Avira Antivirus Premium 2012

Manuel de l'utilisateur

AVIRA

Marque déposée et copyright

Marque déposée

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 sont utilisés pour Avira Antivirus Premium 2012. 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 programme de Avira Antivirus Premium 2012 sous "Licences tiers".

Sommaire

1. Introduction

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

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

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

http://www.avira.com/fr

Sur le site Web Avira, vous pouvez :

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

Votre équipe Avira

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.
	Éléments 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

2.1 Aperçu

Dans ce chapitre, vous obtenez toutes les informations pour l'acquisition et l'utilisation de votre produit Avira :

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

Les produits Avira offrent des outils complets et flexibles permettant de protéger avec fiabilité votre ordinateur des virus, des logiciels malveillants, des 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 cent pour cent de la perte de données. Effectuez régulièrement des copies de sauvegarde (back-ups) de vos données.

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

2.2 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 Système (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 fichiers
- Composant ProActiv pour une surveillance permanente d'actions de programme (uniquement pour systèmes 32 bits, non disponible sous Windows 2000)
- Protection E-mail (scanner POP3, scanner IMAP et scanner SMTP) pour le contrôle permanent de vos emails à la recherche de virus et logiciels malveillants. Inclut la vérification des pièces jointes aux emails
- Gestion de quarantaines intégrée pour l'isolation et le traitement des fichiers suspects
- Protection Rootkits pour localiser les logiciels malveillants installés de manière cachée dans le système de l'ordinateur (appelés 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 définitions de virus (VDF) et du moteur de recherche grâce à la mise à jour de fichiers individuels et à la mise à jour incrémentielle VDF via un serveur Web basé sur Internet
- Attribution de licence intuitive dans la gestion de licence
- Le planificateur intégré pour la planification des tâches uniques ou répétées comme les mises à jour et les contrôles
- Identification extrêmement efficace des virus et logiciels malveillants grâce à des technologies de recherche innovantes (moteur de recherche) comprenant des procédés de recherche heuristique
- Identification de tous les types d'archives courants, y compris des extensions d'archives imbriquées et des extensions intelligentes
- Grande performance grâce à la capacité de multithreading (scannage simultané de nombreux fichiers à vitesse élevée)

2.3 Configuration système minimale

Les configurations minimales du système sont les suivantes :

- Processeur Pentium et plus, au moins 1 GHz
- Système d'exploitation
  - Windows XP, SP3 (32 ou 64 bits) ou
  - Windows Vista (32 ou 64 bits, SP1 recommandé) ou
  - Windows 7 (32 ou 64 bits)
- 150 Mo minimum d'espace mémoire disponible sur le disque dur (voire plus en cas d'utilisation de la fonction de quarantaine et pour la mémoire temporaire)
- 512 Mo minimum de mémoire vive sous Windows XP
- 1 024 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)

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

La clé d'activation vous est transmise par email si vous avez acheté votre produit Avira sur Internet ou est mentionné sur l'emballage du produit.

Pour obtenir la licence de votre programme, entrez la clé d'activation lors de l'activation du programme. L'activation du produit peut s'effectuer lors de l'installation. Toutefois, vous pouvez aussi activer votre produit Avira après l'installation, dans le gestionnaire de licences sous Aide > Gestion des licences.

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

Afin d'obtenir une fiabilité et une sécurité élevées sur votre ordinateur, Avira vous rappelle la mise à niveau avec la nouvelle version. Cliquez sur **Mise à niveau** dans la fenêtre popup pour la migration vers la nouvelle version afin d'accéder à la page de mise à niveau spécifique à votre produit. Vous avez la possibilité d'effectuer une mise à niveau de votre produit actuel ou d'acheter un produit Avira complet. La page Aperçu de votre produit Avira vous montre quel produit vous utilisez actuellement et vous permet de le comparer avec d'autres produits Avira. Pour de plus amples informations, cliquez sur l'icône Information à droite du nom du produit. Si vous souhaitez conserver votre produit actuel, cliquez sur **Mise à niveau** afin d'installer immédiatement la nouvelle version avec des fonctions améliorées. Si vous souhaitez acheter un produit complet, cliquez sur **Acheter** en bas de la colonne correspondant au produit. Vous êtes alors redirigé dans la boutique en ligne Avira pour passer votre commande.

Remarque
Selon votre produit et votre système d'exploitation, il peut être nécessaire d'avoir les droits d'administrateur pour effectuer la mise à niveau. Veuillez vous connecter en tant qu'administrateur et installez la nouvelle version.

Les mises à niveau de produit suivantes peuvent être effectuées :

- Mise à niveau d'Avira AntiVir Personal vers Avira Free Antivirus.
- Mise à niveau d'Avira AntiVir Personal vers Avira Antivirus Premium 2012.
- Mise à niveau d'Avira AntiVir Premium vers Avira Internet Security 2012.
- Mise à niveau d'Avira Antivir Premium Security Suite vers Avira Professional Security.

2.4.1 Gestion de licence

La gestion de licence Avira Internet Security 2012 permet une installation très simple de la licence Avira Internet Security 2012.

Gestion de licence Avira Internet Security 2012

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

Remarque
La gestion de licence Avira Internet Security 2012 copie la licence correspondante automatiquement dans le dossier de produit correspondant. Si une licence est déjà disponible, un message s'affiche demandant si le fichier de

licence doit être remplacé. Dans ce cas, le fichier de licence existant est écrasé par le fichier de licence actuel.

3. Installation et désinstallation

3.1 Aperçu

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

- voir le chapitre : Avant installation : conditions requises, préparation de l'ordinateur pour l'installation
- voir le chapitre : Installation express : installation standard selon les réglages par défaut
- voir le chapitre : Installation personnalisée : installation configurable
- voir le chapitre : Installation du produit test
- voir le chapitre : Assistant de configuration
- voir le chapitre : Installation modifiée
- voir le chapitre : Modules d'installation
- voir le chapitre : Désinstallation : exécuter la désinstallation

3.1.1 Types d'installation

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

Express

- Les fichiers de programme sont installés dans un répertoire par défaut sous *C:\Programme*.
- 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 le chapitre Installation et désinstallation > Modules d'installation).
- Vous pouvez choisir un dossier cible 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 dans le menu Démarrer.
- À l'aide de l'assistant de configuration, vous pouvez effectuer des réglages personnalisés pour votre produit Avira et lancer un bref contrôle système exécuté automatiquement après l'installation.

3.2 Avant installation

Remarque
Avant l'installation, vérifiez que votre ordinateur présente la configuration système minimale. Si votre ordinateur présente la configuration minimale requise, 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 installation

✓ Fermez votre programme de messagerie électronique. Il est en outre recommandé de fermer toutes les applications ouvertes.
✓ Assurez-vous qu'aucune autre solution antivirus n'est installée. Les fonctions de protection automatiques des différentes solutions de sécurité peuvent s'entraver.
  ↪ Le produit Avira cherche sur votre ordinateur d'éventuels logiciels incompatibles.
  ↪ Une liste des programmes concernés est générée si des logiciels incompatibles sont trouvés.
  ↪ Il est conseillé de désinstaller les logiciels qui menacent la sécurité de votre ordinateur.

▸ Dans la liste, sélectionnez les programmes qui doivent être supprimés automatiquement de votre ordinateur et cliquez sur **Continuer**.

▸ Certains programmes ne peuvent être supprimés de votre ordinateur que manuellement. Sélectionnez les programmes et cliquez sur **Continuer**.
  ↪ La désinstallation d'un ou de plusieurs programme(s) exige le redémarrage de votre ordinateur. Après le redémarrage, l'installation se poursuit.

Avertissement
Votre ordinateur n'est protégé qu'une fois la procédure d'installation de votre produit Avira terminée.

Installation

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

Les principaux boutons disposent des fonctions suivantes :

- **OK** : confirmer l'action.

- **Annuler** : abandonner l'action.
- **Continuer** : passer à l'étape suivante.
- **Précédent** : retourner 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 définitions des virus du jour par le biais du programme d'installation (en cas d'installation basée sur Internet)
- Activation du programme
- Si nécessaire, exécution d'une mise à jour une fois l'installation terminée

Conservez la clé de licence de votre produit Avira à portée de main, si vous souhaitez activer le programme.

Remarque
Installation basée sur Internet :
Pour l'installation du programme basée sur Internet, il existe un programme d'installation qui charge les fichiers programme actuels des serveurs Web d'Avira avant l'exécution de l'installation. Cette procédure garantit que le produit Avira est installé avec le fichier de définitions des virus du jour.

Installation à l'aide d'un pack d'installation :
Le pack d'installation contient non seulement le programme d'installation mais aussi tous les fichiers programme nécessaires. Il n'y a toutefois pas de possibilité de sélection de la langue pour votre produit Avira lors d'une installation à l'aide d'un pack d'installation. Il est recommandé, à l'issue de l'installation, d'effectuer une mise à jour afin d'actualiser le fichier de définitions des virus.

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

3.3 Installation express

Voici comment installer votre produit Avira :

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

Installation basée sur Internet

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

- Cliquez sur **Continuer** pour poursuivre l'installation.
  ↳ La fenêtre de dialogue **Sélection de la langue** s'affiche à l'écran.
- Sélectionnez la langue dans laquelle vous souhaitez installer votre 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 des serveurs Web d'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 va être démarrée.

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

Remarque
Par défaut, l'**installation express**, avec laquelle les composants standard sont installés sans possibilités de configuration, est préréglée. Si vous souhaitez utiliser une **Installation personnalisée**, veuillez lire ce qui suit : Installation > Installation personnalisée.

- Vous pouvez prendre part à l'Avira ProActiv Communité (Configuration > Protection Temps Réel > ProActiv).
- Confirmez que vous acceptez l'**accord de licence pour utilisateur final**. Si vous souhaitez lire les détails concernant les accords de licence, cliquez sur le lien correspondant.
- Cliquez sur **Suivant**.
- Si vous avez validé votre participation à l'Avira ProActiv Communité, la fenêtre d'information **ProActiv Communité**, dans laquelle vous pouvez obtenir de plus amples informations sur le contrôle en ligne, *s'affiche.*
- Cliquez sur **Suivant**.
  ↳ L'*assistant de licence* s'ouvre et vous guide pour activer votre produit.

  ↳ Vous avez ici la possibilité de configurer un serveur proxy.

  Cliquez sur **Réglages proxy** pour configurer le serveur proxy et confirmez vos réglages avec **OK**.

  ↳ Si vous avez déjà obtenu un code d'activation, sélectionnez **Activer le produit**.

  Vous pouvez aussi cliquer sur le lien **Je possède déjà un fichier de licence hbedv.key valide**.

- Dans la boîte de dialogue **Ouvrir le fichier**, sélectionnez le fichier *HBEDV.KEY* et cliquez sur **Ouvrir**.
  - ↪ Le code d'activation est copié dans l'assistant de licence.
- Si vous souhaitez tester le produit, veuillez poursuivre la lecture dans le chapitre Installation du produit test.
  - ↪ La progression de l'installation est représentée par une barre verte.
  - ↪ Cliquez sur **Terminer** pour terminer l'installation et quitter le programme d'installation.
  - ↪ L'icône de programme Avira est placée dans la barre des tâches.
  - ↪ Le module **Updater** recherche d'éventuelles mises à jour afin de protéger votre ordinateur de façon optimale.
  - ↪ Lors d'une première recherche directe du scanner, la fenêtre d'état **Luke Filewalker** s'ouvre, vous informe sur l'état du contrôle et affiche les résultats.
- S'il vous est demandé de redémarrer le système après un contrôle de celui-ci, procédez au redémarrage afin que votre système soit totalement protégé.

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

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

3.4 Installation personnalisée

Voici comment installer votre produit Avira :

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

Installation basée sur Internet

- ↪ La fenêtre de dialogue **Bienvenue** apparaît.
- Cliquez sur **Continuer** pour poursuivre l'installation.
  - ↪ La fenêtre de dialogue **Sélection de la langue** s'affiche à l'écran.
- Sélectionnez la langue dans laquelle vous souhaitez installer votre 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 des serveurs Web d'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 va être démarrée.

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

Remarque
Par défaut, l'**installation express**, avec laquelle les composants standard sont installés sans possibilités de configuration, est préréglée. Si vous souhaitez l'utiliser, veuillez lire ce qui suit : Installation > Installation express.

- Sélectionnez **Personnalisée** comme type d'installation souhaité.
- Confirmez que vous acceptez l'**accord de licence pour utilisateur final**. Si vous souhaitez lire les détails concernant les accords de licence, cliquez sur le lien correspondant.
- Cliquez sur **Suivant**.

  ↳ La fenêtre **Sélectionner le répertoire d'installation** s'affiche.

  ↳ Par défaut, il s'agit du répertoire *C:\Programmes\Avira\AntiVir Desktop*
- Cliquez sur **Continuer** pour poursuivre l'installation.

  - OU -

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

  ↳ La fenêtre de dialogue **Choisir les composants à installer** s'affiche :
- Activez ou désactivez les composants souhaités et confirmez avec **Suivant**.

  ↳ Si vous avez choisi les composants ProActiv pour l'installation, la fenêtre **Avira ProActiv Communité** s'affiche.
  Vous avez la possibilité de valider une participation à l'Avira ProActiv Communité : Si l'option est activée, Avira ProActiv envoie à l'Avira Malware Research Center les données sur les programmes suspects indiqués par le composant ProActiv. Les données sont utilisées uniquement pour un contrôle en ligne étendu et pour étendre et affiner la technologie de détection. Le lien **Autres informations** vous permet d'avoir des détails sur le contrôle en ligne étendu.
- Si la fenêtre **Avira ProActiv Communité** est affichée, activez ou désactivez la participation à l'Avira ProActiv Communité et confirmez avec **Suivant**.

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

↳ L'*assistant de licence* s'ouvre.

Vous pouvez sélectionner les options suivantes pour activer le programme :

- Entrée d'une clé d'activation
  En saisissant votre clé d'activation, vous activez votre produit Avira avec votre licence.
- Sélection de l'option **Tester le produit**
  Si vous sélectionnez **Tester le produit**, une licence test est générée lors du processus d'activation, grâce à laquelle le programme est activé. Vous pouvez tester l'intégralité des fonctions du produit Avira pendant une période définie (voir Installation du produit test).

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

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

Remarque
Une connexion aux serveurs d'Avira est établie pour activer le programme. Sous **Réglages proxy**, vous pouvez configurer la connexion Internet via un serveur proxy.

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

Activation de produit

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

- Saisissez vos données et cliquez sur **Suivant.**

↳ Vos données sont transférées vers les serveurs d'Avira puis vérifiées. Votre produit Avira est activé avec votre licence.

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

- Cliquez sur **Suivant**.

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

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

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

- Choisissez le fichier de licence *hbedv.key* avec vos données de licence pour le programme et cliquez sur **Ouvrir**.

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

- Cliquez sur **Suivant**.

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

Dans l'assistant de licence, vous avez la possibilité de vous inscrire en tant que client et de vous abonner au *bulletin d'actualité Avira*. Il est nécessaire pour cela d'indiquer vos données personnelles.

- Entrez vos données, le cas échéant et confirmez vos indications avec **Suivant**.

  ↳ Lors d'une inscription, le résultat de l'activation s'affiche dans la fenêtre de dialogue suivante.

- Cliquez sur **Suivant**.

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

- Une fois le processus d'installation terminé, finissez l'installation avec **Terminer**.

  ↳ L'assistant d'installation se ferme, l'assistant de configuration s'ouvre.

3.5 Installation du produit test

Voici comment installer votre produit Avira :

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

Installation basée sur Internet

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

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

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

- Sélectionnez la langue dans laquelle vous souhaitez installer votre 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 des serveurs Web d'Avira. Une fois le téléchargement terminé, la fenêtre **Téléchargement** se referme.

Remarque
Par défaut, l'**installation express**, avec laquelle les composants standard sont installés sans possibilités de configuration, est préréglée. Si vous souhaitez utiliser une *Installation personnalisée*, veuillez lire ce qui suit : Installation > Installation personnalisée.

- Vous pouvez prendre part à l'Avira ProActiv Communité (Configuration > Protection Temps Réel > ProActiv).
- Confirmez que vous acceptez l'**accord de licence pour utilisateur final**. Si vous souhaitez lire les détails concernant les accords de licence, cliquez sur le lien correspondant.
- Cliquez sur **Suivant**.
- Si vous avez validé votre participation à l'Avira ProActiv Communité, la fenêtre d'information **ProActiv Communité**, dans laquelle vous pouvez obtenir de plus amples informations sur le contrôle en ligne, s'affiche.
- Cliquez sur **Suivant**.
  - L'*assistant de licence* s'ouvre pour vous guider dans l'activation de votre produit.
  - L'assistant vous permet également de définir un serveur proxy.
- Cliquez sur **Réglages proxy** pour effectuer la configuration nécessaire et confirmez avec **OK**.
- Sélectionnez **Tester le produit** dans l'assistant de licence et cliquez sur **Suivant**.
- Saisissez vos données dans les champs nécessaires à l'enregistrement. Choisissez si vous souhaitez vous abonner au *bulletin d'actualité Avira* et cliquez sur **Suivant**.
  - La progression de l'installation est représentée par une barre verte.
- Cliquez sur **Terminer** pour terminer l'installation et fermer l'assistant de licence.
- Il vous est demandé de redémarrer l'ordinateur afin d'activer le produit Avira. Cliquez sur **Oui** pour lancer une redémarrage immédiat.
  - L'icône de programme Avira est placée dans la barre des tâches.
  - Votre licence test dispose d'une validité de 31 jours.

3.6 Assistant de configuration

En cas d'installation personnalisée, l'assistant de configuration s'ouvre à la fin. Vous pouvez effectuer d'importants préréglages pour votre produit Avira dans l'assistant de configuration.

- Dans la fenêtre de bienvenue de l'assistant de configuration, cliquez sur **Suivant**, pour commencer la configuration du programme.
  - Vous pouvez choisir un niveau de détection pour la technologie AHeAD dans la fenêtre de dialogue **Configurer AHeAD**. Le niveau de détection choisi est validé

pour le réglage de la technologie AHeAD du Scanner Système (recherche directe) et de la Protection Temps Réel (recherche en temps réel).

