McAfee®

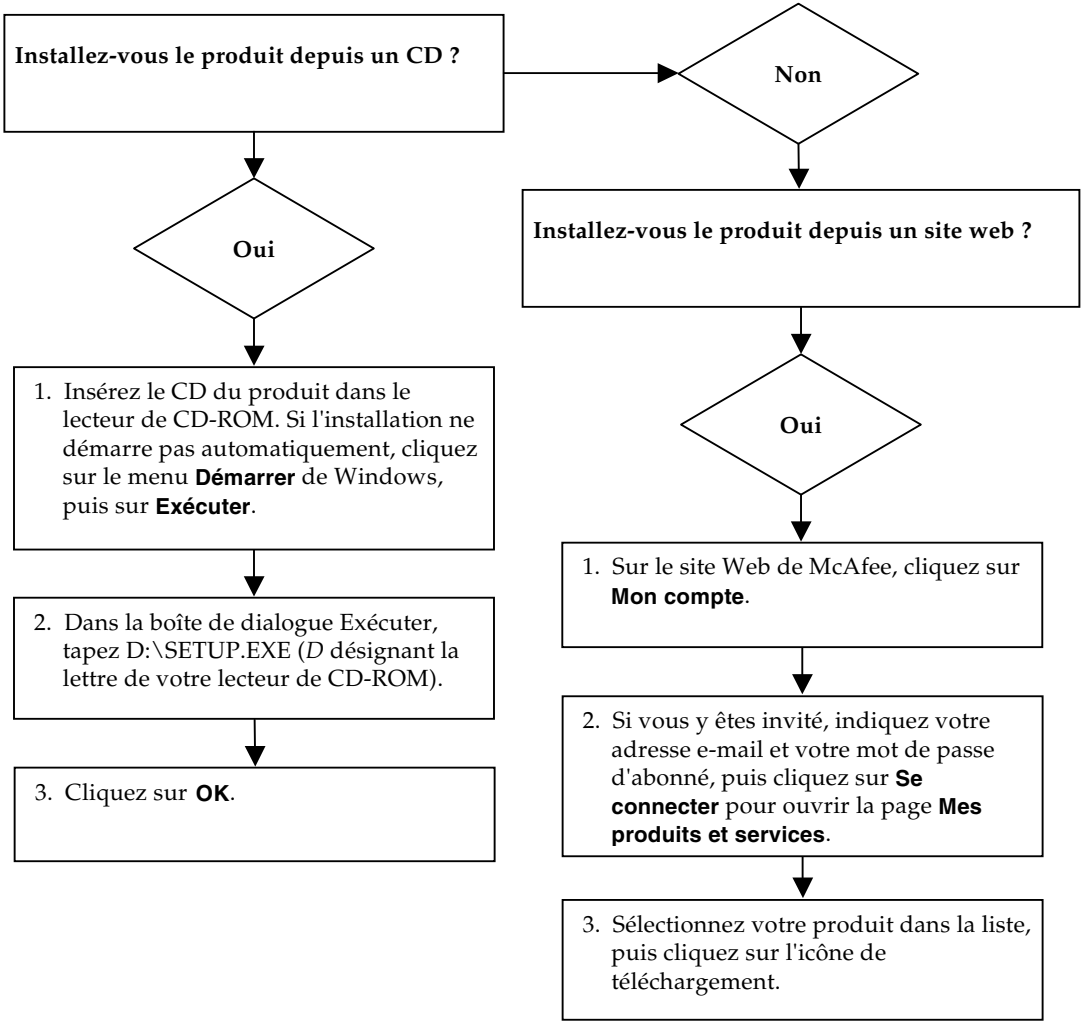
internet security suite

Guide de l’utilisateur

McAfee®

Carte de configuration rapide

Si vous installez le produit à partir d'un CD ou du site Web, imprimez cette page comme référence.



Pour plus d'informations

Pour pouvoir consulter les Guides d'utilisateurs qui se trouvent sur le CD du produit, assurez-vous qu'Acrobat Reader est installé sur votre ordinateur ; sinon, installez-le depuis le CD du produit McAfee.

1. Insérez le CD du produit dans le lecteur CD-ROM.
2. Ouvrez l'Explorateur Windows : cliquez sur le menu **Démarrer** de Windows, puis sur **Rechercher**.
3. Localisez le dossier Manuals et double-cliquez sur le fichier PDF du guide de l'utilisateur à ouvrir.

Avantages de l'enregistrement

Nous vous conseillons de suivre les instructions fournies dans votre produit pour nous transmettre directement l'enregistrement. Grâce à cet enregistrement, vous bénéficierez d'un support technique compétent et opportun, ainsi que des avantages suivants :

- Un support électronique GRATUIT.
- Des mises à jour des fichiers de définition de virus (.DAT) pendant un an à compter de la date d'installation du logiciel VirusScan si vous achetez ce logiciel.

  Consultez le site http://fr.mcafee.com pour obtenir la tarification d'une année supplémentaire de signatures de virus.
- Une garantie de 60 jours couvrant le remplacement du CD-ROM de votre logiciel si celui-ci est défectueux ou endommagé.
- Des mises à jour des filtres SpamKiller pendant un an à compter de la date d'installation si vous achetez ce logiciel.

  Consultez le site http://fr.mcafee.com pour obtenir la tarification d'une année supplémentaire de mises à jour de filtres.
- Des mises à jour de McAfee Internet Security Suite pendant un an à compter de la date d'installation du logiciel MIS si vous achetez ce logiciel.

  Consultez le site http://fr.mcafee.com pour obtenir la tarification d'une année supplémentaire de mises à jour du contenu.

Assistance technique

Pour toute question relative au support technique, consultez notre site http://www.mcafeeaide.com/. Notre site de support offre 24 h/24 un accès à un Assistant convivial permettant d'obtenir des solutions aux questions de support les plus courantes.

Les utilisateurs confirmés peuvent également essayer nos options avancées, parmi lesquelles une fonction de recherche par mot clé et notre arborescence d'aide. Si vous ne parvenez pas à résoudre votre problème, vous pouvez aussi accéder aux options gratuites de conversation et de courrier électronique. Ces options vous permettent de communiquer rapidement et gratuitement avec nos ingénieurs du support technique, via Internet. Vous trouverez également des informations relatives à notre service d'assistance téléphonique sur notre site http://www.mcafeeaide.com/.

Table des matières

Introduction 1

Internet est une mine d'informations et de divertissements à portée de main. Pourtant, dès que vous vous connectez, vous exposez votre ordinateur à une multitude de menaces au niveau de la confidentialité et de la sécurité. Protégez votre confidentialité et sécurisez votre ordinateur et vos données avec McAfee Internet Security Suite. Intégrant les technologies primées de McAfee, Internet Security Suite fournit l'un des ensembles d'outils de confidentialité et de sécurité les plus complets du marché. McAfee Internet Security Suite détruit les virus, dépiste les pirates informatiques, sécurise vos données personnelles, garantit la confidentialité de votre navigation sur le Web, bloque les publicités et fenêtres instantanées, gère vos cookies et mots de passe, verrouille vos fichiers, dossiers et disques, filtre les contenus inappropriés et vous donne le contrôle des communications entrantes et sortantes de votre PC. McAfee Internet Security Suite offre une protection efficace aux internautes d'aujourd'hui.

Pour plus d'informations sur l'ensemble des produits McAfee, consultez les chapitres suivants :

- *McAfee VirusScan* à la page 15
- *McAfee Personal Firewall Plus* à la page 47
- *McAfee Privacy Service* à la page 77
- *McAfee SpamKiller* à la page 97

Logiciel McAfee Internet Security

- **McAfee SecurityCenter** : évalue la vulnérabilité de votre PC et vous communique les résultats. Chaque indice de sécurité évalue rapidement les menaces liées à Internet et les risques auxquels vous êtes exposé, puis vous conseille sur la protection rapide et efficace de votre PC.
- **McAfee VirusScan** : traite les problèmes Internet liés aux virus. Vous pouvez décider du mode d'analyse antivirus, de la procédure à suivre en cas de détection d'un virus et du type d'alerte à recevoir. Vous pouvez également demander à VirusScan de tenir un enregistrement des actions entreprises sur votre ordinateur.
- **McAfee Personal Firewall Plus** : protège votre ordinateur lorsqu'il est connecté à Internet. Que vous soyez connecté à Internet par DSL, modem câble ou numérotation standard, la communication Internet entrante ou sortante de votre PC est sécurisée.
- **McAfee Privacy Service** : associe la protection des informations d'identification au blocage des publicités et au filtrage du contenu en ligne. Ce service sécurise vos informations personnelles tout en offrant un plus grand contrôle de l'utilisation Internet de votre famille. McAfee Privacy Service vous garantit de ne pas exposer vos informations confidentielles aux menaces en ligne et de protéger votre famille et vous des contenus en ligne inappropriés.
- **McAfee SpamKiller** : de nombreux e-mails illégaux, inappropriés et choquants étant quotidiennement envoyés aux adultes, enfants et entreprises, il est essentiel d'inclure la protection antispam dans votre stratégie de sécurité PC.

Configuration système requise

- Microsoft® Windows Me, 2000 ou XP
- Ordinateur personnel avec processeur
  Windows Me : Pentium 150 MHz ou supérieur
  Windows 2000 ou XP : Pentium 233 MHz ou supérieur
- Mémoire vive
  Windows Me, 2000 ou XP : 64 Mo (128 Mo recommandés)
- 70 Mo d'espace disque
- Microsoft® Internet Explorer 5.5 ou ultérieur

  REMARQUE
  Pour mettre à niveau Internet Explorer vers la version la plus récente, consultez le site Web de Microsoft à l'adresse http://www.microsoft.com/worldwide/.

Utilisation de McAfee SecurityCenter

McAfee SecurityCenter est votre centre de sécurité unifié, accessible à partir de son icône de la barre d'état système ou depuis votre bureau Windows. Il permet d'exécuter les tâches utiles suivantes :

- Obtenir une analyse gratuite de la sécurité de votre ordinateur.
- Lancer, gérer et configurer tous vos abonnements McAfee à partir d'une seule icône.
- Consulter des alertes de virus et des informations produit continuellement mises à jour.
- Obtenir des liens rapides vers le forum de questions et les détails de votre compte sur le site Web de McAfee.

> **REMARQUE**
> Pour plus d'informations sur les fonctionnalités de SecurityCenter, cliquez sur **Aide** dans la boîte de dialogue **SecurityCenter**.

Lorsque vous exécutez SecurityCenter et que toutes les fonctionnalités McAfee installées sur votre ordinateur sont activées, une icône **M** rouge  apparaît dans la barre d'état système Windows. Cette zone se trouve dans l'angle inférieur droit du bureau Windows et contient l'horloge.

Si une ou plusieurs des applications McAfee installées sur votre ordinateur sont désactivées, l'icône McAfee devient noire  .

Pour ouvrir McAfee SecurityCenter :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee  .
2. Cliquez sur **Ouvrir SecurityCenter**.

Pour accéder à votre produit McAfee :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee  .
2. Pointez sur le produit McAfee de votre choix et sélectionnez la fonction à utiliser.

Désinstallation d'Internet Security Suite

Il se peut que vous ayez besoin de désinstaller Internet Security Suite ou l'un de ses programmes.

REMARQUE
Pour désinstaller Internet Security Suite, les utilisateurs doivent disposer de droits d'administrateur.

1. Enregistrez votre travail et fermez toutes les applications ouvertes.
2. Ouvrez le **Panneau de configuration**.
   - Utilisateurs de Windows ME et 2000 : dans la barre des tâches Windows, cliquez sur **Démarrer**, pointez sur **Paramètres**, puis sélectionnez **Panneau de configuration**.
   - Utilisateurs de Windows XP : dans la barre des tâches Windows, cliquez sur **Démarrer**, puis sélectionnez **Panneau de configuration**.
3. Cliquez sur **Ajout/Suppression de programmes**.

   REMARQUE
   Avant de désinstaller McAfee Internet Security Service, vous devez désinstaller chacun des programmes qui le constituent (McAfee Personal Firewall, McAfee Privacy Service, McAfee SpamKiller, McAfee VirusScan et McAfee SecurityCenter).
4. Sélectionnez un programme McAfee dans la liste des programmes et cliquez sur **Modifier/Supprimer**.
5. Une boîte de dialogue de confirmation apparaît. Cliquez sur **Oui** pour confirmer la désinstallation. Le processus de désinstallation est lancé.
6. Si l'ordinateur vous y invite, cliquez sur **Redémar**.
7. Si vous désinstallez Internet Security Suite, répétez la procédure de l'Étape 1 à l'Étape 6 pour chaque programme.
8. Dans la boîte de dialogue Ajout/Suppression de programmes, sélectionnez **McAfee SecurityCenter**, puis cliquez sur **Modifier/Supprimer**.
9. Si l'ordinateur vous y invite, cliquez sur **Redémar**.

McAfee VirusScan 2

Bienvenue dans McAfee VirusScan.

McAfee VirusScan est un service d'abonnement offrant une protection antivirus complète, fiable et à jour. Grâce à une technologie d'analyse McAfee primée, VirusScan protège votre ordinateur contre les virus, vers, chevaux de Troie, scripts malveillants et attaques hybrides.

Ses fonctions sont les suivantes.

ActiveShield : analyse les fichiers à l'accès.

Analyse : recherche des virus et des programmes potentiellement indésirables sur les disques durs et les disquettes, ainsi que dans les dossiers et les fichiers individuels.

Mise en quarantaine : chiffre et isole temporairement les fichiers infectés ou suspects dans le dossier de quarantaine jusqu'à ce qu'une action appropriée puisse être entreprise.

Détection des activités hostiles : surveille votre ordinateur à la recherche d'une activité virale causée par des scripts malveillants ou d'une activité de ver.

Nouvelles fonctions

Cette version de VirusScan offre les nouvelles fonctions suivantes.

- **Analyse des e-mails**
  Pour les clients de messagerie les plus couramment utilisés (notamment Microsoft Outlook, Netscape Mail, Eudora et Pegasus), VirusScan analyse automatiquement les e-mails entrants (POP3) et sortants (SMTP) ainsi que leurs pièces jointes.

- **Analyse de messages instantanés**
  Pour les clients de messagerie instantanée les plus couramment utilisés (notamment Yahoo Messenger, AOL Instant Messenger et MSN Messenger), VirusScan analyse automatiquement les fichiers entrants.

- **Détection des activités hostiles**
  VirusScan fournit les outils ScriptStopper™ et WormStopper™ pour détecter, signaler et bloquer les activités virales causées par des scripts malveillants et les activités de ver.

- **Intégration à l'Explorateur Windows**
  VirusScan permet d'utiliser un menu contextuel pour analyser les fichiers, dossiers ou lecteurs sélectionnés dans l'Explorateur Windows.

- **Intégration à Microsoft Outlook**
  VirusScan permet d'utiliser une icône de la barre d'outils pour analyser les messages, dossiers ou banques de messages sélectionnés dans Microsoft Outlook.

- **Nettoyage automatique des fichiers infectés**
  VirusScan tente automatiquement de nettoyer les fichiers infectés ou suspects dès qu'ils sont détectés.

- **Analyse programmée**
  Pour lancer une recherche complète de virus sur l'ordinateur, vous pouvez maintenant planifier une analyse automatique à intervalles définis.

- **Intégration à McAfee SecurityCenter**
  L'intégration transparente à McAfee SecurityCenter offre une vue globale de l'état de sécurité de votre ordinateur, ainsi qu'un accès aux dernières alertes de sécurité et de virus. Pour lancer SecurityCenter, cliquez sur l'icône McAfee de la barre d'état système ou du bureau Windows.

- **Mise en quarantaine des fichiers**
  Vous pouvez utiliser la fonction de mise en quarantaine pour chiffrer et temporairement isoler les fichiers infectés ou suspects dans le dossier de quarantaine jusqu'à ce qu'une action appropriée puisse être entreprise. Une fois désinfecté, un fichier mis en quarantaine peut être restauré à son emplacement d'origine.

- **Soumission de fichiers à AVERT**
  Grâce à la fonction de mise en quarantaine, VirusScan permet maintenant de soumettre (à des fins d'analyse) des fichiers suspects à McAfee AntiVirus Emergency Response Team (AVERT™).

- **Notification dans World Virus Map**
  De manière anonyme, vous pouvez maintenant envoyer des informations de suivi de virus et ainsi enrichir notre World Virus Map (carte mondiale des virus). Pour accéder à ce service gratuit et sécurisé, vous pouvez vous enregistrer automatiquement. Grâce à McAfee SecurityCenter, vous pouvez également afficher les derniers taux d'infection mondiaux.

Test de VirusScan

Avant la première utilisation de VirusScan, il est judicieux de tester votre installation. Pour tester séparément la fonction ActiveShield et celle d'analyse, procédez aux opérations ci-dessous.

Test d'ActiveShield

Pour tester ActiveShield :

1. Utilisez votre navigateur Web pour accéder au site http://www.eicar.com/.
2. Cliquez sur le lien **The AntiVirus testfile eicar.com (Fichier de test EICAR)**.
3. Défilez jusqu'en bas de la page. Sous **Download area (Télécharger)**, quatre liens apparaissent.
4. Cliquez sur **eicar.com**.

ActiveShield doit alors détecter le fichier eicar.com. Afin d'appréhender le traitement ActiveShield des virus, vous pouvez tenter de supprimer ou de mettre en quarantaine des fichiers infectés. Pour plus d'informations, consultez la section *Détection d'un virus avec ActiveShield* à la page 28.

Test de la fonction d'analyse

D'abord, vous devez désactiver ActiveShield (sinon, il détectera les fichiers infectés avant la fonction d'analyse). Ensuite, téléchargez les fichiers de test.

Pour les télécharger :

1. Désactivez ActiveShield. Dans cet objectif, cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Désactiver**.
2. Téléchargez les fichiers de test EICAR à partir du site Web.
   a. Accédez au site http://www.eicar.com/.
   b. Cliquez sur le lien **The AntiVirus testfile eicar.com (Fichier de test EICAR)**.

c Défilez jusqu'en bas de la page. Sous **Download area (Télécharger)**, les liens suivants apparaissent.

eicar.com contient une ligne de texte que VirusScan identifie comme un virus.

eicar.com.txt (facultatif) a le même contenu mais il porte un autre nom pour les utilisateurs qui ont des difficultés de téléchargement avec le premier lien. Après l'avoir téléchargé, renommez-le simplement eicar.com.

eicar_com.zip est une copie du virus de test à l'intérieur d'un fichier compressé .ZIP (archive de fichier WinZip™).

eicarcom2.zip est une copie du virus de test à l'intérieur d'un fichier compressé .ZIP, qui se trouve lui-même à l'intérieur d'un fichier compressé .ZIP.

d Ces liens permettent de télécharger les fichiers correspondants. Pour chacun, une boîte de dialogue **Téléchargement de fichier** s'affiche.

e Cliquez sur **Enregistrer**, sur le bouton **Créer un nouveau dossier**, puis renommez-le **dossier d'analyse VSO**.

f Double-cliquez sur le **dossier d'analyse VSO**, puis cliquez sur **Enregistrer** dans chacune des boîtes de dialogue **Enregistrer sous**.

3 Une fois les fichiers téléchargés, quittez votre navigateur.

4 Activez ActiveShield : cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Activer**.

Pour tester la fonction d'analyse :

1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Analyse antivirus**.

2 Dans le volet gauche de la boîte de dialogue, développez l'arborescence de répertoires jusqu'au **dossier d'analyse VSO** contenant les fichiers de test.

a Cliquez sur le signe **+** en regard de l'icône du lecteur C.

b Cliquez sur le **dossier d'analyse VSO** pour le mettre en surbrillance (et non sur son signe **+**).

Ainsi, vous indiquez à la fonction d'analyse de limiter la recherche des virus à ce dossier. Pour obtenir une démonstration encore plus probante des possibilités de cette fonction, vous pouvez placer les fichiers dans des emplacements aléatoires sur votre disque dur.

3 Dans la zone **Options d'analyse** de la boîte de dialogue **McAfee VirusScan – Recherche de virus**, vérifiez que toutes les options sont sélectionnées.

4 Dans la partie inférieure droite, cliquez sur **Analyser**.

VirusScan analyse le **dossier d'analyse VSO**. Si le contenu EICAR de ce dossier s'affiche dans la **liste des fichiers détectés**, la fonction d'analyse fonctionne correctement.

Afin d'appréhender son traitement des virus, vous pouvez tenter de supprimer ou de mettre en quarantaine les fichiers infectés. Pour plus d'informations, consultez la section *Détection d'un virus ou d'un programme potentiellement indésirable* à la page 37.

Utilisation de McAfee VirusScan

Cette section présente les modes d'utilisation de VirusScan.

Utilisation d'ActiveShield

Une fois démarré (chargé dans la mémoire de l'ordinateur) et activé, ActiveShield protège votre ordinateur en permanence. Il analyse les fichiers à l'accès. Quand ActiveShield détecte un fichier infecté, il tente automatiquement de le nettoyer. S'il ne parvient pas à éradiquer le virus, vous pouvez supprimer ou mettre en quarantaine le fichier.

Activation ou désactivation d'ActiveShield

Dès le redémarrage de Windows qui suit le processus d'installation, ActiveShield est par défaut démarré (chargé dans la mémoire de l'ordinateur) et activé (d'après l'icône rouge de la barre d'état système).

S'il est arrêté (non chargé) ou désactivé (d'après l'icône noire), il peut être exécuté manuellement et configuré pour se lancer automatiquement au démarrage de Windows.

Activation d'ActiveShield

Pour activer ActiveShield lors de cette session Windows uniquement :

Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Activer**. L'icône McAfee devient rouge.

Si le lancement d'ActiveShield au démarrage de Windows est toujours défini, un message indique que vous êtes maintenant protégé contre les virus. Dans le cas contraire, une boîte de dialogue permet d'obtenir cette configuration (Figure 2-1 à la page 20).

Désactivation d'ActiveShield

Pour désactiver ActiveShield lors de cette session Windows uniquement :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Désactiver**.
2. Pour confirmer, cliquez sur **Oui**.

   L'icône McAfee devient noire.

Si le lancement d'ActiveShield à l'ouverture de Windows est toujours défini, la protection antivirus sera réactivée au redémarrage de votre ordinateur.

Configuration des options d'ActiveShield

Vous pouvez modifier les options de démarrage et d'analyse dans l'onglet **ActiveShield** de la boîte de dialogue **McAfee VirusScan – Options** (Figure 2-1) accessible à l'aide de l'icône McAfee de la barre d'état système Windows.

