vous avertit lorsqu'il détecte un scareware.

Programmes de décompression inhabituels

Fichiers compressés avec un programme de compression inhabituel et qui peuvent donc être considérés comme suspects.

Votre produit Avira détecte les « programmes de décompression inhabituels ». Si, dans la configuration, sous Catégories de dangers, l'option **Programmes de compressions inhabituels (PCK)** est activée, votre produit Avira vous avertit lorsqu'il détecte l'un de ces programmes.

8.3 Virus et autres logiciels malveillants

Logiciels publicitaires

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

Backdoors

Un backdoor (porte de derrière en français) peut accéder à un ordinateur en contournant sa protection.

Un programme fonctionnant de manière cachée offre à un agresseur des droits quasi illimités. À l'aide du backdoor, il est possible d'espionner les données personnelles de l'utilisateur. Mais les backdoors 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 est infecté de préférence avec des virus 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 (faille de sécurité) est un programme informatique ou script qui exploite les faiblesses ou dysfonctionnements spécifiques 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 (hoaxes en anglais)

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

Pot de miel

Un pot de miel (honeypot en anglais) 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 recherche alors les points faibles d'un réseau et sollicite les services proposés par un pot de miel, il est enregistré et une alarme se déclenche.

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 uniquement dans les documents de cette application. 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 évoluée de l'hameçonnage. Les escrocs au pharming entretiennent leurs propres grandes fermes de serveurs sur lesquelles sont hébergés des sites Web contrefaits. Le pharming s'est établi comme terme générique pour plusieurs types d'attaques DNS. Lors de la manipulation du fichier hôte, une manipulation ciblée du système est réalisée à l'aide d'un cheval de Troie ou d'un virus. En conséquence, seuls les sites Web contrefaits sont encore accessibles par le système, 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 d'apparence officielle, comme par exemple des e-mails l'incitant à communiquer sans méfiance des informations confidentielles, 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 certaine : les banques et assurances ne demandent jamais d'envoyer les numéros de cartes de crédit, PIN, TAN ou autres données d'accès par e-mail, 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 et de les infecter, une fois qu'il a été ouvert. 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.

Rootkits

Un rootkit est un ensemble d'outils logiciels furtifs qui s'installent après avoir infiltré un système informatique, pour masquer la pénétration de l'envahisseur, cacher des processus et récupérer 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 - par e-mail dans le monde entier en quelques heures.

Les virus et vers de script utilisent l'un des langages de script, par ex. Javascript, VBScript etc., pour s'insérer dans de nouveaux scripts ou se répandre par l'activation de fonctions du système d'exploitation. La contamination a souvent lieu par e-mail ou lors de l'échange de fichiers (documents).

On appelle ver un programme qui se multiplie sans contaminer d'hôte. Les vers ne peuvent donc pas devenir partie intégrante d'autres processus programmes. Les vers constituent souvent la seule possibilité d'infiltrer des programmes nuisibles sur les systèmes équipés de mesures de sécurité très strictes.

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 comportement de navigation de l'utilisateur sur Internet et à afficher des bannières ou fenêtres publicitaires intempestives 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 dévoilent leur véritable finalité 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. Ils sont actifs dès l'exécution et formatent par exemple le disque dur. Les droppers qui inoculent des virus dans un système informatique constituent un type particulier de cheval de Troie.

Logiciels frauduleux

Également appelés « scareware » (logiciel destiné à effrayer) ou « rogueware » (logiciels fripouilles), il s'agit de logiciels frauduleux simulant des attaques virales et se proposant comme un logiciel antivirus professionnel. Le scareware est conçu pour inquiéter ou intimider l'utilisateur. Si la victime tombe dans le panneau et se pense menacée, elle se voit proposer contre paiement l'élimination du danger inexistant. Dans certains cas, la victime pensant être la cible d'une attaque est amenée à effectuer des manipulations qui elles, permettent alors une véritable attaque.

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 e-mails d'hameçonnage.

9. Info et service

Dans ce chapitre, vous trouverez les informations nécessaires pour nous contacter.

- voir le chapitre Adresse de contact
- voir le chapitre Support technique
- voir le chapitre Fichier suspect
- voir le chapitre Signaler une fausse alerte

9.1 Adresse de contact

Nous serons heureux de vous aider en cas de questions et de suggestions concernant la gamme de produits Avira. Vous trouverez nos adresses de contact dans le Control Center sous **Aide > À propos de Avira Free Antivirus**.

9.2 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 pour bénéficier de notre vaste service de support :
http://www.avira.com/fr/personal-support

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

- **Informations de version**. Vous trouverez ces informations sous l'option de menu **Aide > À propos de Avira Free Antivirus > Informations de version**. Voir Informations de version.
- **Version du système d'exploitation** et service packs éventuellement installés.
- **Packs logiciels installés**, par ex. logiciels d'antivirus d'autres fabricants.
- **Messages précis** du programme ou du fichier rapport.

9.3 Fichier suspect

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

- Sélectionnez le fichier dans le Gestionnaire de quarantaine du Control Center puis, via le menu contextuel ou le bouton correspondant, sélectionnez le point **Envoyer fichier**.

- Envoyez le fichier souhaité sous forme compressée (WinZIP, PKZip, Arj, etc.) en pièce jointe par e-mail à l'adresse suivante :
  virus-personal-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).

9.4 Signaler une fausse alerte

Si vous pensez que votre produit Avira notifie un résultat positif dans un fichier très vraisemblablement « propre », envoyez ce fichier compressé (WinZIP, PKZIP, Arj, etc.) en pièce jointe par mail à l'adresse suivante :
virus-personal-fr@avira.com

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

10. Référence : options de configuration

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

10.1 Scanner

La rubrique **Scanner** de la configuration concerne la configuration de la recherche directe, c'est-à-dire de la recherche à la demande. (Options disponibles uniquement si le mode expert est activé.)

10.1.1 Recherche

Vous pouvez définir le comportement de base de la routine de recherche lors d'une recherche directe (Options disponibles uniquement si le mode expert est activé). Si vous choisissez certains répertoires à contrôler lors de la recherche directe, le scanner effectue le contrôle en fonction de la configuration :

- avec un niveau de recherche défini (priorité),
- plus les secteurs d'amorçage et la mémoire principale,
- tous les fichiers du répertoire, ou seulement certains.

Fichiers

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

Tous les fichiers

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

> **Remarque**
> Si l'option **Tous les fichiers** est activée, le bouton **Extensions de fichiers** ne peut pas être utilisé.

Sélection intelligente des fichiers

Si cette option est activée, la sélection des fichiers à contrôler est effectuée automatiquement par le programme. Cela signifie que votre programme Avira décide en fonction du contenu d'un fichier si celui-ci doit être contrôlé quant à l'absence de virus et programmes indésirables. Ce processus est un peu plus lent que 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 paramètre est activé par défaut et recommandé.

Remarque
Si l'option **Sélection intelligente des fichiers** est activée, le bouton **Extensions de fichiers** ne peut pas être utilisé.

Utiliser la liste des extensions de fichiers

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

Remarque
Si cette option est activée et que vous avez supprimé toutes les entrées de la liste des extensions de fichiers, ceci est signalé avec le texte « *Aucune extension de fichiers* », sous le bouton **Extensions de fichiers**.

Extensions de fichiers

Ce bouton permet d'ouvrir une boîte 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 par défaut peut changer d'une version à l'autre.

Autres paramètres

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 paramètre est activé par défaut.

Scanner les secteurs d'amorçage maître

Si cette option est activée, le scanner contrôle les secteurs d'amorçage maître du ou des disques durs utilisés dans le système.

Ignorer les fichiers hors ligne

Si cette option est activée, la recherche directe ignore complètement les fichiers hors ligne lors d'une recherche. Cela signifie que la présence de virus et programmes indésirables n'est pas contrôlée sur ces fichiers. Les fichiers hors ligne sont des fichiers qui ont été déplacés physiquement par un système de gestion hiérarchique de

la mémoire (HSMS), du disque dur vers une bande, par exemple. Ce paramètre est activé par défaut.

Contrôle d'intégrité de fichiers système

Si cette 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.

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

Remarque
Si vous utilisez des outils de fournisseurs tiers qui modifient les fichiers système et adaptent l'écran d'amorçage ou de démarrage à vos besoins, veuillez ne pas utiliser cette option. Voici quelques exemples de ces outils : Skinpacks, TuneUp Utilities ou Vista Customization.

Recherche optimisée

Si cette option est activée, la capacité du processeur est utilisée de façon optimale lors d'une recherche effectuée par le scanner. Pour des raisons liées à la performance, la consignation lors d'une recherche optimisée s'effectue au maximum à un niveau par défaut.

Remarque
L'option n'est disponible que sur les ordinateurs multiprocesseurs.

Suivre les liens symboliques

Si cette option est activée, le scanner suit, lors d'une 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.

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

Remarque
La recherche de rootkits n'est pas disponible sous Windows XP 64 bits .

Scanner le registre

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

Processus de contrôle

Autoriser l'arrêt

Si cette option est activée, la recherche de virus ou programmes indésirables peut être arrêtée à tout moment avec le bouton « **Arrêt** » dans la fenêtre « **Luke Filewalker** ». Si vous avez désactivé ce paramètre, le bouton **Arrêt** est grisé dans la fenêtre « **Luke Filewalker** ». L'arrêt prématurée d'une recherche n'est alors pas possible. Ce paramètre 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 fonctionnent en même temps sur l'ordinateur. Le choix influe sur la vitesse de la recherche.

basse

Le scanner reçoit du système d'exploitation du temps processeur uniquement si aucun autre processus ne nécessite de temps de calcul, c'est-à-dire que tant que le scanner fonctionne seul, la vitesse est maximale. Globalement, 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.

moyenne

Le scanner est exécuté avec le niveau de priorité normal. Tous les processus reçoivent du système d'exploitation le même temps processeur. Ce paramètre est activé par défaut et recommandé. Dans certaines conditions, le travail avec d'autres applications peut être entravé.

élevée

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 à la vitesse maximale.

Action si résultat positif

Vous pouvez définir des actions que le scanner doit exécuter quand un virus ou programme indésirable a été détecté. (Options disponibles uniquement si le mode expert est activé.)

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 un message d'avertissement comportant une liste des fichiers contaminés qui ont été trouvés. Vous avez la possibilité de sélectionner une action à exécuter pour les différents fichiers contaminés, via le menu contextuel. Vous pouvez exécuter les actions choisies pour tous les fichiers contaminés ou arrêter le scanner.

Remarque
L'action **Quarantaine** est présélectionnée par défaut dans la boîte de dialogue pour le traitement des virus. Vous pouvez sélectionner d'autres actions via un menu contextuel.

Automatique

Si l'option est activée, aucune boîte de 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 des paramètres que vous avez définis dans cette section.

Copier le fichier en quarantaine avant l'action

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

Action primaire

L'action primaire est l'action exécutée lorsque le scanner trouve un virus ou un programme indésirable. Si l'option « **Réparer** » est sélectionnée, mais que la réparation du fichier contaminé est impossible, l'action sélectionnée sous « **Action secondaire** » est exécutée.

Remarque
L'option **Action secondaire** ne peut être sélectionnée que si, sous **Action primaire**, le paramètre **Réparer** a été sélectionné.

Réparer

Si l'option est activée, le scanner répare automatiquement les fichiers contaminés. Si le scanner ne peut pas réparer un fichier contaminé, 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.

Renommer

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

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 l'Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé.

Ignorer

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

Avertissement
Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

Action secondaire

L'option « **Action secondaire »** ne peut être sélectionnée que si le paramètre **Réparer** a été sélectionnée sous « **Action primaire »**. Cette option permet de décider ce qui doit advenir du fichier contaminé s'il n'est pas réparable.

Renommer

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

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 l'Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé.

Ignorer

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

Avertissement
Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

Remarque
Si vous avez sélectionné **Supprimer** ou comme action primaire ou secondaire, tenez compte de ce qui suit : dans le cas de résultats heuristiques, les fichiers contaminés ne sont pas supprimés, mais déplacés en quarantaine.

Archives

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. (Options disponibles uniquement si le mode expert est activé.)

Contrôler les archives

Si cette option est activée, les archives sélectionnées dans la liste des archives sont contrôlées. Ce paramètre est activé par défaut.

Tous les types d'archives

Si cette option est activée, toutes les archives figurant dans la liste des 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 paramètre est activé par défaut.

Remarque
Seuls les types d'archives sélectionnés 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 déterminer s'il y a un virus ou un programme indésirable au sein d'une archive, le scanner doit scanner celle-ci jusqu'au niveau de récursivité dans lequel le virus ou le programme indésirable se trouve.