- Choisissez un degré d'identification et poursuivez la configuration avec **Continuer**.
  - ↪ La fenêtre de dialogue suivante **Choisir des catégories de dangers étendues** vous permet d'adapter les fonctions de protection de votre produit Avira grâce à la sélection de catégories de dangers.
- Activez d'autres catégories de dangers le cas échéant et poursuivez la configuration avec **Continuer**.
  - ↪ Si vous avez choisi le module d'installation Protection Temps Réel Avira pour l'installation, la fenêtre de dialogue **Mode de démarrage de la Protection Temps Réel** s'affiche. Vous pouvez définir le point 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 pour la Protection Temps Réel est consigné dans le registre et ne peut pas être modifié par la configuration.

Remarque
Avec le choix du mode de démarrage par défaut pour la Protection Temps Réel (démarrage normal) et une connexion rapide du compte d'utilisateur, au démarrage de l'ordinateur, il se peut que les programmes démarrant automatiquement avec le système ne soient pas scannés car ils démarrent avant le chargement complet de la Protection Temps Réel.

- Activez l'option souhaitée et poursuivez la configuration avec **Continuer**.
  - ↪ La fenêtre de dialogue suivante **Contrôle du système** permet d'activer ou de désactiver l'exécution d'un bref contrôle du système. Le bref contrôle du système est exécuté une fois la configuration terminée et avant le redémarrage de l'ordinateur. Il parcourt les programmes lancés et les fichiers système les plus importants, à la recherche de virus et de logiciels malveillants.
- Activez ou désactivez l'option **Bref contrôle du système** et poursuivez la configuration avec **Continuer**.
  - ↪ La fenêtre de dialogue suivante vous permet de finir la configuration avec **Terminer**.
  - ↪ Les réglages indiqués et sélectionnés sont validés.
  - ↪ Si vous avez activé l'option **Bref contrôle du système**, la fenêtre **Luke Filewalker** s'ouvre. Le Scanner Système effectue un bref contrôle du système.
  - ↪ S'il vous est demandé de redémarrer le système après un contrôle de celui-ci, procédez au redémarrage afin que votre système soit totalement protégé.

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

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

3.7 Installation modifiée

Vous avez la possibilité d'ajouter ou de supprimer certains composants de programme 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** pour **ajouter/désinstaller** des programmes dans le **panneau de configuration Windows**.

Sélectionnez votre produit Avira et cliquez sur **Modifier**. Dans la boîte de dialogue *Bienvenue* du programme, sélectionnez l'option **Modifier le programme**. Vous êtes guidé à travers l'installation modifiée.

3.8 Modules d'installation

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

- **Avira Antivirus Premium 2012**
  Ce module contient tous les composants nécessaires à l'installation réussie de votre produit Avira.
- **Protection Temps Réel Avira**
  La Protection Temps Réel Avira fonctionne en arrière-plan. Il surveille et répare si possible les fichiers lors d'opérations comme l'ouverture, l'écriture et la copie en temps réel (On-Access = à l'accès). Si un utilisateur effectue une opération sur le fichier (charger, exécuter ou copier le fichier), le produit Avira parcourt automatiquement le fichier. Lors de l'opération Renommer, aucune recherche de la Protection Temps Réel Avira n'est effectuée.
- **Avira ProActiv**
  Le composant ProActiv surveille les actions des applications et signale si elles présentent un comportement suspect. Avec cette détection basée sur la détection, vous pouvez vous protéger contre des logiciels malveillants inconnus. Le composant ProActiv est intégré dans la Protection Temps Réel Avira.
- **Protection E-mail Avira**
  La Protection E-mail est l'interface entre votre ordinateur et le serveur d'email à partir duquel votre programme de messagerie électronique (client email) télécharge les

emails. La Protection E-mail se place comme proxy entre le programme d'email et le serveur d'email. Tous les emails entrants sont transférés via ce proxy, la présence de virus et de programmes indésirables est recherchée, puis ils sont transmis à votre programme email. Selon la configuration, le programme traite les emails automatiquement ou demande à l'utilisateur quoi faire.

- **Protection Web Avira**
  En "naviguant" sur Internet, vous demandez des données en provenance d'un serveur Web via votre navigateur Web. Les données transmises par le serveur Web (fichiers HTML, script et images, fichiers flash, flux vidéo et musique, etc.) arrivent normalement de la mémoire cache du navigateur directement pour être exécutées dans le navigateur Web, ce qui exclut un contrôle par une recherche en temps réel comme la Protection Temps Réel Avira le propose. De cette manière, des virus et programmes indésirables peuvent arriver sur 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 sur les données transférées. Selon la configuration, le programme traite les fichiers concernés automatiquement ou demande à l'utilisateur quoi faire.
- **Protection Rootkits Avira**
  La Protection Rootkits Avira contrôle si un logiciel s'est déjà installé sur votre ordinateur qui ne peut être détecté par les méthodes habituelles après infiltration dans votre système.
- **Shell Extension**
  La 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.

3.9 Désinstallation

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

Voici comment désinstaller votre produit Avira (exemple avec Windows XP et Windows Vista) :

- Ouvrez le **panneau de configuration** via le menu **Démarrer** de Windows.
- Double-cliquez sur **Programmes** (Windows XP : **Logiciels**).
- Sélectionnez votre produit Avira dans la liste et cliquez sur **Supprimer/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 alors désinstallé et votre ordinateur est redémarré si besoin est. Ce faisant, tous les répertoires, tous les fichiers et toutes les entrées de registre du programme sont supprimés.

4. Aperçu

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

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

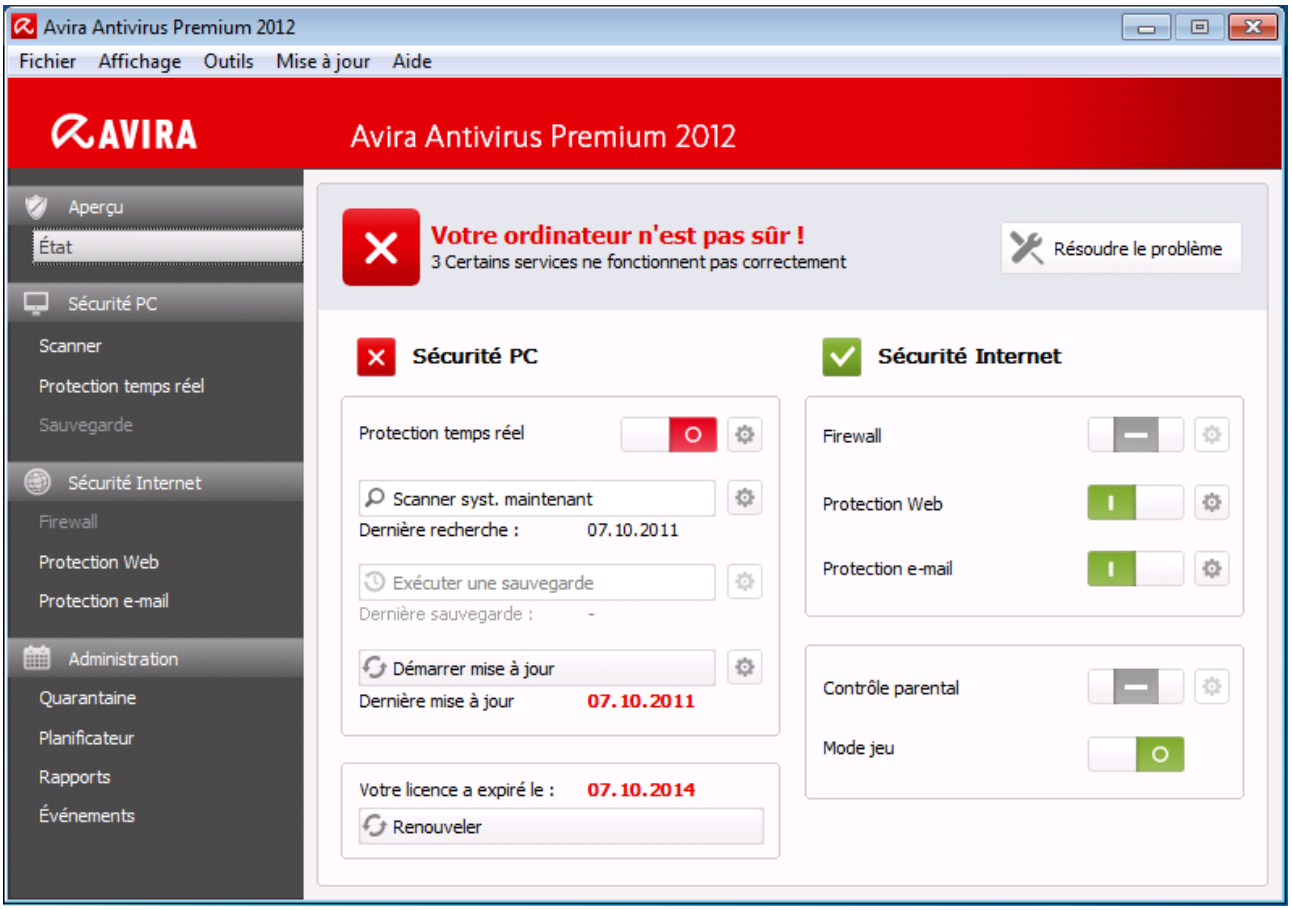
4.1 Interface et commande

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

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

4.1.1 Control Center

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



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

- **Barre de menus :** 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 : Secteur de tâches **Sécurité PC** - rubrique **Protection Temps Réel**.
- **État :** l'écran de démarrage État offre la possibilité de voir d'un seul coup d'œil si votre ordinateur est suffisamment protégé, quels modules sont actifs, et quand la dernière sauvegarde et le dernier contrôle du système ont été effectués. La fenêtre **État** affiche tous les boutons d'exécution des fonctions ou actions, comme par ex. l'activation ou désactivation du Contrôle Parental.

Démarrage et arrêt du Control Center

Vous avez les possibilités suivantes pour démarrer le Control Center :

- Cliquez deux fois sur l'icône du programme sur le Bureau.
- Via l'entrée de programme dans le menu **Démarrer > Programmes**
- Via l'icône de programme de votre produit Avira.

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

Utilisation du Control Center

Voici comment naviguer dans le Control Center :

- Dans la barre de navigation, cliquez sur un secteur de tâches sous une rubrique.
  - ↪ Le secteur de tâches s'affiche avec d'autres fonctions et possibilités de configuration dans la fenêtre de détail.
- Cliquez éventuellement sur un autre secteur de tâches pour l'afficher dans la fenêtre de détail.

> **Remarque**
> La navigation au clavier dans la barre des menus s'active avec la touche [**Alt**]. La touche **Enter** vous permet d'activer l'option de menu actuellement sélectionnée.
> Pour ouvrir, fermer des menus dans le Control Center, ou naviguer dans les menus, vous pouvez également utiliser des combinaisons de touches : touche [**Alt**] + la lettre soulignée dans le menu ou la commande de menu. Maintenez la touche [**Alt**] enfoncée quand vous souhaitez accéder à une commande de menu ou à un sous-menu à partir d'un menu.

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

- Repérez les données ou objets que vous souhaitez traiter.

  Pour sélectionner plusieurs événements, maintenez la touche **Ctrl** ou **Shift** (sélection d'éléments situés les uns sous les autres) pendant la sélection des éléments.
- Cliquez sur le bouton souhaité dans la barre supérieure de la fenêtre de détail pour traiter l'objet.

Aperçu du Control Center

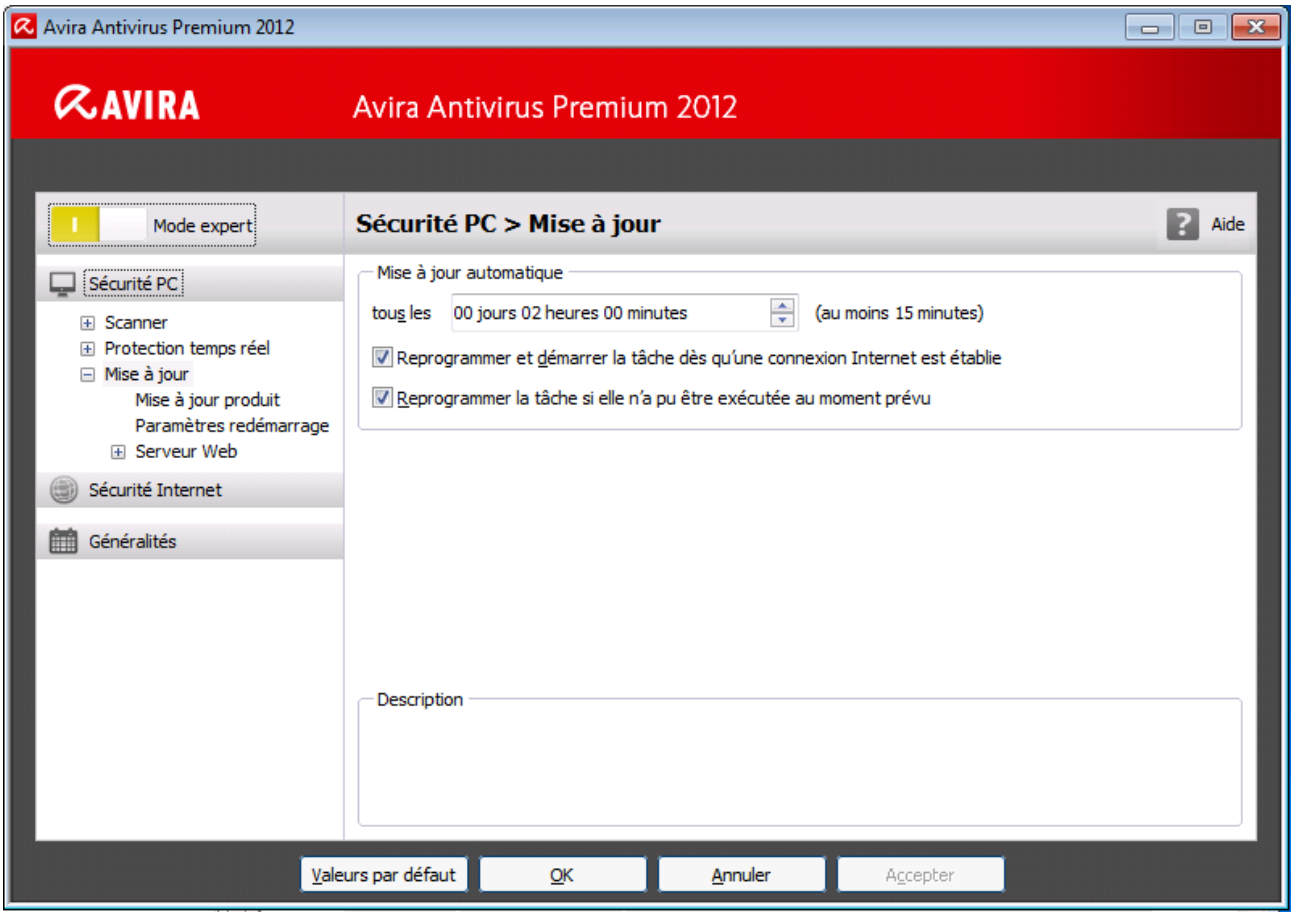
- **État** : dans l'écran de démarrage **État** se trouvent toutes les rubriques vous permettant de surveiller le fonctionnement de votre produit Avira.
  - La fenêtre **État** offre la possibilité de voir d'un seul coup d'œil quels modules de programme sont actifs et fournit des informations sur la dernière mise à jour effectuée. De plus, elle vous permet de voir si vous êtes détenteur d'une licence valide.
- **Sécurité PC** : vous trouverez sous **Sécurité PC** les composants vous permettant de contrôler l'absence de virus et de logiciels malveillants dans les fichiers de votre ordinateur.

- La rubrique Scanner Système vous permet de configurer et de démarrer simplement la recherche directe. Les profils prédéfinis permettent d'effectuer une recherche avec des options standard adaptées. À l'aide de la sélection manuelle (qui n'est pas enregistrée) ou en créant des profils personnalisés, vous pouvez également adapter la recherche de virus et de programmes indésirables à vos besoins personnels.
- La rubrique Protection Temps Réel vous fournit des informations sur les fichiers contrôlés, ainsi que d'autres données statistiques pouvant être à tout moment réinitialisées et permet d'accéder au fichier de rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles quasiment par simple "pression d'un bouton".

- **Sécurité Internet** : vous trouverez sous **Sécurité Internet** les composants vous permettant de protéger votre ordinateur contre les virus et logiciels malveillants provenant d'Internet ainsi que des accès réseau indésirables.
  - La rubrique Protection E-mail vous indique les emails contrôlés, leurs propriétés ainsi que d'autres données statistiques.
  - La rubrique Protection Web vous donne des informations sur les URL contrôlées et les virus détectés, ainsi que d'autres données statistiques pouvant être à tout moment réinitialisées et permet d'accéder au fichier de rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles quasiment par simple "pression d'un bouton".
- **Administration** : sous **Administration** se trouvent des outils vous permettant d'isoler et de gérer les fichiers suspects ou infectés par des virus ainsi que de planifier des tâches récurrentes.
  - Sous la rubrique Quarantaine se trouve le gestionnaire de quarantaine. Emplacement central pour les fichiers déjà en quarantaine ou suspects que vous souhaitez mettre en quarantaine. En outre, vous avez la possibilité d'envoyer un fichier par email à Avira Malware Research Center.
  - La rubrique Planificateur vous donne la possibilité de créer des tâches de contrôle et de mise à jour programmées et d'ajuster ou de supprimer les tâches existantes.
  - La rubrique Rapports vous permet de visualiser les résultats des actions effectuées.
  - La rubrique Evénements vous donne la possibilité de vous informer sur les événements générés par les modules du programme.

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

Accès à la configuration

Vous avez plusieurs possibilités pour accéder à la configuration :

- Via le Panneau de configuration Windows.
- Via le Centre de sécurité Windows - à partir de Windows XP Service Pack 2.
- Via l'icône de programme de votre programme Avira.
- Dans le Control Center via l'option de menu Outils > Configuration.
- Dans le Control Center via le bouton Configuration.

Remarque
Si vous accédez à la configuration via le bouton **Configuration** du Control Center, vous arrivez au répertoire de configuration de la rubrique active dans le Control Center. Pour sélectionner les divers répertoires de configuration, le

mode expert de la configuration doit être activé. Dans ce cas, un dialogue s'affiche vous invitant à activer le **mode expert**.

Commande de la configuration

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

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

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

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

Si vous souhaitez valider vos réglages dans la configuration :

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

  - OU -

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

Si vous souhaitez terminer la configuration sans valider vos réglages :

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

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

- Cliquez sur **Valeurs par défaut**.