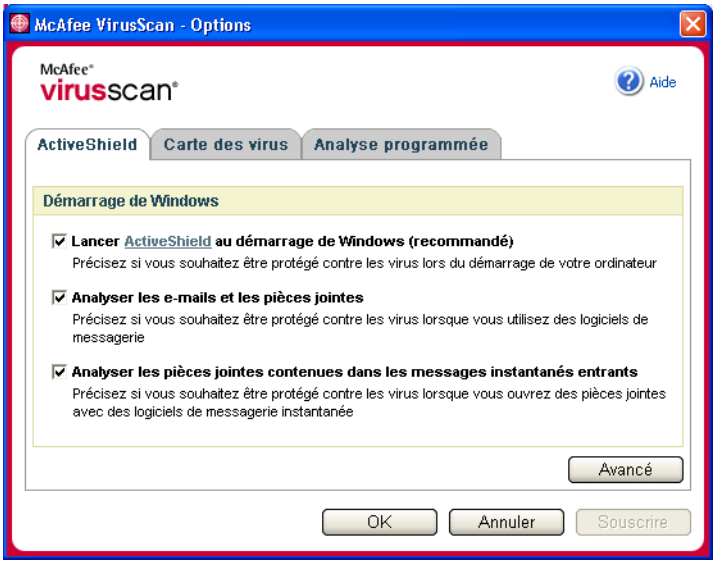


Figure 2-1. Options d'ActiveShield

Démarrage d'ActiveShield

Dès le redémarrage système qui suit le processus d'installation, ActiveShield est par défaut lancé (chargé dans la mémoire de l'ordinateur) et activé (d'après l'icône rouge).

S'il est arrêté (d'après l'icône noire), il peut être défini pour se lancer automatiquement au démarrage de Windows (recommandé).

> **REMARQUE**
> Pour installer de nouveaux fichiers, l'**Assistant de mise à jour** peut quitter temporairement ActiveShield. Lorsqu'il vous invite à terminer le processus, ActiveShield redémarre.

Pour démarrer ActiveShield automatiquement au démarrage de Windows :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Options**.

   La boîte de dialogue **McAfee VirusScan – Options** s'affiche (Figure 2-1 à la page 20).

2. Cochez la case **Lancer ActiveShield au démarrage de Windows (recommandé)**, puis enregistrez vos modifications.

3. Pour confirmer votre choix, cliquez sur **OK** à deux reprises.

Arrêt d'ActiveShield

> **AVERTISSEMENT**
> Sans ActiveShield, votre ordinateur ne sera plus protégé contre les virus. Si vous devez arrêter ActiveShield pour une raison autre que la mise à jour de VirusScan, vérifiez que vous n'êtes pas connecté à Internet.

Pour empêcher ActiveShield de se lancer au démarrage de Windows :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Options**.

   La boîte de dialogue **McAfee VirusScan – Options** s'affiche (Figure 2-1 à la page 20).

2. Décochez la case **Lancer ActiveShield au démarrage de Windows (recommandé)**, puis enregistrez vos modifications.

3. Pour confirmer votre choix, cliquez sur **OK** à deux reprises.

Analyse des e-mails et des pièces jointes

Par défaut, les options **Analyser les e-mails et les pièces jointes** (Figure 2-1 à la page 20) et **Nettoyer automatiquement les pièces jointes infectées (recommandé)** (Figure 2-2 à la page 24) sont activées.

Dans ce cas, ActiveShield tente de désinfecter automatiquement les e-mails entrants (POP3)/sortants (SMTP) et les pièces jointes provenant des clients de messagerie électronique les plus couramment utilisés, notamment :

- Microsoft Outlook Express version 4.0 ou ultérieure
- Microsoft Outlook version 97 ou ultérieure
- Netscape Messenger version 4.0 ou ultérieure
- Netscape Mail version 6.0 ou ultérieure
- Eudora Light version 3.0 ou ultérieure
- Eudora Pro version 4.0 ou ultérieure
- Eudora version 5.0 ou ultérieure
- Pegasus version 4.0 ou ultérieure

REMARQUE

L'analyse des e-mails n'est pas disponible pour les clients de messagerie basés sur le Web, IMAP, AOL, POP3 SSL et Lotus Notes. Toutefois, ActiveShield analyse les pièces jointes des e-mails dès leur ouverture.

La désactivation de l'option **Analyser les e-mails et les pièces jointes** entraîne celle de la fonction d'analyse des e-mails (Figure 2-2 à la page 24) et de WormStopper (Figure 2-5 à la page 28). Par ailleurs, la désactivation de l'analyse des e-mails sortants entraîne celle de WormStopper.

Si vous modifiez les options d'analyse des e-mails, vous devez redémarrer votre programme de messagerie pour appliquer les modifications.

E-mails entrants

En cas d'infection d'un e-mail ou d'une pièce jointe entrant(e), ActiveShield :

- Tente de désinfecter l'e-mail
- Tente de mettre en quarantaine ou de supprimer un e-mail impossible à nettoyer
- Intègre un fichier d'alerte dans l'e-mail entrant qui précise les actions de désinfection réalisées

E-mails sortants

En cas d'infection d'un e-mail ou d'une pièce jointe sortant(e), ActiveShield :

- Tente de désinfecter l'e-mail
- Tente de mettre en quarantaine ou de supprimer un e-mail impossible à nettoyer
- Vous envoie un fichier d'alerte dans un nouvel e-mail qui précise les actions de désinfection réalisées

> **REMARQUE**
> Pour plus d'informations sur les erreurs d'analyse des e-mails sortants, reportez-vous à l'aide en ligne.

Par défaut, ActiveShield analyse les e-mails entrants et sortants. Toutefois, pour un meilleur contrôle, vous pouvez paramétrer ActiveShield de manière à ce qu'il analyse uniquement les e-mails entrants ou sortants.

Pour désactiver l'analyse des e-mails entrants ou sortants :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Options**.
2. Cliquez sur **Avancé**, puis sur l'onglet **Analyse e-mails** (Figure 2-2 à la page 24).
3. Désélectionnez **E-mails entrants** ou **E-mails sortants**, puis cliquez sur **OK**.

Si votre serveur de messagerie est défini pour envoyer et recevoir des e-mails uniquement lorsque vous êtes à votre poste, vous pouvez choisir de recevoir des invites de désinfection de messages en désactivant le nettoyage automatique. Procédez aux opérations ci-dessous pour désactiver le nettoyage automatique, puis consultez la section *Gestion des e-mails infectés* à la page 29 pour obtenir plus d'informations sur la réponse aux alertes.

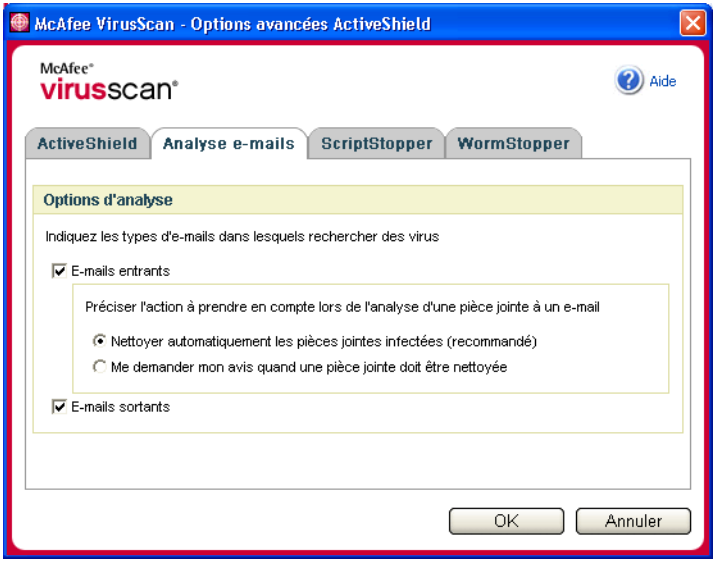


Figure 2-2. Options d'analyse des e-mails

Pour désactiver le nettoyage automatique des e-mails infectés :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Options**.
2. Cliquez sur **Avancé**, puis sur l'onglet **Analyse e-mails** (Figure 2-2).
3. Cliquez sur **Me demander mon avis quand une pièce jointe doit être nettoyée**, puis sur **OK**.

Analyse des pièces jointes de messages instantanés entrants

Par défaut, l'option **Analyser les pièces jointes contenues dans les messages instantanés entrants** est activée (Figure 2-1 à la page 20).

Si cette option est activée, VirusScan tente de désinfecter automatiquement les pièces jointes entrantes provenant des clients de messagerie instantanée les plus couramment utilisés, notamment :

- MSN Messenger version 6.0 ou ultérieure
- Yahoo Messenger version 4.1 ou ultérieure
- AOL Instant Messenger version 2.1 ou ultérieure

REMARQUE
Pour votre protection, il est impossible de désactiver le nettoyage automatique des pièces jointes de messages instantanés.

En cas d'infection d'une pièce jointe de message instantané entrant, VirusScan :

- Tente de désinfecter le message
- Invite à mettre en quarantaine ou à supprimer un message impossible à nettoyer

Analyse de tous les fichiers

L'option par défaut **Tous les fichiers (recommandé)** de l'onglet ActiveShield entraîne l'analyse à l'accès. Elle permet d'effectuer la recherche la plus complète possible.

Pour qu'ActiveShield analyse tous les types de fichier :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Options**.
2. Cliquez sur **Avancé**, puis sur l'onglet **ActiveShield** (Figure 2-3).
3. Cliquez sur **Tous les fichiers (recommandé)**, puis sur **OK**.

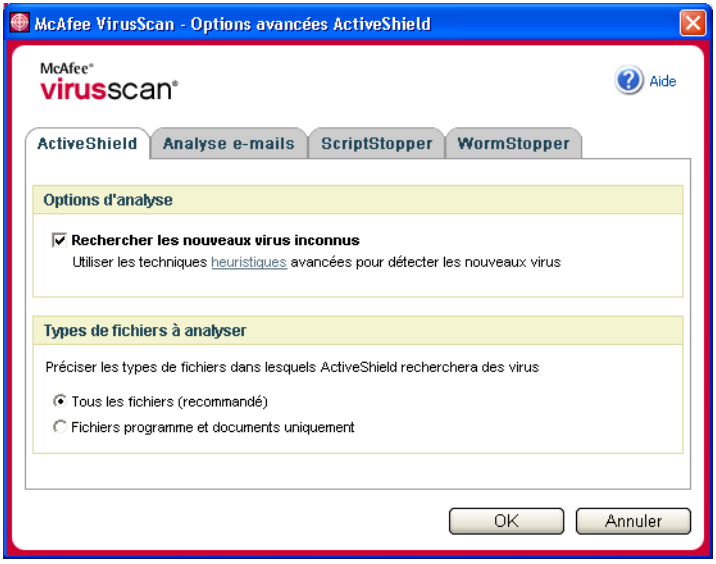


Figure 2-3. Options ActiveShield avancées

Analyse des fichiers programme et des documents uniquement

Si vous activez l'option **Fichiers programme et documents uniquement**, ActiveShield n'analyse aucun des autres fichiers utilisés par votre ordinateur. Le dernier fichier de signature de virus (.DAT) détermine les types de fichier qu'analysera ActiveShield. Pour qu'ActiveShield analyse les fichiers programme et les documents uniquement :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Options**.
2. Cliquez sur **Avancé**, puis sur l'onglet **ActiveShield** (Figure 2-3 à la page 25).
3. Cliquez sur **Fichiers programme et documents uniquement**, puis sur **OK**.

Recherche de nouveaux virus inconnus

Si vous laissez l'option par défaut **Rechercher les nouveaux virus inconnus** (recommandé), ActiveShield utilise des techniques heuristiques avancées qui tentent de faire correspondre les fichiers aux signatures des virus connus, tout en recherchant des signes révélateurs de virus non identifiés dans les fichiers.

Pour qu'ActiveShield recherche les nouveaux virus inconnus :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Options**.
2. Cliquez sur **Avancé**, puis sur l'onglet **ActiveShield** (Figure 2-3 à la page 25).
3. Cliquez sur **Rechercher les nouveaux virus inconnus** (recommandé), puis sur **OK**.

Recherche des scripts et des vers

Sur votre ordinateur, VirusScan recherche toute activité suspecte qui pourrait indiquer la présence d'une menace. Au lieu de procéder à la désinfection, ScriptStopper™ et WormStopper™ empêchent virus, vers et chevaux de Troie de se répandre davantage.

Leurs mécanismes de protection permettent de détecter, de signaler et de bloquer les activités malveillantes, notamment :

- Une exécution de script qui entraîne la création/copie/suppression de fichiers ou l'ouverture de votre registre Windows
- Une tentative de transfert des e-mails à une grande partie de vos contacts
- Des tentatives de transfert de plusieurs e-mails à intervalles rapprochés

Si vous laissez les options par défaut **Activer ScriptStopper (recommandé)** et **Activer WormStopper (recommandé)** de la boîte de dialogue **McAfee VirusScan -Options avancées ActiveShield**, ces deux fonctions permettent de surveiller l'exécution des scripts et l'activité des e-mails à la recherche de schémas suspects et de vous alerter lorsqu'un nombre défini d'e-mails ou de destinataires est dépassé dans un intervalle donné.

Pour qu'ActiveShield recherche les scripts malveillants et les activités de type ver :

1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Options**.

2 Cliquez sur **Avancé**, puis sur l'onglet **ScriptStopper**.

3 Cliquez sur **Activer ScriptStopper (recommandé)** (Figure 2-4).

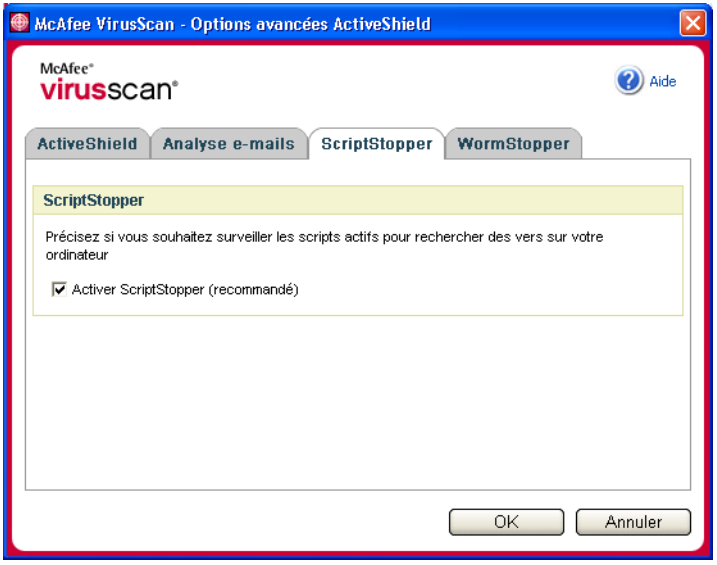


Figure 2-4. Options de ScriptStopper

4 Cliquez sur l'onglet **WormStopper**, sur **Activer WormStopper (recommandé)**, puis sur **OK** (Figure 2-5 à la page 28).

Par défaut, les options ci-dessous sont activées :

- Activer le filtrage (recommandé)
- Me signaler quand un e-mail est envoyé à 40 destinataire(s) ou plus
- Me signaler quand 5 e-mails sont envoyés pendant 30 secondes

REMARQUE
Si vous modifiez le nombre de destinataires ou de secondes destiné à la surveillance des e-mails envoyés, des détections erronées risquent de se produire. Pour conserver les valeurs par défaut, McAfee vous recommande d'**annuler** l'opération. Dans le cas contraire, cliquez sur **OK**.

La fonction suivante peut être automatiquement activée après la première détection d'un ver potentiel (pour plus d'informations, reportez-vous à la section *Gestion des vers potentiels* à la page 30) :

- Blocage automatique des e-mails sortants suspects

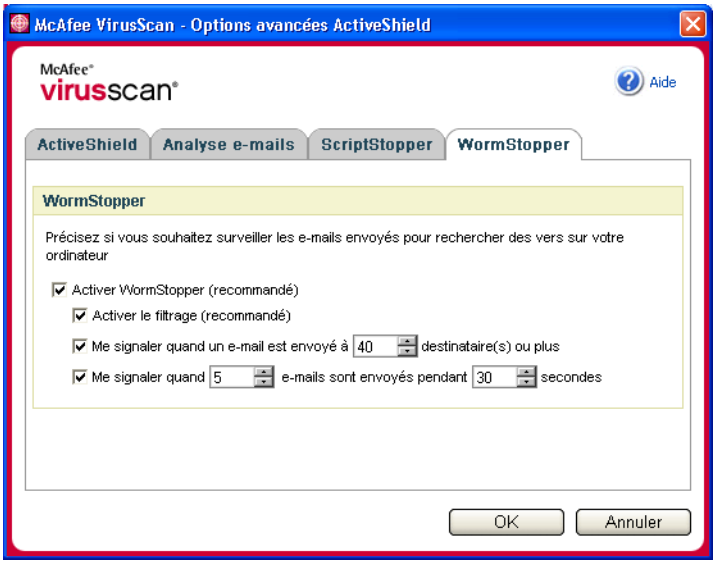


Figure 2-5. Options de WormStopper

Détection d'un virus avec ActiveShield

Si ActiveShield trouve un virus, une alerte similaire à celle de la Figure 2-6 à la page 29 s'affiche. Pour la plupart des virus, des chevaux de Troie et des vers, ActiveShield tente automatiquement de nettoyer le fichier. Vous pouvez alors choisir la méthode de traitement des éléments contaminés, des scripts suspects et des vers potentiels ainsi que la soumission des fichiers infectés aux laboratoires de McAfee AVERT à des fins d'analyse.

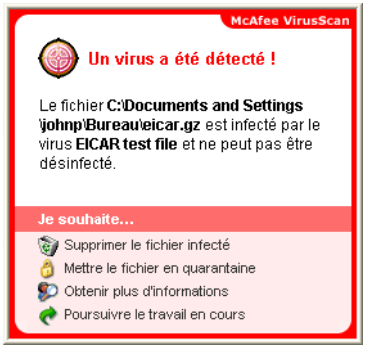


Figure 2-6. Alerte de virus

Gestion des fichiers infectés

1 Si ActiveShield parvient à nettoyer le fichier, vous pouvez en savoir davantage ou ignorer l'alerte :

- Pour afficher le fichier infecté, son emplacement et le virus incriminé, cliquez sur **Obtenir plus d'informations**.
- Pour ignorer et fermer l'alerte, cliquez sur **Poursuivre le travail en cours**.

2 Si ActiveShield ne parvient pas à nettoyer le fichier, cliquez sur **Mettre le fichier en quarantaine** pour chiffrer et temporairement isoler les fichiers infectés et suspects dans le dossier de quarantaine jusqu'à ce qu'une action appropriée puisse être entreprise.

Un message de confirmation vous invite à effectuer une analyse antivirus de votre ordinateur. Pour terminer le processus de mise en quarantaine, cliquez sur **Analyser**.

3 Si ActiveShield ne parvient pas à mettre le fichier en quarantaine, tentez de **supprimer le fichier infecté**.

Gestion des e-mails infectés

1 Si vous avez désactivé le nettoyage automatique des e-mails, vous pouvez obtenir plus d'informations et procéder à la désinfection :

a Pour afficher le fichier, le virus, l'état d'infection, l'expéditeur et l'objet de l'e-mail infecté, cliquez sur **Obtenir plus d'informations**.

b Cliquez sur l'option de **désinfection des pièces jointes**.

2 Si ActiveShield ne parvient pas à nettoyer l'e-mail, **mettez les pièces jointes en quarantaine** pour chiffrer et temporairement isoler les fichiers infectés et suspects dans le dossier de quarantaine jusqu'à ce qu'une action appropriée puisse être entreprise.

Un message de confirmation vous invite à effectuer une analyse antivirus de votre ordinateur. Pour terminer le processus de mise en quarantaine, cliquez sur **Analyser**.

3 Si ActiveShield ne parvient pas à mettre l'e-mail en quarantaine, tentez de **supprimer la pièce jointe infectée**.

Gestion des scripts suspects

1 Si ActiveShield détecte un script suspect, vous pouvez obtenir plus d'informations et bloquer l'exécution non voulue de ce code :

   a Pour afficher le nom, l'emplacement et la description de l'activité associée au script suspect, cliquez sur **Obtenir plus d'informations**.

   b Pour bloquer l'exécution, **arrêtez ce script**.

2 Si vous êtes certain de la fiabilité du script, vous pouvez autoriser son exécution :

   a Pour permettre l'exécution unique de tous les scripts contenus dans un seul fichier, **autorisez cette fois ce script**.

   b Pour ignorer l'alerte et permettre l'exécution du script, **poursuivez l'opération en cours**.

Gestion des vers potentiels

1 Si ActiveShield détecte un ver potentiel, vous pouvez obtenir plus d'informations et arrêter l'activité non voulue de messagerie :

   a Pour afficher la liste des destinataires, l'objet, le corps du message et la description de l'activité suspecte associée à l'e-mail infecté, cliquez sur **Obtenir plus d'informations**.

   b Pour supprimer le message suspect de la file d'attente d'envoi, **arrêtez cet e-mail**.

2 Si vous êtes certain de la fiabilité de l'activité de messagerie, **poursuivez l'action en cours** pour ignorer l'alerte et permettre l'envoi de l'e-mail.

Analyse manuelle de votre ordinateur

La fonction d'analyse permet de rechercher de manière sélective des virus et des programmes potentiellement indésirables sur les disques durs et les disquettes, ainsi que dans les fichiers et dossiers individuels. Lorsqu'elle détecte un fichier infecté, elle tente automatiquement de le nettoyer, sauf en cas de programme potentiellement indésirable. Si la fonction d'analyse ne peut pas procéder à la désinfection, vous pouvez mettre en quarantaine ou supprimer le fichier.

Recherche manuelle de virus et de programmes potentiellement indésirables

Pour analyser votre ordinateur :

1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Analyse antivirus**.

La boîte de dialogue **McAfee VirusScan – Recherche de virus** s'affiche (Figure 2-7).