Profondeur maximale de récursivité

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

Valeurs par défaut

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

Liste des archives

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

Exceptions

Objets de fichier à exclure par le scanner (Options disponibles uniquement si le mode expert est activé.)

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 de contrôler 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 6 000 caractères au total.

Avertissement
Ces fichiers sont ignorés lors de la recherche.

Remarque
Les fichiers inscrits 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, supprimez le nom de ce fichier de la liste.

Champ de saisie

Entrez dans ce champ le nom de l'objet de fichier qui doit être ignoré par la recherche en temps réel. Aucun objet de 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, seul ce fichier n'est pas contrôlé. Si vous avez saisi un nom de fichier sans chemin, tout fichier portant ce nom (quel que soit le chemin ou le lecteur) ne sera pas contrôlé.

Ajouter

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

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas actif 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 rechercher effectuée par le scanner, `D:\folder\file.txt` n'est pas exclu de la recherche.

Heuristique

Cette rubrique de configuration contient les paramètres pour l'heuristique du moteur de recherche. (Options disponibles uniquement si le mode expert est activé.)

Les produits Avira 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 complexe et un examen 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 peuvent aussi survenir. 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 signalé est digne de confiance.

Heuristique de macrovirus

Heuristique de macrovirus

Votre produit Avira contient une heuristique de macrovirus très performante. Si l'option est activée, toutes les macros du document contaminé sont supprimées si une réparation est possible ; les documents suspects peuvent aussi être seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce paramètre est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

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

Niveau de détection bas

Si l'option est activée, moins de logiciels malveillants inconnus sont détectés, le risque de détections erronées est faible dans ce cas.

Niveau de détection moyen

Si l'option est activée, une protection équilibrée est assurée avec peu de messages d'erreurs. Ce paramètre est activé par défaut si vous avez choisi l'utilisation de cette heuristique.

Niveau de détection élevé

Si l'option est activée, nettement plus de logiciels malveillants inconnus sont détectés, sachant qu'il faut toutefois s'attendre à des messages erronés.

10.1.2 Rapport

Le scanner dispose d'une fonction de consignation étendue. Vous obtenez ainsi des informations précises 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. (Options disponibles uniquement si le mode expert est activé.)

> **Remarque**
> Pour vous permettre de savoir quelles actions le scanner a effectuées lors de la détection de virus ou de programmes indésirables, un fichier rapport doit systématiquement être généré.

Consignation

Désactivée

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

Par défaut

Si cette option est activée, le scanner consigne les noms des fichiers contaminés en indiquant leur chemin. En outre, la configuration de la recherche actuelle, les informations sur la version et sur le détenteur de la licence sont inscrites dans le fichier rapport.

Étendue

Si cette option est activée, le scanner consigne les avertissements et remarques en plus des informations standard. un suffixe

Intégrale

Si cette option est activée, le scanner consigne également tous les fichiers contrôlés. En outre, tous les fichiers contaminés, ainsi que les avertissements et remarques sont repris dans le fichier rapport.

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

10.2 Protection temps réel

La rubrique Protection temps réel de la configuration permet la configuration de la recherche en temps réel. (Options disponibles uniquement si le mode expert est activé.)

10.2.1 Recherche

En règle générale, vous voudrez surveiller votre système en continu. Pour ce faire, utilisez la protection temps réel (recherche en temps réel = On-Access Scanner). Cette protection vous permet de faire contrôler « à la volée » tous les fichiers copiés ou ouverts sur l'ordinateur à la recherche de virus et de programmes indésirables. (Option disponible uniquement si le mode expert est activé.)

Fichiers

La protection temps réel 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, quels que soient leur contenu et leur extension.

> **Remarque**
> Si l'option **Tous les fichiers** est activée, le bouton **Extensions de fichiers** ne peut pas être utilisé.

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 quant à l'absence de virus et programmes indésirables. Ce processus est un peu plus lent que l'option **Utiliser la liste des extensions de fichiers**, mais beaucoup plus sûr, car le contrôle n'a pas lieu uniquement sur la base des extensions de fichiers.

> **Remarque**
> Si l'option **Sélection intelligente des fichiers** est activée, le bouton **Extensions de fichiers** ne peut pas être utilisé.

Utiliser la liste des extensions de fichiers

Si cette option est activée, seuls les fichiers dont l'extension a été présélectionnée sont contrôlés. Sont présélectionnés par défaut tous les types de fichiers pouvant contenir des virus et programmes indésirables. Cette liste peut être modifiée manuellement à l'aide du bouton « **Extension de fichiers** ». Ce paramètre 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 est signalé avec le texte « *Aucune extension de fichiers* », sous le bouton **Extensions de fichiers**.

Extensions de fichiers

Ce bouton permet d'ouvrir une boîte 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 des extensions de fichiers peut changer d'une version à l'autre.

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, la protection temps réel contrôle les fichiers avant qu'ils ne soient lus ou exécutés par une application ou le système d'exploitation.

Contrôler pendant l'écriture

Si cette option est activée, la protection temps réel contrôle un fichier lors de l'écriture. Ce n'est qu'après cette opération que vous pouvez accéder à nouveau au fichier.

Contrôler pendant la lecture et l'écriture

Si cette option est activée, la protection temps réel contrôle les fichiers avant l'ouverture, la lecture et l'exécution, et après l'écriture. Ce paramètre est activé par défaut et recommandé.

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.

Prof. de récursivité max.

Lors de la recherche dans les archives, la protection temps réel peut utiliser 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 pour la profondeur de récursivité, qui est de 1, est conseillée : tous les fichiers se trouvant directement dans l'archive principale sont contrôlés.

Nombre max. de fich.

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 recommandée.

Taille max. (Ko)

Lors de la recherche dans les archives, celle-ci est limitée à une taille maximale d'archive à décompresser. La valeur par défaut de 1 000 Ko est recommandée.

Action si résultat positif

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 paramètre est activé par défaut. (Option disponible uniquement si le mode expert est activé.)

Exceptions

Ces options vous permettent de configurer des objets d'exclusion pour la protection temps réel (recherche en temps réel). Les objets correspondants sont alors ignorés lors de la recherche en temps réel. La protection temps réel peut ignorer via la liste des processus à exclure leurs accès aux fichiers lors de la recherche en temps réel. Ceci est utile notamment pour les bases de données ou solutions de sauvegarde. (Options disponibles uniquement si le mode expert est activé.)

Tenez compte de ce qui suit lors de l'indication des processus et objets de fichiers à exclure : 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. Gardez la liste aussi courte que possible.

Processus à exclure par la protection temps réel

Tous les accès aux fichiers par les processus de cette liste sont exclus de la surveillance par la protection temps réel.

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.

Le chemin indiqué et le nom de fichier du processus peuvent contenir 255 signes au maximum. Vous pouvez saisir jusqu'à 128 processus. Les entrées de la liste ne doivent pas dépasser 6 000 caractères au total.

Les caractères Unicode sont acceptés pour indiquer le processus. Vous pouvez par conséquent saisir des noms de processus ou de répertoires contenant des caractères spéciaux.

Les lecteurs doivent être indiqués comme suit : `[lettre du lecteur]:\`

Le caractère deux-points (:) ne peut être utilisé que pour indiquer des lecteurs.

Pour indiquer le processus, vous pouvez utiliser les caractères de remplacement * (un nombre illimité de caractères) et ? (un seul caractère) :

```
C:\Programmes\Application\application.exe
C:\Programmes\Application\applicatio?.exe
C:\Programmes\Application\applica*.exe
C:\Programmes\Application\*.exe
```

Pour éviter d'exclure des processus globalement de la surveillance de la protection temps réel, les indications comprenant exclusivement les caractères suivants ne sont pas valables : * (étoile), ? (point d'interrogation), / (barre oblique), \ (barre oblique inversée), . (point), : (deux-points).

Vous avez la possibilité d'exclure des processus de la surveillance de la protection temps réel sans en indiquer complètement le chemin : `application.exe`

Cela s'applique toutefois exclusivement aux processus dont les fichiers exécutables se trouvent sur les lecteurs du disque dur.

N'indiquez aucune exception pour les processus dont les fichiers exécutables se trouvent sur des lecteurs dynamiques. Les lecteurs dynamiques sont utilisés pour des supports de données tels que des CD, DVD ou clé USB.

Avertissement
Notez que tous les accès aux fichiers initiés par les processus inclus dans la liste sont exclus de la recherche de virus et de programmes indésirables.

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

Ce bouton vous permet de valider dans la fenêtre d'affichage le processus entré dans le champ de saisie.

Supprimer

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

Objets de fichiers à exclure par la protection temps réel

Tous les accès fichiers aux objets de cette liste sont exclus de la surveillance par la protection temps réel.

Champ de saisie

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

Les entrées de la liste ne doivent pas dépasser 6 000 caractères au total.

Pour indiquer les objets de fichiers à exclure, vous pouvez utiliser les caractères de remplacement * (un nombre illimité de caractères) et ? (un seul caractère). Des extensions de fichiers individuelles peuvent aussi être exclues (y compris avec des caractères de remplacement) :

```
C:\Répertoire\*.mdb
*.mdb
*.md?
*.xls*
C:\Répertoire\*.log
```

Les noms de répertoires doivent se terminer par une barre oblique inversée \.

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

Vous pouvez indiquer 20 exceptions au maximum par lecteur avec le chemin complet (commençant par la lettre du lecteur).

Ex. : `C:\Programmes\Application\Nom.log`

Le nombre maximum d'exceptions sans chemin complet s'élève à 64. Ex. :

```
*.log
```

Pour les lecteurs dynamiques qui sont connectés (mounted) en tant que répertoire d'un autre lecteur, vous devez utiliser, dans la liste des exceptions, l'alias du système d'exploitation pour le lecteur relié :
ex. `\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1`
Si vous utilisez le point de montage (mount point) lui-même, par ex. `C:\DynDrive`, le lecteur dynamique est malgré tout contrôlé. Vous pouvez déterminer l'alias du système d'exploitation à utiliser, à partir du fichier rapport de la protection temps réel.

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

Ajouter

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

Supprimer

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

Tenez compte des autres remarques pour indiquer les exceptions

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.

Un nom de fichier contenant des caractères de remplacement ne doit pas se terminer par une barre oblique inversée.
Par exemple :
`C:\Programmes\Application\applic*.exe\`
Cette entrée n'est pas valable et n'est pas considérée comme une exception.

Vous pouvez déterminer les chemins utilisés par la protection temps réel lors de la recherche de fichiers contaminés, à partir du fichier rapport de la protection temps réel. Utilisez systématiquement les mêmes chemins dans la liste des exceptions. Réglez la fonction de consignation de la protection temps réel sur **Intégrale** dans la configuration sous Rapport. La protection temps réel étant activée, accédez maintenant aux fichiers, répertoires, lecteurs intégrés . Vous pouvez maintenant lire le chemin à utiliser à partir du fichier rapport de la protection temps réel. Vous consultez le fichier rapport dans le Control Center sous Protection temps réel.

Heuristique

Cette rubrique de configuration contient les paramètres pour l'heuristique du moteur de recherche. (Option disponible uniquement si le mode expert est activé.)

Les produits Avira 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 complexe et un examen 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 peuvent aussi survenir. 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 signalé est digne de confiance.

Heuristique de macrovirus

Heuristique de macrovirus

Votre produit Avira contient une heuristique de macrovirus très performante. Si l'option est activée, toutes les macros du document contaminé sont supprimées si une réparation est possible ; les documents suspects peuvent aussi être seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce paramètre est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

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

Niveau de détection bas

Si l'option est activée, moins de logiciels malveillants inconnus sont détectés, le risque de détections erronées est faible dans ce cas.

Niveau de détection moyen

Si l'option est activée, une protection équilibrée est assurée avec peu de messages d'erreurs. Ce paramètre est activé par défaut si vous avez choisi l'utilisation de cette heuristique.

Niveau de détection élevé

Si l'option est activée, nettement plus de logiciels malveillants inconnus sont détectés, sachant qu'il faut toutefois s'attendre à des messages erronés.

10.2.2 Rapport

La protection temps réel dispose d'une fonction étendue de consignation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif. (Option disponible uniquement si le mode expert est activé.)

Consignation

Ce groupe permet de définir le contenu du fichier rapport.

Désactivée

Si l'option est activée, la protection temps réel ne génère pas de rapport.
Ne renoncez à la consignation que dans des cas exceptionnels, par ex. uniquement lorsque vous effectuez des tests avec de nombreux virus ou programmes indésirables.