↳ Tous les réglages de la configuration sont réinitialisés aux valeurs par défaut. Toutes les modifications et vos entrées sont perdues en cas de réinitialisation aux valeurs par défaut.

Aperçu des options de configuration

Vous disposez des options de configuration suivantes :

- **Scanner Système** : Configuration de la recherche directe
  - Options de recherche
  - Actions en cas de résultat positif
  - Options pour la recherche dans les archives
  - Exceptions de la recherche directe
  - Heuristique de la recherche directe
  - Réglage de la fonction de rapport
- **Protection Temps Réel** : Configuration de la recherche en temps réel
  - Options de recherche
  - Actions en cas de résultat positif
  - Exceptions de la recherche en temps réel
  - Heuristique de la recherche en temps réel
  - Réglage de la fonction de rapport
- **Protection E-mail** : configuration de la Protection E-mail
  - Options de recherche : activation de la surveillance des comptes POP3, des comptes IMAP, des emails sortants (SMTP)
  - Actions en cas de logiciel malveillant
  - Heuristique de la recherche de la Protection E-mail
  - Exceptions de la recherche de la Protection E-mail
  - Configuration de la mémoire tampon, vider la mémoire tampon
  - Réglage de la fonction de rapport
- **Protection Web** : configuration de la Protection Web
  - Options de recherche, activation et désactivation de la Protection Web
  - Actions en cas de résultat positif
  - Accès bloqués :Types de fichiers et types MIME indésirables, filtre Web pour les URL indésirables connues (logiciels malveillants, hameçonnage, etc.)
  - Exceptions de la recherche de la Protection Web : URL, types de fichiers, types MIME
  - Heuristique de la Protection Web
  - Réglage de la fonction de rapport
- **Généralités** :
  - Catégories de dangers étendues pour la recherche directe et en temps réel
  - Protection par mot de passe pour l'accès au Control Center et à la configuration

- Sécurité : affichage d'état de la mise à jour, affichage d'état du contrôle intégral du système, protection du produit
- WMI : Activer la prise en charge WMI
- Configuration de la documentation des événements
- Configuration des fonctions de rapport
- Réglage des répertoires utilisés
- Mise à jour : configuration de la connexion au serveur de téléchargement, réglage des mises à jour produit
- Configuration des avertissements sonores en cas de détection de logiciel malveillant

4.1.3 Icône de programme

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

Symbole	Description
	La Protection Temps Réel Avira est activée
	La Protection Temps Réel Avira est désactivée

L'icône de programme indique l'état de la Protection Temps Réel.

Via le menu contextuel de l'icône de programme, les fonctions centrales de votre produit Avira sont rapidement accessibles.

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

Entrées dans le menu contextuel

- **Activer la Protection Temps Réel** : active ou désactive la Protection Temps Réel Avira.
- **Activer la Protection E-mail** : active ou désactive la Protection E-mail Avira.
- **Activer la Protection Web Avira** : active ou désactive la Protection Web Avira.
- **Démarrer Avira** : ouvre le Control Center.
- **Configurer Avira** : ouvre la Configuration.
- **Démarrer mise à jour...** : démarre une Mise à jour.
- **Aide** : ouvre l'aide en ligne.

- **À propos de Avira Antivirus Premium 2012 :** ouvre une fenêtre de dialogue comportant des informations sur votre produit Avira : informations sur le produit, informations sur la version, informations sur la licence.
- **Avira sur Internet** : ouvre le portail Web Avira sur Internet. La condition est de disposer d'un accès actif à Internet.

4.2 Comment procéder

4.2.1 Activer la licence

Voici comment activer la licence de votre produit Avira :

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

Si vous n'avez pas encore installé votre produit Avira :

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

Si vous avez déjà installé votre produit Avira :

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

  - OU -

  Dans le Control Center de votre produit Avira, sélectionnez l'option de menu **Aide > Gestion de licence**

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

- Sélectionnez le fichier de licence et cliquez sur **Ouvrir**.
  ↳ Un message apparaît.
- Validez avec **OK**.
  ↳ La licence est activée.
- Redémarrez le système si nécessaire.

4.2.2 Renouveler la licence

Voici comment renouveler automatiquement la licence de votre produit Avira :

Vous pouvez renouveler automatiquement la licence de votre produit Avira en activant l'option correspondante dans la zone *Renouvellement de licence* de la boutique en ligne.

Si vous n'avez pas encore installé votre produit Avira :

- Sélectionnez le produit souhaité dans la boutique en ligne d'Avira.
- Sélectionnez l'option **Renouvellement automatique de la licence à expiration**.
- Cliquez sur **Suivant** pour voir les données de vos commandes.
- Ici également, activez l'option **Renouvellement automatique de la licence à expiration**.
- Acceptez les clauses de la licence du logiciel.
- Cliquez sur **Terminer la commande** pour enregistrer celle-ci et la transmettre à Avira.

Si vous avez déjà installé votre produit Avira :

- Dans le Control Center, cliquez dans la barre latérale gauche sur **État**.

  Cliquez sur **Renouveler** à côté de *Votre produit est activé jusqu'au...*
- Votre demande est transmise à la zone *Aperçu des licences* de la page d'accueil Avira.

  ↳ Dans Aperçu des licences, vous pouvez voir pour quels produits Avira vous détenez une licence. Vous pouvez y modifier l'état des produits et activer ou désactiver l'option **Renouvellement automatique de la licence à expiration**. Cette option vous permet d'activer ou de désactiver un renouvellement automatique de la licence. Si une licence ne peut bénéficier d'une prolongation automatique, *S/O* s'affiche. Modifiez l'état en cliquant sur **ACTIVÉ** ou **DÉSACTIVÉ**. Si vous faites passer l'état du renouvellement automatique de la licence de **ACTIVÉ** à **DÉSACTIVÉ**, une fenêtre de confirmation s'ouvre pour vous indiquer que votre licence ne sera plus prolongée automatiquement.
- Cliquez sur **OK** pour valider votre choix.

  ↳ Si vous faites passer l'état du renouvellement automatique de la licence de **DÉSACTIVÉ** à **ACTIVÉ**, vous êtes informé que votre licence valide sera automatiquement prolongée 35 jours avant son expiration.
- Cliquez sur **OK** pour valider cette remarque.

  ↳ Si l'option **Renouvellement automatique de la licence à expiration** est activée, la date d'expiration est affichée sur la ligne concernant le produit.
- Saisissez votre adresse email dans le champ **Envoyer la(les) licence(s) à :...** et cliquez sur **Envoyer**.

↳ Si vous avez activé l'option **Renouvellement automatique de la licence à expiration**, Avira vous le rappelle 40 jours avant la date d'expiration de votre licence par un email indiquant la prochain renouvellement automatique de la licence.

4.2.3 Activer le produit

Pour activer votre produit Avira, vous disposez des options suivantes :

- Activation avec une licence complète valide

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

- Activation avec une licence d'évaluation

  Votre produit Avira est activé par une licence d'évaluation générée automatiquement, grâce à laquelle vous pouvez tester l'intégralité des fonctions du produit Avira pendant une période limitée.

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

Voici comment activer votre produit Avira :

Si vous n'avez pas encore installé votre produit Avira :

- Installez votre produit Avira.
  - ↳ Au cours de l'installation, il vous est demandé de choisir une option d'activation
  - **Activer le produit**= Activation avec une licence complète valide
  - **Tester le produit**= Activation avec une licence d'évaluation
- Indiquez la clé d'activation dans le cas d'une activation avec licence complète.
- Confirmez la sélection du processus d'activation en cliquant sur **Suivant**.
- Entrez vos données personnelles pour une inscription, le cas échéant et confirmez votre saisie en cliquant sur **Suivant**.
  - ↳ Vos données de licence s'affichent dans la fenêtre de dialogue suivante. Votre produit Avira a été activé.

- Poursuivez l'installation.

Si vous avez déjà installé votre produit Avira :

- Dans le Control Center, sélectionnez l'option de menu **Aide > Gestion de licence**.
  - ↪ L'assistant de licence s'affiche, dans lequel vous pouvez choisir l'option d'activation. Les étapes suivantes de l'activation du produit sont identiques à celles de la procédure présentée ci-avant.

4.2.4 Exécution des mises à jour automatisées

Voici comment créer une tâche d'actualisation automatisée de votre produit Avira avec le planificateur Avira :

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

> **Remarque**
> Nous conseillons d'effectuer des mises à jour régulières et fréquentes.
> L'intervalle de mise à jour recommandé est : 2 heures.

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

- **Reprogrammer la tâche si elle n'a pu être exécutée au moment prévu**
  Le programme effectue les tâches situées dans le passé qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.
- **Démarrer la tâche en plus en cas de connexion Internet**
  Outre la fréquence définie, la tâche est exécutée à chaque démarrage d'une connexion Internet.

▸ Cliquez sur **Suivant**.

↳ La fenêtre de dialogue **Affichage de la fenêtre** apparaît.

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

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

▸ Cliquez sur **Terminer**.

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

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

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

 Afficher les caractéristiques d'une tâche

 Modifier la tâche

 Supprimer la tâche

 Démarrer la tâche

 Arrêter la tâche

4.2.5 Démarrer manuellement une mise à jour

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

Voici comment démarrer manuellement une mise à jour de votre produit Avira :

- Cliquez avec le bouton droit de la souris 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 **Aperçu > État**, puis cliquez dans la zone **Dernière mise à jour** sur le lien **Démarrer mise à jour**.

  - OU -

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

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

Remarque
Nous conseillons d'effectuer des mises à jour régulières. L'intervalle de mise à jour recommandé est : 2 heures.

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

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

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

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

- Utiliser un profil de recherche prédéfini

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

  Si vous souhaitez chercher avec un profil de recherche individualisé.
- Créer et utiliser un nouveau profil de recherche

  Si vous souhaitez créer votre propre profil de recherche.

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

- Sous Windows XP et 2000 :

   À l'aide de ce symbole, vous démarrez la recherche d'un profil de recherche.
- Sous Windows Vista :

Sous Microsoft Windows Vista, le 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 accès aux fichiers qu'avec des droits d'administrateur étendus. Ces droits d'administrateur étendus doivent être attribués à chaque démarrage d'une recherche via un profil de recherche.

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

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

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

- Dans le Control Center, choisissez la rubrique **Sécurité PC > Scanner Système**.
  - ↪ Les profils de recherche prédéfinis apparaissent.
- Sélectionnez l'un des profils de recherche prédéfinis.

  -OU-

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

  -OU-

  Créez un nouveau profil de recherche
- Cliquez sur le symbole (Windows XP :  ou Windows Vista : ).
- La fenêtre **Luke Filewalker** apparaît et la recherche directe démarre.
  - ↪ A la fin du processus de recherche, les résultats s'affichent.

Si vous souhaitez ajuster un profil de recherche :

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

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

Si vous souhaitez créer un nouveau profil de recherche :

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

  Vous avez les possibilités suivantes pour sélectionner des répertoires :

- Répertoire avec ses sous-répertoires (coche noire)
- Uniquement les sous-répertoires d'un répertoire (coche grise, les sous-répertoires ont une coche noire)
- Aucun répertoire (pas de coche)

4.2.7 Recherche directe : Chercher des virus et logiciels malveillants par glisser-déplacer

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

- ✓ Le Control Center de votre programme Avira est ouvert.
- Sélectionnez le fichier ou le répertoire qui doit être contrôlé.
- Glissez avec le bouton gauche de la souris le fichier ou le répertoire sélectionné dans le Control Center.
  - ↪ La fenêtre **Luke Filewalker** apparaît et la recherche directe démarre.
  - ↪ A la fin du processus de recherche, les résultats s'affichent.

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

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

- Cliquez (par ex. dans l'explorateur Windows, sur le bureau ou dans un répertoire Windows ouvert) avec le bouton droit de la souris sur le fichier ou le répertoire / que vous souhaitez contrôler.
  - ↪ Le menu contextuel de l'explorateur Windows apparaît.
- Sélection dans le menu contextuel **Contrôler les fichiers sélectionnés avec Avira**.
  - ↪ La fenêtre **Luke Filewalker** apparaît et la recherche directe démarre.
  - ↪ A la fin du processus de recherche, les résultats s'affichent.

4.2.9 Recherche directe : recherche automatisée de virus et logiciels malveillants

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

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

- Dans le Control Center, choisissez la rubrique **Administration > Planificateur**.
- Cliquez sur le symbole  **Créer la nouvelle tâche avec l'assistant**.
  - ↪ La fenêtre de dialogue **Nom et description de la tâche** apparaît.
- Nommez la tâche et décrivez-la si besoin est.
- Cliquez sur **Suivant**.
  - ↪ La fenêtre de dialogue **Type de tâche** apparaît.
- Sélectionnez la **tâche de contrôle**.
- Cliquez sur **Suivant**.
  - ↪ La fenêtre de dialogue **Sélection du profil** apparaît.
- Choisissez le profil qui doit être parcouru.
- Cliquez sur **Suivant**.
  - ↪ La fenêtre de dialogue **Heure de la tâche** s'affiche.
- Sélectionnez quand la recherche doit être effectuée :

- **Immédiatement**
- **Tous les jours**
- **Toutes les semaines**
- **Par intervalle**
- **Une fois**
- **Connexion**

- Le cas échéant, saisissez la date selon votre sélection.
- Sélectionnez le cas échéant l'option supplémentaire suivante (disponible en fonction du type de tâche) : **Reprogrammer la tâche si elle n'a pu être exécutée au moment prévu**
  - ↪ Le programme effectue les tâches situées dans le passé qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.
- Cliquez sur **Suivant**.

↳ La fenêtre de dialogue **Affichage de la fenêtre** apparaît.

- Sélectionnez le mode de représentation de la fenêtre des tâches :
- **Invisible** : pas de fenêtre des tâches
- **Réduit** : uniquement la barre de progression
- **Agrandi** : fenêtre des tâches intégrale
- 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 de représentation agrandi ou réduit.
- Cliquez sur **Terminer**.

  ↳ La tâche que vous venez de créer apparaît comme activée (cochée) sur la page d'accueil de la rubrique **Administration > Planificateur**.
- Désactivez éventuellement les tâches qui ne doivent pas être exécutées.

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

 Afficher les caractéristiques d'une tâche

 Modifier la tâche

 Supprimer la tâche

 Démarrer la tâche

 Arrêter la tâche

4.2.10 Recherche directe : chercher les rootkits actifs de manière ciblée

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

Voici comment rechercher les rootkits actifs de manière ciblée :

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

  ↳ Les profils de recherche prédéfinis apparaissent.
- Sélectionnez le profil de recherche prédéfini **Recherche de rootkits et logiciels malveillants actifs**.
- Sélectionnez les éventuels autres nœuds et répertoires à contrôler en cliquant une fois dans la case du niveau de répertoire concerné.

- Cliquez sur le symbole (Windows XP :  ou Windows Vista : ).
  - ↪ La fenêtre **Luke Filewalker** apparaît et la recherche directe démarre.
  - ↪ A la fin du processus de recherche, les résultats s'affichent.

4.2.11 Réagir aux virus et logiciels malveillants détectés

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

Pour le composant ProActiv de la Protection Temps Réel, il n'y a aucune option d'action configurable : Un résultat positif s'affiche toujours dans la fenêtre **Protection Temps Réel : comportement suspect d'une application**.

Options d'action avec Scanner Système :

- **Interactif**

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

- **Automatique**

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

Options d'action avec la Protection Temps Réel :

- **Interactif**

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

- **Automatique**

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

Options d'action avec Protection E-mail, Protection Web :

- **Interactif**

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

- **Automatique**

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

Mode d'action interactif

- En mode d'action interactif, vous réagissez aux virus et programmes indésirables détectés en sélectionnant dans le message d'avertissement une **action pour les objets concernés** et en exécutant l'action choisie par votre **validation**.

Les actions suivantes de traitement des objets concernés sont disponibles :

> **Remarque**
> Les actions disponibles à la sélection dépendent du système d'exploitation, du composant de protection (Scanner Système Avira, Protection Temps Réel Avira, Protection E-mail Avira, Protection Web Avira) qui signale le résultat positif et du logiciel malveillant détecté.

Actions du Scanner Système et de la Protection Temps Réel (sans résultat positif de ProActiv) :

- **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 (en cliquant deux fois par ex.) n'est alors plus possible. Les fichiers peuvent être réparés et renommés ultérieurement.

- **Quarantaine**

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

- **Supprimer**

  Le fichier va être supprimé. Cette procédure est beaucoup plus rapide que **Écraser et supprimer**.

Si le résultat positif est un virus de secteur d'amorçage, le secteur d'amorçage est effacé en cas de suppression. Un nouveau secteur d'amorçage est écrit.

- **Ignorer**

  Aucune autre action n'est effectuée. Le fichier concerné reste actif sur votre ordinateur.

- **Ecraser et supprimer**

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

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

- **Toujours ignorer**

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

- **Copier dans la quarantaine**

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

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

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

Actions de la Protection Temps Réel en cas de résultats positifs du composant ProActiv (indication d'actions suspectes d'une application) :

- **Programme fiable**

  L'exécution de l'application se poursuit. Le programme est ajouté à la liste des applications autorisées, et il est exclu de la surveillance du composant ProActiv. En cas d'ajout à la liste des applications autorisées, il y a activation du type de surveillance *Contenu*. Cela signifie que l'application n'est exclue d'une surveillance

par le composant ProActiv que si le contenu reste inchangé (voir Filtre des applications : Applications à exclure).

- **Bloquer le programme une fois**

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

- **Bloquer toujours ce programme**

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

- **Ignorer**

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

Actions de la Protection E-mail : emails entrants

- **Déplacer en quarantaine**

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

- **Supprimer le mail**

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

- **Supprimer la pièce jointe**

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

- **Déplacer la pièce jointe en quarantaine**

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

- **Ignorer**

  L'email concerné est livré.

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

Actions de la Protection E-mail : emails sortants

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

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

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

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

- **Ignorer**

  L'email concerné est envoyé.

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

Actions 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 quarantaines s'il a une valeur informative ou - si nécessaire - être envoyé à Avira Malware Research Center.

- **Ignorer**

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

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

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

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

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

Voici comment manipuler les fichiers en quarantaine :

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

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

- Sélectionnez le fichier et cliquez sur  .
  - ↳ La fenêtre de dialogue **Caractéristiques** avec d'autres informations sur le fichier apparaît.