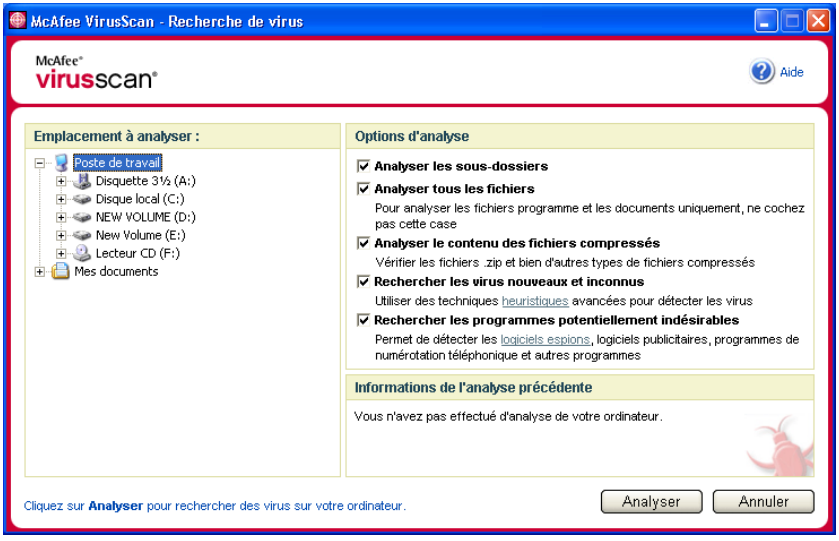


Figure 2-7. Recherche de virus

2 Cliquez sur le lecteur, le dossier ou le fichier à analyser.

3 Sélectionnez vos **options d'analyse**. Par défaut, toutes les **options d'analyse** sont présélectionnées pour exécuter l'analyse la plus complète possible (Figure 2-7).

- **Analyser les sous-dossiers** : cochez cette case pour analyser les fichiers contenus dans vos sous-dossiers. Décochez-la pour limiter l'analyse aux fichiers visibles à l'ouverture d'un dossier ou d'un lecteur.

  Exemple : les fichiers de la Figure 2-8 à la page 32 sont les seuls fichiers analysés si vous décochez la case **Analyser les sous-dossiers**. Les dossiers et leur contenu ne sont donc pas analysés. Pour les analyser, ne décochez pas la case.

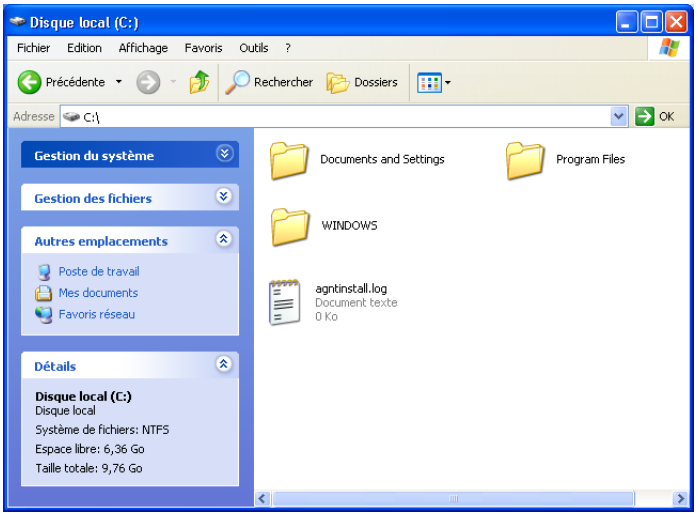


Figure 2-8. Contenu du disque local

- **Analyser tous les fichiers** : cochez cette case pour permettre l'analyse complète de tous les types de fichier. Décochez-la pour réduire la durée de l'analyse et permettre la vérification des fichiers programme et des documents uniquement.
- **Analyser le contenu des fichiers compressés** : cochez cette case pour détecter les fichiers infectés cachés dans des fichiers .ZIP et autres fichiers compressés. Décochez-la pour empêcher la vérification des fichiers, compressés ou non, contenus dans le fichier compressé.

  Parfois, les auteurs de virus placent des virus dans un fichier .ZIP, puis insèrent ce fichier .ZIP dans un autre fichier .ZIP afin de déjouer les analyseurs antivirus. Tant que vous ne décochez pas la case, la fonction d'analyse peut détecter ces virus.
- **Rechercher les virus nouveaux et inconnus** : cochez cette case pour rechercher les virus récents probablement encore sans « remèdes ». Cette option utilise des techniques heuristiques avancées qui tentent de faire correspondre les fichiers aux signatures des virus connus tout en recherchant des signes révélateurs de virus non identifiés dans les fichiers.

  Cette méthode d'analyse permet aussi de rechercher des caractéristiques de fichier qui écartent généralement la présence éventuelle de virus dans le fichier. Ainsi, la fonction d'analyse risque moins de fournir une indication erronée. Cependant, si une analyse heuristique détecte un virus, agissez avec les mêmes précautions que vous prendriez avec un fichier à votre connaissance infecté.

  Cette option exécute l'analyse la plus complète mais elle est généralement plus lente qu'une recherche normale.

- **Rechercher les programmes potentiellement indésirables** : cochez cette case pour détecter des logiciels espions, des logiciels publicitaires, des composeurs téléphoniques et d'autres applications indésirables.

  REMARQUE
  Laissez toutes ces options sélectionnées afin d'effectuer l'analyse la plus complète possible. Ces options ayant pour effet d'analyser tous les fichiers contenus sur le lecteur ou dans le dossier sélectionné, prévoyez suffisamment de temps pour le déroulement complet de la recherche. Plus le disque dur est volumineux et plus il contient de fichiers, plus l'analyse dure longtemps.

4 Pour lancer l'analyse des fichiers, cliquez sur **Analyser**.

Une fois la recherche terminée, un résumé affiche le nombre de fichiers analysés, le nombre de fichiers détectés, le nombre de programmes potentiellement indésirables et le nombre de fichiers détectés automatiquement nettoyés.

5 Cliquez sur **OK** pour fermer le résumé et afficher la liste des fichiers détectés dans la boîte de dialogue **McAfee VirusScan – Recherche de virus** (Figure 2-9).

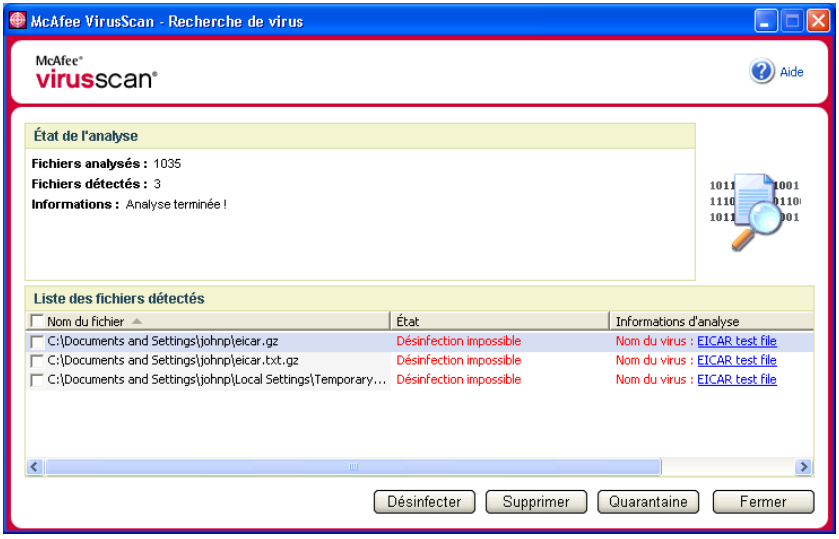


Figure 2-9. Résultats de l'analyse

REMARQUE
La fonction d'analyse compte un fichier compressé (.ZIP, .CAB, etc.) comme un seul fichier dans le nombre de **fichiers analysés**. De plus, le nombre de fichiers analysés peut varier si vous avez supprimé vos fichiers Internet temporaires depuis votre dernière analyse.

6 Si la fonction d'analyse ne trouve aucun virus ni aucun programme potentiellement indésirable, cliquez sur **Précédent** pour sélectionner un autre lecteur ou dossier à analyser ou cliquez sur **Fermer** pour fermer la boîte de dialogue. Dans le cas contraire, reportez-vous à la section *Détection d'un virus ou d'un programme potentiellement indésirable* à la page 37.

Analyse depuis l'Explorateur Windows

VirusScan propose un menu contextuel pour analyser les fichiers, dossiers ou lecteurs sélectionnés dans l'Explorateur Windows à la recherche de virus ou de programmes potentiellement indésirables.

Pour analyser des fichiers depuis l'Explorateur Windows :

1 Ouvrez l'Explorateur Windows.

2 Cliquez avec le bouton droit de la souris sur le lecteur, le dossier ou le fichier à analyser, puis cliquez sur **Analyse antivirus**.

La boîte de dialogue **McAfee VirusScan – Recherche de virus** s'ouvre et l'analyse des fichiers démarre. Par défaut, toutes les **options d'analyse** sont présélectionnées pour exécuter l'analyse la plus complète possible (Figure 2-7 à la page 31).

Analyse depuis Microsoft Outlook

VirusScan permet d'utiliser une icône de la barre d'outils pour rechercher les virus et les programmes potentiellement indésirables dans les banques de messages et leurs sous-dossiers, les dossiers de boîte aux lettres ou messages électroniques sélectionnés contenant des pièces jointes dans Microsoft Outlook version 97 ou ultérieure.

Pour analyser un e-mail dans Microsoft Outlook :

1 Ouvrez Microsoft Outlook.

2 Cliquez sur la banque de messages, le dossier ou l'e-mail contenant une pièce jointe à analyser, puis cliquez sur l'icône de la barre d'outils correspondant à l'analyse des e-mails  .

L'analyseur d'e-mails s'ouvre et commence l'analyse des fichiers. Par défaut, toutes les **options d'analyse** sont présélectionnées pour exécuter l'analyse la plus complète possible (Figure 2-7 à la page 31).

Recherche automatique de virus et de programmes potentiellement indésirables

Bien que VirusScan analyse les fichiers à l'accès, vous pouvez programmer une analyse automatique dans le planificateur de Windows pour lancer une recherche complète de virus et de programmes potentiellement indésirables sur votre ordinateur aux intervalles indiqués.

Pour programmer une analyse :

1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Options**.

La boîte de dialogue **McAfee VirusScan – Options** s'affiche.

2 Cliquez sur l'onglet **Analyse programmée** (Figure 2-10).

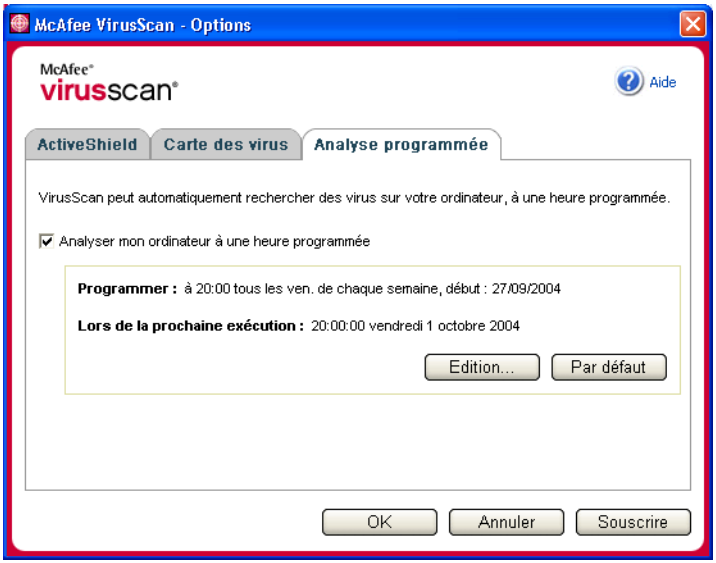


Figure 2-10. Options d'analyse programmée

3 Cochez la case **Analyser mon ordinateur à une heure programmée** pour permettre l'analyse automatique.

4 Choisissez une fréquence d'analyse automatique :

- Pour accepter la planification par défaut (20h00 tous les vendredis), cliquez sur **OK**.
- Pour modifier la programmation :

  a. Cliquez sur **Edition**.

  b. Sélectionnez la fréquence à laquelle vous voulez analyser votre ordinateur dans la liste **Tâche planifiée**, puis sélectionnez des options supplémentaires dans la zone dynamique située en dessous.

  Tous les jours : indique le nombre de jours entre les analyses.

  Toutes les semaines (par défaut) : indique le nombre de semaines entre les analyses, ainsi que le nom du ou des jours de la semaine.

  Tous les mois : indique quel jour du mois lancer l'analyse. Cliquez sur **Choix des mois** pour indiquer les mois concernés par l'analyse, puis cliquez sur **OK**.

  Une seule fois : indique la date de l'analyse.

  REMARQUE
  Les options suivantes ne sont pas prises en charge dans le planificateur de Windows : **Au démarrage du système**, **Si inactif** et **Afficher les différents horaires**. Tant que vous ne sélectionnez pas les options valides, le dernier calendrier pris en charge reste activé.

  c. Sélectionnez l'heure du jour à laquelle vous voulez analyser votre ordinateur dans la zone **Heure de début**.

  d. Pour sélectionner des options avancées, cliquez sur **Avancé**.

  La boîte de dialogue **Options avancées de planification** s'ouvre.

  i. Indiquez une date de début, une date de fin, une durée ainsi qu'une heure de fin et précisez si l'analyse doit s'interrompre à l'heure indiquée même si elle n'est pas encore terminée.

  ii. Cliquez sur **OK** pour enregistrer les modifications et fermer la boîte de dialogue. Autrement, cliquez sur **Annuler**.

5 Cliquez sur **OK** pour enregistrer les modifications et fermer la boîte de dialogue. Autrement, cliquez sur **Annuler**.

6 Pour rétablir la fréquence par défaut, cliquez sur **Par défaut**. Autrement, cliquez sur **OK**.

Détection d'un virus ou d'un programme potentiellement indésirable

Pour la plupart des virus, des chevaux de Troie et des vers, la fonction d'analyse tente automatiquement de nettoyer le fichier. Vous pouvez alors choisir la méthode de traitement des fichiers détectés et décider de les soumettre aux laboratoires de McAfee AVERT à des fins d'analyse. Si la fonction d'analyse détecte un programme potentiellement indésirable, vous pouvez essayer manuellement de le nettoyer, de le mettre en quarantaine ou de le supprimer (la fonction de soumission à AVERT n'est pas disponible).

Pour gérer un virus ou un programme potentiellement indésirable :

1 Si un fichier apparaît dans la **liste des fichiers détectés**, cochez la case en regard de ce fichier pour le sélectionner.

> **REMARQUE**
> Si plusieurs fichiers apparaissent dans la liste, vous pouvez cocher la case en regard de la liste **Nom du fichier** pour exécuter la même action sur l'ensemble des fichiers. Vous pouvez également cliquer sur le nom du fichier dans la liste **Informations d'analyse** pour afficher des détails provenant de la bibliothèque d'informations sur les virus.

2 Si le fichier est un programme potentiellement indésirable, vous pouvez cliquer sur **Désinfecter** pour essayer de le nettoyer.

3 Si la fonction d'analyse ne parvient pas à nettoyer le fichier, cliquez sur **Quarantaine** pour chiffrer et temporairement isoler les fichiers infectés et suspects dans le dossier de quarantaine jusqu'à ce qu'une action appropriée puisse être entreprise. Pour plus d'informations, consultez la section *Gestion des fichiers mis en quarantaine*.

4 Si la fonction d'analyse ne parvient pas à nettoyer ou à mettre en quarantaine le fichier, deux possibilités se présentent à vous.

- Pour supprimer le fichier, cliquez sur **Supprimer**.
- Pour fermer la boîte de dialogue, cliquez sur **Fermer**.

Si la fonction d'analyse ne parvient pas à nettoyer ou à supprimer le fichier détecté, consultez la bibliothèque d'informations sur les virus à l'adresse http://us.mcafee.com/virusInfo/default.asp pour obtenir des instructions sur la suppression manuelle du fichier.

Si un fichier détecté empêche la connexion à Internet ou l'entière utilisation de l'ordinateur, tentez un démarrage à l'aide d'une disquette de secours. La disquette de secours permet généralement de démarrer un ordinateur paralysé par un fichier infecté. Pour plus d'informations, consultez la section *Création d'une disquette de secours* à la page 39.

Pour obtenir une assistance supplémentaire, consultez le service clientèle de McAfee à l'adresse http://www.mcafeeaide.com.

Gestion des fichiers mis en quarantaine

La fonction de mise en quarantaine chiffre et temporairement isole les fichiers infectés et suspects dans le dossier de quarantaine jusqu'à ce qu'une action appropriée puisse être entreprise. Une fois désinfecté, un fichier mis en quarantaine peut être restauré à son emplacement d'origine.

Pour gérer un fichier mis en quarantaine :

1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Gestion des fichiers mis en quarantaine**.

La liste des fichiers mis en quarantaine s'affiche (Figure 2-11).

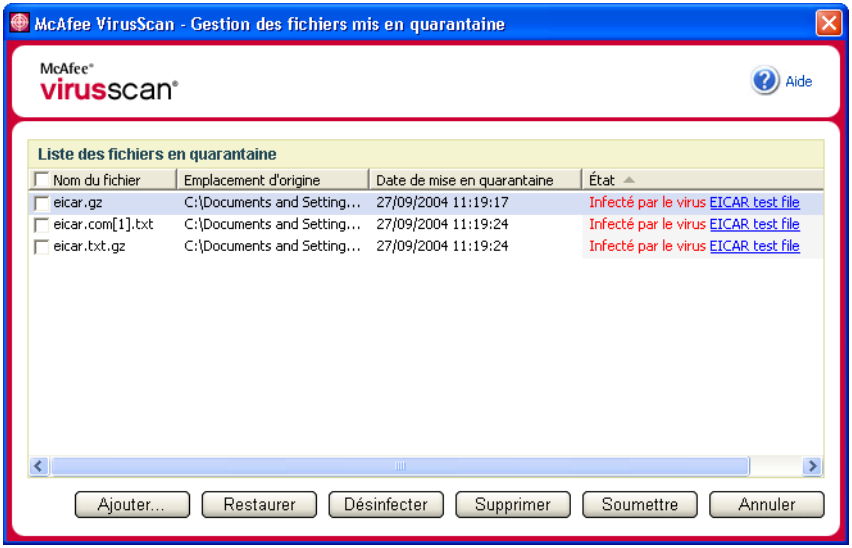


Figure 2-11. Gestion des fichiers mis en quarantaine

2 Cochez la case située en regard du ou des fichiers à nettoyer.

REMARQUE
Si plusieurs fichiers apparaissent dans la liste, vous pouvez cocher la case en regard de la liste **Nom du fichier** pour exécuter la même action sur l'ensemble des fichiers. Vous pouvez également cliquer sur le nom de virus dans la liste **Etat** pour afficher des détails provenant de la bibliothèque d'informations sur les virus.

Vous pouvez également cliquer sur **Ajouter**, sélectionner un fichier suspect à ajouter dans la liste de quarantaine, cliquer sur **Ouvrir**, puis sélectionner le fichier dans la liste.

3 Cliquez sur **Désinfecter**.

4 Si le fichier est nettoyé, cliquez sur **Restaurer** pour le replacer à son emplacement d'origine.

5 Si VirusScan ne parvient pas à éradiquer le virus, cliquez sur **Supprimer** pour supprimer le fichier.

6 Si VirusScan ne parvient pas à nettoyer ou à supprimer un fichier autre qu'un programme potentiellement indésirable, vous pouvez le soumettre à McAfee AVERT™ à des fins d'analyse.

   a Mettez à jour vos fichiers de signature de virus s'ils datent de plus de deux semaines.

   b Vérifiez votre abonnement.

   c Sélectionnez le fichier et cliquez sur **Soumettre** pour envoyer le fichier à AVERT.

   VirusScan envoie le fichier mis en quarantaine sous la forme d'une pièce jointe dans un e-mail précisant votre adresse électronique, votre pays, la version de votre logiciel, votre système d'exploitation ainsi que le nom d'origine et l'emplacement du fichier. La taille maximum du fichier soumis est celle de 1,5 Mo par jour.

7 Pour fermer la boîte de dialogue, cliquez sur **Fermer**.

Création d'une disquette de secours

L'utilitaire Rescue Disk crée une disquette de démarrage qui permet d'initialiser et d'analyser l'ordinateur si un virus empêche de le démarrer normalement.

> **REMARQUE**
> Vous devez être connecté à Internet pour télécharger l'image de la disquette de secours. D'autre part, la disquette de secours est réservée aux ordinateurs à partitions de disque dur FAT (FAT 16 et FAT 32). Elle est inutile pour les partitions NTFS.

Pour créer une disquette de secours :

1 Insérez une disquette non infectée dans le lecteur A d'un ordinateur non infecté. Vous pouvez utiliser la fonction d'analyse pour vérifier que l'ordinateur et la disquette ne contiennent pas de virus. Pour plus d'informations, consultez la section *Recherche manuelle de virus et de programmes potentiellement indésirables* à la page 31.

2 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Créer une disquette de secours**.

La boîte de dialogue **Création d'une disquette de secours** s'affiche (Figure 2-12).

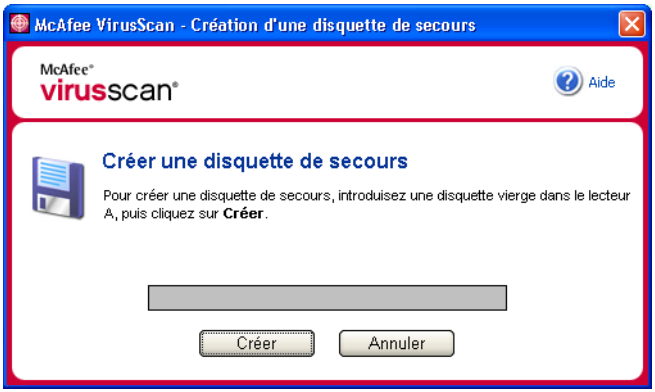


Figure 2-12. Création d'une disquette de secours

3 Cliquez sur **Créer** pour créer la disquette de secours.

Si vous créez une disquette de secours pour la première fois, un message vous indique que Rescue Disk doit télécharger le fichier image de la disquette de secours. Pour télécharger ce composant immédiatement ou ultérieurement, cliquez respectivement sur **OK** ou sur **Annuler**.

Un message d'avertissement vous signale que le contenu de la disquette sera perdu.

4 Cliquez sur **Oui** pour poursuivre la création de la disquette de secours.

Dans la boîte de dialogue **Création d'une disquette de secours**, une barre indique l'état d'avancement.

5 Lorsque le message Création de la disquette de secours terminée s'affiche, cliquez sur **OK**, puis fermez la boîte de dialogue **Création d'une disquette de secours**.

6 Retirez la disquette de secours du lecteur, protégez-la en écriture et rangez-la en lieu sûr.

Protection en écriture d'une disquette de secours

Pour protéger en écriture une disquette de secours :

1. Retournez la disquette, face étiquetée vers le bas (le rond métallique doit être visible).
2. Localisez l'ergot de protection en écriture. Faites glisser l'ergot de manière à ce que le trou soit visible.