Par défaut

Si l'option est activée, la protection temps réel consigne les informations importantes (sur les résultats positifs, les avertissements et les erreurs) dans le fichier rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce paramètre est activé par défaut.

Étendue

Si l'option est activée, la protection temps réel consigne également les informations secondaires dans le fichier rapport.

Intégrale

Si l'option est activée, la protection temps réel consigne toutes les informations dans le fichier rapport, même celles sur la taille et le type des fichiers, la date, etc.

Limiter le fichier de rapport

Limiter la taille à n Mo

Si l'option est activée, il est possible de limiter la taille du fichier rapport ; valeurs possibles : 1 à 100 Mo. En cas de limitation du fichier rapport, une marge d'environ 50 kilo-octets est laissée pour ne pas trop solliciter l'ordinateur. Si la taille du fichier 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 rapport avant de le raccourcir

Si l'option est activée, le fichier rapport est sauvegardé avant d'être raccourci.

Écrire la configuration dans le fichier rapport

Si l'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 limitation du fichier rapport, un nouveau fichier est automatiquement créé lorsque le fichier rapport a atteint une taille de 100 Mo. Une sauvegarde de l'ancien fichier rapport est créée. Jusqu'à trois sauvegardes des anciens fichiers rapport sont conservées. Les sauvegardes les plus anciennes sont supprimées.

10.3 Mise à jour

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

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, sélectionnez l'une des indications de temps dans le champ et modifiez-la via les touches fléchées à droite du champ de saisie.

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. (Option disponible uniquement si le mode expert est activé.)

10.3.1 Mise à jour produit

Sous **Mise à jour produit**, vous configurez l'exécution des mises à jour produit ou la notification des mises à jour produit disponibles. (Options disponibles uniquement si le mode expert est activé.)

Mises à jour produit

Télécharger et installer automatiquement les mises à jour produit

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 paramètre. Les conditions pour cette fonction sont : la configuration intégrale de la mise à jour et une connexion existante vers un serveur de téléchargement.

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

Si cette option est activée, des mises à jour produit sont téléchargées dès qu'elles 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 produit nécessitant un redémarrage de l'ordinateur, la mise à jour produit n'est pas effectuée aussitôt après le téléchargement des fichiers de mise à jour, mais seulement après le prochain redémarrage 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 paramètre. 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 produit sont disponibles. Les mises à jour du fichier de définitions des virus et du moteur de recherche sont toujours effectuées, indépendamment de ce paramètre. 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 produit automatique et n'affiche pas de notification concernant les mises à jour produit disponibles. Les mises à jour du fichier de définitions des virus et du moteur de recherche sont toujours effectuées, indépendamment de ce paramètre.

Avertissement
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 paramètres concernant la mise à jour produit (voir Mises à jour).

Remarque
Si vous avez activé une option de mise à jour produit automatique, vous pouvez configurer d'autres options pour le message et les possibilités d'interruption du redémarrage sous Paramètres de redémarrage. (Options disponibles uniquement si le mode expert est activé.)

10.3.2 Paramètres de redémarrage

Si une mise à jour de votre produit Avira est exécutée, il peut être nécessaire de redémarrer votre ordinateur. Si vous avez défini une exécution automatique des mises à jour produit sous Mise à jour > Mise à jour produit, vous pouvez choisir entre plusieurs options pour le message de redémarrage et pour l'annulation du redémarrage sous **Paramètres de redémarrage**. (Options disponibles uniquement si le mode expert est activé.)

Remarque
Veuillez noter concernant vos paramètres de redémarrage que vous pouvez choisir entre deux options d'exécution d'une mise à jour produit avec redémarrage obligatoire de l'ordinateur, dans la configuration sous Mise à jour > Mise à jour produit :
- **Télécharger et installer automatiquement les mises à jour produit** : la mise à jour et le redémarrage sont exécutés pendant qu'un utilisateur travaille

sur l'ordinateur. Si vous avez activé cette option, des routines de redémarrage avec possibilité d'annulation ou avec fonction de rappel peuvent être judicieuses.
- **Télécharger les mises à jour produit. Si un redémarrage est nécessaire, installer la mise à jour après le prochain redémarrage, sinon l'installer aussitôt** : la mise à jour et le redémarrage sont exécutés après qu'un utilisateur a démarré l'ordinateur et s'est connecté. Pour cette option, les routines de redémarrage automatiques sont conseillées.

Redémarrage de l'ordinateur après n secondes (avec messages de compte à rebours, pas de possibilité d'annulation)

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

Rappel périodique de redémarrage

Si l'option est activée, un redémarrage n'est pas effectué après l'exécution d'une mise à jour produit. Vous recevez aux intervalles définis des messages sur la nécessité du redémarrage mais vous ne pouvez pas les annuler. 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 n'est pas automatiquement effectué après l'exécution d'une mise à jour produit. Vous recevez un message unique où vous pouvez confirmer le redémarrage ou annuler la routine de redémarrage.

Redémarrage de l'ordinateur sans demande

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

10.3.3 Serveur Web

Serveur Web

La mise à jour peut être effectuée directement via un serveur Web sur Internet . (Options disponibles uniquement si le mode expert est activé.)

Connexion au serveur Web

Utiliser la connexion existante (réseau)

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

Utiliser la connexion suivante

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

L'Updater détecte automatiquement quelles options de connexion sont disponibles. Les options de connexion indisponibles sont grisées et ne peuvent pas être activées. Vous pouvez établir une connexion de télétransmission p. ex. manuellement sous Windows par une entrée de répertoire téléphonique.

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 des outils de numérotation (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 est terminé.

Remarque
L'option n'est pas disponible sous Vista et Windows 7. Sous Vista et Windows 7, la connexion de télétransmission ouverte pour la mise à jour est systématiquement interrompue, dès que le téléchargement est terminé.

Paramètres 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 paramètres système de Windows

Si cette option est activée, les paramètres système actuels de Windows pour la connexion au serveur Web via un serveur proxy sont utilisés. Vous configurez les

paramètres système de Windows pour l'utilisation d'un serveur proxy sous **Panneau de configuration > Options Internet > Connexions > Paramètres LAN**. Vous pouvez également accéder aux options Internet dans le menu **Outils** d'Internet Explorer.

Avertissement
Si vous utilisez un serveur proxy qui exige une authentification, indiquez les données complètes sous l'option **Connexion via ce proxy**. L'option **Utiliser les paramètres système de Windows** ne peut être utilisée que pour les serveurs proxy sans authentification.

Connexion via ce serveur proxy

Si l'option est activée, votre connexion au serveur Web a lieu via un serveur proxy, selon les paramètres que vous avez indiqués.

Adresse

Saisissez le nom de l'ordinateur ou l'adresse IP du serveur proxy que vous souhaitez utiliser pour la connexion au serveur Web.

Port

Saisissez le numéro de port du serveur proxy que vous souhaitez utiliser pour la connexion au 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 : `proxy.domaine.fr` Port : `8080`

Adresse : `192.168.1.100` Port : `3128`

10.4 Protection Web

La rubrique **Protection Web** sous **Configuration > Sécurité Internet** sert à la configuration de la protection Web.

10.4.1 Recherche

La protection Web 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 de la protection Web dans la rubrique **Recherche**. (Options disponibles uniquement si le mode expert est activé.)

Recherche

Prise en charge IPv6

Si l'option est activée, la protection Web prend en charge la version 6 du protocole Internet.

Protection contre les téléchargements automatiques intempestifs

La *protection contre les téléchargements automatiques intempestifs* vous permet de définir des paramètres 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 les bandeaux publicitaires. Dans certains cas, les I-Frames servent à dissimuler des logiciels malveillants. La zone de l'I-Frame n'est alors le plus souvent que peu ou pas visible dans le navigateur. L'option **Bloquer les I-Frames suspectes** vous permet de contrôler et de bloquer le chargement des I-Frames.

Bloquer les I-Frames suspectes

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

Action si résultat positif

Vous pouvez définir des actions que la protection Web doit exécuter quand un virus ou programme indésirable a été détecté. (Options disponibles uniquement si le mode expert est activé.)

Interactif

Si l'option est activée, une boîte de dialogue s'affiche dans laquelle vous pouvez sélectionner ce qui doit advenir du fichier contaminé en cas de détection d'un virus ou d'un programme indésirable pendant la recherche directe. Ce paramètre est activé par défaut.

Afficher la barre de progression

Si l'option est activée, un message s'affiche sur le Bureau 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 la protection Web, 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.

Vous trouverez de plus amples informations ici.

Automatique

Si l'option est activée, aucune boîte de dialogue permettant de sélectionner une action ne s'affiche en cas de détection d'un virus ou d'un programme indésirable. La protection Web réagit en fonction des paramètres réglés dans cette section.

Action primaire

L'action primaire est l'action exécutée lorsque la protection Web 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. Un message d'erreur de refus d'accès s'affiche dans le navigateur Web. La protection Web inscrit le résultat positif dans le fichier rapport, dès lors que la fonction de rapport est activée.

Déplacer en 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 l'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 la protection Web. L'accès au fichier est autorisé et le fichier est conservé.

Avertissement
Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

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 la protection Web. La protection Web empêche la transmission des données depuis Internet vers votre ordinateur. (Options disponibles uniquement si le mode expert est activé.)

Types de fichiers / types MIME bloqués par la protection Web

Tous les types de fichiers et les types MIME (types de contenus des données transmises) figurant dans la liste sont bloqués par la protection Web.

Champ de saisie

Saisissez dans ce champ les noms des types MIME et des types de fichiers qui doivent être bloqués par la protection Web. 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 la protection Web, 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 pour les entrées figurant dans la liste des types de fichiers et types MIME à exclure sous 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 quelconque de caractères ou ? pour un caractère exactement).

Types MIME : exemples de types de supports

- `text` = pour fichiers texte
- `image` = pour fichiers graphiques
- `video` = pour fichiers vidéo
- `audio` = pour fichiers son
- `application` = pour les fichiers associés à un programme particulier

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 la protection Web.
- `application/olescript` = les fichiers du type MIME application/olescript (fichiers script ActiveX *.axs) sont bloqués par la protection Web.

- `.exe` = tous les fichiers avec l'extension .exe (fichiers exécutables) sont bloqués par la protection Web.
- `.msi` = tous les fichiers avec l'extension .msi (fichiers Windows Installer) sont bloqués par la protection Web.

Ajouter

Ce bouton vous permet de valider dans la fenêtre d'affichage le type MIME ou de fichier entré dans le champ de saisie.

Supprimer

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

Exceptions

Ces options vous permettent d'exclure des types MIME (types de contenus des données transmises) et des types de fichiers d'URL (adresses Internet) de la recherche effectuée par la protection Web. Les types MIME et les URL indiqués sont ignorés par la protection Web, ce qui signifie que ces données ne sont pas contrôlées quant à l'absence de virus et logiciels malveillants, lors de la transmission sur votre ordinateur. (Options disponibles uniquement si le mode expert est activé.)

Types MIME à exclure par la protection Web

Dans ce champ, vous pouvez sélectionner les types MIME (types de contenus des données transmises) à exclure de la recherche par la protection Web.

Types de fichiers / types MIME à exclure par la protection Web (définis par l'utilisateur)

Tous les types de fichiers et types MIME (types de contenus des données transmises) figurant dans la liste sont exclus de la recherche par la protection Web.

Champ de saisie

Dans ce champ, vous pouvez indiquer les noms des types MIME et des types de fichiers à exclure de la recherche par la protection Web. 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 quelconque de caractères ou ? pour un caractère exactement).

Avertissement
Tous les types de fichiers et de contenus figurant sur la liste d'exclusion sont chargés dans le navigateur Internet sans contrôle additionnel des accès bloqués (liste des types fichiers et types MIME à bloquer sous Accès bloqués) ou de la protection Web : pour toutes les entrées figurant sur la liste d'exclusion, les entrées de la liste des types de fichiers et types MIME à bloquer sont ignorées. Aucune recherche de virus et de logiciels malveillants n'est effectuée.

Types MIME : exemples de types de supports

- `text` = pour fichiers texte
- `image` = pour fichiers graphiques
- `video` = pour fichiers vidéo
- `audio` = pour fichiers son
- `application` = pour les fichiers associés à un programme particulier

Exemples : types de fichiers et types MIME à exclure

- `audio/` = tous les fichiers de type audio sont exclus de la recherche effectuée par la protection Web
- `video/quicktime` = tous les fichiers vidéo du sous-type Quicktime (*.qt, *.mov) sont exclus de la recherche effectuée par la protection Web
- `.pdf` = tous les fichiers PDF Adobe sont exclus de la recherche effectuée par la protection Web.