Si vous souhaitez à nouveau contrôler un fichier :

Le contrôle d'un fichier est recommandé quand le fichier de définitions des virus de votre produit Avira a été actualisé et qu'il y a un soupçon de fausse alerte. Voici comment confirmer une fausse alerte lors du nouveau contrôle et restaurer le fichier.

- Sélectionnez le fichier et cliquez sur  .
  - ↳ L'absence de virus et logiciels malveillants est contrôlée sur le fichier avec les réglages de la recherche directe.
  - ↳ Après le contrôle, la boîte de 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  .
- Vous devez valider votre sélection avec **Oui**.

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

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

↳ La boîte de dialogue *Envoi de fichiers* s'ouvre, contenant un formulaire pour la saisie de vos coordonnées.

- Indiquez les données au complet.
- Sélectionnez un type : **Fichier suspect** ou **Soupçon de fausse alarme**.
- Sélectionnez un format de réponse : **HTML**, **texte**, **HTML et Texte**.
- Cliquez sur **OK.**

↳ Le fichier est téléchargé sur un serveur Web de Avira Malware Research Center.

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

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

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

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

- Sélectionnez l'objet en quarantaine et cliquez sur  .

↳ Le fichier texte *quarantaine - éditeur* s'ouvre avec les données relatives à l'objet de quarantaine sélectionné.

- Mémorisez le fichier texte.

Vous pouvez aussi restaurer les fichiers en quarantaine (voir chapitre :) Quarantaine : restaurer les fichiers en quarantaine

4.2.13 Quarantaine : restaurer les fichiers dans la quarantaine

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

- **Sous Windows XP et 2000** :

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

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

- **Sous Windows Vista** :

  Sous Microsoft Windows Vista, le 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 accès aux fichiers qu'avec des droits d'administrateur étendus. Ces droits d'administrateur étendus doivent être attribués à chaque démarrage d'une recherche via un profil de recherche.

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

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

Voici comment restaurer les fichiers en quarantaine :

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

✓ Fichier recontrôlé par une recherche et réparé.

▸ Dans le Control Center, choisissez la rubrique **Administration > Quarantaine**.

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

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

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

Cette option n'est pas disponible pour les emails.

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

  - ↪ Le système vous demande si vous souhaitez restaurer le fichier.
- Cliquez sur **Oui**.
  - ↪ Le fichier est restauré dans le répertoire à partir duquel il avait été placé en quarantaine.

Si vous souhaitez restaurer un fichier dans un répertoire particulier :

- Sélectionnez le fichier et cliquez sur  .
  - ↪ Le système vous demande si vous souhaitez restaurer le fichier.
- Cliquez sur **Oui**.
  - ↪ La fenêtre standard Windows pour sélectionner un répertoire apparaît.
- Sélectionnez le répertoire dans lequel le fichier doit être restauré et validez.
  - ↪ Le fichier est restauré dans le répertoire choisi.

4.2.14 Quarantaine : déplacer un fichier suspect en quarantaine

Vous pouvez déplacer manuellement un fichier suspect en quarantaine :

- Dans le Control Center, choisissez la rubrique **Administration > Quarantaine**.
- Cliquez sur  .
  - ↪ La fenêtre standard Windows pour sélectionner un fichier apparaît.
- Choisissez un fichier et validez avec **Ouvrir**.
  - ↪ Le fichier est déplacé en quarantaine.

Vous pouvez contrôler les fichiers en quarantaine avec le Scanner Système Avira (voir chapitre : Quarantaine : Manipuler les fichiers (*.qua) en quarantaine).

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

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

✓ Dans le Control Center, choisissez la rubrique **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 fichier**.
- Déployez le menu contextuel en cliquant sur le petit triangle à droite du menu contextuel.
  - ↳ Les entrées **Standard**, **Scanner tous les fichiers** et **Personnalisé** apparaissent.
- Sélectionnez l'entrée **Personnalisé**.
  - ↳ La fenêtre de dialogue **Extensions de fichiers** s'affiche avec une liste de tous les types de fichiers qui sont parcourus avec le profil de recherche.

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

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

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

- Sélectionnez un 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.

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

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

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

✓ Dans le Control Center, choisissez la rubrique **Sécurité PC > Contrôler**.

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

↳ Le lien est créé sur le bureau.

4.2.17 Événements : filtrer les événements

Dans le Control Center, sous **Administration > Événements**, s'affichent les événements qui ont été créés par les composants de programme de votre produit Avira (similaire à l'affichage des événements de votre système d'exploitation Windows). Les composants de programme sont les suivants, dans l'ordre alphabétique :

- Protection Web
- Protection Temps Réel
- Protection E-mail
- AVE Service
- Planificateur
- Scanner Système
- Updater

Les types d'événements suivants s'affichent :

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

Voici comment filtrer les événements affichés :

- Dans le Control Center, choisissez la rubrique **Administration > Événements**.
- Activez la case à cocher des composants de programme pour afficher les événements des composants activés.

  - OU -

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

  - OU -

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

4.2.18 Protection E-mail : exclure des adresses email de la vérification

Voici comment exclure des adresses email (expéditeur) de la vérification par la Protection E-mail (mise sur liste blanche) :

- Dans le Control Center, choisissez la rubrique **Sécurité Internet > Protection E-mail**.

↳ Vous voyez dans la liste les emails reçus.

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

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

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

Avertissement
N'excluez de la vérification par la Protection E-mail que les adresses email absolument dignes de confiance.

Remarque
Dans la configuration, sous Protection E-mail > Généralités > Exceptions, vous pouvez ajouter des adresses email à la liste des exclusions ou supprimer des adresses email de la liste des exclusions.

5. Scanner Système

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

- **Recherche directe via le menu contextuel**
  La recherche directe via le menu contextuel (bouton droit de la souris - entrée **Contrôler les fichiers sélectionnés avec Avira**) est recommandée si vous voulez contrôler des fichiers et répertoires séparément dans l'explorateur Windows par exemple. Un autre avantage est qu'il n'est pas nécessaire de démarrer le Control Center pour la recherche directe via le menu contextuel.
- **Recherche directe via la commande glisser-déplacer**
  En glissant un fichier ou un répertoire dans la fenêtre de programme du Control Center, le Scanner Système contrôle le fichier ou le répertoire, ainsi que tous les sous-répertoires inclus. Cette procédure est recommandée si vous souhaitez contrôler des fichiers et répertoires séparément, que vous avez par ex. déposés sur votre bureau.
- **Recherche directe via les profils**
  Cette procédure est recommandée si vous souhaitez contrôler régulièrement certains répertoires et lecteurs (par ex. votre répertoire de travail ou les lecteurs sur lesquels vous déposez régulièrement des fichiers). Il n'est alors plus nécessaire de sélectionner ces répertoires et lecteurs à chaque contrôle, il suffit d'une simple sélection avec le profil correspondant. Voir Recherche directe via les profils.
- **Recherche directe 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 *Détection de Rootkits et logiciels malveillants actifs*
- Contrôle des processus actifs via le profil de recherche *Processus actifs*
- Recherche de virus de secteurs d'amorçage via la commande de menu **Scanner 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 celle du fichier de définitions des virus et du moteur de recherche. Le composant Updater est intégré dans votre produit Avira pour l'exécution des mises à jour. L'Updater garantit que votre produit Avira fonctionne toujours en étant à jour et qu'il est en mesure de détecter les nouveaux virus apparaissant chaque jour. L'Updater met à jour les composants suivants :

- Fichier de définitions des virus :

  Le fichier de définitions des virus contient un modèle de détection des programmes malveillants que votre 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 ceux-ci sont mis à jour si nécessaire. Selon les réglages effectués dans la configuration, l'Updater effectue en outre une mise à jour produit ou vous informe des mises à jour produit disponibles. Après une mise à jour de produit, il peut être nécessaire d'effectuer un redémarrage de votre système d'ordinateur. S'il n'y a qu'une mise à jour du fichier de définitions des virus et du moteur de recherche, il n'est pas nécessaire de redémarrer l'ordinateur.

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

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

Dans le Control Center, sous **Planificateur**, vous pouvez configurer d'autres tâches de mises à jour qui seront exécutées par l'Updater aux intervalles indiqués. Vous avez aussi la possibilité de démarrer manuellement une mise à jour :

- Dans le Control Center : dans le menu **Mise à jour** et dans la rubrique **État**

- Via le menu contextuel de l'icône de programme

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

7. Résolution des problèmes, astuces

7.1 Aperçu

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

- voir le chapitre Aide en cas de problème
- voir le chapitre Commandes clavier
- voir chapitre Centre de sécurité Windows

7.2 Aide en cas de problème

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

- Le message d'erreur *Le fichier de licence ne s'ouvre pas* s'affiche.
- 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 annonce la Protection Temps Réel Avira et la Protection E-mail Avira dès qu'elles sont activées
- La Protection E-mail Avira ne fonctionne pas.
- Un email envoyé via une connexion TSL a été bloqué par la Protection E-mail.
- Le chat Internet ne fonctionne : Les messages du chat ne s'affichent pas.

Le message d'erreur "Le fichier de licence ne s'ouvre pas" s'affiche.

Cause : le fichier est codé.

- Pour activer la licence, il n'est pas nécessaire d'ouvrir le fichier mais de l'enregistrer dans le répertoire de programmes.

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

Cause : votre connexion Internet est inactive. C'est pourquoi, il est impossible d'établir une connexion au serveur web sur Internet.

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

Cause : le serveur proxy n'est pas accessible.

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

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

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

Sinon :

- Contrôlez vos réglages dans la configuration (mode expert) sous Généralités > Mise à jour.

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.
- Démarrez le produit Avira et la configuration (mode expert).
- Sélectionnez **Scanner Système > Rechercher > Fichiers > Tous les fichiers** et confirmez la fenêtre avec **OK**.
- Démarrez une recherche sur tous les lecteurs locaux.
- Démarrez l'ordinateur en mode normal.
- Effectuez une recherche en mode normal.
- Si aucun autre virus ni logiciel malveillant n'est détecté, activez la restauration du système si elle est disponible et doit être utilisée.

L'icône de programme indique un état de désactivation.

Cause : la Protection Temps Réel Avira est désactivée.

- Dans le Control Center, à la rubrique **Aperçu > État** dans la zone **Protection Temps Réel Avira**, cliquez sur le lien **Activer**.

Cause : la Protection Temps Réel Avira 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. Il en est de même pour la Protection E-mail Avira.

Sinon :

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

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

Cause : lors du processus de sauvegarde, la Protection Temps Réel Avira parcourt tous les fichiers avec lesquels la sauvegarde des données fonctionne.

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

Mon pare-feu annonce la Protection Temps Réel Avira et la Protection E-mail Avira dès qu'elles sont activées.

Cause : la communication de la Protection Temps Réel Avira et de la Protection E-mail Avira a lieu 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 Avira et la Protection E-mail Avira. La Protection Temps Réel Avira fonctionne uniquement avec l'adresse 127.0.0.1 (localhost). Aucune connexion à Internet n'est établie.Il en est de même pour la Protection E-mail Avira.

La Protection E-mail Avira ne fonctionne pas.

✓ Contrôlez la fonctionnalité de la Protection E-mail Avira à l'aide des checklists suivantes, si des problèmes se produisent en rapport avec la Protection E-mail Avira.

Checklist

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

✓ Contrôlez si votre client de mail client se connecte au serveur par SSL (également appelé souvent TSL - Transport Layer Security). La Protection E-mail Avira ne prend pas en charge SSL et arrête donc les connexions codées SSL. Si vous utilisez les connexions codées SSL sans la Protection E-mail Avira, pour la connexion vous devez utiliser un autre port que les ports surveillés par la Protection E-mail. Vous pouvez configurer les ports surveillés par la Protection E-mail dans la configuration sous **Protection E-mail > Rechercher**.

✓ Le service Protection E-mail Avira (service) est-il activé ? Activez le service si nécessaire : sélectionnez dans la barre de démarrage **Démarrer > Panneau de configuration > Performances et maintenance**. Démarrez le panneau de

configuration **Services** en cliquant deux fois dessus (sous Windows 2000 et Windows XP, l'applet des services se trouve dans le sous-dossier *Outils d'administration*). Cherchez l'entrée *Protection E-mail Avira*. Le type de démarrage choisi doit être `Automatique` et l'état `Démarré`. Démarrez le service manuellement si nécessaire en sélectionnant la ligne correspondante et le bouton **Démarrer**. Si un message d'erreur s'affiche, contrôlez l'*affichage des événements*. Si cela ne résout pas le problème, désinstallez complètement le produit Avira via **Démarrer > Panneau de configuration > Performances et maintenance > Logiciel**, redémarrez l'ordinateur et réinstallez votre produit Avira.

Généralités

- Via SSL (Secure Sockets Layer), les connexions POP3 (appelées souvent TLS (Transport Layer Security)) ne peuvent pas être protégées actuellement et sont ignorées.
- L'identification au serveur de messagerie électronique est actuellement prise en charge uniquement via des "mots de passe". "Kerberos" et "RPA" ne sont actuellement pas pris en charge.
- Votre produit Avira ne contrôle pas l'absence de virus et de programmes indésirables lors de l'envoi d'emails.

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

Un email envoyé via une connexion TSL a été bloqué par la Protection E-mail.

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

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

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

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

Cause : 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 d'un 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 > Exceptions).

7.3 Commandes clavier

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

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

7.3.1 Dans les champs de dialogue

Commande clavier	Description
Ctrl + Tab **Ctrl + PgDn**	Navigation dans Control Center Passer à la rubrique suivante.
Ctrl + Shift + Tab **Ctrl + PgDn**	Navigation dans Control Center Passer à la rubrique précédente.
← ↑ → ↓	Navigation dans les rubriques de configuration Mettez d'abord l'accent avec la souris sur une rubrique de configuration.
Tab	Passer à l'option suivante ou au groupe d'options suivant.
Shift + Tab	Passer à l'option précédente ou au groupe d'options précédent.
← ↑ → ↓	Changer d'option dans un champ de liste déroulante sélectionné ou dans un groupe d'options.
Touche espace	Activation et désactivation d'une case à cocher lorsque l'option active est une case à cocher.
Alt + lettre soulignée	Sélectionner une option ou exécuter une commande.

Alt + ↓ **F4**	Ouvrir le champ de liste déroulante sélectionné.
Esc	Fermer le champ de liste déroulante sélectionné. Abandonner la commande et fermer le champ de dialogue.
Touche Enter	Exécuter la commande pour l'option ou le bouton actif.

7.3.2 Dans l'Aide

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

7.3.3 Dans le Control Center

Généralités

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

Rubrique **Contrôler**

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

Rubrique **Quarantaine**

Commande clavier	Description
F2	Contrôler à nouveau l'objet
F3	Restaurer l'objet

F4	Envoyer l'objet
F6	Restaurer l'objet à l'emplacement...
Enter	Caractéristiques
Ins	Ajouter le fichier
Suppr	Supprimer l'objet

Rubrique **Planificateur**

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

Rubrique **Rapports**

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

Rubrique **Événements**

Commande clavier	Description
F3	Exporter les événements
Enter	Afficher l'événement
Suppr	Supprimer les événements

7.4 Centre de sécurité Windows

- à partir de Windows XP Service Pack 2 -

7.4.1 Généralités

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

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

7.4.2 Le Centre de sécurité Windows et votre produit Avira

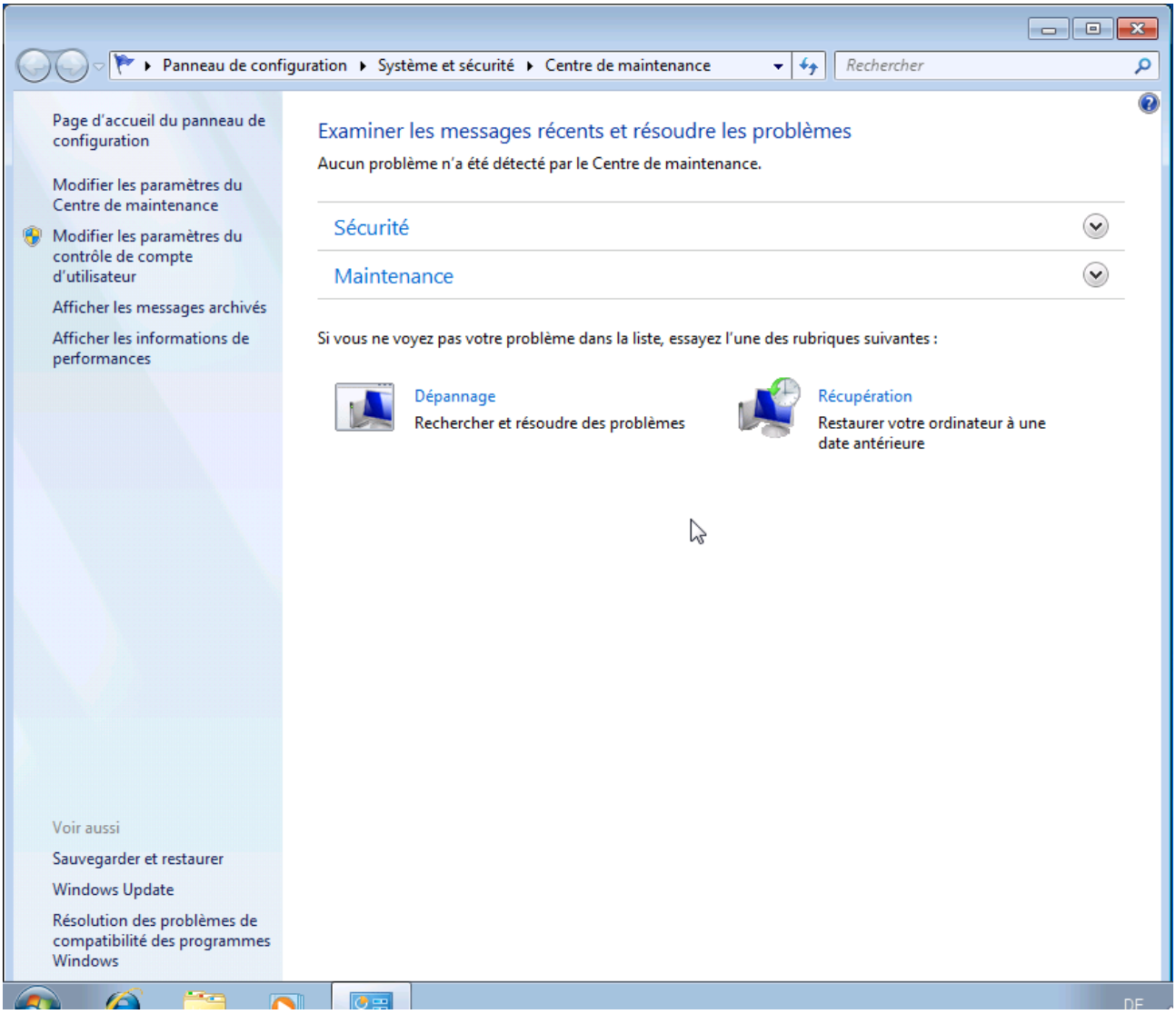
Logiciel antivirus/Protection contre les logiciels nuisibles