Utilisation d'une disquette de secours

Pour utiliser une disquette de secours :

1. Mettez hors tension l'ordinateur infecté.
2. Insérez la disquette de secours dans le lecteur.
3. Mettez sous tension l'ordinateur.

   Une fenêtre grise à choix multiple s'affiche.
4. Choisissez l'option la mieux adaptée à vos besoins en appuyant sur les touches de fonction (par exemple, F2 ou F3).

REMARQUE
Si vous n'appuyez sur aucune touche, la disquette de secours démarre automatiquement au bout de 60 secondes.

Mise à jour d'une disquette de secours

Il est judicieux de mettre à jour régulièrement votre disquette de secours. Pour mettre à jour votre disquette de secours, suivez les mêmes instructions que celles de la création d'une disquette de secours.

Notification automatique de virus

Afin d'enrichir notre World Virus Map, vous pouvez envoyer des informations de suivi de virus de manière anonyme. Pour utiliser cette fonction sécurisée et gratuite, enregistrez-vous automatiquement pendant l'installation de VirusScan (dans la boîte de dialogue **Carte des virus**) ou à tout moment (dans l'onglet **Carte des virus** de **McAfee VirusScan – Options**).

Notification dans World Virus Map

Pour notifier automatiquement des informations sur les virus dans World Virus Map :

1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **Options**.

La boîte de dialogue **McAfee VirusScan – Options** s'affiche.

2 Cliquez sur l'onglet **Carte des virus** (Figure 2-13).

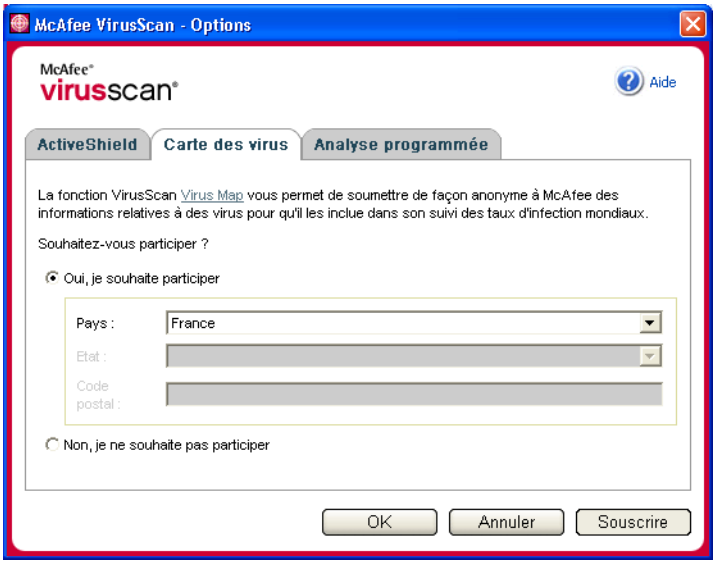


Figure 2-13. Options de Carte des virus

3 Pour ajouter anonymement des informations sur les virus dans World Virus Map (baromètre des taux d'infection mondiaux de McAfee), acceptez l'option par défaut **Oui**, **je souhaite participer**. Dans le cas contraire, sélectionnez **Non**, **je ne souhaite pas participer**.

4 Si vous résidez aux États-Unis, indiquez l'état et le code postal de la localité où se trouve votre ordinateur. Dans le cas contraire, VirusScan tente automatiquement de sélectionner le pays où se trouve votre ordinateur.

5 Cliquez sur **OK**.

Affichage de World Virus Map

Que vous participiez ou non à World Virus Map, vous pouvez afficher les derniers taux d'infection mondiaux à l'aide de l'icône de la barre d'état système Windows.

Pour afficher World Virus Map :

- Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis sélectionnez **World Virus Map**.

  La page Web **World Virus Map** s'affiche (Figure 2-14).

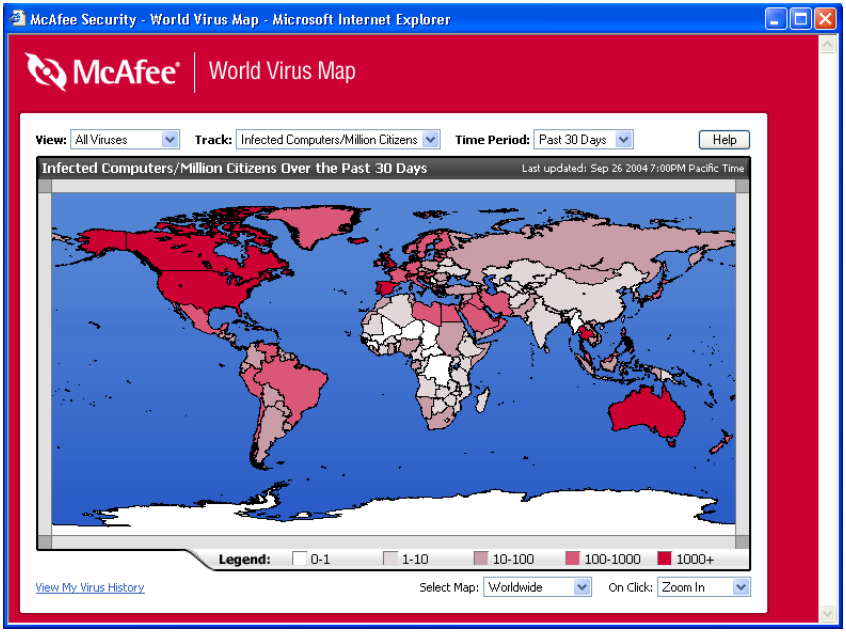


Figure 2-14. World Virus Map

Par défaut, World Virus Map indique le nombre mondial d'ordinateurs infectés au cours des derniers 30 jours et la date de la dernière mise à jour des données de notification. Vous pouvez modifier l'affichage de la carte afin de connaître le nombre de fichiers infectés ou la période afin de visualiser uniquement les résultats des 7 jours précédents ou des dernières 24 heures.

La section **Virus Tracking (Suivi de virus)** présente les nombres totaux cumulés des éléments analysés, des fichiers infectés et des ordinateurs contaminés d'après les signalements remontant à la date indiquée.

Mise à jour de VirusScan

Lorsque vous êtes connecté à Internet, VirusScan recherche automatiquement des mises à jour toutes les quatre heures, puis télécharge automatiquement et installe les mises à jour hebdomadaires de définitions de virus, sans interrompre votre travail.

Les fichiers de définition de virus font environ 100 Ko et ont donc un impact minimum sur les performances du système lors du téléchargement.

En cas de disponibilité d'une mise à jour de produit ou d'attaque virale, une alerte s'affiche. Une fois alerté, vous pouvez choisir de mettre à jour VirusScan afin d'écarter la menace d'attaque virale.

Recherche automatique de mises à jour

McAfee SecurityCenter est automatiquement configuré pour rechercher les mises à jour de l'ensemble de vos services McAfee toutes les quatre heures lorsque vous êtes connecté à Internet. Le cas échéant, il vous informe à l'aide d'alertes et de messages sonores. Par défaut, SecurityCenter télécharge et installe automatiquement les mises à jour disponibles.

REMARQUE
Dans certains cas, vous serez invité à redémarrer votre ordinateur pour terminer la mise à jour. Avant de redémarrer, assurez-vous d'enregistrer tous vos travaux et de fermer toutes les applications.

Recherche manuelle de mises à jour

Parallèlement à la recherche automatique de mises à jour en ligne toutes les quatre heures, vous pouvez rechercher manuellement des mises à jour à tout moment.

Pour rechercher manuellement des mises à jour VirusScan :

1. Vérifiez que l'ordinateur est connecté à Internet.
2. Cliquez avec le bouton droit de la souris sur l'icône McAfee, puis sélectionnez **Mises à jour**.

   La boîte de dialogue **Mises à jour de McAfee SecurityCenter** s'ouvre.
3. Cliquez sur **Vérifier**.

   Si une mise à jour est disponible, la boîte de dialogue des mises à jour **McAfee VirusScan** s'affiche (Figure 2-15 à la page 45). Pour continuer, cliquez sur **Mettre à jour**.

   Si aucune mise à jour n'est disponible, une boîte de dialogue vous indique que VirusScan est à jour. Pour fermer la boîte de dialogue, cliquez sur **OK**.

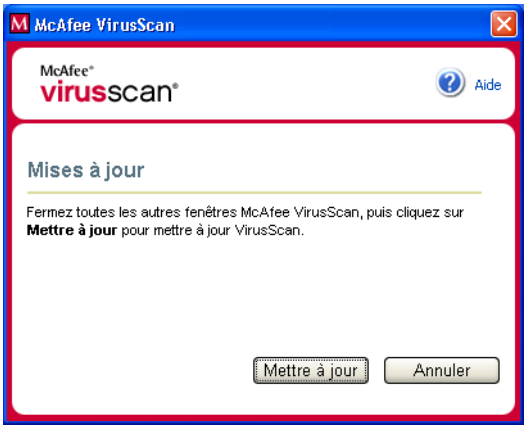


Figure 2-15. Boîte de dialogue des mises à jour

4 Connectez-vous au site Web si vous y êtes invité. L'**Assistant de mise à jour** lance l'installation automatiquement.

5 Une fois la mise à jour installée, cliquez sur **Terminer**.

REMARQUE
Dans certains cas, vous serez invité à redémarrer votre ordinateur pour terminer la mise à jour. Avant de redémarrer, assurez-vous d'enregistrer tous vos travaux et de fermer toutes les applications.

McAfee Personal Firewall Plus 3

Bienvenue dans McAfee Personal Firewall Plus.

Ce logiciel offre une protection avancée à votre ordinateur et à vos données personnelles. Il surveille silencieusement le trafic Internet et signale toute activité suspecte. Ainsi, McAfee Personal Firewall Plus établit une barrière entre votre ordinateur et le réseau.

Ses fonctions sont les suivantes :

- Protéger contre les attaques et tentatives de piratage
- Compléter la protection antivirus
- Surveiller le trafic Internet et l'activité réseau
- Donner l'alerte en cas d'événement potentiellement hostile
- Apporter des informations détaillées sur le trafic Internet suspect
- Intégrer des fonctionnalités de Hackerwatch.org, notamment la constitution de rapports d'événements, l'utilisation d'outils d'autotest et l'envoi d'e-mails de notification à d'autres autorités en ligne
- Fournir le traçage détaillé et la recherche d'événements

Nouvelles fonctions

- **Intégration avancée de HackerWatch.org**
  Le signalement de pirates potentiels n'a jamais été aussi simple. En effet, McAfee Personal Firewall Plus améliore la fonctionnalité de HackerWatch.org, qui permet de soumettre des événements potentiellement nuisibles dans la base de données.

- **Gestion intelligente et étendue des applications**
  Lorsqu'une application cherche à accéder à Internet, Personal Firewall détermine si elle semble fiable ou malveillante. Dans le premier cas, Personal Firewall autorise l'accès automatiquement (à votre place). Pour plus d'informations sur les applications se connectant à Internet, la base de données disponible a été améliorée.

- **Détection avancée des chevaux de Troie**
  McAfee Personal Firewall Plus, qui associe la gestion des connexions des applications à l'utilisation d'une base de données évoluée, vise à détecter et à mieux bloquer les codes potentiellement malveillants. Ces programmes, tels que les chevaux de Troie, risquent de transmettre vos données personnelles par Internet.

- **Amélioration du traçage visuel**
  McAfee Personal Firewall Plus améliore l'outil de traçage des intrus connu sous le nom de Visual Trace. A l'aide de cartes graphiques simples, Visual Trace indique la source des attaques et du trafic hostile à l'échelle mondiale, notamment des informations détaillées de suivi remontant aux adresses IP d'origine. Intégrée à McAfee Personal Firewall Plus, cette fonction s'appuie maintenant sur un plus grand nombre de données géographiques pour affiner visuellement les informations de localisation des intrus. En effet, Visual Trace permet aux utilisateurs de remonter à l'origine des intrusions et d'obtenir, grâce à ces nouvelles données, une meilleure représentation graphique de leurs recherches.

- **Amélioration de la convivialité**
  McAfee Personal Firewall Plus comprend un Assistant de configuration et un Didacticiel utilisateur en guise de références. Bien que le produit soit conçu pour fonctionner sans intervention, McAfee apporte une multitude d'informations destinées à révéler l'intérêt du firewall.

- **Amélioration de la détection d'intrusions**
  Le système de détection d'intrusions (IDS) de Personal Firewall détecte les méthodes d'attaque connues et toute autre activité suspecte. Dans chaque paquet de données, il recherche des transferts ou des moyens de transmission suspects, puis consigne les résultats dans le journal des événements.

- **Amélioration de l'analyse du trafic**
  McAfee Personal Firewall Plus permet aux utilisateurs de visualiser les données entrantes/sortantes de leur ordinateur et d'afficher les connexions des applications, notamment les applications activement « à l'écoute » des connexions ouvertes. Les utilisateurs peuvent ainsi visualiser et agir sur les applications susceptibles de faire l'objet d'une intrusion.

Désinstallation d'autres firewalls

Avant d'installer le logiciel McAfee Personal Firewall Plus, vous devez désinstaller tout autre firewall. Pour ce faire, suivez les instructions de désinstallation de votre firewall.

REMARQUE
Si vous utilisez Windows XP, il est inutile de désactiver le firewall intégré avant d'installer McAfee Personal Firewall Plus. Il est toutefois recommandé de désactiver le firewall intégré. Autrement, vous ne recevrez pas les événements entrants dans le journal de McAfee Personal Firewall Plus.

Définition du firewall par défaut

McAfee Personal Firewall peut gérer les autorisations et le trafic des applications Internet sur votre ordinateur, même en cas de détection de l'activation du firewall Windows.

A son installation, il désactive automatiquement le firewall Windows et devient votre firewall par défaut. Vous bénéficiez alors uniquement des fonctionnalités de McAfee Personal Firewall, notamment celles de messagerie. Si vous activez ensuite le firewall Windows via le Centre de sécurité ou le Panneau de configuration de Windows en laissant les deux firewalls s'exécuter sur votre ordinateur, vous constaterez peut-être une perte partielle de consignation dans McAfee Firewall ainsi qu'une duplication des messages d'état et d'alerte.

REMARQUE

Si les deux firewalls sont activés, McAfee Personal Firewall ne montrera pas toutes les adresses IP bloquées dans son onglet Evénements entrants. Le firewall Windows, qui intercepte généralement et bloque ces événements, empêchera McAfee Personal Firewall de les détecter ou de les consigner. Cependant, McAfee Personal Firewall peut bloquer du trafic supplémentaire en fonction d'autres facteurs de sécurité. Ce trafic sera alors consigné.

Par défaut, la consignation du firewall Windows est désactivée mais, si vous choisissez d'utiliser les deux firewalls, vous pouvez l'activer. Le journal par défaut du firewall Windows est C:\Windows\pfirewall.log.

Pour assurer la protection de votre ordinateur par au moins un firewall, le firewall Windows est automatiquement réactivé lorsque McAfee Personal Firewall est désinstallé.

Si vous désactivez McAfee Personal Firewall ou définissez ses paramètres de sécurité sur **Ouvert** sans activer manuellement le firewall Windows, toute protection par firewall sera supprimée, sauf pour les applications déjà bloquées.

Définition du niveau de sécurité

Vous pouvez configurer des options de sécurité pour indiquer la manière dont Personal Firewall doit réagir lorsqu'il détecte un trafic indésirable. Par défaut, le niveau de sécurité **Standard** est activé. Utilisez ce paramètre si vous êtes un utilisateur débutant du firewall. Si vous êtes un utilisateur expérimenté, vous pouvez définir d'autres paramètres. En mode de sécurité **Standard**, le fait d'autoriser une application à se connecter à Internet revient à lui accorder un accès total. L'accès total permet à l'application d'envoyer ou de recevoir des données non sollicitées sur des ports non-système.

Pour configurer les paramètres de sécurité :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Utilitaires**.
2. Cliquez sur l'icône **Paramètres de sécurité**.
3. Pour définir le niveau de sécurité, faites glisser le curseur jusqu'au niveau souhaité.

   Si vous êtes un utilisateur débutant, acceptez le paramètre par défaut **Standard**. Les niveaux de sécurité vont de Verrouillage à Ouvert.

   - **Verrouillage** : tout le trafic est arrêté. En d'autres termes, vous empêchez toute connexion Internet. Vous pouvez utiliser ce paramètre pour bloquer les ports définis comme étant ouverts dans la page Services système.
   - **Elevé** : vous pouvez d'abord autoriser ou bloquer le type de connexion Internet explicitement nécessaire à une application (par exemple, un accès sortant uniquement). A la demande de l'application partiellement autorisée, vous pouvez ensuite rendre l'accès total. Utilisez ce paramètre si vous êtes un utilisateur expérimenté.
   - **Standard (recommandé)** : dans ce cas, le fait d'autoriser une application à se connecter à Internet revient à lui accorder un accès total. L'accès total permet à l'application d'envoyer ou de recevoir des données non sollicitées sur des ports non-système. Utilisez ce paramètre si vous êtes un utilisateur débutant.
   - **Faible** : toutes les applications sont automatiquement autorisées lorsqu'elles essaient d'accéder à Internet pour la première fois. Toutefois, vous pouvez choisir d'être averti des nouvelles applications autorisées à l'aide d'alertes. Utilisez ce paramètre si vous constatez le non-fonctionnement de certains jeux ou de certaines séquences.
   - **Ouvert** : votre firewall est réellement désactivé. Ce paramètre autorise tout le trafic via Personal Firewall sans filtrage.

     REMARQUE
     Les applications précédemment bloquées le restent lorsque le firewall est défini sur le niveau de sécurité **Ouvert** ou **Désactivé**. Pour empêcher ceci de se produire, vous pouvez modifier les autorisations des applications en **Accès total** ou simplement supprimer la règle d'autorisation **Bloqué** dans la liste **Autorisations**.

4 Sélectionnez d'autres paramètres de sécurité.

REMARQUE
Si plusieurs utilisateurs ont été ajoutés sous Windows XP, ces options sont disponibles uniquement pour l'administrateur.

- **Enregistrer les événements du système de détection d'intrusion (IDS) dans le journal des événements entrants** : si vous sélectionnez cette option, les événements détectés par IDS apparaîtront dans le journal des événements entrants. Ce système détecte les types d'attaque classique et d'autres activités suspectes. Il contrôle chaque paquet de données entrant ou sortant pour détecter les transferts de données ou les moyens de transmission suspects. Il utilise une base de données de signatures à des fins de comparaison et écarte automatiquement les paquets provenant de l'ordinateur en cause.

  IDS recherche des schémas de trafic spécifiques utilisés par les attaquants. Il contrôle chaque paquet reçu par votre machine afin de détecter le trafic suspect ou connu comme une attaque. Par exemple, si Personal Firewall détecte la présence de paquets ICMP, il les analyse pour rechercher des schémas de trafic suspects en comparant le trafic ICMP aux schémas d'attaque connus.

- **Accepter les requêtes de ping ICMP** : le trafic ICMP est principalement utilisé pour réaliser des suivis et des pings. Les pings sont souvent utilisés pour effectuer un test rapide avant une tentative de communication. En cas d'utilisation actuelle ou antérieure d'un programme de partage de fichiers d'égal à égal, vous risquez de recevoir un grand nombre de requêtes de ping. Avec cette option, Personal Firewall autorise toutes les requêtes de ping sans les consigner dans le journal des événements entrants. Sans cette option, il bloque toutes les requêtes de ping qu'il consigne dans le journal des événements entrants.

- **Autoriser les utilisateurs disposant d'un accès restreint à modifier les paramètres de Personal Firewall** : si plusieurs utilisateurs ont été ajoutés sous Windows XP, cochez cette case pour autoriser ceux disposant d'un accès restreint à modifier les paramètres de Personal Firewall.

5 Lorsque vous avez terminé, cliquez sur **OK**.

Test de McAfee Personal Firewall Plus

Pour tester Personal Firewall :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Tester le firewall**.
2. Personal Firewall ouvre Internet Explorer à l'adresse http://www.hackerwatch.org/ (site Web géré par McAfee). Pour tester Personal Firewall, suivez les indications de la page de test Hackerwatch.org.

REMARQUE
Si vous vous connectez à Internet via un serveur proxy ou NAT (Network Address Translation, translation des adresses réseau) à l'instar de la plupart des utilisateurs de réseaux locaux d'entreprise, vous n'obtiendrez pas les bons résultats. Hackerwatch.org permet de tester l'ordinateur à l'origine de la demande. Avec une connexion proxy ou NAT, le serveur transmet votre demande de test de firewall, si bien que Hackerwatch.org teste le mauvais ordinateur. En effet, les résultats obtenus sont ceux du serveur proxy et non ceux de votre ordinateur.

Utilisation de McAfee Personal Firewall Plus

Pour ouvrir Personal Firewall :

Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Afficher le résumé**, **Applications Internet**, **Evénements entrants** ou **Utilitaires**.

À propos de la page Résumé

Le résumé de Personal Firewall comporte quatre pages : Résumé principal, Résumé des applications, Résumé des événements et HackerWatch Summary (Résumé HackerWatch). Les pages de résumé contiennent différents rapports sur les événements entrants récents, l'état des applications et les activités d'intrusion mondiales répertoriées par HackerWatch.org. Elles contiennent également des liens vers les tâches couramment effectuées dans Personal Firewall.

Pour ouvrir les pages de résumé de Personal Firewall, cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Afficher le résumé**. La page Résumé principal apparaît (Figure 3-1 on page 53).

Figure 3-1. Page Résumé principal

Pour passer d'une page de résumé à une autre, utilisez les boutons suivants.

Élément	Description
Modifier l'affichage	Cliquez sur **Modifier l'affichage**, puis sélectionnez une page de résumé dans la liste.
Flèche droite	Cliquez sur la flèche droite pour afficher la page de résumé suivante.
Flèche gauche	Cliquez sur la flèche gauche pour afficher la page de résumé précédente.
Accueil	Cliquez sur l'icône de l'accueil pour revenir à la page **Résumé principal**.

La page Résumé principal fournit les informations suivantes.

Élément	Description
Paramètre de sécurité	L'état du paramètre de sécurité indique le niveau de sécurité sur lequel le firewall est défini. Pour modifier le niveau de sécurité, cliquez sur ce lien.
Événements bloqués	L'état des événements bloqués affiche le nombre d'événements bloqués aujourd'hui. Pour afficher les détails de la page Evénements entrants, cliquez sur ce lien.
Modifications des règles d'application	L'état des règles d'application affiche le nombre de règles d'applications récemment modifiées. Pour afficher la liste des applications autorisées/bloquées et modifier les autorisations des applications, cliquez sur ce lien.