Ajouter

Ce bouton vous permet de valider dans la fenêtre d'affichage le type MIME ou de fichier entré dans le champ de saisie.

Supprimer

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

URL à exclure par la protection Web

Toutes les URL de cette liste sont exclues de la recherche effectuée par la protection Web.

Champ de saisie

Saisissez dans ce champ les URL (adresses Internet) à exclure de la recherche par la protection Web, par ex. **www.nomdedomaine.com**. Vous pouvez indiquer des parties de l'URL en signalant le niveau de domaine avec des points finaux ou de début : nomdedomaine.fr pour tous les sites et tous les sous-domaines du domaine. Notez un site Web avec un domaine de niveau supérieur quelconque (.com ou .net) avec un point final : **nomdedomaine.**. 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.domaine.net).

Remarque
Lors de l'indication des URL, vous pouvez également utiliser le caractère de remplacement * pour un nombre quelconque de caractères. Utilisez aussi des points finaux ou de début en combinaison avec les caractères de remplacement, pour repérer les niveaux de domaine :
`nomdedomaine.*`
`*.nomdedomaine.com`
`.*nom*.com` (applicable mais pas recommandé)
Les indications sans points comme `*nom*` sont interprétées comme des parties d'un domaine de niveau supérieur et ne sont donc pas judicieuses.

Avertissement
Tous les sites Web figurant sur la liste des URL à exclure sont chargés dans le navigateur Internet sans contrôle additionnel : Aucune recherche de virus et de logiciels malveillants n'est effectuée. Par conséquent, n'excluez de la recherche par la protection Web que les URL dignes de confiance.

Ajouter

Ce bouton vous permet de valider dans la fenêtre d'affichage l'URL (adresse Internet) entrée dans le champ de saisie.

Supprimer

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

Exemples : URL à exclure

- `www.avira.com` -OU- `www.avira.com/*`
  = toutes les URL avec le domaine www.avira.com sont exclues de la recherche effectuée par la protection Web : www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,... Les URL avec le domaine www.avira.fr ne sont pas exclues de la recherche effectuée par la protection Web.
- `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 effectuée par la protection Web. 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 effectuée par la protection Web. L'indication implique tous les domaines

de niveau supérieur ou les sous-domaines existants pour .avira. : www.avira.com, www.avira.fr, forum.avira.com,...

- `.*domain*.*`
  = toutes les URL contenant un domaine de second niveau avec la chaîne de caractères domain sont exclues de la recherche effectuée par la protection Web : www.domain.com, www.new-domain.fr, www.sample-domain1.fr, ...
- `net` -OU- `*.net`
  = toutes les URL avec le domaine de niveau supérieur net sont exclues de la recherche effectuée par la protection Web : www.name1.net, www.name2.net,...

Avertissement
Indiquez aussi précisément que possible les URL que vous souhaitez exclure de la recherche effectuée par la protection Web. 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 effectuée par la protection Web par des indications globales définies sous la rubrique Exceptions. Il est recommandé d'indiquer au moins le domaine de second niveau entièrement et le domaine de niveau supérieur : nomdedomaine.com

Heuristique

Cette rubrique de configuration contient les paramètres pour l'heuristique du moteur de recherche. (Options disponibles uniquement si le mode expert est activé.)

Les produits Avira 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 complexe et un examen 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 peuvent aussi survenir. 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 signalé est digne de confiance.

Heuristique de macrovirus

Votre produit Avira contient une heuristique de macrovirus très performante. Si l'option est activée, toutes les macros du document contaminé sont supprimées si une réparation est possible ; les documents suspects peuvent aussi être seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce paramètre est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

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

Niveau de détection bas

Si l'option est activée, moins de logiciels malveillants inconnus sont détectés, le risque de détections erronées est faible dans ce cas.

Niveau de détection moyen

Si l'option est activée, une protection équilibrée est assurée avec peu de messages d'erreurs. Ce paramètre est activé par défaut si vous avez choisi l'utilisation de cette heuristique.

Niveau de détection élevé

Si l'option est activée, nettement plus de logiciels malveillants inconnus sont détectés, sachant qu'il faut toutefois s'attendre à des messages erronés.

10.4.2 Rapport

La protection Web dispose d'une fonction étendue de consignation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif.

Consignation

Ce groupe permet de définir le contenu du fichier rapport.

Désactivée

Si l'option est activée, la protection Web ne génère pas de rapport.
Ne renoncez à la consignation que dans des cas exceptionnels, par ex. uniquement lorsque vous effectuez des tests avec de nombreux virus ou programmes indésirables.

Par défaut

Si l'option est activée, la protection Web consigne les informations importantes (sur les résultats positifs, les avertissements et les erreurs) dans le fichier rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce paramètre est activé par défaut.

Étendue

Si l'option est activée, la protection Web consigne également les informations secondaires dans le fichier rapport.

Intégrale

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

Limiter le fichier de rapport

Limiter la taille à n Mo

Si l'option est activée, il est possible de limiter la taille du fichier rapport ; valeurs possibles : 1 à 100 Mo. Lors de la limitation du fichier rapport, une marge de 50 kilo-octets est laissée pour ne pas surcharger trop l'ordinateur. Si la taille du fichier 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.

Écrire la configuration dans le fichier rapport

Si l'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 limitation du fichier rapport, les anciennes entrées sont automatiquement supprimées lorsque le fichier rapport a atteint une taille de 100 Mo. Les entrées sont supprimées tant que le fichier rapport n'a pas atteint une taille de 80 Mo.

10.5 Contrôle parental

Utilisez les fonctions de *CONTRÔLE PARENTAL* d'Avira pour permettre un accès sécurisé à Internet à vos enfants ou autres personnes utilisant votre ordinateur.

10.6 Protection mobile

Avira ne protège pas uniquement votre ordinateur des virus et logiciels malveillants, mais empêche également la perte et/ou le vol des téléphones portables et smartphones équipés d'un système d'exploitation Android. La liste noire d'Avira Free Android Security vous permet en outre de bloquer les appels et SMS indésirables. Il vous suffit d'ajouter des numéros de téléphone à la liste noire depuis votre journal d'appels, votre journal de SMS ou votre liste de contacts, ou de créer manuellement des contacts que vous souhaitez bloquer.

10.6.1 Sécurité pour Android

Avira Free Android Security

Avira Free Android Security comprend deux composants :

- L'application proprement dite, installée sur votre appareil Android
- La console Web Avira Android pour l'enregistrement et le contrôle des fonctionnalités

Configuration requise

Système d'exploitation :

- Android 2.2 (Froyo)
- Android 2.3.7 (Gingerbread)
- Android 4.0.x (Ice Cream Sandwich)

Mémoire vive :

- 1,28 Mo d'espace mémoire libre.

Navigateur :

- Mozilla Firefox
- Google Chrome
- Opera
- Internet Explorer 7 ou une version ultérieure.

> **Remarque**
> Notez que Java doit être installé et activé et qu'une connexion Internet opérationnelle est nécessaire.

Caractéristiques de fonctionnement

Si vous ne retrouvez pas votre appareil, Avira Free Android Security vous propose quatre fonctions de protection de vos données personnelles via la console Web Avira Android :

Alerte sonore à distance

Vous déclenchez sur votre appareil une alarme qui retentit pendant 20 secondes.

Suivi de la localisation à distance

Vous activez une commande de localisation qui indique les paramètres de localisation de l'appareil.

Verrouillage à distance

Vous pouvez verrouiller votre appareil instantanément à l'aide d'un code PIN à 4 chiffres.

Suppression à distance

Vous pouvez supprimer des données de la carte SIM ou des cartes mémoire internes et externes. Vous pouvez également restaurer les paramètres d'usine de votre appareil via la console Web.

Remarque
Pour permettre à une commande de **restauration à distance des paramètres d'usine** de supprimer toutes les données de votre appareil en cas de perte ou de vol, vous devez activer l'option **Administrateur d'appareil** lors de la configuration.

Pour bloquer les appels et SMS indésirables, Avira Free Android Security propose une fonction de liste noire.

Liste noire

Vous pouvez ajouter des contacts à la liste noire depuis le journal d'appels, le journal de SMS ou votre liste de contacts, ou créer manuellement un contact que vous souhaitez bloquer.

Console Web

La console Web Avira est une application qui s'affiche dans un navigateur et qui permet la gestion des fonctions de sécurité. Le tableau de bord de la console Web vous permet de gérer votre compte et de déclencher des fonctionnalités à distance, telles que **Localiser**, **Verrouiller**, **Déclencher une alerte sonore** ou **Supprimer**.

La console Web Avira est composée d'une barre de titre, d'une barre latérale et d'un écran principal avec différents onglets. La barre de titre affiche vos informations de connexion et contient des liens vers la section Support et la gestion de votre compte. Vos appareils enregistrés sont répertoriés dans la barre latérale. L'écran principal de la console Web répertorie toutes les fonctionnalités de sécurité de l'application ainsi que les informations concernant la fonctionnalité **Liste noire** de votre appareil.

La barre de titre de la console Web

Informations sur le compte

La barre de titre contient des liens vous permettant d'accéder au **support technique** d'Avira, à votre **compte**, à vos informations de connexion, et de vous **déconnecter**.

- Cliquez sur le lien **Compte**.
  - ↪ La fenêtre **Informations sur le compte** s'affiche et comporte les champs suivants :

Date de création

Indique la date et l'heure à laquelle vous avez enregistré le compte.

Prénom

Ce champ vous permet d'indiquer votre prénom.

Nom

Ce champ vous permet d'indiquer votre nom de famille.

Langue

Dans le menu déroulant, sélectionnez votre langue préférée.

Pays

Dans le menu déroulant, sélectionnez un pays.

Type de compte

Indique le type de compte que vous utilisez.

Enregistrer les modifications

- Cliquez sur l'option **Enregistrer les modifications** pour enregistrer les données modifiées sur votre compte.

Gestion des mots de passe

La barre de titre de la console Web Avira contient un lien vers votre **compte** où vous pouvez également gérer votre mot de passe.

- Cliquez sur le lien **Compte**.
  - ↪ La fenêtre **Gestion des mots de passe** s'affiche et comporte les champs suivants :

Mot de passe

Entrez un nouveau mot de passe pour votre compte Avira Free Android Security.

Confirmation du mot de passe

Entrez de nouveau le mot de passe afin de le confirmer.

Modifier le mot de passe

- Cliquez sur ce bouton pour enregistrer les modifications apportées.

Sécurité du compte

La barre de titre de la console Web Avira contient un lien vers votre **compte**, où vous pouvez également définir une question de sécurité. La question de sécurité permet d'améliorer la sécurité de votre compte. Si vous oubliez vos informations de connexion ou si vous souhaitez modifier votre adresse e-mail, vous pouvez vous authentifier à l'aide de la question de sécurité.

- Cliquez sur le lien **Compte**.

↳ La fenêtre **Sécurité du compte** s'affiche et comporte les champs suivants :

Question de sécurité

Ouvre le menu déroulant avec les questions de sécurité ; parmi celles-ci, choisissez-en une à laquelle vous êtes le seul à pouvoir répondre. Cette question doit vous correspondre personnellement.

Réponse

- Entrez votre réponse dans ce champ.
- Assurez-vous que votre réponse ne comporte pas de faute de frappe et que vous vous en souviendrez aisément.

Enregistrer les modifications

- Cliquez sur l'option Enregistrer les modifications pour enregistrer la question de sécurité et votre réponse.

Gestion des appareils

La barre de titre de la console Web Avira contient un lien vers votre **compte**, où vous pouvez également gérer votre appareil.

↳ Cliquez sur le lien **Compte**.

↳ La fenêtre **Gestion des appareils** s'affiche et comporte les champs suivants :

Appareils disponibles

Ouvrez le menu déroulant pour sélectionner un appareil.

Supprimer l'appareil

- Cliquez sur ce bouton pour supprimer l'appareil sélectionné de votre compte.

Comment procéder

Comment modifier mon adresse e-mail ?

Adressez-vous au support d'Avira si vous devez modifier votre adresse e-mail. Votre adresse e-mail ne sert pas uniquement à vous contacter, elle fait aussi office d'identifiant. Par conséquent, vous ne pouvez pas la modifier vous-même à l'aide de la console Web ou via une application de votre appareil.

Comment protéger les données enregistrées sur mon appareil ?

La méthode la plus simple et la plus rapide pour protéger les données enregistrées sur votre appareil consiste à verrouiller celui-ci.