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

- Protection antivirus NON TROUVÉE
- Antivirus EXPIRÉ
- Protection antivirus ACTIVÉE
- Protection antivirus DÉSACTIVÉE
- Protection antivirus NON SURVEILLÉE

Protection antivirus NON TROUVÉE

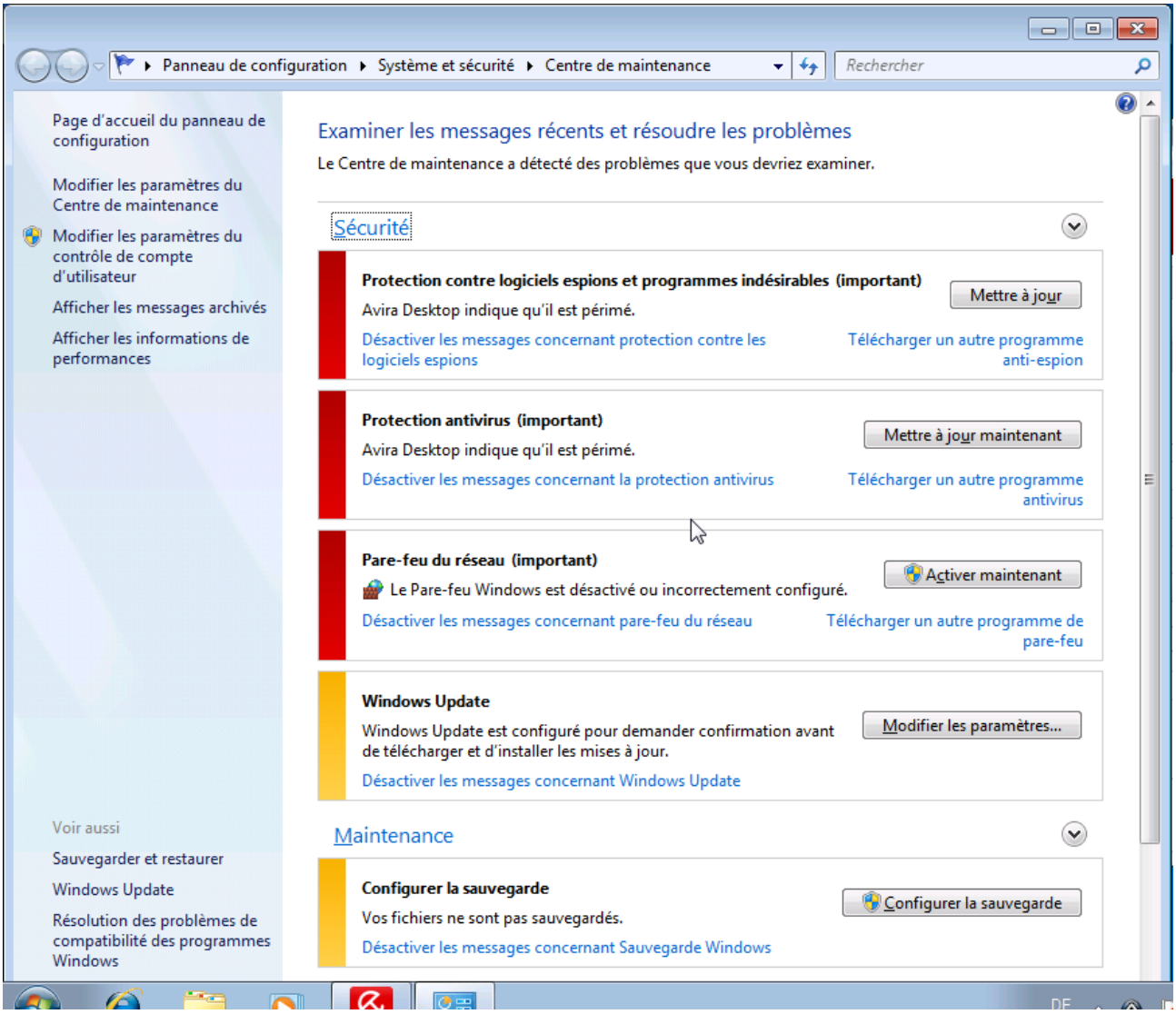
Cette remarque du Centre de sécurité Windows apparaît si le Centre de sécurité Windows n'a trouvé aucun logiciel antivirus sur votre ordinateur.



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

Antivirus EXPIRÉ

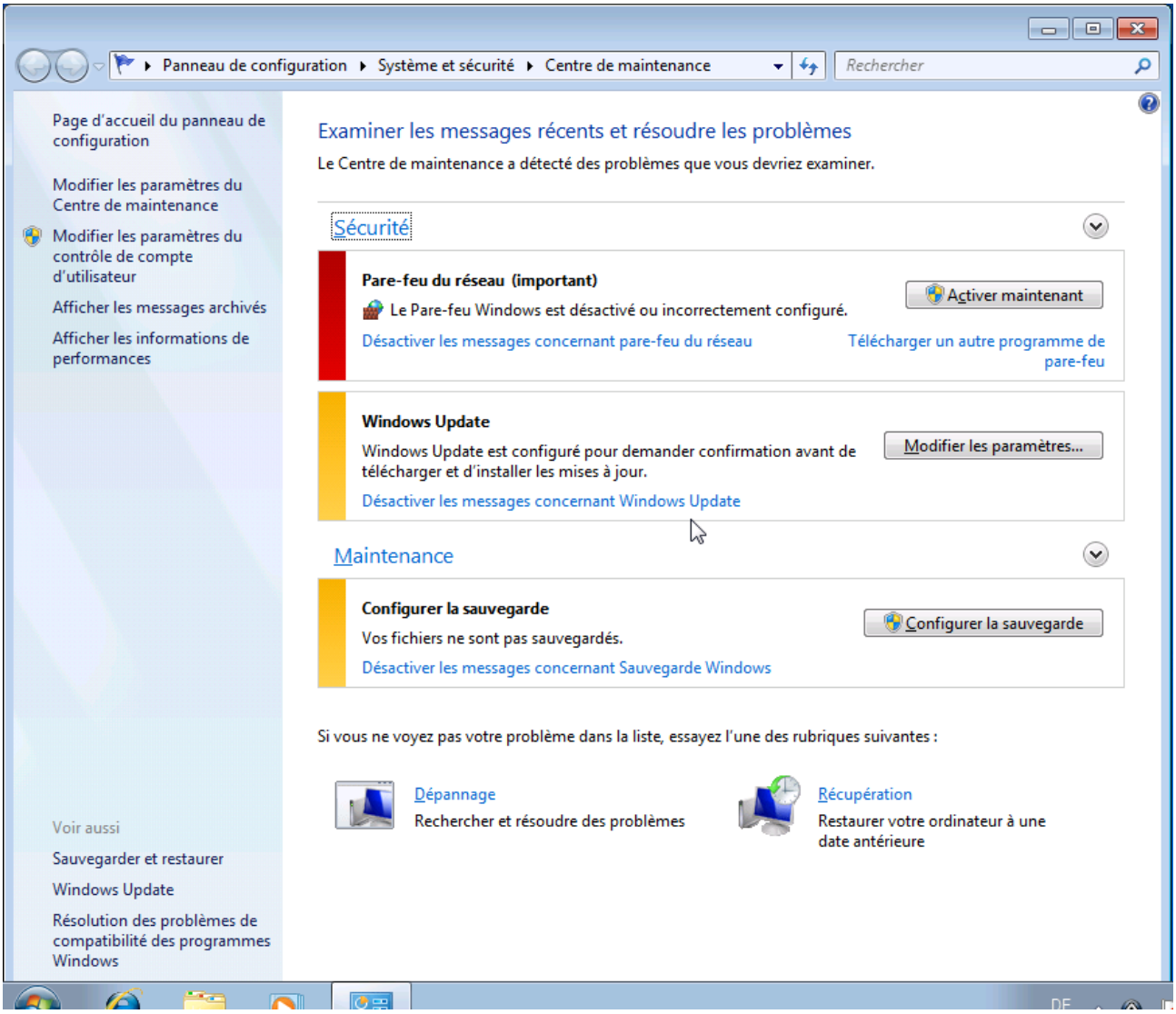
Si vous avez installé Windows XP Service Pack 2 ou Windows Vista, puis votre produit Avira, ou si vous avez installé Windows XP Service Pack 2 ou Windows Vista sur un système accueillant déjà votre produit Avira, vous recevez le message suivant :



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

Protection antivirus ACTIVÉE

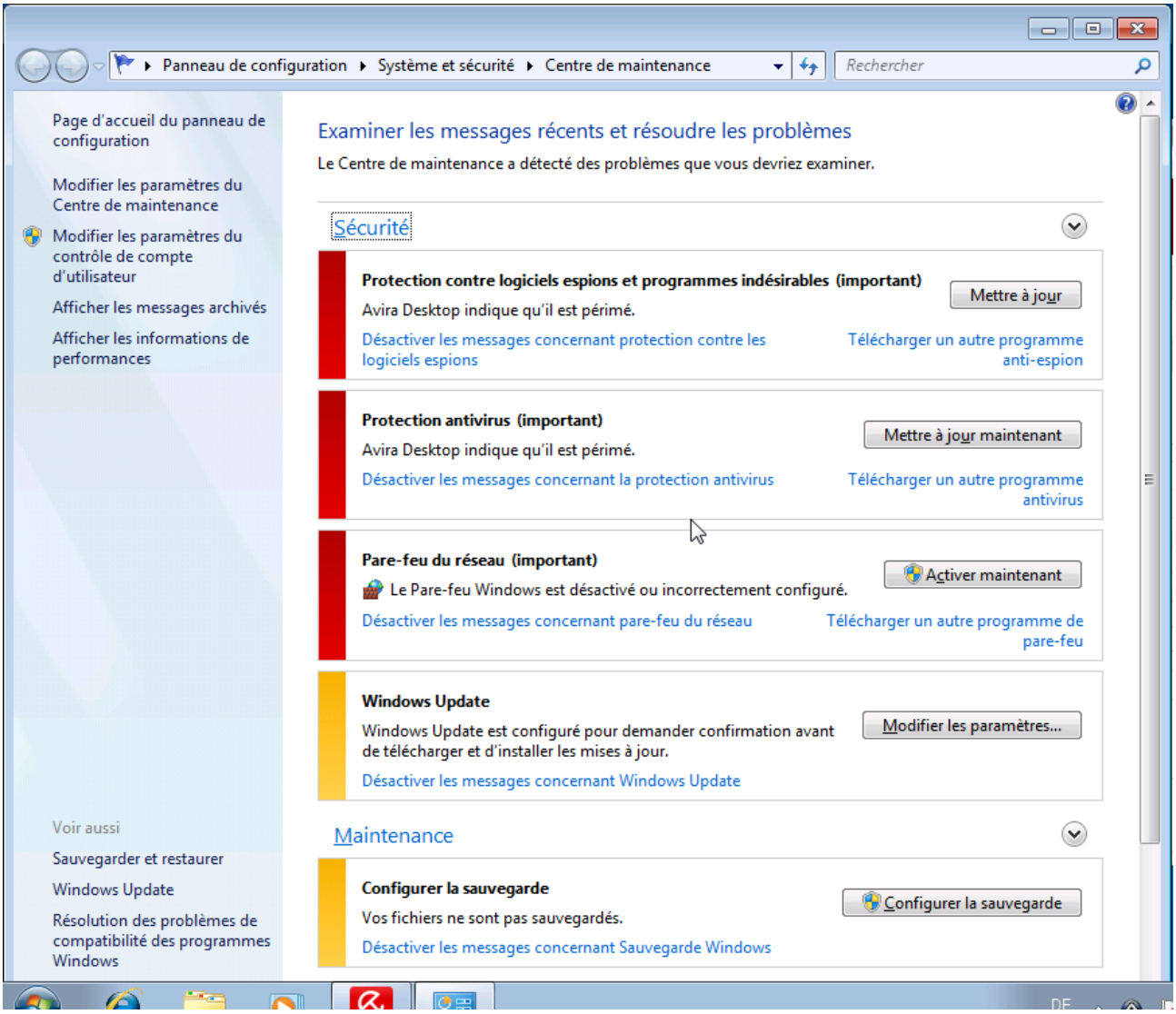
Après l'installation de votre produit Avira et une mise à jour effectuée immédiatement après, vous recevez le message suivant :



Votre produit Avira est désormais à jour et la Protection Temps Réel Avira est activée.

Antivirus DÉSACTIVÉ

Vous recevez le message suivant si vous désactivez la Protection Temps Réel Avira ou si vous arrêtez le service Protection Temps Réel.

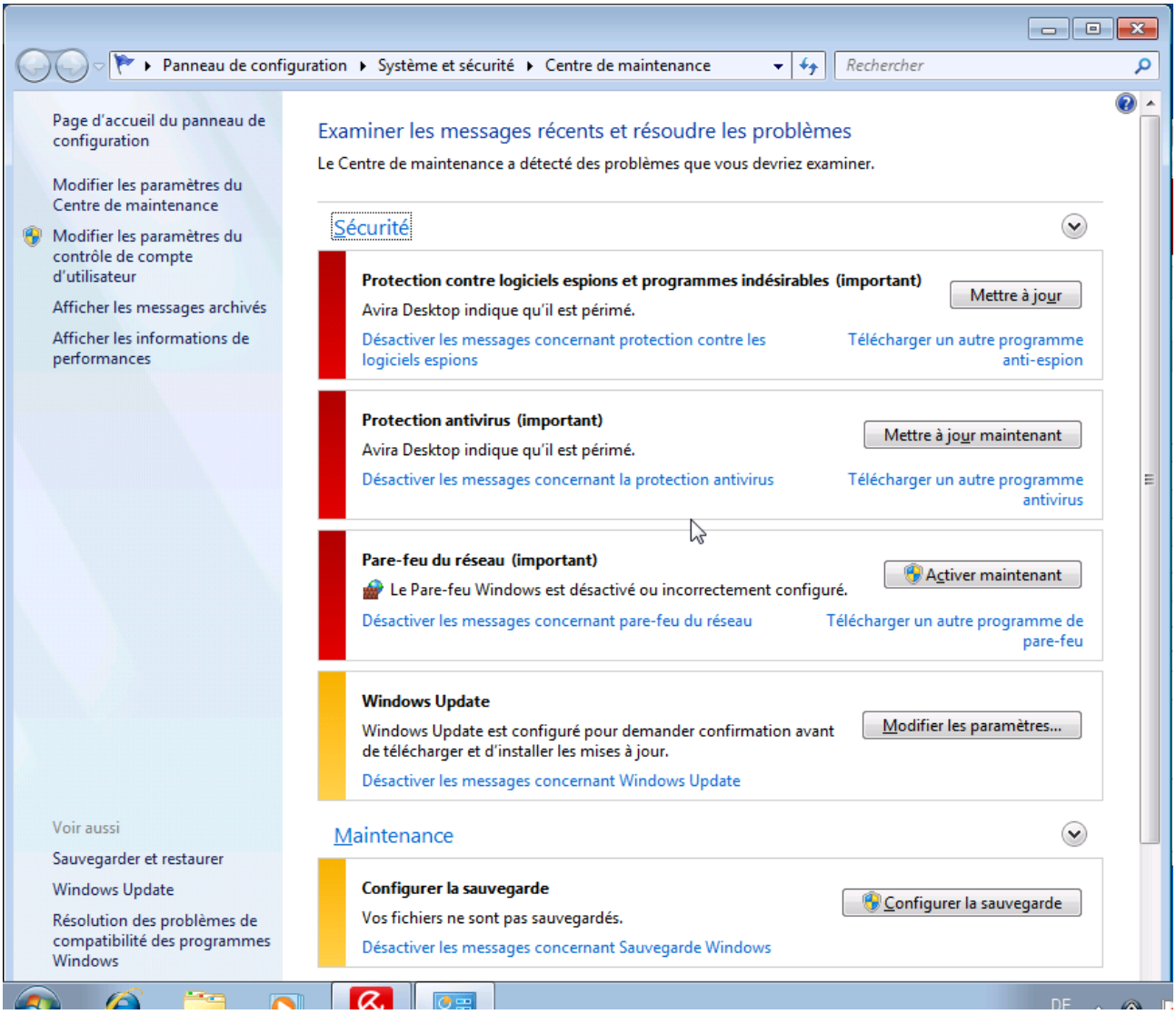


Remarque
Vous pouvez activer et désactiver la Protection Temps Réel Avira dans la rubrique Aperçu > État du Control Center. Vous voyez en outre que la Protection Temps Réel Avira est activée si le parapluie rouge est ouvert dans votre barre des tâches.

Protection antivirus NON SURVEILLÉE

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

Remarque
Windows Vista ne prend pas en charge la fonction.



Remarque

Le Centre de sécurité Windows est pris en charge par votre 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 XP Service Pack 2 surveille votre logiciel antivirus, il ne dispose d'aucune fonction antivirus. Sans protection antivirus supplémentaire, vous ne seriez donc pas protégé des virus et autres logiciels malveillants !

8. Virus et autres

8.1 Catégories de dangers

Logiciels publicitaires

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

Votre produit Avira détecte les logiciels publicitaires. Si, dans la configuration, l'option **Logiciel publicitaire** est cochée sous Catégories de dangers, vous recevez un message d'avertissement quand votre produit Avira détecte un tel logiciel.

Logiciel publicitaire/Logiciel espion

Logiciel affichant de la publicité ou logiciel envoyant des données 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, l'option **Logiciel publicitaire/Logiciel espion** est cochée sous Catégories de dangers, vous recevez un avertissement quand votre produit Avira en a détecté un.

Application

La désignation Application concerne une application dont l'utilisation peut être liée à un risque ou dont l'origine est douteuse.
Votre produit Avira détecte les applications (APPL). Si, dans la configuration, l'option **Application** est cochée sous Catégories de dangers, vous recevez un avertissement si votre produit Avira détecte ce type de comportement.