Élément	Description
Nouveautés	**Nouveautés** désigne la dernière application à laquelle a été accordé un accès total à Internet.
Dernier événement	**Dernier événement** affiche les derniers événements entrants. Pour tracer l'événement ou autoriser l'adresse IP, cliquez sur ce lien. Le fait d'autoriser une adresse IP revient à accepter tout le trafic en sa provenance sur votre ordinateur.
Rapport quotidien	**Rapport quotidien** affiche le nombre d'événements entrants bloqués par Personal Firewall aujourd'hui, cette semaine et ce mois. Pour afficher les détails de la page Evénements entrants, cliquez sur ce lien.
Applications actives	**Applications actives** répertorie les applications ouvertes de votre ordinateur qui accèdent à Internet. Pour afficher les adresses IP auxquelles une application se connecte, cliquez sur le programme.
Tâches communes	Pour accéder aux pages de Personal Firewall qui présentent l'activité du firewall et permettent d'exécuter des tâches, cliquez sur un lien de **Tâches communes**.

Pour afficher la page Résumé des applications, cliquez sur **Modifier l'affichage**, puis sélectionnez **Résumé des applications**. La page Résumé des applications fournit les informations suivantes.

Élément	Description
Moniteur de trafic	Le **Moniteur de trafic** présente les volumes de trafic Internet entrant et sortant au cours des dix dernières minutes. Pour afficher les détails du suivi du trafic, cliquez sur le graphique.
Applications actives	**Applications actives** présente la largeur de la bande passante utilisée par les applications les plus actives au cours des dernières 24 heures. **Application** : application qui accède à Internet. **%** : pourcentage de la bande passante utilisé par l'application. **Autorisation** : type de connexion Internet accordé à l'application. **Règle créée** : moment de création de la règle d'application.
Nouveautés	**Nouveautés** désigne la dernière application à laquelle a été accordé un accès total à Internet.
Applications actives	**Applications actives** répertorie les applications ouvertes de votre ordinateur qui accèdent à Internet. Pour afficher les adresses IP auxquelles une application se connecte, cliquez sur le programme.
Tâches communes	Pour accéder aux pages Personal Firewall qui présentent l'état des applications et permettent d'exécuter des tâches relatives aux applications, cliquez sur un lien de **Tâches communes**.

Pour afficher la page Résumé des événements, cliquez sur **Modifier l'affichage**, puis sélectionnez **Résumé des événements**. La page Résumé des événements fournit les informations suivantes.

Élément	Description
Comparaison des ports	L'option **Comparaison des ports** affiche un graphique à secteurs des ports de votre ordinateur les plus fréquemment sollicités au cours des 30 derniers jours. Pour afficher les détails de la page Evénements entrants, cliquez sur le nom d'un port. Par ailleurs, vous pouvez afficher une description du port en déplaçant le pointeur de votre souris sur son numéro.
Premiers attaquants	**Premiers attaquants** affiche les adresses IP les plus fréquemment bloquées, le dernier événement entrant de chaque adresse et le nombre total d'événements entrants au cours des trente derniers jours pour chaque adresse. Pour afficher les détails de la page Evénements entrants, cliquez sur un événement.
Rapport quotidien	**Rapport quotidien** affiche le nombre d'événements entrants bloqués par Personal Firewall aujourd'hui, cette semaine et ce mois. Pour afficher les détails du journal des événements entrants, cliquez sur un nombre.
Dernier événement	**Dernier événement** affiche les derniers événements entrants. Pour tracer l'événement ou autoriser l'adresse IP, cliquez sur ce lien. Le fait d'autoriser une adresse IP revient à accepter tout le trafic en sa provenance sur votre ordinateur.
Tâches communes	Pour accéder aux pages de Personal Firewall qui présentent les détails des événements et permettent d'effectuer des tâches relatives aux événements, cliquez sur un lien de **Tâches communes**.

Pour afficher la page Résumé HackerWatch, cliquez sur **Modifier l'affichage**, puis sélectionnez **HackerWatch Summary**. La page Résumé HackerWatch fournit les informations suivantes.

Élément	Description
Activité mondiale	**World Activity** affiche une carte mondiale qui identifie les activités récemment bloquées et surveillées par HackerWatch.org. Pour ouvrir la carte d'analyse des menaces globales dans HackerWatch.org, cliquez dessus.
Volume des événements	**Event Tracking** affiche le nombre d'événements entrants soumis à HackerWatch.org.
Activité globale des ports	**Global Port Activity** affiche les premiers ports qui sont apparus comme des menaces au cours des 5 derniers jours. Pour afficher le numéro et la description du port, cliquez sur lui.
Tâches communes	Pour accéder aux pages de HackerWatch.org qui présentent des informations sur les activités de piratage dans le monde entier, cliquez sur un lien dans **Common Tasks**.

À propos de la page Applications Internet

Utilisez la page Applications Internet pour afficher la liste des applications autorisées et bloquées.

Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Applications Internet**. La page Applications Internet s'affiche (Figure 3-2).

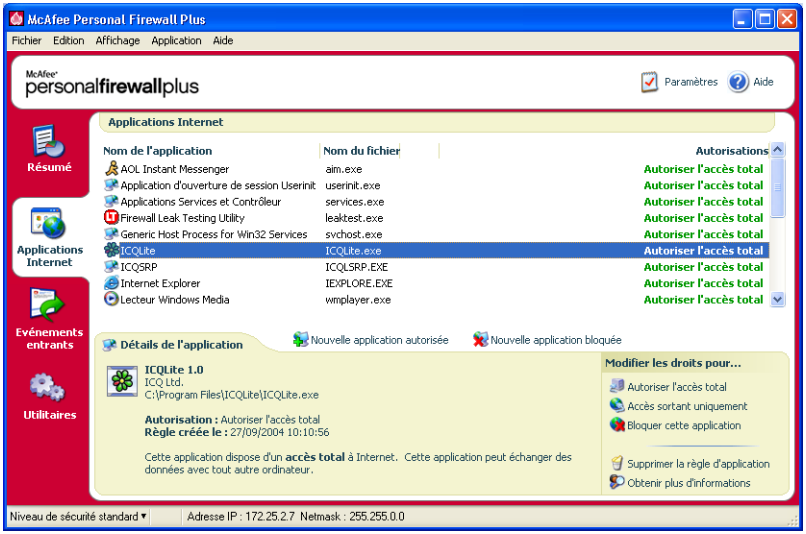


Figure 3-2. Page Applications Internet

La page Applications Internet fournit les informations suivantes.

- Nom des applications
- Nom des fichiers
- Niveaux d'autorisation actuels
- Détails de l'application : chemin d'accès, horodatage des autorisations et description des types d'autorisation

Modification des autorisations

Personal Firewall permet de définir le niveau d'autorisation de chaque application demandant l'accès à Internet.

Pour modifier un niveau d'autorisation :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Applications Internet**.
2. Dans la liste **Autorisations**, cliquez avec le bouton droit de la souris sur le niveau d'autorisation d'une application, puis choisissez un niveau différent :
   - **Autoriser l'accès total** permet à l'application d'envoyer et de recevoir des données.
   - **Accès sortant uniquement** empêche l'application de recevoir des données.
   - **Bloquer cette application** empêche l'application d'envoyer ou de recevoir des données.

     REMARQUE
     Lorsque le firewall est défini sur le niveau de sécurité **Ouvert** ou **Désactivé**, les applications précédemment bloquées le restent. Pour empêcher ceci de se produire, vous pouvez modifier les autorisations des applications en **Accès total** ou simplement supprimer la règle d'autorisation **Bloqué** dans la liste **Autorisations**.

Pour supprimer un niveau d'autorisation :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Applications Internet**.
2. Dans la liste **Autorisations**, cliquez avec le bouton droit de la souris sur le niveau d'autorisation d'une application, puis cliquez sur **Supprimer la règle d'application**.

La prochaine fois que cette application demandera l'accès à Internet, vous pourrez définir son niveau d'autorisation afin de l'ajouter de nouveau dans la liste.

Modification des applications

Pour modifier la liste des applications Internet autorisées et bloquées :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Applications Internet**.
2. Dans la liste **Nom de l'application**, ajoutez ou supprimez des éléments :
   - Pour ajouter une application « autorisée », cliquez sur **Nouvelle application autorisée**, sélectionnez l'application à autoriser, puis cliquez sur **Ouvrir**.
   - Pour ajouter une application « bloquée », cliquez sur **Nouvelle application bloquée**, sélectionnez l'application à bloquer, puis cliquez sur **Ouvrir**.
   - Pour supprimer une application de la liste, cliquez sur **Supprimer la règle d'application**.

À propos de la page Evénements entrants

La page Evénements entrants permet d'afficher le journal des événements entrants généré lorsque Personal Firewall bloque un trafic Internet non sollicité.

Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Evénements entrants**. La page Evénements entrants s'affiche (Figure 3-3).

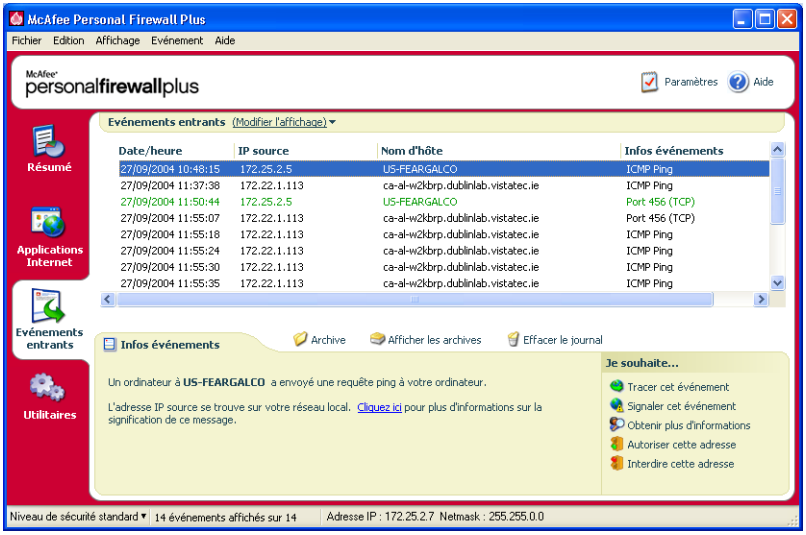


Figure 3-3. Page Evénements entrants

La page Evénements entrants fournit les informations suivantes.

- Horodatage
- Adresses IP source
- Noms d'hôte
- Noms de service ou d'application
- Détails des événements : types de connexion, ports de connexion et description des événements de port

Compréhension des événements

À propos des adresses IP

Les adresses IP sont des nombres. Plus particulièrement, chaque adresse IP est constituée de quatre nombres compris entre 0 et 255, qui identifient un lieu spécifique vers lequel le trafic peut être dirigé sur Internet.

Adresses IP spéciales

Certaines adresses IP se présentent différemment pour diverses raisons.

Adresses IP non routables : elles sont également appelées « Espace d'adressage IP privé ». Ces adresses IP ne peuvent pas être utilisées sur Internet. Les blocs d'adresses IP privées sont 10.x.x.x, 172.16.x.x - 172.31.x.x et 192.168.x.x.

Adresses IP en boucle : ces adresses sont utilisées à des fins de test. Le trafic envoyé à ce bloc est renvoyé au périphérique qui a généré le paquet. Essentiellement utilisé à des fins de tests matériels et logiciels, il ne quitte jamais le périphérique. Le bloc d'adresses IP en boucle est 127.x.x.x.

Adresse IP nulle : adresse non valide. Elle apparaît lorsque l'adresse IP du trafic était vierge. De toute évidence, elle est anormale et signifie souvent que l'expéditeur masque délibérément l'origine du trafic. L'expéditeur aura une réponse à son trafic uniquement si le paquet est reçu par une application en mesure de comprendre son contenu, notamment des instructions propres à l'application en question. Toute adresse commençant par 0 (0.x.x.x) est une adresse nulle. Par exemple, 0.0.0.0 est une adresse IP nulle.

Événements provenant de 0.0.0.0

Si vous détectez des événements provenant de l'adresse IP 0.0.0.0, il existe deux causes probables. L'un des cas de figure est le plus courant : pour une raison indéterminée, votre ordinateur a reçu un paquet au format non valide. Internet n'est pas toujours fiable à 100 %, d'où la possibilité de paquets au format non valide. Comme Personal Firewall détecte les paquets avant que ceux-ci ne soient validés par TCP/IP, il risque de les signaler comme événements.

L'autre cas de figure se présente lorsque l'adresse IP source est bidon ou fausse. Le paquet bidon peut signifier qu'un utilisateur est à la recherche d'un cheval de Troie et teste votre ordinateur. N'oubliez pas que Personal Firewall bloque cette tentative et que votre ordinateur est donc protégé.

Événements provenant de l'adresse 127.0.0.1

Les événements indiquent parfois une adresse IP source de type 127.0.0.1. Il s'agit d'une adresse IP spéciale, appelée adresse de bouclage.

En réalité, 127.0.0.1 désigne toujours l'ordinateur sur lequel vous vous trouvez, quel qu'il soit. Cette adresse est également appelée « localhost » (hôte local) car le nom d'ordinateur localhost sera toujours traduit par l'adresse IP 127.0.0.1.

Votre ordinateur tente-t-il donc de s'auto-pirater ? Un cheval de Troie ou un logiciel espion cherche-t-il à prendre le contrôle de votre ordinateur ? En aucun cas. De nombreux programmes légitimes utilisent l'adresse de bouclage à des fins de communication entre leurs composants. Par exemple, de nombreux serveurs de messagerie ou serveurs Web personnels sont configurables via une interface Web, généralement accessible depuis une adresse de type http://localhost/.

Comme Personal Firewall autorise toutefois le trafic provenant de ces programmes, il est fort probable que l'adresse IP source soit bidon ou fausse si vous détectez des événements provenant de 127.0.0.1. Le paquet bidon indique généralement un utilisateur à la recherche d'un cheval de Troie. N'oubliez pas que Personal Firewall bloque cette tentative et que votre ordinateur est donc protégé. De toute évidence, il est inutile de signaler les événements provenant de 127.0.0.1.

Toutefois, certains programmes, notamment Netscape version 6.2 ou ultérieure, vous demandent d'ajouter 127.0.0.1 dans la liste des adresses IP autorisées. Les composants de ces programmes communiquent entre eux de telle manière que Personal Firewall ne peut pas déterminer si le trafic est local ou non.

Par exemple, avec Netscape 6.2, vous devez autoriser l'adresse 127.0.0.1 pour pouvoir utiliser votre liste d'amis. Si vous détectez du trafic provenant de 127.0.0.1 et, si toutes les applications de votre ordinateur fonctionnent normalement, vous pouvez donc bloquer ce trafic en toute sécurité. Toutefois, si un programme (tel que Netscape) rencontre des difficultés, ajoutez 127.0.0.1 dans la liste des adresses IP autorisées de Personal Firewall, puis déterminez si le problème est résolu.

Si le problème est résolu, vous serez confronté à l'alternative suivante : si vous autorisez 127.0.0.1, votre programme fonctionnera mais vous serez davantage exposé aux attaques bidon ; si vous n'autorisez pas cette adresse, votre programme ne fonctionnera pas mais vous demeurerez protégé contre ce trafic malveillant.

Événements provenant d'ordinateurs de votre réseau local

Des événements peuvent être générés à partir d'ordinateurs de votre réseau local (LAN). Pour indiquer que ces événements proviennent d'un emplacement « proche de chez vous », Personal Firewall les affiche en vert.

Lors de la configuration d'un réseau local d'entreprise, il est généralement utilisé l'option **Autoriser tous les ordinateurs du réseau LAN** de la page Adresses IP autorisées.

Toutefois, il est important de noter que, dans certaines situations, votre réseau « local » peut être aussi dangereux, voire plus, que le réseau extérieur. Ceci se vérifie notamment lorsque vous êtes connecté à un réseau public à large bande passante, par exemple, via un modem DSL ou câble. Dans ce cas, il est préférable de ne pas sélectionner l'option **Autoriser tous les ordinateurs du réseau LAN**.

De même, si vous utilisez une connexion de réseau domestique à large bande, vous devrez ajouter manuellement les adresses IP de vos ordinateurs locaux dans la liste Adresses IP autorisées. N'oubliez pas que vous pouvez utiliser des adresses de type .255 pour autoriser un bloc entier. Par exemple, vous pouvez autoriser votre réseau ICS (réseau de partage de connexion Internet) entier en autorisant l'adresse IP 192.168.255.255.

Événements provenant d'adresses IP privées

Les adresses IP au format 192.168.xxx.xxx, 10.xxx.xxx.xxx et 172.16.0.0 - 172.31.255.255 sont appelées adresses IP non routables ou privées. Ces adresses IP ne doivent jamais quitter votre réseau et peuvent être autorisées la plupart du temps.

Le bloc 192.168 est utilisé avec le partage de connexion Internet de Microsoft (ICS). Si vous utilisez ICS et si vous détectez des événements provenant de ce bloc d'adresses IP, vous voudrez peut-être ajouter l'adresse IP 192.168.255.255 dans votre liste d'adresses IP autorisées. Vous autoriserez ainsi la totalité du bloc d'adresses 192.168.xxx.xxx.

Si vous n'êtes pas connecté à un réseau privé et si vous détectez des événements provenant de ces plages d'adresses IP, l'adresse IP source peut être bidon ou fausse. Le paquet bidon signifie généralement qu'un utilisateur est à la recherche d'un cheval de Troie. N'oubliez pas que Personal Firewall bloque cette tentative et que votre ordinateur est donc protégé.

Puisque les adresses IP privées désignent des ordinateurs différents selon le type de votre réseau, il est inutile de signaler ces événements.

Affichage des événements dans le journal des événements entrants

Le journal des événements entrants permet d'afficher de manière pratique les événements de différentes manières. L'affichage par défaut limite l'affichage aux événements survenus le jour même. Personal Firewall permet d'afficher les événements survenus au cours de cette semaine ou le journal complet.

Il permet également d'afficher les événements entrants de jours spécifiques, d'adresses Internet spécifiques (adresses IP) ou des événements avec les mêmes informations.

Pour plus d'informations sur un événement, cliquez dessus : les informations s'affichent alors dans la zone **Infos événements**, au bas de la page Evénements entrants.

Affichage des événements de la journée

Pour afficher uniquement les événements survenus dans la journée :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Evénements entrants**.
2. Dans le menu **Affichage**, cliquez sur **Afficher les événements de la journée**.

   Le journal des événements entrants affiche uniquement les événements survenus aujourd'hui.

Affichage des événements de cette semaine

Pour afficher les événement survenus cette semaine :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Dans le menu **Affichage**, cliquez sur **Afficher les événements de cette semaine**.

   Le journal des événements entrants affiche uniquement les événements survenus cette semaine.

Affichage du journal complet des événements entrants

Pour afficher tous les événements du journal des événements entrants :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Dans le menu **Affichage**, cliquez sur **Afficher le journal complet**.

   La page Evénements entrants affiche tous les événements du journal sans les archives.

Affichage des événements du jour sélectionné uniquement

Cette fonction permet de consulter les événements survenus un jour donné. Tous les événements n'ayant pas eu lieu ce jour-là sont masqués.

Pour afficher tous les événements survenus un jour donné :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Dans le menu **Affichage**, cliquez sur **Afficher uniquement les événements du jour sélectionné**.

   Les événements de la journée apparaissent dans le journal des événements entrants.

Affichage des événements relatifs à l'adresse Internet sélectionnée uniquement

Cette fonction est utile lorsque vous devez consulter d'autres événements provenant d'une adresse Internet spécifique. Tous les autres événements sont masqués.

Pour afficher tous les événements provenant d'une adresse Internet spécifique :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Dans le menu **Affichage**, cliquez sur **Afficher uniquement les événements relatifs à l'adresse Internet sélectionnée**.

   Les événements provenant de l'adresse Internet sélectionnée s'affichent dans le journal des événements entrants.

Affichage des événements dont les informations sont identiques uniquement

Cette option permet de voir si le journal contient d'autres événements dont les informations (colonne **Infos événements**) sont identiques à celles de l'événement sélectionné. Vous pouvez ainsi déterminer la fréquence de cet événement et la similitude de la source. La colonne Infos événements fournit une description de l'événement et, le cas échéant, le nom du programme ou du service qui utilise ce port.

Pour afficher tous les événements dont les informations sont identiques :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Dans le menu **Affichage**, cliquez sur **Afficher uniquement les événements dont les informations sur les événements sont identiques**.

   Les événements avec les mêmes informations apparaissent dans le journal des événements entrants.

Réponse aux événements entrants

Vous pouvez non seulement obtenir des détails du journal des événements entrants mais aussi effectuer un traçage visuel des adresses IP associées à un événement ou obtenir des informations sur le site Web HackerWatch.org (communauté anti-piratage en ligne).

Traçage de l'événement sélectionné

Pour effectuer un traçage visuel des adresses IP associées à un événement entrant du journal :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Cliquez avec le bouton droit de la souris sur l'événement à tracer, puis sélectionnez **Tracer l'événement sélectionné**.

   Vous pouvez également double-cliquer sur l'événement.

   Par défaut, Personal Firewall lance un traçage visuel à l'aide du programme intégré Visual Trace.

Consultation du site HackerWatch.org

Sur le site de la communauté anti-piratage HackerWatch.org, vous pouvez également essayer d'obtenir plus d'informations sur un événement :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Localisez et sélectionnez l'événement sur lequel vous souhaitez obtenir plus d'informations.
3. Dans le menu **Evénement**, choisissez **Plus d'informations sur l'événement**.

Votre navigateur Web s'ouvre. Vous pouvez alors accéder au site www.hackerwatch.org pour obtenir plus d'informations sur le type de l'événement et déterminer s'il est nécessaire de le signaler.

Notification d'un événement

Pour signaler un événement représentant selon vous une attaque de votre ordinateur :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Cliquez sur l'événement à signaler, puis sur **Signaler cet événement** dans le volet inférieur droit.

   Personal Firewall transmet l'événement au site Web HackerWatch.org en utilisant votre ID unique.

Abonnement à HackerWatch.org

Lorsque vous ouvrez la page Résumé de Personal Firewall pour la première fois, celui-ci contacte le site HackerWatch.org afin de générer votre ID utilisateur unique. Si vous êtes déjà inscrit, votre abonnement est automatiquement validé. Si vous êtes un nouvel utilisateur, vous devez entrer un pseudonyme et une adresse e-mail, puis cliquer sur le lien de validation dans l'e-mail de confirmation de HackerWatch.org pour pouvoir utiliser les fonctions de filtrage/transmission électronique d'événements à ce site Web.