- Connectez-vous à la console Web.
- Accédez à l'onglet **Verrouiller**.
- Entrez un code PIN à 4 chiffres.
- Confirmez le code PIN.
- Cliquez sur **Verrouiller**.
  - ↪ Le code PIN peut désormais être utilisé pour verrouiller et déverrouiller votre appareil.

> **Remarque**
> Le code PIN n'est valable que temporairement. Un nouveau code PIN est nécessaire pour chaque commande de verrouillage/déverrouillage.

Comment déverrouiller mon appareil si j'ai oublié le code PIN ou entré un code PIN incorrect à trois reprises ?

Dans ce cas, vous devez vous connecter à la console Web et modifier votre code PIN.

- Connectez-vous à la console Web.
- Accédez à l'onglet **Verrouiller**.
- Entrez un code PIN à 4 chiffres.
- Confirmez le code PIN.
- Cliquez sur **Verrouiller**.
  - ↪ Le code PIN peut désormais être utilisé pour verrouiller et déverrouiller votre appareil.

Comment modifier mon code PIN ?

Vous ne pouvez modifier votre code PIN que via la console Web. Il n'est pas possible de le faire via l'application proprement dite.

- Connectez-vous à la console Web.
- Accédez à l'onglet **Verrouiller**.
- Entrez un code PIN à 4 chiffres.
- Confirmez le code PIN.
- Cliquez sur **Verrouiller**.
  - ↪ Le code PIN peut désormais être utilisé pour verrouiller et déverrouiller votre appareil.

Comment retrouver mon appareil en cas de vol ou de perte ?

Si vous avez perdu votre appareil ou s'il vous a été volé, Avira Free Android Security vous propose deux options qui vous permettront de le récupérer :

Déclencher une alerte sonore

La fonctionnalité de **déclenchement d'une alerte sonore** permet de vous aider à retrouver votre appareil. C'est particulièrement utile si vous l'avez perdu à proximité immédiate, par exemple, dans votre habitation.

- Connectez-vous à la console Web.
- Sélectionnez l'onglet **Alerte sonore** et cliquez sur **Déclencher une alerte sonore**.
  - ↪ Votre appareil émet alors un son puissant pendant 20 secondes pour vous aider à le retrouver. L'alerte sonore dure 20 secondes et elle ne peut pas être arrêtée ni interrompue pendant cette période. L'alerte sonore est émise même si votre appareil est en mode silencieux.

> **Remarque**
> L'alerte sonore ne se déclenche pas si l'appareil est éteint ou si la batterie est déchargée.

Localiser l'appareil

Si vous ne savez pas où vous avez perdu votre appareil ou si vous avez des raisons de penser qu'il a été volé, vous pouvez le localiser.

> **Remarque**
> Le processus de localisation peut durer jusqu'à 3 minutes. Vous ne pouvez pas relancer une commande **Localiser** si le processus est déjà en cours pour un même appareil. Par contre, vous pouvez utiliser la commande **Localiser** pour un autre appareil enregistré sur votre compte.

- Connectez-vous à la console Web.
- Sélectionnez l'onglet **Localiser**.
  - ↪ Un extrait de Google Maps s'affiche dans la console Web Avira.
- Cliquez sur l'option **Localiser** sous la carte affichée.
  - ↪ La durée écoulée du processus de localisation s'affiche. L'emplacement exact de votre appareil sera indiqué sur la carte. Les données géophysiques sont indiquées sous la forme de latitude et de longitude.

Comment enregistrer un nouvel appareil ?

Vous pouvez ajouter jusqu'à 5 appareils sur votre compte. Tous les appareils, ajoutés au même compte Google ou à la même adresse e-mail via l'application, sont enregistrés sur le même compte Avira Free Android Security. En d'autres termes, un compte de messagerie correspond à un compte Avira Free Android Security pouvant compter jusqu'à 5 appareils différents.

- Utilisez l'appareil que vous souhaitez ajouter à votre compte pour télécharger Avira Free Android Security.
- Installez l'application sur votre appareil.
- Sélectionnez le compte Google ou entrez une autre adresse e-mail et appuyez sur **Accepter le CLUF et continuer**.
  - ↪ Vous recevrez un message à cette adresse, confirmant l'enregistrement d'un nouvel appareil sur votre compte Avira Free Android Security existant.
  - ↪ Si vous vous connectez à la console Web, le nouvel appareil se trouve déjà dans la section **Tous vos appareils**, dans la partie gauche de la console Web.
- Vous pouvez à présent cliquer sur **Modifier** sous l'onglet « Appareil » pour accéder aux paramètres afin de modifier le nom de l'appareil, ainsi que le numéro de téléphone.

> **Remarque**
> Étant donné que vous ne pouvez ajouter que 5 appareils à un compte Avira Free Android Security, vous devez d'abord supprimer l'application de l'un de vos appareils enregistrés pour pouvoir en ajouter un nouveau. Vous pouvez également accéder aux paramètres du **compte** dans la console Web et sélectionner un appareil dans la liste déroulante sous **Gestion des appareils**, puis cliquer sur **Supprimer l'appareil**.

Résolution de problèmes

Résolution de problèmes

Messages d'erreur

Message	Signification
Connectez-vous à un réseau mobile ou Wi-Fi pour continuer.	Aucune connexion réseau n'a été trouvée pendant le processus d'enregistrement. Activez la connexion au réseau pour continuer.
Le service est actuellement indisponible. Veuillez réessayer plus tard.	Le service Google est actuellement indisponible.
Avira Free Android Security s'est bloqué. Appuyez ici pour nous aider à résoudre le problème.	Une erreur inattendue s'est produite, forçant l'arrêt de l'application. Il vous suffit d'appuyer pour nous envoyer automatiquement le journal d'erreurs.
Vous avez besoin d'un compte Google pour enregistrer votre appareil. Créez-en un, puis réessayez.	Aucun compte Google n'a été trouvé sur l'appareil.
Le mot de passe de votre compte Google a été modifié. Ouvrez l'application Google Mail ou Google Play pour mettre à jour le mot de passe sur votre appareil.	Le mot de passe du compte Google par défaut sur cet appareil n'est pas valide. Vérifiez si vous avez modifié l'authentification de votre compte Google. Mettez à jour et synchronisez le mot de passe de votre appareil en lançant l'application Google Mail ou Google Play.
Un nombre trop important d'applications sur votre appareil utilisent le service Push de Google (C2DM). Désinstallez-en une, puis réessayez.	Google limite le nombre d'applications installées sur votre appareil qui utilisent C2DM.
Une erreur s'est produite. Veuillez réessayer plus tard.	Une erreur inconnue s'est produite.
Plus de cinq appareils sont enregistrés avec ce compte. Supprimez-en un pour en ajouter un autre.	Vous avez atteint le nombre maximal de cinq appareils enregistrés sur Avira Free Android Security.

L'appareil n'est plus enregistré sur un compte Avira Free Android Security. L'application a par conséquent été réinitialisée.	Votre enregistrement a été réinitialisé, car cet appareil a été supprimé de la liste des appareils enregistrés.
Une erreur de serveur s'est produite. Veuillez réessayer plus tard.	Une erreur de serveur inconnue s'est produite.
Une erreur inattendue s'est produite, forçant l'arrêt de l'application. Aidez-nous à résoudre ce problème. Cliquez sur OK, et nous recevrons automatiquement le journal d'erreurs. Vous pouvez également ajouter des commentaires concernant ce problème :	Une erreur inattendue a fermé l'application. Aidez-nous à résoudre ce problème en cliquant sur OK. Cela nous permet de recevoir automatiquement le journal d'erreurs.
Erreur inattendue. Consultez la barre de notification pour plus d'informations.	Une erreur inattendue s'est produite.
Merci beaucoup !	Merci d'avoir signalé le problème, les informations ont été correctement envoyées.
En cas de perte ou de vol de votre appareil, Avira Free Android Security vous permet de restaurer les paramètres d'usine pour effacer les données de l'appareil. Afin d'effectuer cette opération, l'administrateur de l'appareil doit être activé.	Si vous avez perdu votre appareil, Avira Free Android Security vous permet d'effacer les données qu'il contient à l'aide d'une restauration des paramètres d'usine. Pour ce faire, la fonction **Administrateur d'appareil** doit être activée.
Connectez-vous à un réseau mobile ou Wi-Fi pour continuer.	Activez la connexion au réseau pour continuer.
Effacement via restauration des paramètres d'usine activé/désactivé.	La fonction d'effacement avec la commande de **restauration des paramètres d'usine** est activée/désactivée.

Votre appareil a bien été enregistré auprès d'Avira Free Android Security.	Avira Free Android Security a bien été enregistré.
Un e-mail a été envoyé à <jean.dupont@gmail.com>. Consultez votre compte de messagerie pour obtenir plus d'informations, ainsi que d'autres instructions.	Un e-mail contenant des informations d'activation a été envoyé à <jean.dupont@gmail.com>. Consultez ce message pour commencer à utiliser notre logiciel.
En cas de questions, consultez le forum de support ou contactez un collaborateur d'Avira.	En cas de questions, consultez notre forum ou contactez l'un de nos collaborateurs.
L'enregistrement a échoué. Redémarrez l'application, puis réessayez.	Une erreur inattendue s'est produite au cours du processus d'enregistrement. Redémarrez l'application et essayez à nouveau de vous enregistrer.
L'enregistrement a échoué. Il se peut que vous utilisiez une technologie incompatible avec Avira Free Android Security. Redémarrez l'application, puis réessayez.	Il se peut que votre appareil utilise une technologie incompatible avec Avira Free Android Security. Respectez la configuration requise suivante : Système d'exploitation : Android 2.2 (Froyo) - Android 2.3.7 (Gingerbread). Mémoire vive : 1,28 Mo d'espace mémoire libre. Navigateurs : Mozilla Firefox, Google Chrome, Opera et Internet Explorer 7 ou une version ultérieure.
Échec de la création du contact	Impossible d'ajouter le contact à la liste noire car il s'y trouve déjà.

Le nom existe déjà dans la liste noire	Ce nom se trouve déjà dans la liste noire, il ne peut donc pas être ajouté une deuxième fois.
Le contact existe déjà dans la liste noire	Ce contact se trouve déjà dans la liste noire, il ne peut donc pas être ajouté une deuxième fois.
Le numéro existe déjà dans la liste noire pour <Jean Dupont>	Ce numéro de téléphone se trouve déjà dans la liste noire et est associé au contact <Jean Dupont>, il ne peut donc pas être ajouté une deuxième fois.

Glossaire

Abréviation/terme	Signification
C2DM	Le service Android Cloud to Device Messaging (C2DM) de Google permet d'envoyer des données depuis des serveurs vers les applications installées sur votre appareil.
IMEI	L'International Mobile Equipment Identity (littéralement : identité internationale d'équipement mobile) est un numéro unique, semblable à une empreinte digitale, permettant d'identifier les appareils.
Carte SIM	La carte SIM (Subscriber Identification Module, soit : module d'identification de l'abonné) est une carte de fournisseur, sur laquelle différentes informations sont enregistrées, telles que le numéro de série, le numéro de téléphone et votre code PIN.
PIN	Le code PIN (Personal Identification Number) est le numéro d'identification personnel, généralement constitué d'un nombre à 4 chiffres.

SE	Système d'exploitation de votre appareil.
GPS	Le Global Positioning System (littéralement : système de localisation mondial) est un système par satellites qui fournit des données temporelles et de localisation à des récepteurs GPS.
Tour de transmission cellulaire	Technologie radio avancée qui capte les signaux des téléphones mobiles et les transmet à d'autres tours, à l'aide d'ondes radio.
Wi-Fi	Il s'agit d'une norme qui permet l'échange de données et l'accès sans fil à Internet.
WLAN	Accès au réseau sans fil.
Cloud	Il s'agit d'une infrastructure informatique et d'un emplacement de serveur distant. Les données enregistrées dans le cloud ne sont pas enregistrées localement sur l'ordinateur.
Autre numéro de téléphone	Numéro de téléphone auquel vous pouvez être contacté à l'aide du bouton **Appeler le propriétaire** sur l'appareil verrouillé.
Latitude	Coordonnée géographique qui indique la position nord-sud sur Terre.
Longitude	Coordonnée géographique qui indique la position est-ouest sur Terre.

Service

Support

Service de support

Vous trouverez toutes les informations nécessaires concernant notre service complet de support sur notre page Web http://www.avira.com.