Logiciel de commande Backdoor

Pour voler des données ou manipuler l'ordinateur, un programme de serveur backdoor passe "par la porte arrière" sans que l'utilisateur le remarque. Via Internet ou le réseau, ce programme peut être commandé via un logiciel de commande backdoor (client) par des tiers.
Votre produit Avira détecte les "logiciels de commande Backdoor". Si, dans la configuration, l'option **Logiciel de commande Backdoor** est cochée sous Catégories de dangers, vous recevez un avertissement quand votre produit Avira en a détecté un.

Fichiers à extensions déguisées

Fichiers exécutables qui déguisent leur extension de manière suspecte. Cette méthode de déguisement est souvent utilisée par les logiciels malveillants.
Votre produit Avira détecte les "fichiers à extensions déguisées". Si, dans la configuration, l'option **Fichiers à extensions déguisées** est cochée sous Catégories de dangers, vous recevez un avertissement si votre produit Avira en détecte un.

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 claire. L'établissement de la connexion via des programmes de numérotation sérieux s'affiche sans ambigüité. En outre, les dialers sérieux indiquent clairement les frais de connexion.

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

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

Par défaut, votre produit Avira détecte les programmes de numérotation payants qu'il connaît.

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

Hameçonnage

L'hameçonnage, également connu sous le nom de "brand spoofing", est une forme raffinée de vol de données qui vise les clients ou clients potentiels des FAI, banques, services bancaires en lignes, autorités d'enregistrement.
Communiquer son adresse email sur Internet, remplir des formulaires en ligne, entrer dans des Newsgroups ou sur des sites Web présente le risque que vos données soient volées par ce qu'on appelle des "Internet crawling spiders" et utilisées sans votre accord dans le but d'une escroquerie.

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

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 "Security Privacy Risk". Si, dans la configuration, l'option **Programmes portant atteinte à la vie privée** est cochée sous Catégories de dangers, vous recevez un avertissement si votre produit Avira en détecte un.

Programmes de blagues

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

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

Votre produit Avira est capable de détecter les programmes de blagues grâce à l'élargissement de ses routines de recherche et d'identification pour les éliminer éventuellement comme programmes indésirables. Si, dans la configuration, l'option **Programmes de blagues** est cochée sous Catégories de dangers, vous êtes prévenu en cas de détection d'un tel programme.

Jeux

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

circulent : les jeux sont envoyés via les programmes de courrier électronique aux partenaires qui répondent.

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

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

Logiciel frauduleux

Les logiciels frauduleux, aussi connus sous les noms de "scareware" (programme de menace) ou de "rogueware" (programme malhonnête), simulent des infections virales et des dangers, se faisant ainsi passer pour des logiciels antivirus professionnels. Un scareware est conçu pour mettre l'utilisateur dans l'incertitude ou lui faire peur. Si la victime tombe dans le piège et croit être menacée, on lui propose souvent, contre paiement, un moyen de supprimer le danger non existant. Dans d'autres cas, la victime qui croit à une attaque réussie est incitée à exécuter des actions qui rendent alors possible une véritable attaque.

Si, dans la configuration, l'option **Logiciel frauduleux** est cochée sous Catégories de dangers, vous recevez un avertissement en cas de détection d'un scareware.

Programmes de décompression inhabituels

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

Votre produit Avira détecte les "programmes de décompression inhabituels". Si, dans la configuration, l'option Programmes de décompression inhabituels (PCK) est cochée sous **Catégories de dangers**, vous recevez un avertissement quand votre produit Avira en a détecté un.

8.2 Virus et autres logiciels malveillants

Logiciels publicitaires

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

Backdoors

Un programme de commande Backdoor (littéralement de porte arrière) peut accéder à un ordinateur en passant outre sa protection.

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

Virus d'amorçage

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

Bot-Net

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

Exploit

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

Canulars (angl. hoax)

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

Pot de miel

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

Macrovirus

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

Pharming

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

Hameçonnage

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

Virus polymorphes

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

Virus programmes

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

Rootkits

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

Virus de script et vers

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

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

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

Logiciels espions

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

Chevaux de Troie

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

formatent le disque dur par exemple. Les droppers, qui 'déposent' des virus ou l'inséminent dans un système informatique, sont un type particulier de cheval de Troie.

Logiciel frauduleux

Les logiciels frauduleux, aussi connus sous les noms de "scareware" (programme de menace) ou de "rogueware" (programme malhonnête), simulent des infections virales et des dangers, se faisant ainsi passer pour des logiciels antivirus professionnels. Un scareware est conçu pour mettre l'utilisateur dans l'incertitude ou lui faire peur. Si la victime tombe dans le piège et croit être menacée, on lui propose souvent, contre paiement, un moyen de supprimer le danger non existant. Dans d’autres cas, la victime qui croit à une attaque réussie est incitée à exécuter des actions qui rendent alors possible 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 emails d'hameçonnage.

9. Info et service

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

- voir le chapitre Adresse de contact
- voir le chapitre Support technique
- voir le chapitre Fichier suspect
- voir le chapitre Signaler une fausse alerte
- voir le chapitre Vos réactions pour plus de sécurité

9.1 Adresse de contact

Nous serons heureux de vous assister si vous avez des questions et suggestions concernant les produits Avira. Vous trouverez nos adresses de contact dans le Control Center sous Aide > À propos de Avira Internet Security 2012.

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 concernant notre service étendu de support :
http://www.avira.com/fr/technical_support

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

- **Données de licence**. Vous les trouverez dans l'interface du programme sous l'option de menu **Aide > À propos de Avira Internet Security 2012 > Informations de licence**. Voir Informations de licence.
- **Informations de version**. Vous les trouverez dans l'interface du programme sous l'option de menu **Aide > À propos de Avira Internet Security 2012 > Informations de version**. Voir Informations de version.
- **Version du système d'exploitation** et packs de service éventuellement installés.
- **Packs logiciels installés**, par ex. logiciels antivirus d'autres fabricants.
- **Messages précis** du programme ou du fichier rapport.

9.3 Fichier suspect

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

- Sélectionnez le fichier dans le gestionnaire de quarantaine de Control Center et sélectionnez via le menu contextuel ou le bouton correspondant l'option Envoyer fichier.
- Envoyez le fichier souhaité compressé (WinZIP, PKZip, Arj etc.) en pièce jointe d'un email à l'adresse suivante :
  virus-premium-fr@avira.com
  Comme certaines passerelles de courrier électronique fonctionnent avec un logiciel antivirus, dotez le ou les fichier(s) d'un mot de passe (n'oubliez pas de nous communiquer ce mot de passe).
- Alternativement, vous avez la possibilité de nous envoyer le fichier suspect via notre site Web : http://www.avira.com/fr/sample-upload

9.4 Signaler une fausse alerte

Si vous pensez que votre produit Avira indique un résultat positif dans un fichier qui est pourtant très probablement "propre", envoyez ce fichier compressé (WinZIP, PKZIP, Arj, etc.) en pièce jointe dans un email, à l'adresse suivante :
virus-premium-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).

9.5 Vos réactions pour plus de sécurité

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

Si vous croyez avoir trouvé une faiblesse de sécurité dans l'un de nos produits, veuillez envoyer un email à l'adresse suivante :

vulnerabilities-premium-fr@avira.com

10.Référence : options de configuration

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

10.1 Scanner Système

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

10.1.1 Recherche

C'est ici que vous établissez 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 pour contrôle lors de la recherche directe, le Scanner Système contrôle, en fonction de la configuration :

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

Fichiers

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

Tous les fichiers

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

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

Sélection intelligente des fichiers

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

lieu uniquement sur la base des extensions de fichiers. Ce réglage est activé par défaut et recommandé.

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

Utiliser la liste d'extensions des fichiers

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

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

Extensions de fichiers

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

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

Autres réglages

Contrôler secteur d'amorçage des lecteurs

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

Contrôler les secteurs d'amorçage maître

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

Ignorer les fichiers hors ligne

Si cette option est activée, la recherche directe ignore les fichiers hors ligne. Cela signifie que la présence de virus et programmes indésirables n'est pas contrôlée sur les fichiers. Les fichiers hors ligne sont des fichiers qui ont été migrés par un système

de gestion de mémoire hiérarchique (HSMS) physiquement du disque dur sur un volume externe par exemple. Ce réglage est activé par défaut.

Contrôle d'intégrité de fichiers système

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

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

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

Recherche optimisée

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

Remarque
L'option n'est disponible que sur des ordinateurs à processeurs multiples.

Suivre les liens symboliques

Si l'option est activée, le Scanner Système suit, lors de la recherche, tous les liens symboliques du profil de recherche ou du répertoire sélectionné pour contrôler l'absence de virus et de logiciels malveillants dans les fichiers liés.

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 l'option est activée, le Scanner Système contrôle la présence de rootkits actifs en début de contrôle sur le répertoire système de Windows lors d'une procédure rapide. Ce processus contrôle l'absence de rootkits actifs sur votre ordinateur de manière moins détaillée que le profil de recherche "**Recherche de rootkits**", il est toutefois exécuté beaucoup plus rapidement.

Remarque
La recherche Rootkit n'est disponible ni sous Windows XP 64 bits !

Scanner le registre

Si l'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 et programmes indésirables peut être arrêtée à tout moment avec le bouton "**Arrêt"** dans la fenêtre "**Luke Filewalker**". Si vous avez désactivé ce réglage, le bouton **Arrêt** dans la fenêtre "**Luke Filewalker**" est en gris. L'interruption prématurée d'une recherche n'est pas possible ! Ce réglage est activé par défaut.

Priorité scanner

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

basse

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

moyenne

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

élevée

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

Action si résultat positif

Vous pouvez établir des actions que le Scanner Système doit exécuter quand un virus ou un 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 Système sont signalés dans une fenêtre de dialogue. Lors de la recherche du Scanner Système, vous recevez à l'issue de la recherche de fichiers, un message d'avertissement comportant une liste des fichiers contaminés qui ont été trouvés. Vous avez la possibilité de sélectionner une action à exécuter pour les différents fichiers concernés, via le menu contextuel. Vous pouvez exécuter les actions choisies pour tous les fichiers contaminés ou quitter le Scanner Système.

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

Automatique

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

Copier le fichier dans la quarantaine avant l'action

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

Action primaire

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

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

Réparer

Si l'option est activée, le Scanner Système répare les fichiers concernés automatiquement. Si le Scanner Système ne peut pas réparer un fichier concerné, il exécute comme solution de rechange l'option choisie sous Action secondaire.

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

Renommer

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

Quarantaine

Si l'option est activée, le Scanner Système déplace le fichier en quarantaine. Ces fichiers peuvent être réparés ultérieurement ou - si nécessaire - être envoyés à Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette procédure est beaucoup plus rapide que **Écraser et supprimer** (voir ci-dessous).

Ignorer

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

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

Écraser et supprimer

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

Action secondaire

L'option "**Action secondaire"** n'est sélectionnable que si sous "**Action primaire"** le réglage **Réparer** a été sélectionné. Cette option permet de décider ce qui doit être fait avec le fichier touché s'il n'est pas réparable.

Renommer

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

Quarantaine

Si l'option est activée, le Scanner Système déplace le fichier en quarantaine. Ces fichiers peuvent être réparés ultérieurement ou - si nécessaire - être envoyés à Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette procédure est beaucoup plus rapide que "Écraser et supprimer".

Ignorer

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

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

Écraser et supprimer

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

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

Archives

Lors de la recherche dans les archives, le Scanner Système 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, puis à nouveau contrôlés. (Options disponibles uniquement si le mode expert est activé.)

Contrôler les archives

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

Tous les types d'archives

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

Extensions intelligentes

Si cette option est activée, le Scanner Système 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 Système décompresse également cette archive et la contrôle. Ce réglage est activé par défaut.

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

Limiter la profondeur de récursivité

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

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

Profondeur maxi. de récursivité

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

Valeur par défaut

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

Liste d'archives

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

Exceptions

Objets de fichiers à ignorer par le Scanner Système (Options disponibles uniquement si le mode expert est activé.)

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

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

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

Avertissement
Ces fichiers sont ignorés lors de la recherche !

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

Champ de saisie

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

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

Ajouter

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

Supprimer

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

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

Heuristique

Cette rubrique de configuration contient les réglages 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 et un examen complet du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés sont aussi possibles. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code annoncé est digne de confiance.

Heuristique de macrovirus

Heuristique de macrovirus

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

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

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

Niveau de détection bas

Si cette option est activée, la détection de logiciels malveillants inconnus est moins performante, le risque de messages erronés est faible dans ce cas.

Niveau de détection moyen

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

Niveau de détection élevé

Si l'option est activée, un nombre beaucoup plus élevé de logiciels malveillants inconnus est détecté, mais vous devez vous attendre aussi à des messages erronés.

10.1.2 Rapport

Le Scanner Système dispose d'une fonction de documentation étendue. Vous obtenez ainsi des informations exactes sur les résultats d'une recherche directe. Le fichier de rapport contient toutes les entrées 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 suivre quelles actions le Scanner Système a effectuées lors de la détection de virus ou de programmes indésirables, un fichier de rapport doit toujours être généré.

Documentation

Désactivé

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

Standard

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

Étendu

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

Intégral

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

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

10.2 Protection Temps Réel

La rubrique Protection Temps Réel de la configuration sert à configurer 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 cela, utilisez la Protection Temps Réel (recherche en temps réel = On-Access-Scanner). Avec, vous pouvez faire parcourir tous les fichiers copiés ou ouverts sur l'ordinateur à la recherche de virus et de programmes indésirables, tout en faisant autre chose. (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, indépendamment de leur contenu et de leur extension.

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

Sélection intelligente des fichiers

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

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

Utiliser la liste d'extensions des fichiers

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

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

Extensions de fichiers

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

Remarque
Notez que la liste d'extensions des 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.

Beim Lesen durchsuchen

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.

Scanner 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 procédure que vous pouvez accéder à nouveau au fichier.

Scanner 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 réglage 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. max récursivité

Lors de la recherche dans les archives, la Protection Temps Réel utilise une recherche récursive : les archives dans les archives sont décompressées et l'absence de virus et de programmes indésirables est contrôlée. Vous pouvez définir la profondeur de récursivité. La valeur par défaut est de 1 pour la profondeur de récursivité et est celle recommandée : tous les fichiers situés 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 celle recommandée.

Taille maxi (Ko)

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

Action si résultat positif

Vous pouvez établir des actions que la Protection Temps Réel 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 notification est affichée sur le bureau en cas de résultat positif de la Protection Temps Réel. Vous avez la possibilité de retirer le logiciel malveillant trouvé ou d'appeler d'autres actions possibles pour le traitement du virus via le bouton "**Détails**". Les actions sont affichées dans une fenêtre de dialogue. Cette option est activée par défaut.

Automatique

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

Copier le fichier dans la quarantaine avant l'action

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

Action primaire

L'action primaire est l'action effectuée lorsque la Protection Temps Réel trouve un virus ou un programme indésirable. Si l'option "**Réparer**" est sélectionnée, mais que la réparation du fichier concerné est impossible, l'action sélectionnée sous "**Action secondaire**" est exécutée.

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

Réparer

Si l'option est activée, la Protection Temps Réel répare les fichiers concernés automatiquement. Si la Protection Temps Réel ne peut pas réparer un fichier concerné, elle exécute comme solution de rechange l'option choisie sous **Action secondaire**.

Remarque
Une réparation automatique est recommandée, mais cela signifie que la Protection Temps Réel modifie les fichiers sur l'ordinateur.

Renommer

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

Quarantaine

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

Supprimer

Si l'option est activée, le fichier est supprimé. Cette procédure est beaucoup plus rapide que "Écraser et supprimer".

Ignorer

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

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

Écraser et supprimer

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

Refuser l'accès

Si l'option est activée, la Protection Temps Réel inscrit le résultat positif dans le fichier de rapport uniquement si la fonction de rapport est activée. En outre, la Protection Temps Réel écrit une entrée dans le Protocole d'événement, si cette option est activée.

Avertissement
Si la Protection Temps Réel est réglée sur **Scanner pendant l'écriture**, le fichier concerné n'est pas créé.

Action secondaire

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

Renommer

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

Quarantaine

Si l'option est activée, la Protection Temps Réel déplace le fichier en quarantaine. Les fichiers peuvent être réparés ultérieurement ou - si nécessaire - être envoyés à Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette procédure est beaucoup plus rapide que "Écraser et supprimer".

Ignorer

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

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

Écraser et supprimer

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

Refuser l'accès

Si l'option est activée, le fichier concerné n'est pas créé. La Protection Temps Réel n'inscrit le résultat positif dans le fichier de rapport que si la fonction de rapport est activée. En outre, la Protection Temps Réel écrit une entrée dans le Protocole d'événement, si cette option est activée.

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

Autres actions

Utiliser le protocole d'événement

Si cette option est activée, une entrée est inscrite dans le protocole d'événement Windows à chaque résultat positif. Les événements peuvent être consultés dans l'affichage des événements Windows. Ce réglage est activé par défaut. (Options disponibles uniquement si le mode expert est activé.)

Exceptions

Avec ces options, vous pouvez configurer les objets 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 par exemple sur les bases de données ou solutions de sauvegarde. (Options disponibles uniquement si le mode expert est activé.)

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

Processus à exclure de la Protection Temps Réel

Tous les accès aux fichiers par les processus de cette liste sont exclus 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 128 processus au maximum. Les entrées de la liste ne doivent pas dépasser 6000 caractères au total.

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

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

Le caractère (:) ne doit servir qu'à désigner des lecteurs.

Lorsque vous indiquez un processus, vous pouvez utiliser des caractères de remplacement * (nombre de caractères au choix) et ? (un seul caractère) :

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

Pour éviter que les processus soient exclus globalement de la surveillance de la Protection Temps Réel, les indications contenant uniquement les caractères suivants sont incorrectes : * (astérisque), ? (point d'interrogation), / (barre oblique), \ (barre oblique inverse), . (point), : (deux points).

Vous avez la possibilité d'exclure des processus de la surveillance de la Protection Temps Réel, sans indiquer le chemin complet : `application.exe`

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

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

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

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

Processus

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

Ajouter

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

Supprimer

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

Objets de fichiers à exclure de 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 fichier qui doit être ignoré par la recherche en temps réel. Aucun objet fichier n'est indiqué par défaut.

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

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

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

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

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

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

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

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

```
*.log
```

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

...