Vous pouvez signaler des événements à HackerWatch.org sans valider votre ID utilisateur. Cependant, pour filtrer des événements et les transmettre par e-mail à un ami, vous devez vous abonner au service.

L'abonnement au service permet le suivi des envois : il nous permet de vous prévenir lorsque HackerWatch.org a besoin de plus d'informations ou lorsqu'une intervention de votre part est nécessaire. En outre, il nous permet de valider les informations que nous recevons.

Toutes les adresses e-mails fournies à HackerWatch.org restent confidentielles. Si un fournisseur d'accès Internet soumet une requête en vue d'obtenir plus informations, sa demande est routée via HackerWatch.org mais votre adresse e-mail n'est jamais divulguée.

Autorisation d'une adresse

Si le journal consigne un événement entrant avec une adresse IP à autoriser, vous pouvez configurer Personal Firewall pour qu'il autorise définitivement les connexions en sa provenance :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Cliquez avec le bouton droit de la souris sur l'événement dont vous voulez autoriser l'adresse IP, puis cliquez sur **Autoriser l'adresse IP source**.
3. Vérifiez que l'adresse IP affichée dans le message de confirmation est correcte, puis cliquez sur **OK**.

   L'adresse IP est ajoutée dans la liste **Adresses IP autorisées**.

Pour vérifier que l'adresse IP a été ajoutée :

1. Cliquez sur l'onglet **Utilitaires**.
2. Cliquez sur l'icône **Adresses IP autorisées ou interdites**, puis sur l'onglet **Adresses IP autorisées**.

   L'adresse IP apparaît dans la liste **Adresses IP autorisées**.

Interdiction d'une adresse

Si une adresse IP apparaît dans le journal des événements entrants, le trafic en provenance de cette adresse est bloqué. Par conséquent, l'interdiction d'une adresse ne vous apportera aucune protection supplémentaire, sauf si votre ordinateur est doté de ports délibérément ouverts à l'aide de la fonction Services système ou exécute une application autorisée à recevoir du trafic.

Ajoutez une adresse IP dans votre liste de sites interdits uniquement si un ou plusieurs ports sont délibérément ouverts sur votre ordinateur et si, pour une raison, vous estimez nécessaire d'empêcher cette adresse d'accéder aux ports ouverts.

Si le journal des événements entrants contient une adresse IP à interdire, vous pouvez configurer Personal Firewall pour qu'il bloque définitivement les connexions en sa provenance :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Cliquez avec le bouton droit de la souris sur l'événement dont vous voulez interdire l'adresse IP, puis cliquez sur **Interdire l'adresse IP source**.
3. Vérifiez que l'adresse IP affichée dans le message de confirmation est correcte, puis cliquez sur **OK**.

   L'adresse est ajoutée dans la liste **Adresses IP interdites**.

Pour vérifier que l'adresse IP a été ajoutée :

1. Cliquez sur l'onglet **Utilitaires**.
2. Cliquez sur l'icône **Adresses IP autorisées ou interdites**, puis sur l'onglet **Adresses IP interdites**.

   L'adresse IP apparaît dans la liste **Adresses IP interdites**.

Gestion du journal des événements entrants

La page Evénements entrants permet de gérer les événements du journal des événements entrants généré lorsque Personal Firewall bloque un trafic Internet non sollicité.

Archivage du journal des événements entrants

Vous pouvez archiver le journal des événements entrants en cours dans un fichier de votre disque dur. Nous vous recommandons d'archiver régulièrement le journal des événements car il peut devenir très volumineux.

Pour archiver le journal des événements entrants :

1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.

2 Dans le menu **Fichier**, cliquez sur **Archiver le journal**.

3 Un message de confirmation s'affiche. Cliquez sur **Oui**.

4 Cliquez sur **Enregistrer** pour enregistrer l'archive à l'emplacement par défaut ou naviguez jusqu'à l'emplacement de votre choix.

Affichage d'un journal archivé des événements entrants

Vous pouvez afficher un journal des événements entrants précédemment archivé.

> **REMARQUE**
> Avant d'afficher vos archives, vous devez archiver le journal des événements entrants en cours. Si vous négligez cette opération, le journal des événements entrants en cours sera effacé lorsque vous afficherez une archive.

1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.

2 Dans le menu Fichier, cliquez sur **Afficher les journaux archivés**.

3 Cliquez sur le nom du fichier d'archive (vous devrez peut-être naviguer dans le système pour y accéder), puis cliquez sur **Ouvrir**.

Les données archivées s'affichent dans le journal des événements entrants.

Effacement du contenu du journal des événements entrants

Vous pouvez effacer la totalité du contenu du journal des événements entrants.

> **REMARQUE**
> Une fois le contenu du journal effacé, vous ne pourrez plus le récupérer. Si vous pensez en avoir besoin ultérieurement, archivez-le.

1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.

2 Dans le menu **Fichier**, cliquez sur **Effacer le journal**.

3 Un message de confirmation s'affiche. Cliquez sur **Oui**.

Le journal des événements ne contient plus aucune entrée.

Exportation des événements affichés

Vous pouvez exporter le journal des événements dans un fichier texte pour les besoins de votre fournisseur d'accès Internet, de votre support technique ou des personnes chargées de faire appliquer la loi.

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Dans le menu Fichier, cliquez sur **Exporter les événements affichés**.
3. Naviguez jusqu'à l'emplacement à utiliser pour l'enregistrement des événements.
4. Renommez le fichier si nécessaire, puis cliquez sur **Enregistrer**.

   Vos événements sont enregistrés dans un fichier au format .txt à l'emplacement choisi.

Copie d'un événement dans le Presse-papiers

Vous pouvez copier un événement dans le Presse-papiers pour le coller dans un fichier texte à l'aide du Bloc-notes.

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Dans le journal, cliquez sur l'événement entrant à exporter.
3. Dans le menu **Edition**, cliquez sur **Copier l'événement sélectionné dans le Presse-papiers**.
4. Ouvrez le Bloc-notes :

   Cliquez sur le bouton Démarrer de Windows, pointez sur Programmes et sur Accessoires, puis sélectionnez Bloc-notes.
5. Dans le menu **Edition**, cliquez sur **Coller**. L'événement s'affiche dans le Bloc-notes. Répétez cette procédure pour tous les événements souhaités.
6. Sauvegardez le fichier Bloc-notes en lieu sûr.

Suppression de l'événement sélectionné

Vous pouvez supprimer des entrées du journal des événements entrants.

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Evénements entrants**.
2. Dans le journal, cliquez sur l'événement entrant à supprimer.
3. Dans le menu **Edition**, cliquez sur **Supprimer l'événement sélectionné**.

   L'événement est supprimé du journal.

À propos des alertes

Nous vous recommandons vivement de vous familiariser avec les différents types d'alerte que vous pouvez rencontrer en utilisant Personal Firewall. Passez en revue les types d'alerte et les réponses possibles de façon à les traiter en toute confiance.

REMARQUE
Des recommandations peuvent vous aider à décider de la gestion d'une alerte. Pour afficher les recommandations dans les alertes, cliquez sur l'onglet **Utilitaires**, puis sur l'icône **Paramètres d'alerte**. Dans la liste **Recommandations intelligentes**, sélectionnez **Utiliser les recommandations intelligentes** (option par défaut) ou **Afficher uniquement les recommandations intelligentes**.

Alertes rouges

Les alertes rouges contiennent des informations importantes à traiter immédiatement.

- **L'application Internet a été bloquée** : cette alerte s'affiche lorsque Personal Firewall empêche une application d'accéder à Internet. Par exemple, si une alerte relative à un cheval de Troie s'affiche, McAfee refuse automatiquement l'accès Internet au programme et recommande de rechercher des virus sur l'ordinateur.
- **L'application demande l'accès à Internet** : cette alerte s'affiche lorsque Personal Firewall détecte du trafic Internet ou réseau pour de nouvelles applications (niveau de sécurité standard ou élevé).
- **L'application a été modifiée** : cette alerte s'affiche lorsque Personal Firewall détecte la modification d'une application précédemment autorisée à accéder à Internet. Si vous n'avez pas récemment mis à niveau l'application en question, réfléchissez bien avant de lui accorder l'accès à Internet (niveau de sécurité faible, standard ou élevé).
- **L'application demande l'accès au serveur** : cette alerte s'affiche lorsque Personal Firewall détecte qu'une application précédemment autorisée à accéder à Internet demande un accès en qualité de serveur (niveau de sécurité élevé).

REMARQUE
Le paramètre par défaut de Windows XP SP2 Mises à jour automatiques télécharge et installe des mises à jour du système d'exploitation Windows et d'autres programmes Microsoft de votre ordinateur sans vous en informer. Lorsqu'une application Microsoft est modifiée à partir d'une des mises à jour silencieuses de Windows, des alertes McAfee Personal Firewall apparaîtront lors de la prochaine exécution de cette application.

IMPORTANT
Vous devez autoriser aux applications l'accès Internet nécessaire pour des mises à jour de produits en ligne (par exemple, les services McAfee).

L'application Internet a été bloquée

Si une alerte relative à un cheval de Troie s'affiche (Figure 3-4), Personal Firewall refuse automatiquement l'accès Internet au programme et recommande de rechercher des virus sur votre ordinateur.

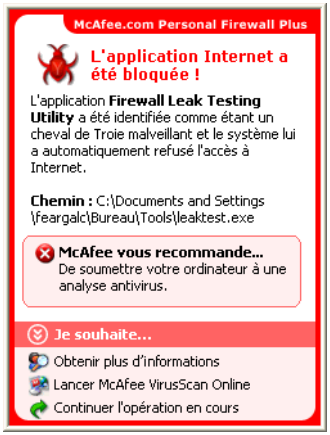


Figure 3-4. L'application Internet a été bloquée

Consultez la description générale de l'événement, puis sélectionnez l'une des options suivantes :

- Cliquez sur **Obtenir plus d'informations** pour afficher les détails de l'événement entrant du journal (pour plus d'informations, reportez-vous à la section *À propos de la page Evénements entrants* à la page 58).
- Cliquez sur **Lancer McAfee VirusScan Online** pour procéder à la recherche de virus.
- Cliquez sur **Continuer l'opération en cours** si l'action entreprise par Personal Firewall vous convient.

L'application demande l'accès à Internet

Si vous avez sélectionné un niveau de sécurité **Standard** ou **Elevé**, Personal Firewall affiche un message d'alerte (Figure 3-5) lorsqu'il détecte du trafic Internet ou réseau pour des applications nouvelles ou modifiées.

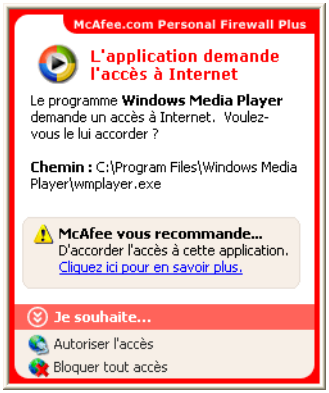


Figure 3-5. L'application demande l'accès à Internet

Suite à un message d'avertissement sur l'accès Internet de l'application, **cliquez ici pour en savoir plus** (le cas échéant). Ce lien est disponible uniquement si Personal Firewall est configuré pour utiliser les recommandations intelligentes.

McAfee peut ne pas reconnaître l'application qui tente d'accéder à Internet (Figure 3-6).

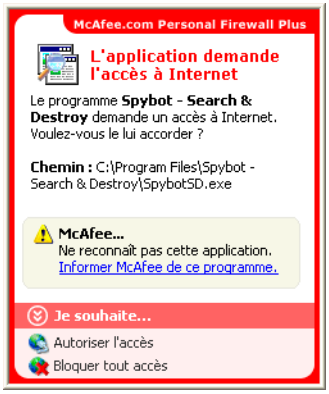


Figure 3-6. Application non reconnue

McAfee n'est donc pas en mesure de vous recommander le mode de gestion de l'application. Vous pouvez signaler l'application en question à McAfee en cliquant sur **Informer McAfee de ce programme**. Une page Web de demande d'informations liées à l'application apparaît. Veuillez fournir toutes les informations à votre disposition.

Nos opérateurs HackerWatch combinent les informations envoyées et d'autres outils de recherche pour déterminer si une application mérite d'être répertoriée dans notre base de données d'applications connues et, le cas échéant, la manière dont elle doit être gérée par Personal Firewall.

Consultez la description générale de l'événement, puis sélectionnez l'une des options suivantes :

- Cliquez sur **Autoriser l'accès** pour permettre à l'application d'envoyer ou de recevoir des données non sollicitées sur des ports non-système.
- Cliquez sur **Bloquer tout accès** pour empêcher l'application d'envoyer ou de recevoir des données.

L'application a été modifiée

Si vous avez sélectionné le niveau de sécurité **Faible**, **Standard** ou **Elevé** dans les paramètres de sécurité, Personal Firewall affiche une alerte (Figure 3-7) lorsqu'il détecte qu'une application précédemment autorisée à accéder à Internet a été modifiée. Si vous n'avez pas récemment mis à niveau l'application en question, réfléchissez bien avant de lui accorder l'accès à Internet.

Figure 3-7. L'application a été modifiée

Consultez la description générale de l'événement, puis sélectionnez l'une des options suivantes :

- Cliquez sur **Autoriser l'accès** pour permettre à l'application d'envoyer ou de recevoir des données non sollicitées sur des ports non-système.
- Cliquez sur **Bloquer tout accès** pour empêcher l'application d'envoyer ou de recevoir des données.

L'application demande l'accès au serveur

Si vous avez choisi un niveau de sécurité **Elevé** dans les paramètres de sécurité, Personal Firewall affiche une alerte (Figure 3-8) lorsqu'une application précédemment autorisée à accéder à Internet demande l'accès en qualité de serveur.

Figure 3-8. L'application demande l'accès au serveur

Par exemple, une alerte s'affiche lorsque MSN Messenger demande l'accès au serveur pour envoyer un fichier au cours d'une discussion en ligne.

Consultez la description générale de l'événement, puis sélectionnez l'une des options suivantes :

- Cliquez sur **Autoriser l'accès au serveur** pour permettre à l'application d'envoyer et de recevoir des données.
- Cliquez sur **Autoriser uniquement l'accès sortant** pour empêcher l'application de recevoir des données.
- Cliquez sur **Bloquer tout accès** pour empêcher l'application d'envoyer ou de recevoir des données.

Alertes vertes

Les alertes vertes vous informent des modifications apportées à Personal Firewall. Par exemple, elles vous indiquent le nom des applications auxquelles Personal Firewall a automatiquement accordé un accès Internet ou vous signalent de nouvelles règles d'application.

Programme autorisé à accéder à Internet : cette alerte s'affiche lorsque Personal Firewall autorise automatiquement l'accès Internet à toutes les applications nouvelles ou modifiées, puis émet une notification (niveau de sécurité faible). Par exemple, une application modifiée est un programme dont les règles ont été modifiées pour lui accorder un accès automatique à Internet.

Programme autorisé à accéder à Internet

Si vous avez sélectionné le niveau de sécurité **Faible** dans les paramètres de sécurité, Personal Firewall autorise automatiquement l'accès Internet à toutes les applications nouvelles ou modifiées, puis émet une alerte (Figure 3-9).

Figure 3-9. Programme autorisé à accéder à Internet

Consultez la description générale de l'événement, puis sélectionnez l'une des options suivantes :

- Cliquez sur **Afficher le journal des applications** pour consulter les détails de l'événement dans le journal des applications Internet (pour plus d'informations, reportez-vous à la section *À propos de la page Applications Internet* à la page 56).
- Cliquez sur **Désactiver ce type d'alerte** pour empêcher l'affichage des alertes de ce type.
- Cliquez sur **Continuer l'opération en cours** si l'action entreprise par Personal Firewall vous convient.

Alertes bleues

Les alertes bleues ne sont qu'informatives. Elles ne nécessitent aucune réponse.

- **Tentative de connexion bloquée** : cette alerte s'affiche lorsque Personal Firewall bloque du trafic Internet ou réseau non sollicité. (niveau de sécurité faible, standard ou élevé).

Tentative de connexion bloquée

Si vous avez sélectionné un niveau de sécurité **Faible**, **Standard** ou **Elevé**, Personal Firewall affiche une alerte (Figure 3-10) lorsqu'il bloque du trafic Internet ou réseau non sollicité.

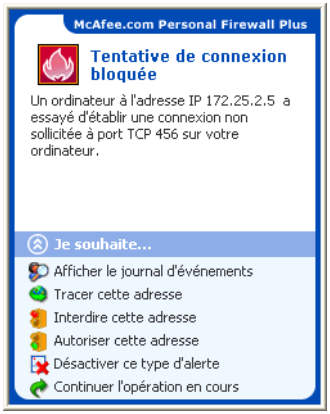


Figure 3-10. Tentative de connexion bloquée

Consultez la description générale de l'événement, puis sélectionnez l'une des options suivantes :

- Cliquez sur **Afficher le journal d'événements** pour consulter les détails sur l'événement entrant dans le journal de Personal Firewall (pour plus d'informations, reportez-vous à la section *À propos de la page Evénements entrants* à la page 58).
- Cliquez sur **Tracer cette adresse** pour effectuer un traçage visuel des adresses IP relatives à cet événement.
- Cliquez sur **Interdire cette adresse** pour empêcher cette adresse d'accéder à votre ordinateur. L'adresse est ajoutée dans la liste Adresses IP interdites.
- Cliquez sur **Autoriser cette adresse** pour autoriser cette adresse IP à accéder à votre ordinateur.
- Cliquez sur **Continuer l'opération en cours** si l'action entreprise par Personal Firewall vous convient.

McAfee Privacy Service 4

Nous vous remercions d'avoir acheté le logiciel McAfee® Privacy Service™. Ce logiciel offre une protection avancée pour vous, votre famille, vos données personnelles et votre ordinateur.

Fonctions

Cette version de McAfee Privacy Service inclut les fonctions suivantes :

- Blocage des pixels invisibles : bloque les pixels invisibles (objets obtenus sur des sites Web potentiellement dangereux) pour qu'ils ne soient pas chargés à partir des pages Web consultées.
- Blocage des fenêtres instantanées : empêche l'affichage des fenêtres instantanées lorsque vous naviguez sur Internet.
- Shredder : McAfee Shredder protège votre confidentialité en supprimant rapidement et en toute sécurité les fichiers indésirables.

L'administrateur

L'administrateur détermine quels utilisateurs peuvent accéder à Internet, à quel moment et ce qu'ils peuvent faire sur Internet.

REMARQUE
L'administrateur est considéré comme un adulte et, en tant que tel, il peut accéder à tous les sites Web, mais il est invité à autoriser ou à refuser la transmission des informations personnelles identifiables ajoutées.

Assistant de configuration

L'assistant de configuration vous permet de créer l'administrateur (si ce n'est pas déjà fait), de gérer les paramètres généraux, d'entrer des données personnelles et d'ajouter des utilisateurs.

REMARQUE
Mémorisez votre mot de passe d'administrateur et votre réponse de sécurité afin de pouvoir vous connecter à Privacy Service. Si vous ne parvenez pas à vous connecter, vous ne pourrez pas utiliser Privacy Service ni Internet. Gardez votre mot de passe confidentiel. Ainsi, vous seul pourrez modifier les paramètres de Privacy Service.

Pour fonctionner correctement, certains sites Web requièrent l'activation des cookies.

Privacy Service accepte toujours les cookies de McAfee.com.

Récupération du mot de passe administrateur

Si vous avez oublié votre mot de passe administrateur, vous pouvez le retrouver grâce aux informations de sécurité que vous avez entrées lorsque vous avez créé le profil Administrateur.

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, placez le curseur sur **Privacy Service**, puis sélectionnez **Connexion**.
2. Sélectionnez **Administrateur** dans le menu déroulant **Nom d'utilisateur**.
3. Cliquez sur **Vous avez oublié votre mot de passe ?**

   Entrez la réponse à la question de sécurité qui s'affiche et cliquez sur **Mot de passe**. Un message indiquant votre mot de passe apparaît. Si vous avez oublié la réponse à la question de sécurité, contactez le Service clientèle.

L'utilisateur au démarrage

L'utilisateur au démarrage est automatiquement connecté à Privacy Service au démarrage de l'ordinateur.

Par exemple, si un utilisateur passe plus de temps que d'autres sur l'ordinateur ou sur Internet, vous pouvez le définir comme utilisateur au démarrage. Lorsque l'utilisateur au démarrage utilise l'ordinateur, il n'a pas besoin de se connecter à Privacy Service.

Si vous avez de jeunes enfants, vous pouvez également définir le plus jeune comme utilisateur au démarrage. Ainsi, lorsqu'un utilisateur plus âgé utilise l'ordinateur, il peut se déconnecter du compte du plus jeune, puis se reconnecter avec ses propres nom d'utilisateur et mot de passe. Cette précaution empêche les utilisateurs les plus jeunes de consulter des sites Web inappropriés.

Ouverture de McAfee Privacy Service

Lors de l'installation de McAfee Privacy Service, l'icône McAfee apparaît dans la barre d'état système Windows située près de l'horloge système. Cette icône vous permet d'accéder à McAfee Privacy Service, à McAfee SecurityCenter et aux autres produits McAfee installés sur votre ordinateur.

Ouverture de Privacy Service et connexion

Pour ouvrir Privacy Service :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, placez le curseur sur **Privacy Service**, puis sélectionnez **Connexion**.
2. Sélectionnez votre nom d'utilisateur dans le menu déroulant **Nom d'utilisateur**.
3. Entrez votre mot de passe dans le champ prévu à cet effet.
4. Cliquez sur **Connexion**.

REMARQUE
Si **Déconnexion** apparaît à la place de **Connexion**, cela signifie que vous êtes déjà connecté.

Désactivation de Privacy Service

Vous devez être connecté à Privacy Service en tant qu'administrateur pour pouvoir le désactiver.

Pour désactiver Privacy Service :

Cliquez avec le bouton droit de la souris sur l'icône McAfee , placez le curseur sur **Privacy Service**, puis sélectionnez **Déconnexion**.

REMARQUE
Si **Connexion** apparaît à la place de **Déconnexion**, cela signifie que vous êtes déjà déconnecté.

Mise à jour de McAfee Privacy Service

McAfee SecurityCenter recherche régulièrement les mises à jour de Privacy Service lorsque votre ordinateur fonctionne et qu'il est connecté à Internet. Si une mise à jour est disponible, McAfee SecurityCenter vous propose de procéder à son installation immédiatement ou de la remettre à plus tard.