Forum de la communauté

Avant de contacter notre service d'assistance téléphonique, nous vous recommandons de consulter notre forum d'utilisateurs à l'adresse http://forum.avira.com.
Il se peut que votre problème ait déjà été évoqué et résolu au sein de la communauté.

FAQ

Passez également en revue la section FAQ, disponible sur notre site Web : http://www.avira.com/fr/support-for-home-knowledgebase
. Il se peut que votre question y ait déjà été posée et qu'une réponse ait déjà été publiée par d'autres utilisateurs.

Contact

Adresse

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
D-88069 Tettnang
Allemagne

Internet

Vous trouverez davantage d'informations nous concernant et relatives à nos produits à l'adresse suivante :
http://www.avira.com

Commande

Console Web

Une fois l'installation terminée, vous devez enregistrer votre appareil pour accéder à la console Web Avira.

- La console Web Avira est composée d'une barre de titre, d'une barre latérale et d'un écran principal avec différents onglets.
- La barre de titre affiche vos informations de connexion et contient des liens vers la section Support et la gestion de votre compte. En outre, vous pouvez sélectionner les paramètres linguistiques de la console Web Avira à cet endroit.
- Vos appareils enregistrés sont répertoriés dans la barre latérale.
- Chaque appareil s'affiche dans un champ distinct :
  - Cliquez sur le bouton **Modifier** présent dans le champ relatif à l'appareil pour accéder à l'onglet **Paramètres** de la console Web, depuis lequel vous pouvez gérer le nom et le numéro de téléphone de votre appareil.
- Dans le bas de la barre latérale, un lien vous permet d'indiquer et d'enregistrer une question de sécurité personnelle.

- L'écran principal de la console Web répertorie toutes les fonctionnalités de sécurité permettant de contrôler votre appareil Android ainsi que les informations concernant le contenu de votre liste noire.

Onglets de la console Web

La console Web comporte les onglets suivants :

- Tableau de bord
- Localiser
- Effacer
- Alerte sonore
- Verrouiller
- Liste noire
- Paramètres

Tableau de bord de la console Web Avira Free Android Security

L'onglet **Tableau de bord** contient différentes informations sur chaque appareil ainsi que des boutons de commande permettant de déclencher des actions visant à protéger l'appareil.

Informations sur l'appareil

- Marque : marque de l'appareil.
- Modèle : désignation du modèle de l'appareil.
- IMEI : l'International Mobile Equipment Identity (littéralement : identité internationale d'équipement mobile) est un numéro unique à 15 chiffres, permettant d'identifier les téléphones mobiles et certains téléphones satellite.
- Version du SE : numéro de version du système d'exploitation Android.
- Version de l'application : numéro de version de l'application Avira installée. Si vous utilisez une version obsolète, un symbole d'avertissement s'affiche en rouge.
- Admin. app. : indique si l'administrateur de l'appareil est activé. Un symbole d'avertissement rouge s'affiche si cette fonction est désactivée.
- Batterie : informations concernant le niveau de charge de la batterie (en pourcent).
- Numéro de téléphone : numéro de téléphone enregistré sur la carte SIM.
- Réseau : réseau mobile auquel la carte SIM appartient.
- Pays : pays d'origine de la carte SIM.
- **Actualiser** : bouton d'actualisation permettant de mettre à jour les informations sur l'appareil.

Suivi de la localisation

- Dernière localisation : moment de la dernière localisation de l'appareil, par ex. « il y a 5 heures », « il y a 3 jours ».
- Latitude : latitude exacte de l'emplacement de l'appareil.
- Longitude : longitude exacte de l'emplacement de l'appareil.

Verrouiller l'appareil

- Dernière action : dernière action effectuée via la console Web, par ex. « Verrouiller ».
- Dernier déclenchement : moment du dernier verrouillage / déverrouillage de l'appareil.

Déclencher une alerte sonore

- Dernier déclenchement : période écoulée depuis le dernier envoi d'une alerte à l'appareil.

Supprimer les données

- Dernier effacement : période écoulée depuis le dernier effacement sur l'appareil.
- Type : type d'action d'effacement effectuée sur l'appareil.

Liste noire

- Cette fonction permet de bloquer des appels et SMS indésirables.

Localiser

L'onglet **Localiser** affiche un extrait de Google Maps. Le statut du suivi de la localisation est affiché sous la carte.

- Cliquez sur le bouton **Localiser** pour lancer la localisation de l'appareil égaré.
  - ↪ La localisation peut prendre quelques minutes, en fonction des performances du réseau et de la force du signal.

  Avira Free Android Security recherche l'appareil via GPS, tours de transmission cellulaire et réseau local sans fil.

  La durée écoulée du processus de localisation s'affiche.

  - ↪ L'emplacement exact de l'appareil égaré est ensuite indiqué sur la carte. Vous pouvez effectuer un zoom avant ou arrière sur la carte.

Effacer

Remarque
Si votre version d'Avira Free Android Security ne prend pas en charge la

fonction d'effacement, mettez l'application à jour sur votre appareil en suivant les instructions décrites dans notre base de connaissances. Ensuite, il vous suffit d'actualiser cette page pour accéder à l'ensemble des fonctionnalités de la **fonction d'effacement**.

Trois options de suppression de données sont disponibles sous l'onglet **Effacer**. Vous pouvez également sélectionner une combinaison de ces options d'effacement. La fonction d'effacement entraîne la suppression définitive des données. En d'autres termes, les données supprimées par cette procédure ne peuvent pas être restaurées.

Remarque
Vous devez verrouiller votre appareil pour pouvoir déclencher une commande d'effacement. Nous vous conseillons vivement de sauvegarder vos données importantes avant de lancer toute commande d'effacement.

Carte SIM

La fonction d'effacement de la **carte SIM** supprime toutes les données de votre carte SIM. Toutes les informations de contact et les SMS enregistrés sur la carte SIM sont supprimés. Une fois supprimées, ces données ne peuvent plus être restaurées. L'effacement de la carte SIM n'affecte pas les données enregistrées sur votre appareil ou sur la carte SD.

Remarque
Selon le type de carte, l'effacement de la carte SIM n'est pas toujours possible.

- Cliquez sur **Carte SIM** pour supprimer toutes les données enregistrées sur la carte SIM.
- Confirmez la suppression en cliquant sur **OK**.
  - ↪ Le message **La carte SIM a été effacée !** s'affiche.
- Cliquez sur **OK** pour fermer le message et revenir sous l'onglet Effacer.

Toute la mémoire

La fonction d'effacement de **toute la mémoire** supprime toutes les données enregistrées sur votre appareil ou votre carte SD. Une fois supprimées, ces données ne peuvent plus être restaurées. L'effacement de **toute la mémoire** n'affecte pas les données enregistrées sur la carte SIM.

- Cliquez sur **Effacer la mémoire** pour supprimer les données enregistrées directement sur votre appareil ou sur la carte SD.
- Confirmez la suppression en cliquant sur **OK**.
  - ↪ Le message **La mémoire a été effacée !** s'affiche.

- Cliquez sur **OK** pour fermer le message et revenir sous l'onglet Effacer.

Restauration des paramètres d'usine

L'option **Restauration des paramètres d'usine** rétablit les paramètres par défaut de votre appareil et supprime également tous les comptes, applications et données d'application de l'appareil. La **restauration des paramètres d'usine** n'affecte pas les données enregistrées sur la carte SIM ou sur la carte SD.

> **Remarque**
> Pour permettre à une commande de **restauration des paramètres d'usine** de supprimer toutes les données de votre appareil en cas de perte ou de vol, vous devez activer l'option **Administrateur d'appareil** lors de la configuration.

- Cliquez sur **Restauration des paramètres d'usine** pour rétablir les paramètres par défaut de votre appareil.
- Confirmez ce type de suppression en cliquant sur **OK**.
- Cliquez à nouveau sur **OK** pour continuer.
- Pour fermer le message vous informant de la réussite de la **restauration des paramètres d'usine**, cliquez sur **OK**.

> **Avertissement**
> La **restauration des paramètres d'usine** désinstalle également Avira Free Android Security. Vous ne serez alors plus en mesure de transmettre des commandes à votre appareil via la console Web, par ex. vous ne pourrez plus verrouiller ni localiser votre appareil.

Suppression groupée

L'option de **suppression groupée** vous permet de recourir à un, deux ou trois types d'effacement à la fois.

- Sélectionnez les types d'effacement que vous souhaitez utiliser ou cliquez sur **Tout sélectionner** pour lancer tous les types d'effacement en une fois.
- Cliquez sur **Lancer les actions d'effacement sélectionnées**.
- Confirmez votre choix en cliquant sur **OK**.
  - ↪ Selon votre sélection et la taille de la mémoire de votre appareil, cette action peut prendre jusqu'à 60 minutes.
- Cliquez sur **OK** pour continuer.
- Pour fermer le message vous informant de la réussite de la **suppression groupée**, cliquez sur **OK**.

Les effets des trois types d'effacement sont les suivants :

Mémoire affectée	Carte SIM	Toute la mémoire	Restauration des paramètres d'usine
SMS sur l'appareil			suppression
SMS sur la carte SIM	suppression		
Contacts sur l'appareil			suppression
Contacts sur la carte SIM	suppression		
Données de la carte SD		suppression	
Données de la mémoire USB interne		suppression	
Comptes, applications, données d'application			suppression

Alerte sonore

L'onglet **Alerte sonore** vous permet de déclencher un son puissant émis par votre appareil. Cette fonction vous aide à retrouver rapidement votre appareil.

- Cliquez sur le bouton **Déclencher une alerte sonore** pour lancer cette fonction.
  - ↪ Votre appareil émet un son puissant pendant 20 secondes. L'alerte sonore ne peut pas être arrêtée ni interrompue pendant ce laps de temps.

Verrouiller

Sous l'onglet **Verrouiller**, vous pouvez entrer un code PIN à 4 chiffres pour verrouiller et déverrouiller votre appareil. Vous pouvez entrer un message personnalisé qui s'affichera sur l'écran de verrouillage de votre appareil. Vous pouvez ajouter un numéro de téléphone à appeler à l'aide du bouton **Appeler le propriétaire** sur l'appareil verrouillé.

> **Remarque**
> Vous devez verrouiller votre appareil pour pouvoir déclencher une commande d'effacement. Nous vous conseillons en outre de verrouiller votre appareil afin de protéger vos données personnelles.

- Entrez un code PIN à 4 chiffres dans le champ **Entrer code PIN**.
- Confirmez votre code PIN dans le champ situé en dessous.
  - ↪ Si vous avez défini un code PIN précédemment, vous ne pouvez déverrouiller votre appareil que manuellement. Si vous avez oublié votre code PIN, vous devez déverrouiller votre appareil via la console Web.
- Dans le champ **Message en cas de perte**, entrez un message à afficher sur votre appareil verrouillé. Rédigez par exemple un texte suivi de votre adresse e-mail afin que la personne qui le trouve puisse vous contacter facilement.
- Dans le champ **Autre numéro de téléphone**, entrez un numéro de téléphone grâce auquel vous pouvez être contacté à l'aide du bouton **Appeler le propriétaire** sur l'appareil verrouillé. Utilisez un numéro fiable, tel que votre numéro de téléphone fixe ou le numéro d'un ami.
- Cliquez sur **Verrouiller** pour enregistrer le code PIN sur votre appareil et pour verrouiller ce dernier.
- Cliquez sur **Déverrouiller** si vous souhaitez déverrouiller votre appareil à l'aide de la console Web.

Liste noire

Si vous ne voulez pas être dérangé par certains appels et SMS, vous pouvez simplement ajouter ces numéros à la liste noire. Cette fonction vous permet de bloquer des appels et SMS indésirables. Vous pouvez ajouter des numéros à partir de vos contacts, de votre journal d'appels et de vos messages, ou entrer manuellement un numéro.

Ajouter des numéros à la liste noire depuis les journaux de votre appareil

Ajoutez simplement des numéros à la liste noire depuis vos journaux d'appels et de messages ou depuis vos contacts.

- Ouvrez Avira Free Android Security sur votre appareil.
- Sélectionnez **Liste noire**.
  - ↪ L'écran **Liste noire** s'affiche.

- Sélectionnez le bouton **Ajouter**.
  - ↪ L'écran **Ajouter les contacts à la liste noire** s'affiche.
- Sélectionnez le champ correspondant au journal depuis lequel vous souhaitez ajouter un numéro à la liste noire.

  Si vous ne souhaitez pas ajouter de numéro à la liste noire, appuyez sur **Annuler**.