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

Ajouter

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

Supprimer

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

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

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 un antislash.
Exemple :
`C:\Programmes\Application\applic*.exe\`
Cette saisie n'est pas valable et n'est pas traitée 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 de rapport de la Protection Temps Réel. Utilisez systématiquement les mêmes chemins dans la liste des exceptions. Procédez comme suit : réglez la fonction de protocole de la Protection Temps Réel sur **Intégral** 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 de rapport de la Protection Temps Réel. Vous accédez au fichier de rapport dans le Control Center sous Protection Temps Réel.

Heuristique

Cette rubrique de configuration contient les réglages 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 et un examen complet du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés sont aussi possibles. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code annoncé est digne de confiance.

Heuristique de macrovirus

Heuristique de macrovirus

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

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

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

Niveau de détection bas

Si cette option est activée, la détection de logiciels malveillants inconnus est moins performante, le risque de messages erronés est faible dans ce cas.

Niveau de détection moyen

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

Niveau de détection élevé

Si l'option est activée, un nombre beaucoup plus élevé de logiciels malveillants inconnus est détecté, mais vous devez vous attendre aussi à des messages erronés.

10.2.2 ProActive

ProActiv

En utilisant Avira ProActiv, vous vous protégez contre de nouvelles menaces et des menaces inconnues pour lesquelles il n'existe encore aucune définition de virus ni d'heuristique. La technologie ProActiv est intégrée au composant Protection Temps Réel. Elle observe et analyse les actions exécutées par les programmes. Le comportement de

programmes est examiné à la recherche de modèles d'action typiques de logiciel malveillant : type d'action et suites d'actions. Si un programme présente un comportement typique d'un logiciel malveillant, il est traité et signalé comme un virus détecté : vous avez la possibilité de bloquer l'exécution du programme ou d'ignorer le message et de poursuivre l'exécution du programme. Vous pouvez classifier le programme comme étant digne de confiance et l'ajouter ainsi au filtre des applications des programmes autorisés. Vous avez également la possibilité d'ajouter le programme au filtre des applications des programmes à bloquer via l'instruction *Toujours bloquer*

Pour déterminer le comportement suspect, le composant ProActiv utilise un ensemble de règles mises au point par le centre de recherche sur les logiciels malveillants Avira Malware Research Center. Les ensembles de règles sont fournies par la banque de données Avira. Pour la saisie d'information dans les banques de données Avira, Avira ProActiv envoie des informations sur les programmes signalés comme suspects. Vous avez la possibilité de désactiver la transmission de données aux banques de données Avira.

Remarque
La technologie ProActiv n'est pas encore disponible sur les systèmes 64 bits !

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

Activer Avira ProActiv

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

Améliorer la sécurité de votre ordinateur en faisant partie de la communauté Avira ProActiv.

Si l'option est activée, Avira ProActiv envoie à l'Avira Malware Research Center les données sur les programmes suspects et, dans certains cas, les fichiers de programmes suspects (fichiers exécutables) pour un contrôle en ligne étendu. Après leur exploitation, les données sont intégrées aux ensembles de règles de l'analyse de comportement ProActiv. Ainsi, vous participez à la communauté Avira ProActiv et contribuez au perfectionnement constant de la technologie de sécurité ProActiv. Si l'option est désactivée, aucune donnée n'est envoyée. Ceci n'a aucune influence sur la fonctionnalité de ProActiv.

Cliquez ici pour obtenir de plus amples informations.

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

Applications à bloquer

Sous *Applications à bloquer*, vous pouvez ajouter les applications que vous classifiez comme nuisibles et qui doivent être bloquées par défaut par Avira ProActiv. Les applications ajoutées ne peuvent pas être exécutées sur votre système d'ordinateur. Vous pouvez également ajouter des programmes comme ayant un comportement suspect au filtre des applications pour les applications à bloquer via les messages de la Protection Temps Réel à l'aide de l'option **Bloquer toujours ce programme**.

Applications à bloquer

Application

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

Champ de saisie

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

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

Ajouter

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

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

Supprimer

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

Applications à exclure

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

Applications à exclure

Application

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

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

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

Champ de saisie

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

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

Ajouter

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

Supprimer

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

10.2.3 Rapport

La Protection Temps Réel dispose d'une fonction étendue de documentation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif. (Options disponibles uniquement si le mode expert est activé.)

Documentation

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

Désactivé

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

Standard

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

Étendu

Si l'option est activée, la Protection Temps Réel consigne également les informations secondaires dans le fichier de rapport.

Intégral

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

Restreindre le fichier de rapport

Limiter la taille à n Mo

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

Sauvegarder le fichier de rapport avant de raccourcir

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

Ecrire la configuration dans le fichier de rapport

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

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

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

Reprogrammer et démarrer la tâche dès qu'une connexion Internet est établie

Si l'option est activée, en plus de l'intervalle de mise à jour défini, la tâche de mise à jour est exécutée à chaque démarrage d'une connexion Internet. (Option disponible uniquement si le mode expert est activé.)

Reprogrammer la tâche si elle n’a pu être exécutée au moment prévu

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 Démarrer la mise à jour produit...

Sous **Démarrer la mise à jour produit...**, vous configurez l’exécution de 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 les mises à jour produit et installer automatiquement

Si cette option est activée, les mises à jour produit sont téléchargées et installées automatiquement par le composant de mise à jour dès qu'elles sont disponibles. Les mises à jour du fichier de définitions des virus et du moteur de recherche sont toujours effectuées, indépendamment de ce réglage. Les conditions pour cette fonction sont : la configuration intégrale de la mise à jour et une connexion existante vers un serveur de téléchargement.

Télécharger les mises à jour produit. Si un redémarrage est nécessaire, installer la mise à jour après celui-ci, sinon l’installer aussitôt.

Si cette option est activée, des mises à jour du produit sont téléchargées dès que des mise à jour de produit sont disponibles. La mise à jour est installée automatiquement après le téléchargement des fichiers de mise à jour, au cas où aucun redémarrage n’est nécessaire. S’il s’agit d’une mise à jour de produit nécessitant un redémarrage de l’ordinateur, la mise à jour du produit n’est pas effectuée aussitôt après le téléchargement des fichiers de mise à jour, mais seulement après le redémarrage suivant du système commandé par l’utilisateur. Ceci présente l’avantage que le redémarrage n’est pas effectué au moment où un utilisateur travaille sur l’ordinateur. Les mises à jour du fichier de définitions des virus et du moteur de recherche sont toujours effectuées, indépendamment de ce réglage. Les conditions pour cette fonction sont : la configuration intégrale de la mise à jour et une connexion existante vers un serveur de téléchargement.

Informer lorsque des nouvelles mises à jour produit sont disponibles

Si cette option est activée, vous n'êtes prévenu que si de nouvelles mises à jour du produit sont disponibles. Les mises à jour du fichier de définitions des virus et du moteur de recherche sont toujours effectuées, indépendamment de ce réglage. Les conditions pour cette fonction sont : la configuration intégrale de la mise à jour et une connexion existante vers un serveur de téléchargement. Vous êtes prévenu par un message affiché sur le bureau sous la forme d'une fenêtre popup et par un message d'avertissement de l'Updater dans le Control Center sous Aperçu > Événements.

Informer de nouveau après n jour(s)

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

Ne pas télécharger les mises à jour produit

Si cette option est activée, l'Updater n'effectue aucune mise à jour automatique du produit ni notification concernant les mises à jour du produit disponibles. Les mises à jour du fichier de définitions des virus et du moteur de recherche sont toujours effectuées, indépendamment de ce réglage.

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 réglages concernant la mise à jour produit (voir Mises à jour).

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

10.3.2 Paramètres redémarrage

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

Remarque
Lors de vos réglages pour le redémarrage, veuillez noter que sous Mise à jour > Démarrer la mise à jour produit..., vous pouvez choisir dans la configuration entre deux options pour l'exécution d'une mise à jour avec redémarrage nécessaire de l'ordinateur :
- **Télécharger les mises à jour produit et installer automatiquement** : la mise à jour et le redémarrage sont exécutés pendant qu'un utilisateur travaille sur l'ordinateur. Si vous avez activé cette option, les routines de redémarrage avec possibilité d'interruption ou avec fonction de rappel peuvent être adaptées.
- **Télécharger les mises à jour produit. Si un redémarrage est nécessaire, installer la mise à jour après celui-ci, sinon l'installer aussitôt** : la mise à jour et le redémarrage sont exécutés après le démarrage de l'ordinateur par un

utilisateur et après sa connexion. Pour cette option, les routines de redémarrage automatiques sont conseillées.

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

Rappel périodique de redémarrage

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

Demande si le redémarrage de l'ordinateur doit être effectué

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

Redémarrage de l'ordinateur sans demande

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

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

Utiliser la connexion suivante :

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

L'Updater détecte automatiquement quelles options de connexion sont disponibles. Les options de connexion indisponibles sont sur fond gris et ne peuvent pas être

activées. Vous pouvez établir une connexion de télétransmission par ex. manuellement via une entrée de répertoire téléphonique dans Windows.

Utilisateur

Saisissez l'identifiant du compte sélectionné.

Mot de passe

Saisissez le mot de passe pour ce compte. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Remarque
Adressez-vous au fournisseur d'accès Internet si vous avez oublié l'identifiant ou le mot de passe d'un compte Internet existant.

Remarque
La numérotation automatique automatique de l'Updater via les outils Dial-Up (par ex. SmartSurfer, Oleco, ...) n'est pas encore disponible.

Arrêter une connexion de télétransmission ouverte pour la mise à jour

Si cette option est activée, la connexion de télétransmission ouverte pour la mise à jour est interrompue automatiquement dès que le téléchargement a été effectué avec succès.

Remarque
L'option n’est disponible ni sous Vista ni sous Windows 7. La connexion de télétransmission ouverte pour la mise à jour est systématiquement interrompue sous Vista et Windows 7 dès que le téléchargement a été effectué.

Réglages proxy

Serveur proxy

Ne pas utiliser de serveur proxy

Si cette option est activée, votre connexion au serveur web n'a pas lieu via un serveur proxy.

Utiliser les réglages système de Windows

Si cette option est activée, les paramètres système actuels de Windows pour la connexion au serveur web via un serveur proxy sont utilisés. Les paramètres systèmes de Windows pour l'utilisation d'un serveur proxy se configurent sous **Performances et maintenance > Options Internet > Connexions > Paramètres de réseau local**. Dans Internet Explorer, vous pouvez également accéder aux options Internet dans le menu **Outils**.

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

Connexion via ce serveur proxy

Si l'option est activée, votre connexion au serveur web a lieu via un serveur proxy, mais les réglages que vous avez indiqués sont utilisés.

Adresse

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

Port

Saisissez le numéro de port du serveur proxy que vous souhaitez utiliser pour la connexion avec le serveur web.

Identifiant de connexion

Saisissez un identifiant pour la connexion au serveur proxy.

Mot de passe de connexion

Saisissez le mot de passe correspondant pour la connexion au serveur proxy. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Exemples :

Adresse : `proxy.domain.de` Port : `8080`

Adresse : `192.168.1.100` Port : `3128`

10.4 Protection Web

La rubrique **Protection Web** sous **Configuration > Sécurité Internet** permet de configurer 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 **Rechercher**. (Options disponibles uniquement si le mode expert est activé.)

Recherche

Prise en charge IPv6

Si l'option est activée, la version 6 du protocole Internet est prise en charge par la Protection Web.

Protection contre les téléchargements automatiques intempestifs

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

Bloquer les I-Frames suspects

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

Action si résultat positif

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

Interactif

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

Afficher la barre de progression

Si l'option est activée, un message affiché sur le bureau apparaît avec une barre de progression de téléchargement, lorsque le téléchargement de contenus de sites Internet dépasse un délai d'attente de 20 secondes. Ce message affiché sur le bureau sert notamment à contrôler le téléchargement de sites Internet avec de gros volumes de données : lors de la navigation avec 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, aucun 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 de vos réglages effectués dans cette section.

Action primaire

L'action primaire est l'action effectuée 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. Dans le navigateur Web, un message d'erreur de refus d'accès s'affiche. La Protection Web inscrit le résultat positif dans le fichier de rapport, à condition que la fonction de rapport soit activée.

Quarantaine

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

Ignorer

La page Web demandée par le serveur Web ou les données et fichiers transmis sont envoyés à votre navigateur Web par la Protection Web. L'accès au fichier est autorisé et le fichier est conservé.

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

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. Le filtre Web vous permet de bloquer des URL indésirables connues, comme par ex. des URL à hameçonnage et de logiciel malveillant. La Protection Web empêche la transmission des données d'Internet vers votre ordinateur. (Options disponibles uniquement si le mode expert est activé.)

Types de fichiers/Types MIME à bloquer 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 si des entrées figurent 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 au choix de caractères ou ? pour un caractère exactement).

Types MIME : exemples de types de médias

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

Exemples : types de fichiers et types MIME à exclure

- `application/octet-stream` = les fichiers du type MIME application/octet-stream (fichiers exécutables *.bin, *.exe, *.com, *dll, *.class) sont bloqués par 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

Avec ce bouton, vous pouvez valider le type MIME ou de fichier entré dans le champ de saisie dans la fenêtre d'affichage.

Supprimer

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

Filtre Web

Le filtre Web dispose d'une base de données interne mise à jour quotidiennement, dans laquelle les URL sont classées par critères de contenus.

Activer le filtre Web

Si l'option est activée , toutes les URL figurant parmi les catégories sélectionnées dans la liste du filtre Web sont bloquées.

Liste du filtre Web

La liste du filtre Web vous permet de choisir les catégories de contenus dont les URL doivent être bloquées par la Protection Web.

Remarque
Le filtre Web est ignoré si des entrées figurent dans la liste des URL à ignorer sous Exceptions.

Remarque
Sous **URLs de spam** figurent les URL, triées par catégories, diffusées par des spams. La catégorie **Escroqueries / Fraudes** englobe les sites Internet comportant des 'pièges d'abonnement' et autres offres de services dont les coûts sont dissimulés par le fournisseur.

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 URL indiqués sont ignorés par la Protection Web, ce qui signifie que les virus et logiciels malveillants ne sont pas recherchés dans ces données 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 (personnalisés)

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

Champ de saisie

Dans ce champ, vous pouvez sélectionner les types MIME et 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 au choix de caractères ou ? pour un caractère exactement).

Avertissement
Tous les types de fichiers et types de contenus figurant dans la liste d'exceptions sont chargés dans le navigateur Internet sans autre contrôle des accès bloqués (liste des types de fichiers et types MIME à bloquer sous Accès bloqués) ou de la Protection Web : toutes les entrées de la liste d'exceptions concernant les types de fichiers et les types MIME à bloquer sont ignorées. Aucune recherche n'est effectuée quant à l'absence de virus et de logiciels malveillants.

Types MIME : exemples de types de médias

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

Exemples : types de fichiers et types MIME à exclure

- `audio/` = tous les fichiers de type de média audio sont exclus de la recherche de la Protection Web
- `video/quicktime` = tous les fichiers vidéo du sous-type Quicktime (*.qt, *.mov) sont exclus de la recherche de la Protection Web

- `.pdf` = tous les fichiers PDF Adobe sont exclus de la recherche de la Protection Web.

Ajouter

Avec ce bouton, vous pouvez valider le type MIME ou de fichier entré dans le champ de saisie dans la fenêtre d'affichage.

Supprimer

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

URLs à exclure par la Protection Web

Toutes les URL de cette liste sont exclues de la recherche de la Protection Web.

Champ de saisie

Saisissez dans ce champ les URL (adresses Internet) à exclure de la recherche de la Protection Web, par ex. **www.domainname.com**. Vous pouvez indiquer des parties de l'URL en marquant le niveau de domaine avec des points finaux ou de début : .nom de domaine.fr pour tous les sites et tous les sous-domaines du domaine. Notez un site Web avec un domaine de premier niveau quelconque (.com ou .net) avec un point final : **domainname.**. Si vous notez une suite de caractères sans point final ou point de début, celle-ci sera interprétée comme un domaine de niveau supérieur, par ex. **net** pour tous les domaines NET (www.domain.net).

Remarque
Lors de l'indication des URL, vous pouvez également utiliser le caractère de remplacement * pour un nombre au choix de caractères. Utilisez aussi des points finaux ou de début en combinaison avec les caractères de remplacement, pour repérer les niveaux de domaine :
`.domainname.*`
`*.domainname.com`
`.*name*.com` (valable mais n'est pas conseillé)
Les indications sans points comme `*name*` sont interprétées comme des parties d'un domaine de premier niveau et ne sont pas pertinentes.

Avertissement
Tous les sites Web figurant dans la liste des URL à ignorer sont chargés dans le navigateur Internet sans autre contrôle du filtre Web ou de la Protection Web :toutes les entrées de la liste des URL à ignorer concernant le filtre Web (voir Accès bloqués) sont ignorées. Aucune recherche n'est effectuée quant à l'absence de virus et de logiciels malveillants. Par conséquent, n'excluez de la recherche de la Protection Web que les URL dignes de confiance.

Ajouter

Avec ce bouton, vous pouvez valider l'URL (adresse Internet) entrée dans le champ de saisie de la fenêtre d'affichage.

Supprimer

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

Exemples : URLs à exclure

- `www.avira.com` -OU- `www.avira.com/*`
  = Toutes les URL avec le domaine 'www.avira.com' sont exclues de la recherche de 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 de la Protection Web.
- `avira.com` -OU- `*.avira.com`
  = Toutes les URL avec les domaines de premier et second niveaux 'avira.com' sont exclues de la recherche de 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 de la Protection Web. L'indication implique tous les domaines de niveau supérieur ou sous-domaines existants pour '.avira.' : www.avira.com, www.avira.de, forum.avira.com,...
- `.*domain*.*`
  = Toutes les URL contenant un domaine de second niveau avec la chaîne de caractères 'domaine' sont exclues de la recherche de la Protection Web : www.domaine.com, www.new-domaine.fr, www.sample-domaine1.fr, ...
- `net` -OU- `*.net`
  = Toutes les URL avec le domaine de premier niveau 'net' sont exclues de la recherche de la Protection Web : www.name1.net, www.name2.net, …

Avertissement
Indiquez aussi précisément que possible les URL que vous souhaitez exclure de la recherche de la Protection Web. Évitez d'indiquer des ensembles de domaines de premier niveau 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 de la Protection Web par des indications globales définies sous la rubrique Exceptions. Il est recommandé d'indiquer au moins le domaine de second niveau dans son entier et le domaine de niveau supérieur : domainname.com

Heuristique

Cette rubrique de configuration contient les réglages 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 et un examen complet du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés sont aussi possibles. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code annoncé est digne de confiance.