Pour rechercher manuellement les mises à jour, cliquez sur l'icône Mises à jour située dans le volet supérieur.

Désinstallation et réinstallation de Privacy Service

Vous devez être connecté à Privacy Service en tant qu'administrateur pour pouvoir le désinstaller.

REMARQUE
Lorsque vous désinstallez Privacy Service, vous supprimez également toutes les données associées.

Désinstallation de Privacy Service

1. Enregistrez votre travail et fermez toutes les applications ouvertes.
2. Ouvrez le Panneau de configuration.

- Utilisateurs de Windows Me et Windows 2000 : sélectionnez **Démarrer**, placez le curseur sur **Paramètres**, puis cliquez sur **Panneau de configuration**.
- Utilisateurs de Windows XP : dans la barre des tâches Windows, sélectionnez **Démarrer**, puis cliquez sur **Panneau de configuration**.

3 Ouvrez la boîte de dialogue **Ajout/Suppression de programmes**.

- Utilisateurs de Windows Me et 2000 : double-cliquez sur **Ajout/Suppression de programmes**.
- Utilisateurs de Windows XP : double-cliquez sur **Ajout/Suppression de programmes**.

4 Sélectionnez McAfee Privacy Service dans la liste des programmes et cliquez sur **Modifier/Supprimer**.

5 Une boîte de dialogue de confirmation apparaît. Cliquez sur **Oui** pour confirmer la désinstallation. Le processus de désinstallation de Privacy Service est lancé.

6 Lorsque le programme vous demande de redémarrer le système, cliquez sur **Fermer**. Votre ordinateur redémarre afin de terminer le processus de désinstallation.

Installation de Privacy Service

1 Allez sur le site Web de McAfee et naviguez jusqu'à la page de Privacy Service.

2 Cliquez sur le lien **Télécharger** sur la page de Privacy Service.

3 Répondez **Oui** à tous les messages vous invitant à télécharger des fichiers à partir du site Web de McAfee.

4 Cliquez sur **Lancer l'installation** dans la fenêtre d'installation de Privacy Service.

5 Une fois le téléchargement terminé, cliquez sur **Redémarrer** pour redémarrer l'ordinateur. Si vous devez enregistrer votre travail ou fermer des applications, cliquez sur **Fermer**, puis redémarrez l'ordinateur selon la procédure habituelle. Vous devez impérativement redémarrer l'ordinateur pour que Privacy Service fonctionne correctement.

Une fois l'ordinateur redémarré, vous devez recréer l'Administrateur.

Ajout d'utilisateurs

Pour ajouter des utilisateurs, vous devez vous connecter à Privacy Service en tant qu'administrateur.

1 Cliquez avec le bouton droit de la souris sur l'icône McAfee  .

2 Placez le curseur sur **Privacy Service** et sélectionnez **Gérer les utilisateurs**. La boîte de dialogue **Sélectionner un utilisateur** apparaît.

3 Cliquez sur **Ajouter** et entrez le nom du nouvel utilisateur dans le champ **Nom d'utilisateur**.

Définition du mot de passe

1. Entrez un mot de passe dans le champ **Mot de passe**. Le mot de passe est limité à 50 caractères et peut contenir des majuscules et des minuscules, ainsi que des chiffres.
2. Entrez à nouveau le mot de passe dans le champ **Confirmer le mot de passe**.
3. Sélectionnez **Faire de cet utilisateur l'utilisateur au démarrage** si vous souhaitez qu'il soit l'utilisateur au démarrage.
4. Cliquez sur **Suivant**.

Lorsque vous attribuez des mots de passe, tenez compte de l'âge de la personne. Par exemple, si vous attribuez un mot de passe à un enfant, choisissez un mot de passe simple. Si vous attribuez un mot de passe à un adolescent ou à un adulte, choisissez un mot de passe plus complexe.

Définition de la classification du contenu

Sélectionnez la tranche d'âge appropriée, puis cliquez sur **Suivant**.

Configuration du blocage des cookies

Sélectionnez l'option appropriée, puis cliquez sur **Suivant**.

- **Rejeter tous les cookies** : rend les cookies illisibles pour les sites Web qui vous les ont envoyés. Certains sites Web nécessitent que vous activiez les cookies pour fonctionner correctement.
- **Inviter l'utilisateur à accepter les cookies** : vous permet d'accepter ou de refuser les cookies au cas par cas. Privacy Service vous prévient lorsqu'un site Web que vous êtes sur le point de consulter tente d'envoyer un cookie à votre ordinateur. Une fois que vous avez décidé d'accepter ou de refuser le cookie, vous ne recevez plus de notification le concernant.
- **Accepter tous les cookies** : permet aux sites Web de lire les cookies qu'ils envoient à votre ordinateur.

  REMARQUE
  Pour fonctionner correctement, certains sites Web requièrent l'activation des cookies.

  Privacy Service accepte systématiquement les cookies de McAfee.

Définition des durées limites de connexion à Internet

Pour permettre au nouvel utilisateur de se connecter à Internet sans limite de temps :

1. Sélectionnez l'option **Peut utiliser Internet à tout moment**.
2. Cliquez sur **Créer**. Le nouvel utilisateur apparaît dans la liste Sélectionner un utilisateur.

Pour définir des durées limites de connexion pour le nouvel utilisateur :

1. Sélectionnez **Restreindre l'utilisation d'Internet**, puis cliquez sur **Modifier**.
2. Dans le menu déroulant **Jour**, sélectionnez le(s) jour(s) où le nouvel utilisateur peut utiliser Internet.
3. Sélectionnez l'**Heure de début** et l'**Heure de fin** dans les champs appropriés, puis cliquez sur **Ajouter**.
4. Cliquez sur **OK** dans la boîte de dialogue de confirmation. Les jours et heures que vous avez sélectionnés apparaissent dans la zone Jour. Pour supprimer une durée limite de connexion, sélectionnez le jour et cliquez sur **Supprimer**.
5. Cliquez sur **Terminé** lorsque vous avez terminé d'ajouter les heures.
6. Cliquez sur **Créer**. Le nouvel utilisateur apparaît dans la liste Sélectionner un utilisateur. Si un utilisateur tente de se connecter à Internet à un moment où il n'y est pas autorisé, Privacy Service affiche un message le lui indiquant.

Pour empêcher un nouvel utilisateur d'accéder à Internet

Sélectionnez **Restreindre l'utilisation d'Internet**, puis cliquez sur **Créer**. Lorsque l'utilisateur se sert de l'ordinateur, il est invité à se connecter à Privacy Service. Il peut utiliser l'ordinateur, mais pas se connecter à Internet.

Modification des utilisateurs

Pour modifier les utilisateurs, vous devez vous connecter à Privacy Service en tant qu'administrateur.

Modification des mots de passe

1. Sélectionnez l'utilisateur dont vous souhaitez modifier les informations et cliquez sur **Modifier**.
2. Sélectionnez **Mot de passe** et entrez le nouveau mot de passe de l'utilisateur dans le champ **Nouveau mot de passe**. Le mot de passe est limité à 50 caractères et peut contenir des majuscules et des minuscules, ainsi que des chiffres.
3. Entrez une nouvelle fois le nouveau mot de passe de l'utilisateur dans le champ **Confirmer le mot de passe**, puis cliquez sur **Appliquer**.
4. Cliquez sur **OK** dans la boîte de dialogue de confirmation.

REMARQUE
Un administrateur peut changer le mot de passe d'un utilisateur même s'il ne le connaît pas.

Modification des informations concernant un utilisateur

1. Sélectionnez l'utilisateur dont vous souhaitez modifier les informations et cliquez sur **Modifier**.
2. Sélectionnez **Info util**.
3. Entrez le nouveau nom d'utilisateur dans le champ correspondant.
4. Cliquez sur **Appliquer**, puis sur **OK** dans la boîte de dialogue de confirmation.
5. Pour qu'un utilisateur ne puisse consulter que les sites Web figurant dans la liste Sites Web autorisés, sélectionnez **Limiter l'accès de cet utilisateur aux sites Web de la liste « Sites Web autorisés »**.

Modification de la configuration du blocage des cookies

1. Sélectionnez l'utilisateur dont vous souhaitez modifier les informations et cliquez sur **Modifier**.
2. Sélectionnez **Cookies**, puis l'option appropriée.
   - **Rejeter tous les cookies** : rend les cookies illisibles pour les sites Web qui vous les ont envoyés. Certains sites Web nécessitent que vous activiez les cookies pour fonctionner correctement.

- **Inviter l'utilisateur à accepter les cookies** : vous permet d'accepter ou de refuser les cookies au cas par cas. Privacy Service vous prévient lorsqu'un site Web que vous êtes sur le point de consulter tente d'envoyer un cookie à votre ordinateur. Une fois que vous avez décidé d'accepter ou de refuser le cookie, vous ne recevez plus de notification le concernant.
- **Accepter tous les cookies** : permet aux sites Web de lire les cookies qu'ils envoient à votre ordinateur.

3 Cliquez sur **Appliquer**, puis sur **OK** dans la boîte de dialogue de confirmation.

Modification de la liste des sites Web pouvant placer des cookies et ne pouvant pas en placer

1 Sélectionnez **Inviter l'utilisateur à accepter les cookies** et cliquez sur **Modifier** pour spécifier les sites Web autorisés à lire les cookies.

2 Précisez la liste que vous modifiez en sélectionnant **Sites Web qui sont autorisés à placer des cookies** ou **Sites Web qui ne sont pas autorisés à placer des cookies**.

3 Dans le champ **http://**, entrez l'adresse du site Web dont vous acceptez ou refusez les cookies.

4 Cliquez sur **Ajouter**. Le site Web apparaît dans la liste.

5 Cliquez sur **Terminé** lorsque vous avez effectué toutes les modifications.

REMARQUE
Pour fonctionner correctement, certains sites Web requièrent l'activation des cookies.

Privacy Service accepte systématiquement les cookies de McAfee.

Modification de la tranche d'âge

1 Sélectionnez l'utilisateur dont vous souhaitez modifier les informations et cliquez sur **Modifier**.

2 Sélectionnez **Tranche d'âge**.

3 Choisissez la nouvelle tranche d'âge de l'utilisateur et cliquez sur **Appliquer**.

4 Cliquez sur **OK** dans la boîte de dialogue de confirmation.

Modification des durées limites de connexion à Internet

1. Sélectionnez l'utilisateur dont vous souhaitez modifier les informations et cliquez sur **Modifier**.
2. Sélectionnez **Restrictions temps** et procédez aux opérations suivantes :

Pour autoriser l'utilisateur à accéder à Internet en permanence

1. Sélectionnez l'option **Peut utiliser Internet à tout moment** et cliquez sur **Appliquer**.
2. Cliquez sur **OK** dans la boîte de dialogue de confirmation.

Pour limiter l'accès de l'utilisateur à Internet

1. Sélectionnez **Restreindre l'utilisation d'Internet** et cliquez sur **Modifier**.
2. Dans le menu déroulant **Jour**, sélectionnez le(s) jour(s) où l'utilisateur peut utiliser Internet.
3. Sélectionnez l'**Heure de début** et l'**Heure de fin**, puis cliquez sur **Ajouter**.
4. Cliquez sur **OK** dans la boîte de dialogue de confirmation. Les jours et heures que vous avez sélectionnés apparaissent dans la zone située sous les listes.
5. Cliquez sur **Terminé** lorsque vous avez terminé d'ajouter les heures.

Modification de l'utilisateur au démarrage

1. Sélectionnez l'utilisateur que vous souhaitez définir comme nouvel utilisateur au démarrage et cliquez sur **Modifier**.
2. Sélectionnez **Info util**.
3. Sélectionnez l'option **Faire de cet utilisateur l'utilisateur au démarrage**.
4. Cliquez sur **Appliquer**, puis sur **OK** dans la boîte de dialogue de confirmation.

REMARQUE
S'il existe déjà un utilisateur au démarrage, vous n'avez pas besoin de le désélectionner.

Suppression d'utilisateurs

1. Sélectionnez l'utilisateur à supprimer et cliquez sur **Supprimer**.
2. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.
3. Fermez la fenêtre de Privacy Service une fois les modifications effectuées.

Options

Pour configurer les options de Privacy Service, vous devez vous connecter à Privacy Service en tant qu'administrateur.

Blocage de sites Web

1. Cliquez sur **Options** et sélectionnez **Liste de blocage**.
2. Dans le champ **http://**, entrez l'URL du site Web dont vous souhaitez bloquer l'accès, puis cliquez sur **Ajouter**. Le site Web apparaît dans la liste **Sites Web bloqués**.

REMARQUE
Les utilisateurs adultes ont accès à tous les sites Web, même ceux qui figurent dans la liste Sites Web bloqués.

Autorisation de sites Web

L'administrateur peut autoriser tous les utilisateurs à consulter certains sites Web. Cette autorisation prévaut sur les paramètres par défaut de Privacy Service et sur les sites Web ajoutés à la liste des sites bloqués.

1. Cliquez sur **Options** et sélectionnez **Liste des autorisations**.
2. Dans le champ **http://**, entrez l'URL du site Web dont vous souhaitez autoriser l'accès, puis cliquez sur **Ajouter**. Le site Web apparaît dans la liste **Sites Web autorisés**.

Blocage d'informations

L'administrateur peut empêcher d'autres utilisateurs d'envoyer des données personnelles spécifiques via Internet (mais il peut lui-même en envoyer).

Lorsque Privacy Service détecte des informations personnelles identifiables dans un élément sur le point d'être envoyé, il se comporte comme suit :

- Si vous êtes connecté en tant qu'administrateur, il vous demande si vous voulez envoyer ou non les informations.
- Si vous n'êtes pas connecté en tant qu'administrateur, les informations bloquées sont remplacées par *mcgdog*. Par exemple, si vous souhaitez envoyer l'e-mail *Lance Armstrong est le gagnant du Tour* et que Armstrong est l'information personnelle à bloquer, alors l'e-mail envoyé sera *Lance mcgdogmcg est le gagnant du Tour*.

Ajout d'informations

1. Cliquez sur **Options** et sélectionnez **Bloquer les infos**.
2. Cliquez sur **Ajouter**. Le menu déroulant **Sélectionner un type** apparaît.
3. Sélectionnez le type d'information que vous souhaitez bloquer.
4. Entrez les informations dans les champs prévus à cet effet, puis cliquez sur **OK**. Les informations entrées apparaissent dans la liste.

Modification des informations

1. Cliquez sur **Options** et sélectionnez **Bloquer les infos**.
2. Sélectionnez les informations à modifier, puis cliquez sur **Modifier**.
3. Cliquez sur **OK** une fois les modifications effectuées. Si vous n'avez pas besoin d'effectuer de modifications, cliquez sur **Annuler**.

Suppression d'informations personnelles

1. Cliquez sur **Options** et sélectionnez **Bloquer les infos**.
2. Sélectionnez les informations à supprimer, puis cliquez sur **Supprimer**.
3. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.

Blocage des pixels invisibles

Les pixels invisibles sont des petits fichiers graphiques qui envoient des messages à des tiers, espionnent vos habitudes de navigation sur Internet ou transmettent des informations personnelles à une base de données externe. Les destinataires de ces informations peuvent ensuite s'en servir pour créer des profils utilisateur.

Pour empêcher le chargement des pixels invisibles à partir des pages Web consultées, sélectionnez **Bloquer les pixels invisibles sur cet ordinateur**.

Blocage des publicités

Les publicités sont généralement des graphiques hébergés par un domaine tiers sous forme de pages Web ou de fenêtres instantanées. Privacy Service ne bloque pas les publicités qui sont hébergées sur le même domaine que la page Web hôte.

Les fenêtres instantanées sont des fenêtres de navigateur secondaires qui affichent automatiquement des publicités indésirables lorsque vous consultez un site Web. Privacy Service bloque uniquement les fenêtres instantanées qui apparaissent automatiquement lors du chargement d'une page Web et non celles qui apparaissent lorsque vous cliquez sur un lien. Pour afficher une fenêtre instantanée qui a été bloquée, maintenez la touche CTRL enfoncée et actualisez la page Web.

Configurez Privacy Service de façon à ce qu'il bloque les publicités et les fenêtres instantanées lorsque vous êtes connecté à Internet.

1. Cliquez sur **Options** et sélectionnez **Bloquer les publicités**.
2. Sélectionnez l'option appropriée.
   - **Bloquer les publicités sur cet ordinateur** : bloque les publicités lorsque vous êtes connecté à Internet.
   - **Bloquer les fenêtres instantanées sur cet ordinateur** : bloque les fenêtres instantanées lorsque vous êtes connecté à Internet.
3. Cliquez sur **Appliquer**, puis sur **OK** dans la boîte de dialogue de confirmation.

Pour désactiver le blocage des fenêtres instantanées, cliquez avec le bouton droit de la souris sur la page Web, placez le curseur sur **Programme de blocage de fenêtres instantanées McAfee**, puis désélectionnez **Activer le programme de blocage des fenêtres instantanées**.

Autorisation des cookies de sites Web spécifiques

Si vous avez bloqué des cookies ou souhaitez recevoir une notification avant de les accepter et que certains sites Web fonctionnent moins bien, configurez Privacy Service pour qu'il autorise ces sites à lire leurs cookies.

1. Cliquez sur **Options** et sélectionnez **Cookies**.
2. Dans le champ **http://**, entrez l'adresse du site Web autorisé à lire ses cookies, puis cliquez sur **Ajouter**. L'adresse apparaît dans la liste **Sites Web dont les cookies sont acceptés**.

Sauvegarde de la base de données de Privacy Service

Le fichier de sauvegarde de la base de données ne peut être utilisé que si la base de données initiale est endommagée ou a été supprimée. Dans ce cas, Privacy Service vous invite à restaurer la base de données.

1. Cliquez sur **Options** et sélectionnez **Sauvegarder**.
2. Cliquez sur **Parcourir** pour sélectionner l'emplacement du fichier de base de données, puis sur **OK**.
3. Entrez un mot de passe dans le champ **Mot de passe**.
4. Entrez à nouveau le mot de passe dans le champ **Confirm mot passe**, puis cliquez sur **Sauvegarder**.
5. Cliquez sur **OK** dans la boîte de dialogue de confirmation.

REMARQUE
Gardez ce mot de passe confidentiel et mémorisez-le. Vous ne pouvez pas restaurer les paramètres de Privacy Service sans ce mot de passe.

Utilisation de la base de données de sauvegarde

1. Entrez le chemin d'accès au fichier de sauvegarde dans le champ **Emplacement du fichier de sauvegarde** ou cliquez sur **Parcourir** pour localiser le fichier.
2. Entrez votre mot de passe dans le champ prévu à cet effet.
3. Cliquez sur **Restaurer**.

Si vous n'avez pas créé de fichier de sauvegarde de la base de données de Privacy Service, si vous avez oublié le mot de passe de sauvegarde ou si vous n'arrivez pas à restaurer la base de données, vous devez désinstaller, puis réinstaller Privacy Service.

Journal des événements

Pour afficher le journal des événements, connectez-vous à Privacy Service en tant qu'administrateur. Sélectionnez ensuite **Journal des événements** et cliquez sur une entrée du journal pour en afficher les détails.

Date et heure

Par défaut, le journal des événements affiche les informations par ordre chronologique, les événements les plus récents apparaissant en haut. Si les entrées du journal ne sont pas classées par ordre chronologique, cliquez sur le titre Date et heure.

La date s'affiche selon le format jour/mois/année, et l'heure au format 24 heures.

Utilisateur

L'utilisateur est la personne qui était connectée et qui utilisait Internet au moment où Privacy Service a enregistré l'événement.

Résumé

Les résumés décrivent brièvement l'action de Privacy Service pour protéger les utilisateurs et ce que ces derniers font sur Internet.

Détails de l'événement

Le champ Détails de l'événement affiche les informations de chaque entrée.

Options utilisateur

Ces instructions ne concernent pas l'administrateur.

Vous pouvez modifier vos mot de passe et nom d'utilisateur. Nous vous conseillons de modifier le mot de passe que l'administrateur vous a donné. Modifiez-le ensuite une fois par mois ou chaque fois que vous pensez que quelqu'un le connaît. Ainsi, personne ne peut utiliser Internet avec votre nom d'utilisateur.

Modification de votre mot de passe

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, placez le curseur sur **Privacy Service**, puis sélectionnez **Options**.
2. Cliquez sur **Mot de passe** et entrez votre ancien mot de passe dans le champ **Ancien mot de passe**.
3. Entrez votre nouveau mot de passe dans le champ **Nouveau mot de passe**.
4. Entrez une nouvelle fois votre nouveau mot de passe dans le champ **Confirmer le mot de passe**, puis cliquez sur **Appliquer**.
5. Cliquez sur **OK** dans la boîte de dialogue de confirmation. Votre nouveau mot de passe est maintenant confirmé.

Modification de votre nom d'utilisateur

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, placez le curseur sur **Privacy Service**, puis sélectionnez **Options**.
2. Cliquez sur **Info util**.
3. Tapez votre nouveau nom d'utilisateur dans le champ **Nouveau nom d'utilisateur**, puis cliquez sur **Appliquer**.
4. Cliquez sur **OK** dans la boîte de dialogue de confirmation. Votre nouveau nom d'utilisateur est maintenant confirmé.

Vidage de votre cache

Nous vous conseillons de vider votre cache pour éviter qu'un enfant n'accède aux pages Web que vous avez consultées récemment. Pour cela, procédez comme suit :

1. Ouvrez Internet Explorer.
2. Dans le menu **Outils**, cliquez sur **Options Internet**. La boîte de dialogue Options Internet apparaît.
3. Dans la zone **Fichiers Internet temporaires**, cliquez sur **Supprimer les fichiers**. La boîte de dialogue Supprimer les fichiers apparaît.
4. Sélectionnez **Supprimer tout le contenu hors connexion**, puis cliquez sur **OK**.
5. Cliquez sur **OK** pour fermer la boîte de dialogue Options Internet.

Acceptation des cookies

Cette option n'est disponible que si l'administrateur vous laisse le choix d'accepter ou de refuser les cookies lorsqu'ils sont interceptés.

Si vous consultez des sites Web qui requièrent des cookies, vous pouvez les autoriser à lire les cookies.

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, placez le curseur sur **Privacy Service**, puis sélectionnez **Options**.
2. Cliquez sur **Cookies acceptés**.
3. Entrez l'URL du site Web dans le champ **http://**, puis cliquez sur **Ajouter**. Le site Web apparaît dans la liste **Site Web**.

Si vous devez supprimer un site Web de cette liste

1. Sélectionnez l'URL du site Web dans la liste **Site Web**.
2. Cliquez sur **Supprimer**, puis sur **Oui** dans la boîte de dialogue de confirmation.