  Sélectionnez le numéro que vous souhaitez bloquer.
  - ↪ L'écran suivant affiche le numéro et le nom du contact que vous souhaitez bloquer.
- Sélectionnez le type de blocage que vous souhaitez effectuer. Vous disposez des options **Appels et SMS**, uniquement **Appels** ou uniquement **SMS**.
- Cliquez sur **Enregistrer** afin d'enregistrer le numéro dans la liste noire.
- Le numéro bloqué s'affiche sur l'écran **Liste noire**.

> **Remarque**
> Si le contact que vous souhaitez ajouter se trouve déjà dans la liste noire, vous recevez un message d'erreur.

Ajouter manuellement des numéros à la liste noire

Vous pouvez également entrer manuellement des numéros dans la liste noire.

- Ouvrez Avira Free Android Security sur votre appareil.
- Sélectionnez **Liste noire**.
  - ↪ L'écran **Liste noire** s'affiche.
- Sélectionnez le bouton **Ajouter**.
  - ↪ L'écran **Ajouter les contacts à la liste noire** s'affiche.
- Sélectionnez l'option **Créer un contact manuellement** si vous souhaitez entrer un numéro.
  - ↪ L'écran **Entrer les coordonnées** s'affiche.
- Touchez le champ **Nom** afin d'accéder au clavier permettant d'entrer les lettres.
- Touchez le champ **Numéro de téléphone** afin d'accéder au clavier permettant d'entrer les chiffres.
- Sélectionnez le type de blocage que vous souhaitez effectuer. Vous disposez des options **Appels et SMS**, uniquement **Appels** ou uniquement **SMS**.
- Cliquez sur **Enregistrer** afin d'enregistrer le numéro dans la liste noire.

Modifier la liste noire

Vous pouvez modifier le numéro de téléphone et le nom de votre contact bloqué.

- Ouvrez Avira Free Android Security sur votre appareil.

- Sélectionnez **Liste noire**.
  - ↪ L'écran **Liste noire** s'affiche.
- Sélectionnez le contact que vous souhaitez modifier.
  - ↪ L'écran **Entrer les coordonnées** s'affiche.
- Touchez le champ **Nom** afin d'accéder au clavier permettant de modifier le nom.
- Touchez le champ **Numéro de téléphone** afin d'accéder au clavier permettant de modifier le numéro.
- Cliquez sur **Enregistrer** afin d'enregistrer le contact modifié dans la liste noire.
- Cliquez sur **Annuler** si vous ne souhaitez pas enregistrer les modifications effectuées.

Événements bloqués

Vous pouvez consulter l'historique de tous vos contacts bloqués sous l'onglet **Événements bloqués**. Vous pouvez trier la liste par ordre chronologique et par type de prise de contact, par ex. appels ou SMS. Le nom du contact, la date, l'heure, ainsi que le type de tentative de contact sont affichés.

- Sélectionnez le bouton **Tous** pour pouvoir sélectionner les événements suivants : **Tous**, **Aujourd'hui** ou **Nouveau**.
- Sélectionnez le bouton **Appels et SMS** pour afficher à la fois les appels et messages bloqués. Sélectionnez l'option **Appels** pour vérifier quels sont les contacts bloqués qui ont tenté de vous appeler. Sélectionnez l'option **SMS** pour afficher les messages bloqués.

Supprimer des entrées des événements bloqués

Vous pouvez supprimer des entrées des **événements bloqués**. Triez la liste en fonction des événements suivants : **Tous**, **Aujourd'hui** ou **Nouveau,** et sélectionnez l'option **Appels et SMS**, **Appels** ou **SMS**. Vous pouvez supprimer tous les événements ou le faire individuellement. Par exemple, si vous filtrez sur **Tous** et **Appels**, tous les appels bloqués sont répertoriés. Vous avez alors la possibilité de supprimer chronologiquement tous les appels bloqués de vos contacts. Ou vous sélectionnez certains contacts et ne supprimez que les appels affichés.

- Sélectionnez le contact dont vous souhaitez supprimer les événements bloqués.
  - ↪ L'heure et le nombre d'appels et/ou SMS reçus s'affichent.
- Sélectionnez le champ **SMS** pour afficher le contenu des SMS bloqués.
  - ↪ Vous pouvez alors ouvrir et lire les messages.
  - ↪ Vous pouvez supprimer tous les SMS ou le faire individuellement.

  L'option **Sélectionner tout** permet de sélectionner tous les SMS pour suppression ; vous pouvez également sélectionner les SMS individuellement.

Sélectionnez l'option **Supprimer** pour supprimer tous ces messages, ou appuyez sur **Retour** pour annuler la suppression.

↪ Vous êtes invité à confirmer la suppression des SMS bloqués.

Appuyez sur **Supprimer** pour supprimer les SMS sélectionnés de l'historique.

Appuyez sur **Annuler** pour arrêter la suppression.

- Sélectionnez le champ **Appels** pour afficher tous les appels de vos contacts bloqués.

  ↪ Vous pouvez supprimer tous les appels ou le faire individuellement.

  L'option **Sélectionner tout** permet de sélectionner tout l'historique des appels pour suppression ; vous pouvez également sélectionner les appels individuellement.

  Sélectionnez l'option **Supprimer** pour supprimer tous ces appels, ou appuyez sur **Retour** pour annuler la suppression.

  ↪ Vous êtes invité à confirmer la suppression des appels bloqués.

  Appuyez sur **Supprimer** pour supprimer les appels sélectionnés de l'historique.

  Appuyez sur **Annuler** pour arrêter la suppression.

Rapports

L'onglet **Paramètres** comporte la section **Rapports** qui permet d'afficher toutes les activités d'Avira Free Android Security effectuées à l'aide de la console Web.

Les informations répertoriées sont classées par date et heure.

Exemple d'informations affichées par le rapport d'activités :

Date	Heure	Message
Mardi 7 août 2012	15 h 17	Informations sur l'appareil actualisées
Mardi 7 août 2012	14 h 05	Appareil localisé
Lundi 13 août 2012	18 h 11	Appareil déverrouillé

Paramètres

L'onglet Paramètres vous permet de gérer le nom et le numéro de téléphone de votre appareil. En outre, la section **Rapports** permet de vérifier toutes les activités d'Avira Free Android Security effectuées à l'aide de la console Web.

- Dans la barre de navigation, cliquez sur l'appareil que vous souhaitez gérer.
- Entrez le nom de votre appareil dans le champ **Nom de l'appareil**.
- Entrez le numéro de téléphone de cet appareil dans le champ **Numéro de téléphone**.
- Cliquez sur **Enregistrer les modifications** pour enregistrer les paramètres que vous avez définis pour cet appareil.
  - ↪ La console Web Avira Android indique que les paramètres ont bien été enregistrés.

Installation et désinstallation

Installation et désinstallation

Téléchargement et installation

Téléchargez l'application Avira Free Android Security directement depuis Google Play sur votre appareil et installez-la. Une fois l'installation terminée, vous êtes invité à enregistrer votre appareil via l'écran d'enregistrement d'Avira Free Android Security. Pour ce faire, vous pouvez utiliser votre compte Google ou une adresse e-mail créée auprès d'un autre fournisseur. Une connexion Internet stable est nécessaire pour effectuer cette procédure.

- Appuyez sur **Ouvrir** pour ouvrir le formulaire d'enregistrement.
- Entrez votre compte Google ou une autre adresse e-mail.
- Appuyez sur **Accepter le CLUF et continuer** pour poursuivre.
  - ↪ Vous recevrez un message de confirmation d'Avira pour votre nouveau compte Avira Free Android Security à l'adresse e-mail indiquée. Ce message de confirmation comprend un lien vous permettant de définir un mot de passe personnel pour vous connecter à la console Web Android.
- Cliquez sur le lien repris dans le message de confirmation pour définir un mot de passe et activer la console Web Android.
  - ↪ La console Web vous permet désormais de contrôler à distance vos appareils.

Pour permettre à une commande de **restauration des paramètres d'usine** de supprimer toutes les données de votre appareil en cas de perte ou de vol, vous devez activer l'option **Administrateur d'appareil** lors de la configuration :

- Pour activer la fonction Administrateur d'appareil, appuyez sur le bouton **Activer**.
  - ↪ La boîte de dialogue **Activer l'administrateur d'appareil** s'affiche.

- Confirmez l'activation de l'**administrateur d'appareil** en appuyant sur le bouton **Activer**.
  - ↪ Vous autorisez alors Avira Free Android Security à effacer toutes les données de l'appareil au cas où vous souhaiteriez exécuter une commande de **restauration des paramètres d'usine**.

Si vous hésitez à installer l'administrateur d'appareil pendant la configuration, vous pouvez activer cette option de configuration ultérieurement. Procédez comme suit :

- Ouvrez Avira Free Android Security sur votre appareil.
- Appuyez sur le bouton **Paramètres**.
  - ↪ Vous pouvez vérifier si l'option d'**effacement grâce à une commande de restauration des paramètres d'usine** est activée.
- Appuyez sur le champ **Paramètres d'effacement**.
  - ↪ La boîte de dialogue **Activer l'administrateur d'appareil** s'affiche.
- Appuyez sur le bouton **Activer** situé dans le bas de la boîte de dialogue.
- Confirmez l'activation de l'administrateur d'appareil en appuyant à nouveau sur le bouton **Activer**.
  - ↪ Vous pouvez alors voir que la fonction d'**effacement grâce à une commande de restauration des paramètres d'usine** est activée.

- **Remarque**
  Vous pouvez activer et désactiver l'**administrateur d'appareil** à tout moment via l'application Avira Free Android Security de votre appareil, en sélectionnant **Paramètres > Paramètres d'effacement > Effacer avec restauration des paramètres d'usine > Activer / Désactiver**.

Installation via un ordinateur

Vous pouvez télécharger l'application Avira Free Android Security via un ordinateur.

- Ouvrez Google Play sur votre ordinateur.
- Recherchez l'application Avira Free Android Security.
- Cliquez sur **Installer** pour télécharger l'application sur votre ordinateur.
  - ↪ Vous êtes invité à vous connecter pour installer l'application.
- Cliquez sur **Se connecter** pour accéder à votre compte Google.
- Entrez vos informations de connexion.
- Cliquez sur **OK** pour télécharger l'application vers un appareil sélectionné.
  - ↪ L'application Avira Free Android Security est téléchargée sur cet appareil.
- Cliquez sur **OK** pour fermer la boîte de dialogue de téléchargement.

↪ Le site Web de Google Play s'affiche à nouveau et le bouton **Installé** indique que l'application est déjà téléchargée sur l'appareil.

Désinstallation

Pour désinstaller Avira Free Android Security, deux étapes sont nécessaires. Vous devez désinstaller l'application de votre appareil, puis supprimer l'appareil de votre compte depuis la console Web Avira Android.

> **Remarque**
> Assurez-vous que l'**administrateur d'appareil** est désactivé avant de désinstaller Avira Free Android Security.

Si vous souhaitez désinstaller Avira Free Android Security, accédez au gestionnaire d'applications de votre appareil.

- Appuyez sur l'application Avira Free Android Security et sélectionnez l'option **Désinstaller**.
- Confirmez la désinstallation.

En outre, vous devez supprimer l'appareil du compte Avira Free Android Security depuis la console Web.

- Ouvrez la console Web Avira.
- Cliquez sur le lien **Compte** de la barre de titre.
- Accédez à la gestion des appareils et ouvrez le menu déroulant **Appareils disponibles**.
- Sélectionnez l'appareil duquel vous souhaitez supprimer l'application Avira Free Android Security.
- Cliquez sur **Supprimer l'appareil** afin de supprimer l'appareil de votre compte.

Réinstallation

Une fois tous vos appareils désinstallés, vous ne pouvez plus accéder à la console Web Avira.

Vous pouvez toutefois réinstaller Avira Free Android Security sur un appareil à l'aide de votre compte de messagerie précédent.

- Accédez à la console Web en utilisant vos anciennes informations de connexion.
- Une fois connecté, vous pouvez modifier votre mot de passe via la section relative à la **gestion des mots de passe**.

  Sélectionnez **Compte > Gestion des mots de passe**, tapez votre nouveau mot de passe et confirmez-le.

- Si vous avez oublié votre mot de passe, cliquez sur le lien **Mot de passe oublié ?** sur la page de connexion.
  - ↪ Nous vous invitons à nous envoyer votre adresse e-mail. Nous vous enverrons ensuite un lien vous permettant de redéfinir votre mot de passe.

Création du compte Android

Pour garder un œil en permanence sur votre smartphone et protéger vos données personnelles à l'aide de diverses fonctions à distance via la console Web, vous devez d'abord créer un compte Avira Free Android Security. Vous pouvez créer un compte avant de télécharger l'application sur votre appareil.