Heuristique de macrovirus

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

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

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

Niveau de détection bas

Si cette option est activée, la détection de logiciels malveillants inconnus est moins performante, le risque de messages erronés est faible dans ce cas.

Niveau de détection moyen

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

Niveau de détection élevé

Si l'option est activée, un nombre beaucoup plus élevé de logiciels malveillants inconnus est détecté, mais vous devez vous attendre aussi à des messages erronés.

10.4.2 Rapport

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

Documentation

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

Désactivé

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

Standard

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

Étendu

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

Intégral

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

Restreindre le fichier de rapport

Limiter la taille à n Mo

Si cette option est activée, le fichier rapport peut être limité à une taille définie ; valeurs possibles : 1 à 100 Mo. En cas de limitation du fichier de rapport, une tolérance de 50 kilo-octets environ est accordée pour maintenir la charge de l'ordinateur à un faible niveau. Si la taille du fichier de rapport dépasse la taille indiquée de 50 kilo-octets, les anciennes entrées sont supprimées automatiquement jusqu'à ce que la taille indiquée moins 20 % soit atteinte.

Ecrire la configuration dans le fichier de rapport

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

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

10.5 Protection E-mail

La rubrique Protection E-mail de la configuration est en charge de la configuration de la Protection E-mail.

10.5.1 Recherche

Vous utilisez la Protection E-mail pour contrôler les emails entrants quant à l'absence de virus, de logiciels malveillants . Il est possible de faire contrôler les emails sortants par la Protection E-mail quand à l'absence de virus de logiciels malveillants.

Activer la Protection E-mail

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

Contrôler les emails entrants

Si l'option est activée, les emails sortants sont contrôlés quant à l'absence de virus, de logiciels malveillants . La Protection E-mail prend en charge les protocoles POP3 et IMAP. Activez le compte de la boîte de réception utilisée par votre client email pour la réception des emails, afin de le faire surveiller par la Protection E-mail.

Surveiller les comptes POP3

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

Ports surveillés

Saisissez dans ce champ le port utilisé comme boîte de réception par le protocole POP3. Vous pouvez indiquer plusieurs ports en les séparant par des virgules. (Option disponible uniquement si le mode expert est activé.)

Standard

Ce bouton permet de réinitialiser les ports indiqués au port par défaut de POP3. (Option disponible uniquement si le mode expert est activé.)

Surveiller les comptes IMAP

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

Ports surveillés

Saisissez dans ce champ le port utilisé par le protocole IMAP. Vous pouvez indiquer plusieurs ports en les séparant par des virgules. (Option disponible uniquement si le mode expert est activé.)

Standard

Ce bouton permet de réinitialiser les ports indiqués au port par défaut d'IMAP. (Option disponible uniquement si le mode expert est activé.)

Contrôler les emails sortants (SMTP)

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

Ports surveillés

Saisissez dans ce champ le port utilisé comme boîte d'envoi par le protocole SMTP. Vous pouvez indiquer plusieurs ports en les séparant par des virgules. (Option disponible uniquement si le mode expert est activé.)

Standard

Ce bouton permet de réinitialiser les ports indiqués au port par défaut de SMTP. (Option disponible uniquement si le mode expert est activé.)

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

Prise en charge IPv6

Si l'option est activée, la version 6 du protocole Internet est prise en charge par la Protection E-mail.

Action si résultat positif

Cette rubrique de configuration contient des réglages concernant les actions effectuées lorsque la Protection E-mail trouve un virus ou un programme indésirable dans un email ou une pièce jointe. (Options uniquement disponibles si le mode expert est activé.)

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

Interactif

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

Afficher la barre de progression

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

Automatique

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

Emails concernés

L'option sélectionnée sous "*Emails concernés*" est exécutée comme action primaire lorsque la Protection E-mail trouve un virus ou un programme indésirable dans un email. Si l'option "**Ignorer**" est sélectionnée, il est en outre possible de choisir sous "*Pièces jointes concernées***"** ce qui doit se passer quand un résultat positif est détecté dans une pièce jointe.

Supprimer

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

Ignorer

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

Déplacer en quarantaine

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

Pièces jointes concernées

L'option "**Pièces jointes concernées**" n'est sélectionnable que si sous "*Emails concernés***"** le réglage "**Ignorer**" a été sélectionné. Cette option permet de décider ce qui doit être fait en cas de pièce jointe concernée.

Supprimer

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

Ignorer

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

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

Déplacer en quarantaine

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

Autres actions

Cette rubrique de configuration contient d'autres réglages concernant les actions effectuées lorsque la Protection E-mail trouve un virus ou un programme indésirable dans un email ou une pièce jointe. (Options uniquement disponibles si le mode expert est activé.)

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

Texte standard pour les emails supprimés et déplacés

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

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

Ctrl + Enter = ajoute un saut de ligne.

Standard

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

Texte standard pour les pièces jointes supprimées et déplacées

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

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

Ctrl + Enter = ajoute un saut de ligne.

Standard

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

Heuristique

Cette rubrique de configuration contient les réglages 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 et un examen complet du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés sont aussi possibles. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code annoncé est digne de confiance.

Heuristique macrovirus

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

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

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

Niveau de détection bas

Si cette option est activée, la détection de logiciels malveillants inconnus est moins performante, le risque de messages erronés est faible dans ce cas.

Niveau de détection moyen

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

Niveau de détection élevé

Si l'option est activée, un nombre beaucoup plus élevé de logiciels malveillants inconnus est détecté, mais vous devez vous attendre aussi à des messages erronés.

10.5.2 Généralités

Exceptions

Adresses emails qui ne sont pas contrôlées

Ce tableau vous donne la liste des adresses emails qui ont été exclues de la surveillance par la Protection E-mail Avira (liste blanche).

> **Remarque**
> La liste des exceptions est utilisée par la Protection E-mail exclusivement pour les emails entrants.

Champ de saisie

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

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

Ajouter

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

Supprimer

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

Adresse email

Adresse email qui ne doit plus être contrôlée.

Logiciels malveillants

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

vers le haut

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

vers le bas

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

Mémoire tampon

La mémoire tampon de la Protection E-mail contient les données sur les emails contrôlés qui sont affichés dans les statistiques du Control Center sous **Protection E-mail**. (Options disponibles uniquement si le mode expert est activé.)

Nombre maximal d'emails dans la mémoire tampon

Dans ce champ, saisissez le nombre maximum d'emails conservés dans la mémoire tampon de la Protection E-mail. Les emails les plus anciens sont supprimés en premier.

Enregistrement maximal d'un email en jours

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

Vider la mémoire tampon

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

10.5.3 Rapport

La Protection E-mail dispose d'une fonction étendue de documentation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif.

Documentation

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

Désactivé

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

Standard

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

Étendu

Si l'option est activée, la Protection E-mail consigne également les informations secondaires dans le fichier de rapport.

Intégral

Si l'option est activée, la Protection E-mail consigne également toutes les informations secondaires dans le fichier de rapport.

Restreindre le fichier de rapport

Limiter la taille à n Mo

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

Sauvegarder le fichier de rapport avant de raccourcir

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

Ecrire la configuration dans le fichier de rapport

Si cette option est activée, la configuration utilisée de la Protection E-mail est écrite dans le fichier de rapport.

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

10.6 Généralités

10.6.1 Catégories de dangers

Sélection des 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 de rechercher les catégories de dangers suivantes.

- Logiciels publicitaires
- Logiciel publicitaire/logiciel espion

- Applications
- Logiciel de commande Backdoor
- Fichiers à extensions déguisées
- Programme de numérotation payant
- Hameçonnage
- Programmes portant atteinte à la vie privée
- Programmes de blagues
- Jeux
- Logiciel frauduleux
- Programmes de décompression inhabituels

En cliquant sur la case, le type choisi est activé (coche) ou désactivé (pas de coche).

Activer tout

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

Valeur par défaut

Ce bouton restaure les valeurs prédéfinies par défaut.

> **Remarque**
> Si un type est désactivé, les fichiers identifiés comme type de programme correspondant, ne sont plus annoncés. Aucune entrée n'est effectuée dans le fichier rapport.

10.6.2 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 devrez saisir ce mot de passe à chaque fois que vous voulez ouvrir la zone protégée.

Mot de passe

Saisir le mot de passe

Saisissez ici votre mot de passe. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*). Vous pouvez saisir 20 caractères au maximum. Si le mot de passe est indiqué une fois, le programme refuse l'accès en cas de saisie d'un mot de passe erroné. Un champ vide signifie "Pas de mot de passe".

Confirmation

Saisissez ici le mot de passe saisi ci-dessus pour le confirmer. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Remarque
La différence est faite entre les majuscules et minuscules !

Mot de passe zones protégées (Option disponible 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 souhait.

Zone protégée par mot de passe	Fonction
Control Center	Si l'option est activée, le mot de passe défini est nécessaire pour le démarrage du Control Center.
Activer/Désactiver la Protection Temps Réel	Si l'option est activée, le mot de passe défini est nécessaire pour l'activation et la désactivation d'Avira Protection Temps Réel.
Activer/Désactiver la Protection E-mail	Si l'option est activée, le mot de passe défini est nécessaire pour l'activation et la désactivation de la Protection E-mail.
Activer/Désactiver la Protection Web	Si l'option est activée, le mot de passe défini est nécessaire pour l'activation et la désactivation de la Protection Web.
Quarantaine	Si l'option est activée, toutes les zones possibles du gestionnaire de quarantaine protégées par mot de passe sont activées. En cliquant sur la case correspondante, la demande de mot de passe peut être désactivée et activée à souhait.
Restauration des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour restaurer un objet.

Nouveau contrôle des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour recontrôler un objet.
Caractéristiques des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour l'affichage des caractéristiques d'un objet.
Suppression des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour supprimer un objet.
Envoyer un email à Avira	Si l'option est activée, le mot de passe défini est nécessaire pour l'envoi d'un objet pour contrôle à Avira Malware Research Center.
Ajouter et modifier des tâches	Si l'option est activée, le mot de passe défini est nécessaire pour ajouter et modifier des tâches dans le planificateur.
Démarrer les mises à jour produit	Si l'option est activée, le mot de passe défini est nécessaire dans le menu Mise à jour pour démarrer la mise à jour produit.
Configuration	Si l'option est activée, la configuration du programme n'est possible qu'après la saisie du mot de passe défini.
Installation/Désinstallation	Si l'option est activée, le mot de passe défini est nécessaire pour l'installation et la désinstallation du programme.

10.6.3 Sécurité

Options disponibles uniquement si le mode expert est activé.

Autodémarrage

Bloquer la fonction d'autodémarrage

Si l'option est activée, l'exécution de la fonction d'autodémarrage Windows est bloquée sur tous les lecteurs intégrés comme les clés USB, les lecteurs CD et DVD, les lecteurs réseau. Avec la fonction d'autodémarrage Windows, les fichiers sur des supports de données ou sur des lecteurs réseau sont immédiatement lus lors de l'insertion ou de la connexion. Ainsi, les fichiers peuvent être démarrés et reproduits automatiquement. Toutefois, cette fonctionnalité présente un risque de sécurité élevé

car elle permet le démarrage automatique de fichiers de logiciels malveillants et de programmes indésirables. La fonction d'autodémarrage est particulièrement critique pour les clés USB car les données sur une clé USB peuvent constamment changer.

Exclure des CD et DVD

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

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

Protection système

Protéger les fichiers hôtes Windows des modifications

Si cette option est activée, les fichiers hôtes Windows sont protégés en écriture. Il n'est plus possible de manipuler les fichiers. 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 via une installation personnalisée.

Protéger les processus d'un arrêt non souhaité

Si l'option est activée, tous les processus du programme sont protégés d'un arrêt non souhaité par des virus et des logiciels malveillants ou d'un arrêt 'incontrôlé' par un utilisateur, par ex. via le gestionnaire des tâches. Cette option est activée par défaut.

Protection étendue des processus

Si l'option est activée, tous les processus du programme sont protégés avec des méthodes étendues contre un arrêt non voulu. Cette protection de processus étendue nécessite beaucoup plus de ressources de l'ordinateur que la protection de processus simple. L'option est activée par défaut. Pour désactiver l'option, il est nécessaire de redémarrer l'ordinateur.

Remarque
La protection de processus n'est disponible ni sous Windows XP 64 bits !

Avertissement
Si la protection des processus est activée, des problèmes d'interaction peuvent survenir avec d'autres logiciels. Désactivez la protection des processus dans ces cas.

Protéger les fichiers et entrées de registre de toute manipulation

Si l'option est activée, toutes les entrées de registre du programme, ainsi que tous les fichiers du programme (fichiers binaires et de configuration) sont protégés contre toute manipulation. La protection contre la manipulation comprend la protection contre l'accès en écriture, en suppression et partiellement en lecture aux entrées de registre ou aux fichiers du programme, par l'utilisateur ou des programmes-tiers. Pour activer l'option, il est nécessaire de redémarrer l'ordinateur.

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

Remarque
Si l'option est activée, les modifications de la configuration ne sont possibles que via l'interface utilisateur, de même que la modification des tâches de contrôle ou de mise à jour.

Remarque
La protection des fichiers et des entrées de registre n'est disponible ni sous Windows XP 64 bits !

10.6.4 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 est compatible WMI et met à disposition les données (informations d'état, données statistiques, rapports, tâches planifiées, etc.), ainsi que les événements sur une interface. WMI vous donne la possibilité d'interroger les données d'exploitation du programme.

Activer la prise en charge WMI

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

10.6.5 Événements

Options disponibles uniquement si le mode expert est activé.

Limiter la taille de la base de données des événements

Limiter la taille au maximum à n entrées

Si l'option est activée, le nombre maximum d'entrées dans la base de données d'événements peut être limité à une taille définie ; les valeurs autorisées sont : 100 à 10 000 entrées. Si le nombre d'entrées saisies est dépassée, les saisies les plus anciennes sont supprimées.

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

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

Pas de limites

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

10.6.6 Rapports

Options disponibles uniquement si le mode expert est activé.

Limiter les rapports

Limiter le nombre maximum à n pièces

Si l'option est activée, le nombre maximum de rapports peut être limité ; les valeurs autorisées sont : 1 à 300. Si le nombre indiqué est dépassé, les rapports les plus anciens sont supprimés.

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

Si l'option est activée, les rapports sont supprimés automatiquement après un certain nombre de jours ; valeurs autorisées : 1 à 90 jours. Cette option est activée par défaut avec une valeur de 30 jours.

Pas de limites

Si cette option est activée, le nombre de rapports n'est pas limité.

10.6.7 Répertoires

Options disponibles uniquement si le mode expert est activé.

Chemin temporaire

Utiliser le réglage système

Si cette option est activée, les réglages du système sont utilisés pour la manipulation des fichiers temporaires.

Remarque
Pour savoir où votre système enregistre les fichiers temporaires sur Windows XP - allez à : **Démarrer > Panneau de configuration > Performances et maintenance > Système >** onglet "**Avancé**" > bouton "**Variables d'environnement**". Les variables temporaires (`TEMP`, `TMP`) pour l'utilisateur connecté et pour les variables du système (`TEMP`, `TMP`) sont visibles ici avec leurs valeurs respectives.

Utiliser le répertoire suivant

En cas d'option activée, c'est le chemin indiqué dans le champ de saisie qui est utilisé.

Champ de saisie

Saisissez dans ce champ de saisie le chemin où les fichiers temporaires doivent être mémorisés par le programme.

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

Standard

Ce bouton restaure le répertoire prédéfini pour le chemin temporaire.

10.6.8 Avertissement acoustique

Options disponibles uniquement si le mode expert est activé.

En cas de détection d'un virus ou d'un logiciel malveillant par le Scanner Système ou la Protection Temps Réel, un bip d'avertissement retentit dans le mode d'action interactif. Vous avez la possibilité de désactiver ou d'activer le bip d'avertissement ainsi que de sélectionner un fichier WAV différent comme bip d'avertissement.

Remarque
Le mode d'action du Scanner Système se règle dans la configuration sous **Scanner Système > Rechercher > Action si résultat positif**. Le mode

d'action de la Protection Temps Réel se règle dans la configuration sous **Protection Temps Réel > Rechercher > Action si résultat positif**.

Pas d'avertissement

Si l'option est activée, aucun avertissement acoustique ne se produit lors de la détection d'un virus par le Scanner Système ou la Protection Temps Réel.

Prévenir via les enceintes du PC (uniquement en mode interactif)

Si l'option est activée, un avertissement acoustique se produit à l'aide d'un bip d'avertissement par défaut lors de la détection d'un virus par le Scanner Système ou la Protection Temps Réel. Le bip d'avertissement est diffusé par le haut-parleur interne du PC.

Utiliser le fichier WAV suivant (uniquement en mode interactif)

Si l'option est activée, un avertissement acoustique se produit à l'aide du fichier WAV sélectionné en cas de détection d'un virus par le Scanner Système ou la Protection Temps Réel. Le fichier WAV sélectionné est diffusé par le haut-parleur externe raccordé.

Fichier WAVE

Dans ce champ de saisie, vous pouvez saisir le nom et le chemin correspondant d'un fichier audio de votre choix. Le bip d'avertissement par défaut du programme est inscrit par défaut.

...

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

Tester

Ce bouton sert à tester le fichier WAVE sélectionné.

10.6.9 Avertissements

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

En cas de notifications affichées sur le bureau, vous avez la possibilité de désactiver directement la notification dans le Slide-Up. Vous pouvez annuler la désactivation de la notification 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 qui doit s'écouler au maximum depuis la dernière mise à jour. Si cet âge est dépassé, une icône rouge s'affiche dans Control Center sous Etat pour l'état de mise à jour.

Afficher la remarque, si le fichier de définitions des virus est obsolète

Si l'option est activée, vous recevez un message d'avertissement en cas de fichier de définitions des virus obsolète. A l'aide de l'option "Avertissement, si la dernière mise à jour a plus de n jour(s)", vous pouvez configurer l'intervalle avant l'avertissement.

Avertissements/Remarques dans les situations suivantes

Une connexion par modem est utilisée

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

Les fichiers ont été actualisés avec succès

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

Échec de la mise à jour

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

Aucune mise à jour n'est nécessaire

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

Edition du 4er trimestre 2011.

AVIRA

live *free.*™

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

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