- Ouvrez le Control Center de votre produit Avira.
- Cliquez sur **Control Center > Protection mobile > Android Security**.
  - ↪ La page de téléchargement d'Avira Free Android Security s'affiche.
- Cliquez sur **Télécharger maintenant**.
  - ↪ La page Web des applications Google Play Android s'affiche.

  Cliquez sur **Installer**.
  - ↪ Vous êtes invité à vous connecter à Google pour télécharger l'application Avira Free Android Security.

  Cliquez sur **Se connecter**.

  Entrez votre adresse e-mail et votre mot de passe.

  Cliquez sur **Se connecter**.

  Sélectionnez l'appareil sur lequel vous souhaitez télécharger Avira Free Android Security.

  Cliquez sur **Installer**.
  - ↪ L'application est téléchargée sur votre appareil Android.
- Ouvrez Avira Free Android Security sur votre appareil.

  Appuyez sur **Démarrage**.
  - ↪ La page de votre compte s'affiche.

  Entrez vos informations de connexion.

  Appuyez sur **Accepter le CLUF et continuer** pour poursuivre.
  - ↪ Vous recevrez un message de confirmation d'Avira pour votre nouveau compte. Ce message de confirmation comprend un lien vous permettant de définir un mot de passe personnel pour vous connecter à la console Web Android.

  Cliquez sur le lien repris dans le message de confirmation pour définir un mot de passe et activer la console Web Android.
  - ↪ La console Web vous permet désormais de contrôler à distance vos appareils via la page Web suivante : https://android.avira.com

Création du compte Android en quelques secondes

Pour garder un œil en permanence sur votre smartphone et protéger vos données personnelles à l'aide de diverses fonctions à distance via la console Web, vous devez d'abord créer un compte Avira Free Android Security. Vous pouvez créer un compte avant de télécharger l'application sur votre appareil.

- Ouvrez la page Web Avira Free Android Security.
  - ↪ Le lien permettant d'accéder à la page de téléchargement d'Avira Free Android Security s'affiche.
- Cliquez sur le bouton **Se connecter maintenant**.
  - ↪ La page de connexion s'affiche.
- Entrez votre adresse Google ou une autre adresse e-mail de votre choix.

  Cliquez sur **Créer un compte**.
  - ↪ Avira envoie le message de confirmation à l'adresse spécifiée. Ce message de confirmation comprend un lien vous permettant d'accéder à la console Web d'Avira Free Android Security.
- Cliquez sur le lien repris dans le message de confirmation.
  - ↪ Vous accédez à la console Web Avira Free Android Security.
  - ↪ La console Web vous permet désormais de contrôler à distance vos appareils via la page suivante : https://android.avira.com

> **Remarque**
> Lorsque vous téléchargez l'application Avira Free Android Security sur votre appareil après vous être enregistré sur la console Web, veillez à utiliser les mêmes informations de connexion sur la page **Votre compte** lors de la configuration.

Connexion au compte Android

- Cliquez sur **Centre de commande > Protection mobile > Android Security**.
  - ↪ La page de téléchargement d'Avira Free Android Security s'affiche.
- Cliquez sur **Se connecter**.
  - ↪ La page de connexion d'Avira Free Android Security s'affiche.

  Entrez votre adresse e-mail enregistrée et votre mot de passe.

  Cliquez sur **Se connecter** pour ouvrir la console Web et accéder à ses fonctions de commande à distance.

10.7 Généralités

10.7.1 Catégories de dangers

Sélection de catégories de dangers étendues (Options disponibles uniquement si le mode expert est activé)

Votre produit Avira vous protège des virus informatiques. En outre, vous avez la possibilité d'effectuer différentes recherches selon les catégories de dangers suivantes.

- Logiciels publicitaires
- Logiciels publicitaires/logiciels espions
- Applications
- Logiciels de commande Backdoor
- Fichiers à extensions déguisées
- Programmes de numérotation payants
- Hameçonnage
- Programmes portant atteinte à la vie privée
- Programmes de blagues
- Jeux
- Logiciels frauduleux
- Logiciels de compression des fichiers exécutables inhabituels

Cliquez sur la case correspondante pour activer le type sélectionné (coché) ou le désactiver (décoché).

Activer tout

Si l'option est activée, tous les types sont activés.

Valeurs par défaut

Ce bouton restaure les valeurs définies par défaut.

Remarque
Si un type est désactivé, les fichiers identifiés comme type de programme correspondant ne sont plus signalés. En outre, aucune entrée n'est ajoutée au fichier de rapport.

10.7.2 Mot de passe

Vous pouvez protéger votre produit Avira dans diverses zones par un mot de passe. Si un mot de passe a été attribué, vous devez 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 le mot de passe de votre choix. 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 « Aucun mot de passe ».

Confirmation

Saisissez ici de nouveau le mot de passe indiqué ci-dessus pour le confirmer. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Remarque
Le mot de passe est sensible à la casse.

Zones protégées par mot de passe (options disponibles uniquement si le mode expert est activé.)

Votre produit Avira 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 volonté.

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 la protection temps réel	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver la protection temps réel Avira.

Activer / désactiver la protection Web	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver la protection Web.
Quarantaine	Si l'option est activée,
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 contrôler à nouveau un objet.
Propriétés des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour afficher les propriétés 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 e-mail à Avira	Si l'option est activée, le mot de passe défini est nécessaire pour envoyer un objet à l'Avira Malware Research Center pour contrôle.
Ajout et modification 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 pour démarrer la mise à jour produit dans le menu Mise à jour.
Configuration	Si l'option est activée, la configuration du programme n'est possible qu'après saisie du mot de passe défini.
Installation / désinstallation	Si l'option est activée, le mot de passe défini est nécessaire pour installer et désinstaller le programme.

10.7.3 Sécurité

Options disponibles uniquement si le mode expert est activé.

Autorun

Bloquer la fonction Autorun

Si cette option est activée, l'exécution de la fonction Autorun de Windows est bloquée sur tous les lecteurs intégrés, tels que les clés USB, les lecteurs CD et DVD, les lecteurs réseau. Avec la fonction Autorun de Windows, les fichiers sont immédiatement lus lors de l'insertion des supports de données ou lors de la connexion aux lecteurs réseau. Les fichiers peuvent ainsi être démarrés et reproduits automatiquement. Cette fonctionnalité implique toutefois un risque élevé pour la sécurité, car des logiciels malveillants ou programmes indésirables peuvent être installés en cas de démarrage automatique des fichiers. La fonction Autorun est particulièrement critique pour les clés USB car les données d'une clé USB peuvent constamment changer.

Exclure les CD et DVD

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

Avertissement
Ne désactivez la fonction Autorun pour les lecteurs de CD et DVD que si vous êtes certain d'utiliser uniquement des supports de données fiables.

Protection système

Protéger le fichier hôte Windows des modifications

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. Cette option est activée par défaut.

Protection du produit

Remarque
Les options de protection du produit ne sont pas disponibles si la protection temps réel n'a pas été installée lors d'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 par des méthodes avancées contre un arrêt non souhaité. La protection étendue des processus utilise beaucoup plus de ressources que la protection simple des

processus. L'option est activée par défaut. Un redémarrage de l'ordinateur est nécessaire pour désactiver l'option.

Remarque
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 (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
Veuillez noter que si l'option est désactivée, il se peut que la réparation des ordinateurs contaminés par certains types de logiciels malveillants échoue.

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.

Remarque
La protection des fichiers et des entrées de registre n'est pas disponible sous Windows XP 64 bits !

10.7.4 WMI

Options disponibles uniquement si le mode expert est activé.

Prise en charge de Windows Management Instrumentation (WMI)

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 produit Avira prend en charge WMI et met à disposition d'une interface, les données (informations sur l'état, données statistiques, rapports, tâches planifiées, etc.) ainsi que les événements . WMI vous donne la possibilité de consulter les données d'exploitation du programme .

Activer la prise en charge WMI

Si l'option est activée, vous avez la possibilité de consulter les données d'exploitation du programme via WMI.

10.7.5 Événements

Options disponibles uniquement si le mode expert est activé.

Limiter la taille de la base de données d'événements

Limiter la taille à n entrées maximum

Si l'option est activée, le nombre maximum d'entrées dans la base de données d'événements peut être limité à une taille définie ; les valeurs autorisées sont : 100 à 10 000 entrées. Si le nombre d'entrées saisies est dépassé, les saisies les plus anciennes sont supprimées.

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

Si l'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 définie par défaut sur une valeur de 30 jours.

Pas de limitation

Si l'option est activée, la taille de la base de données d'événements n'est pas limitée. Toutefois, 20 000 entrées au maximum sont affichées sur l'interface du programme sous Événements.

10.7.6 Rapports

Options disponibles uniquement si le mode expert est activé.

Limiter les rapports

Limiter le nombre maximum à n unités

Si cette 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 cette option est activée, les rapports sont supprimés automatiquement après un certain nombre de jours ; valeurs autorisées : 1 à 90 jours. Cette option est définie par défaut sur une valeur de 30 jours.

Pas de limitation

Si cette option est activée, le nombre de rapports n'est pas limité.

10.7.7 Répertoires

Options disponibles uniquement si le mode expert est activé.

Chemin temporaire

Utiliser le paramètre du système

Si cette option est activée, les paramètres du système sont utilisés pour le traitement des fichiers temporaires.

> **Remarque**
> Pour savoir où votre système enregistre les fichiers temporaires, sur Windows XP par exemple, allez sous : **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

Si l'option est activée, c'est le chemin indiqué dans le champ de saisie qui est utilisé.

Champ de saisie

Entrez dans ce champ de saisie le chemin sous lequel le programme doit enregistrer les fichiers temporaires.

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

Par défaut

Ce bouton restaure le répertoire prédéfini pour le chemin temporaire.

10.7.8 Avertissement sonore

Options disponibles uniquement si le mode expert est activé.

En cas de détection d'un virus ou d'un logiciel malveillant par le scanner ou la protection temps réel, un signal sonore d'avertissement retentit dans le mode d'action interactif. Vous pouvez désactiver ou activer le signal sonore d'avertissement, ou sélectionner un autre fichier WAVE comme signal sonore d'avertissement.

> **Remarque**
> Le mode d'action du scanner se règle dans la configuration sous Sécurité PC > Scanner > Recherche > Action si résultat positif.

Pas d'avertissement

Si l'option est activée, aucun avertissement sonore ne se produit lors de la détection d'un virus par le scanner ou la protection temps réel.

Diffuser par le haut-parleur du PC (uniquement en mode interactif)

Si l'option est activée, un avertissement sonore se produit à l'aide d'un signal sonore d'avertissement par défaut, lors de la détection d'un virus par le scanner ou la protection temps réel. Le signal sonore 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 sonore se produit à l'aide du fichier WAVE sélectionné, en cas de détection d'un virus par le scanner ou la protection temps réel. 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 signal sonore d'avertissement par défaut du programme est indiqué comme préréglage.

...

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

Test

Ce bouton sert à tester le fichier WAVE sélectionné.

10.7.9 Avertissements

Pour certains événements, votre produit Avira affiche des notifications sur le Bureau (slide-up), 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 de 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 dans la fenêtre de configuration **Avertissements**.

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 maximum qui doit s'être écoulé depuis la dernière mise à jour. Si cette période est dépassée, une icône rouge s'affiche dans le Control Center sous État pour l'état de mise à jour.

Afficher un avertissement si le fichier de définitions des virus est obsolète

Si l'option est activée, vous recevez un message d'avertissement en cas de fichier de définitions des virus obsolète. À l'aide de l'option « Avertissement si la dernière mise à jour date de plus de n jour(s) », vous pouvez configurer l'intervalle avant l'avertissement.

Avertissements / remarques dans les situations suivantes

Une connexion par modem est utilisée

Si l'option est activée, une notification s'affiche sur le Bureau pour vous avertir 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 Catégories de dangers : programme de numérotation payant)

Les fichiers ont été actualisés avec succès

Si l'option est activée, une notification s'affiche sur le Bureau lorsqu'une mise à jour a réussi et que les fichiers ont été actualisés.

Échec de la mise à jour

Si l'option est activée, une notification s'affiche sur le Bureau lorsqu'une mise à jour a échoué : la connexion au serveur de téléchargement n'a pas pu être établie ou les fichiers de mise à jour n'ont pas pu être installés.

Aucune mise à jour n'est nécessaire

Si l'option est activée, une notification s'affiche 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.

Edition du 4er trimestre 2012

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