Refus des cookies

Cette option n'est disponible que si l'administrateur vous laisse le choix d'accepter ou de refuser les cookies lorsqu'ils sont interceptés.

Si vous consultez des sites Web qui ne requièrent pas de cookies, vous pouvez les refuser sans y être invité.

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, placez le curseur sur **Privacy Service**, puis sélectionnez **Options**.
2. Cliquez sur **Cookies refusés**.
3. Entrez l'URL du site Web dans le champ **http://** et cliquez sur **Ajouter**. Le site Web apparaît dans la liste **Site Web**.

Si vous devez supprimer un site Web de cette liste

1. Sélectionnez l'URL du site Web dans la liste **Site Web**.
2. Cliquez sur **Supprimer**, puis sur **Oui** dans la boîte de dialogue de confirmation.

Utilitaires

Pour accéder aux utilitaires, connectez-vous à Privacy Service en tant qu'administrateur. Cliquez ensuite sur **Utilitaires** et sélectionnez **McAfee Shredder**.

Suppression définitive de fichiers à l'aide de McAfee Shredder

McAfee Shredder protège votre confidentialité en supprimant rapidement et en toute sécurité les fichiers indésirables.

Vous pouvez récupérer les fichiers supprimés sur votre ordinateur, même après avoir vidé la Corbeille. Lorsque vous supprimez un fichier, Windows considère que cet espace de votre lecteur de disque n'est plus utilisé, mais le fichier est toujours là.

Pourquoi Windows laisse-t-il des éléments de fichiers ?

Pour supprimer un fichier définitivement, vous devez écraser le fichier existant plusieurs fois avec de nouvelles données. Si Microsoft Windows supprimait complètement les fichiers, toutes les opérations liées aux fichiers seraient très lentes. Le fait de broyer un document n'empêche pas sa récupération, car certains programmes créent des copies cachées temporaires des documents ouverts. Si vous ne broyez que les documents visibles dans l'Explorateur, il se peut qu'il existe encore des copies temporaires de ces documents. Nous vous conseillons de broyer régulièrement l'espace libre de votre lecteur de disque pour vous assurer de la suppression définitive de ces copies temporaires.

REMARQUE
Avec des outils d'expertise judiciaire informatique, il serait possible d'accéder à des déclarations d'impôt, des CV ou d'autres documents que vous avez supprimés.

Ce que McAfee Shredder supprime

Grâce à McAfee Shredder, vous pouvez supprimer définitivement et en toute sécurité :

- Un ou plusieurs fichiers ou dossiers
- Un disque complet
- Les traces de votre navigation sur Internet

Suppression définitive de fichiers dans l'Explorateur Windows

Pour broyer un fichier via l'Explorateur Windows :

1. Ouvrez l'Explorateur Windows, puis sélectionnez le ou les fichiers à broyer.
2. Cliquez avec le bouton droit de la souris sur le fichier choisi, placez le curseur sur **Envoyer vers** et sélectionnez **McAfee Shredder**.

Vidage de la Corbeille Windows

Si votre Corbeille contient des fichiers, McAfee Shredder vous propose une méthode plus sûre pour la vider.

Pour broyer le contenu de la Corbeille :

1. Sur le bureau de Windows, cliquez avec le bouton droit de la souris sur la Corbeille.
2. Sélectionnez **Broyer le contenu de la Corbeille**, puis suivez les instructions à l'écran.

Personnalisation des paramètres de Shredder

Vous pouvez :

- Préciser le nombre de broyages.
- Demander l'affichage d'un message d'avertissement lorsque vous broyez des fichiers.
- Rechercher les erreurs éventuelles sur votre disque dur avant de procéder au broyage.
- Ajouter McAfee Shredder à votre menu Envoyer vers.
- Mettre une icône Shredder sur le bureau.

Pour personnaliser les paramètres de Shredder, ouvrez McAfee Shredder, cliquez sur **Propriétés**, puis suivez les instructions à l'écran.

McAfee SpamKiller 5

Bienvenue dans McAfee SpamKiller !

Le logiciel McAfee SpamKiller vous aide à lutter contre les spams. Il fournit les fonctions suivantes :

Options utilisateur

- Blocage des spams à l'aide de filtres et mise en quarantaine dans un dossier autre que celui de la boîte de réception
- Affichage des messages bloqués et acceptés
- Surveillance et filtrage de plusieurs comptes de messagerie
- Importation d'adresses de contacts dans la liste d'amis
- Réaction aux actions des spammeurs (notification, réclamation, création de filtres personnalisés)
- Protection contre l'affichage de spams susceptibles d'être lus par des enfants
- Blocage et récupération en un clic
- Prise en charge du jeu de caractères à deux octets
- Prise en charge de plusieurs utilisateurs (Windows 2000 et Windows XP)

Filtrage

- Mise à jour automatique des filtres
- Création de filtres personnalisés pour bloquer les e-mails qui contiennent principalement des images, du texte masqué ou une mise en forme incorrecte.
- Moteur de filtrage à plusieurs niveaux
- Filtrage d'attaque par dictionnaire
- Filtrage adaptable sur plusieurs niveaux
- Filtres de sécurité

Fonctions

McAfee SpamKiller empêche les spams d'envahir votre boîte de réception.

Présentation

Les icônes suivantes apparaissent dans le volet supérieur de chaque page de SpamKiller.

- Changer d'utilisateur : cliquez sur **Changer d'utilisateur** pour vous connecter avec les paramètres d'un autre utilisateur.

  Remarque : la fonction **Changer d'utilisateur** n'est disponible que si votre ordinateur fonctionne sous Windows 2000 ou Windows XP, si vous avez ajouté plusieurs utilisateurs à SpamKiller et si vous êtes connecté en tant qu'administrateur.

- **Assistance** : cliquez sur **Assistance** pour ouvrir la page d'assistance en ligne de McAfee, qui fournit les toutes dernières informations sur SpamKiller et d'autres produits McAfee, des réponses aux questions les plus fréquentes, etc. Pour y accéder, vous devez être connecté à Internet.

- **Aide** : cliquez sur **Aide** pour ouvrir l'aide en ligne, qui fournit des instructions détaillées sur la configuration et l'utilisation de SpamKiller.

Page Résumé

Cliquez sur l'onglet **Résumé** pour ouvrir la page correspondante, qui fournit les informations suivantes :

- **Résumé de SpamKiller** : cette zone indique si le filtrage est activé, à quel moment a été effectuée la dernière mise à jour d'une liste d'amis et le nombre de spams reçus dans la journée. Vous pouvez ensuite désactiver ou activer le filtrage de SpamKiller, mettre à jour la liste d'amis et ouvrir la page E-mail bloqué.

- **Spam récent** : cette zone indique les derniers spams bloqués par SpamKiller (messages supprimés de votre boîte de réception). Pour replacer un message dans votre boîte de réception, cliquez sur l'icône **Récupérer** située en regard du message.

- **Vue d'ensemble des e-mails** : cette zone indique le nombre total d'e-mails, de spams (messages bloqués) et le pourcentage de spams reçus.

- **Spam récent** : cette zone détaille les types de spam reçus au cours des 30 derniers jours.

Intégration de Microsoft Outlook et Outlook Express

Dans Outlook Express 6.0, Outlook 98, Outlook 2000 et Outlook XP, vous pouvez accéder directement aux principales fonctions de SpamKiller. Vous pouvez bloquer les spams, ajouter des contacts à votre liste d'amis et afficher les e-mails mis en quarantaine en cliquant sur les boutons intégrés aux barres d'outils d'Outlook et d'Outlook Express.

Barre d'outils de Microsoft Outlook

À partir de la barre d'outils de Microsoft Outlook Express 6.0, Outlook 98, Outlook 2000 et Outlook XP, vous pouvez effectuer les tâches suivantes :

- Bloquer le message : cliquez sur l'icône **Bloquer le message** pour supprimer le message sélectionné de la boîte de réception de Microsoft Outlook et le placer dans le dossier E-mail bloqué de SpamKiller.
- Consulter les messages bloqués : cliquez sur l'icône **Consulter les messages bloqués** pour consulter les messages bloqués à partir de votre compte Microsoft Outlook et déplacés vers le dossier E-mail bloqué de SpamKiller.
- Ajouter un ami : cliquez sur l'icône **Ajouter un ami** pour ajouter l'adresse e-mail de l'expéditeur à votre liste personnelle d'amis.

Une barre d'outils SpamKiller apparaît à droite de la barre d'outils par défaut d'Outlook et d'Outlook Express. Si la barre d'outils n'est pas visible, agrandissez la fenêtre de l'application de messagerie ou cliquez sur les flèches pour afficher d'autres barres d'outils.

Lorsqu'elle apparaît pour la première fois dans l'application de messagerie, la barre d'outils SpamKiller ne peut être utilisée que sur les nouveaux messages. Les spams existants doivent être supprimés.

Gestion de comptes de messagerie et d'utilisateurs

Cette section explique comment gérer les comptes et les utilisateurs.

Ajout de comptes de messagerie

SpamKiller filtre les types de compte de messagerie suivants :

- Compte de messagerie standard (POP3) : la plupart des particuliers disposent de ce type de compte.
- Compte MSN/Hotmail : comptes Web MSN/Hotmail.

- Compte de messagerie MAPI : comptes de messagerie se trouvant sur le réseau local. Dans les entreprises, la plupart des utilisateurs possèdent ce type de compte lorsque leur entreprise utilise Microsoft® Exchange Server. A noter que vous devez configurer un profil MAPI correct avant d'ajouter le compte MAPI à SpamKiller.

  REMARQUE
  Si votre ordinateur fonctionne sous Windows 2000 ou Windows XP et que vous prévoyez d'ajouter plusieurs utilisateurs à SpamKiller, vous devez le faire avant d'ajouter les comptes de messagerie aux profils utilisateur correspondants. Pour plus d'informations, consultez la section *Ajout d'utilisateurs* à la page 106. Si vous ajoutez plusieurs utilisateurs à SpamKiller, les comptes correspondants sont ajoutés au profil de l'utilisateur actuellement connecté à SpamKiller.

Pour ajouter un compte de messagerie :

1. Cliquez sur l'onglet **Paramètres**, puis sur **Comptes e-mail**. La boîte de dialogue **Comptes e-mail** apparaît, affichant tous les comptes de messagerie ajoutés à SpamKiller.

   REMARQUE
   Si vous avez ajouté plusieurs utilisateurs à SpamKiller, la liste affiche les comptes de messagerie de l'utilisateur actuellement connecté à SpamKiller.

2. Cliquez sur **Ajouter**. L'assistant Comptes e-mail s'affiche.

3. Suivez les instructions à l'écran.

Si vous ajoutez un compte MSN/Hotmail, SpamKiller recherche un carnet d'adresses MSN/Hotmail à importer dans votre liste personnelle d'amis.

Pour associer votre client de messagerie à SpamKiller :

Si vous avez ajouté un compte que SpamKiller ne détecte pas (il n'apparaît pas dans la boîte de dialogue **Sélectionner un compte**) ou si vous voulez utiliser votre messagerie MSN/Hotmail comme un compte POP3 dans SpamKiller, associez votre client de messagerie à SpamKiller.

1. Changez de serveur de messagerie entrant. Par exemple, si votre serveur de messagerie entrant est « mail.mcafee.com », remplacez-le par « localhost ».

2. Pour les comptes POP3 uniquement, remplacez le nom d'utilisateur par votre adresse e-mail complète. Par exemple, si votre adresse e-mail est « nom@exemple.com », remplacez-la par « nom@exemple.com ».

Suppression de comptes de messagerie

Supprimez un compte de messagerie de SpamKiller lorsque vous ne voulez plus le filtrer à l'aide de SpamKiller.

Pour supprimer un compte de messagerie de SpamKiller :

1. Cliquez sur l'onglet **Paramètres**, puis sélectionnez **Comptes e-mail**. La boîte de dialogue **Comptes e-mail** apparaît, affichant tous les comptes de messagerie ajoutés à SpamKiller.

   REMARQUE
   Si vous avez ajouté plusieurs utilisateurs à SpamKiller, la liste affiche les comptes de messagerie de l'utilisateur actuellement connecté à SpamKiller.

2. Sélectionnez un compte, puis cliquez sur **Supprimer**.

Modification des propriétés des comptes de messagerie

Vous pouvez modifier les informations d'un compte de messagerie ajouté à SpamKiller. Par exemple, modifiez l'adresse e-mail, la description du compte, les informations sur le serveur, la fréquence de recherche des spams par SpamKiller et le mode de connexion de votre ordinateur à Internet.

Comptes POP3

Pour modifier les comptes POP3 :

1. Cliquez sur l'onglet **Paramètres**, puis sur **Comptes e-mail**. La boîte de dialogue **Comptes e-mail** apparaît, affichant tous les comptes de messagerie ajoutés à SpamKiller.

   REMARQUE
   Si vous avez ajouté plusieurs utilisateurs à SpamKiller, la liste affiche les comptes de messagerie de l'utilisateur actuellement connecté à SpamKiller.

2. Sélectionnez un compte POP3, puis cliquez sur **Modifier**.

3. Pour modifier la description du compte et l'adresse e-mail, cliquez sur l'onglet **Général**.

   - **Description** : description du compte. Vous pouvez saisir tout type d'information dans ce champ.
   - **Adresse e-mail** : adresse e-mail du compte.

4 Pour modifier les informations sur le serveur, cliquez sur l'onglet **Serveurs**.

- **E-mail entrant** : nom du serveur qui reçoit les messages entrants.
- **Nom d'utilisateur** : nom d'utilisateur utilisé pour accéder à votre compte. Également appelé Nom de compte.
- **Mot de passe** : mot de passe utilisé pour accéder à votre compte.
- **E-mail sortant** : nom du serveur qui envoie les messages sortants. Pour modifier les conditions d'authentification requises pour le serveur sortant, cliquez sur **Plus**.

5 Pour modifier la fréquence de recherche des spams par SpamKiller, cliquez sur l'onglet **Vérification**.

a Sélectionnez **Vérifier toutes les** ou **Vérif. ts les jours à**, puis choisissez une heure dans le champ correspondant.

b Sélectionnez d'autres heures auxquelles SpamKiller doit filtrer le compte :

Vérifier au démarrage : sélectionnez cette option si vous disposez d'une connexion directe et que vous souhaitez que SpamKiller vérifie le compte à chaque démarrage de l'ordinateur.

Vérifier lorsqu'une connexion est établie : sélectionnez cette option si vous utilisez un modem pour vous connecter et que vous souhaitez que SpamKiller vérifie votre compte à chaque connexion à Internet.

6 Pour indiquer le mode de connexion à Internet et permettre ainsi à SpamKiller de filtrer les nouveaux messages de la boîte de réception, cliquez sur l'onglet **Connexion**.

- **Ne jamais établir une connexion** : SpamKiller n'établit pas de connexion automatiquement. Vous devez établir manuellement votre connexion par numérotation.
- **Numéroter en cas de besoin** : lorsque vous n'arrivez pas à vous connecter à Internet, SpamKiller tente d'établir automatiquement une connexion en utilisant la connexion Internet par numérotation par défaut.
- **Toujours numéroter** : SpamKiller tente d'établir automatiquement une connexion en utilisant la connexion par numérotation que vous avez indiquée.
- **Rester connecté après le filtrage** : votre ordinateur reste connecté à Internet une fois le filtrage terminé.

7 Pour modifier les options avancées, cliquez sur l'onglet **Avancé**.

- **Laisser le courrier indésirable sur le serveur** : cochez cette case pour conserver une copie des messages bloqués sur votre serveur de messagerie.

  En laissant les messages bloqués sur le serveur, vous pouvez les consulter à partir de votre client de messagerie et de la page E-mail bloqué de SpamKiller. Si vous ne cochez pas cette case, vous pouvez consulter les messages bloqués uniquement à partir de la page E-mail bloqué et non à partir de votre client de messagerie.

- **Port POP3** : (numéro de port POP3). Le serveur POP3 traite les messages entrants.

- **Port SMTP** : (numéro de port SMTP). Le serveur SMTP traite les messages sortants.

- **Temporisation serveur** : durée pendant laquelle SpamKiller attend de recevoir des e-mails avant de mettre fin à la connexion.

  Augmentez la durée de temporisation du serveur si vous avez des difficultés à recevoir des e-mails. Comme votre connexion e-mail peut être lente, l'augmentation de la durée de temporisation du serveur permet à SpamKiller d'attendre plus longtemps avant de mettre fin à la déconnexion.

8 Cliquez sur **OK**.

Comptes MSN/Hotmail

Pour modifier les comptes MSN/Hotmail :

1 Cliquez sur l'onglet **Paramètres**, puis sur **Comptes e-mail**.

La boîte de dialogue **Comptes e-mail** apparaît, affichant tous les comptes de messagerie ajoutés à SpamKiller.

> **REMARQUE**
> Si vous avez ajouté plusieurs utilisateurs à SpamKiller, la liste affiche les comptes de messagerie de l'utilisateur actuellement connecté à SpamKiller.

2 Sélectionnez un compte MSN/Hotmail, puis cliquez sur **Modifier**.

3 Pour modifier la description du compte et l'adresse e-mail, cliquez sur l'onglet **Général**.

- **Description** : description du compte. Vous pouvez saisir tout type d'information dans ce champ.

- **Adresse e-mail** : adresse e-mail du compte.

4 Pour modifier les informations sur le serveur, cliquez sur l'onglet **Serveurs**.

- **E-mail entrant** : nom du serveur qui reçoit les messages entrants.
- **Mot de passe** : mot de passe utilisé pour accéder à votre compte.
- **E-mail sortant** : nom du serveur qui envoie les messages sortants.
- **Utiliser un serveur SMTP pour les e-mails sortants** : sélectionnez cette option si vous prévoyez d'envoyer des messages d'erreur et que vous ne souhaitez pas y inclure la signature MSN. La signature MSN simplifie l'identification d'un faux message d'erreur par les spammeurs.

  Pour modifier les conditions d'authentification requises pour le serveur sortant, cliquez sur **Plus**.

5 Pour indiquer la fréquence de recherche des spams par SpamKiller, cliquez sur l'onglet **Vérification**.

a Sélectionnez **Vérifier toutes les** ou **Vérif. ts les jours à**, puis choisissez une heure dans le champ correspondant.

b Sélectionnez d'autres heures auxquelles SpamKiller doit filtrer le compte :

Vérifier au démarrage : sélectionnez cette option si vous disposez d'une connexion directe et que vous souhaitez que SpamKiller vérifie le compte à chaque démarrage.

Vérifier lorsqu'une connexion est établie : sélectionnez cette option si vous utilisez un modem pour vous connecter et que vous souhaitez que SpamKiller vérifie votre compte à chaque connexion à Internet.

6 Pour indiquer le mode de connexion à Internet et permettre ainsi à SpamKiller de filtrer les nouveaux messages de la boîte de réception, cliquez sur l'onglet **Connexion**.

- **Ne jamais établir une connexion** : SpamKiller n'établit pas de connexion automatiquement. Vous devez établir manuellement votre connexion par numérotation.
- **Numéroter en cas de besoin** : lorsque vous n'arrivez pas à vous connecter à Internet, SpamKiller tente d'établir automatiquement une connexion en utilisant la connexion Internet par numérotation par défaut.
- **Toujours numéroter** : SpamKiller tente d'établir automatiquement une connexion en utilisant la connexion par numérotation que vous avez indiquée.
- **Rester connecté après le filtrage** : votre ordinateur reste connecté à Internet une fois le filtrage terminé.

7 Cliquez sur **OK**.

Pour configurer un compte Hotmail de façon à ce qu'il bloque les spams dans Outlook ou Outlook Express

SpamKiller peut filtrer des comptes Hotmail directement. Pour plus d'informations, consultez l'aide en ligne. Toutefois, tant que vous n'avez pas configuré votre compte Hotmail, vous ne pouvez pas bloquer de message ni ajouter d'ami en utilisant la barre d'outils SpamKiller dans Outlook ou Outlook Express.

1. Configurez votre compte Hotmail dans MSK.
2. Si vous possédez déjà un compte Hotmail dans Outlook ou Outlook Express, vous devez d'abord le supprimer.
3. Ajoutez votre compte Hotmail dans Outlook ou Outlook Express. Assurez-vous de sélectionner **POP3** comme type de compte et type de serveur de courrier entrant.
4. Nommez le serveur de courrier entrant `localhost`.
5. Entrez le nom du serveur de courrier SMTP sortant disponible (obligatoire).
6. Terminez la configuration du compte. Vous pouvez maintenant bloquer un nouveau spam Hotmail ou ajouter un ami.

Comptes MAPI

Pour que SpamKiller s'intègre correctement à l'interface MAPI d'Outlook, les conditions suivantes doivent être remplies :

- Outlook 98 a été initialement installé avec la prise en charge Société/Groupe de travail.
- Pour Outlook 98 uniquement, le premier compte de messagerie est un compte MAPI.
- L'ordinateur est connecté au domaine.

Pour modifier les comptes MAPI :

1. Cliquez sur l'onglet **Paramètres**, puis sur **Comptes e-mail**. La boîte de dialogue **Comptes e-mail** apparaît, affichant tous les comptes de messagerie ajoutés à SpamKiller.

   REMARQUE
   Si vous avez ajouté plusieurs utilisateurs à SpamKiller, la liste affiche les comptes de messagerie de l'utilisateur actuellement connecté à SpamKiller.

2. Sélectionnez un compte MAPI, puis cliquez sur **Modifier**.

3 Pour modifier la description du compte et l'adresse e-mail, cliquez sur l'onglet **Général**.

- **Description** : description du compte. Vous pouvez saisir tout type d'information dans ce champ.
- **Adresse e-mail** : adresse e-mail du compte.

4 Pour modifier les informations du profil, cliquez sur l'onglet **Profil**.

- **Profil** : profil MAPI du compte.
- **Mot de passe** : mot de passe qui correspond au profil MAPI si vous en avez configuré un (il ne s'agit pas forcément du mot de passe du compte de messagerie).

5 Pour indiquer le mode de connexion à Internet et permettre ainsi à SpamKiller de filtrer les nouveaux messages de la boîte de réception, cliquez sur l'onglet **Connexion**.

- **Ne jamais établir une connexion** : SpamKiller n'établit pas de connexion automatiquement. Vous devez établir manuellement votre connexion par numérotation.
- **Numéroter en cas de besoin** : lorsque vous n'arrivez pas à vous connecter à Internet, SpamKiller tente d'établir automatiquement une connexion en utilisant la connexion Internet par numérotation par défaut.
- **Toujours numéroter** : SpamKiller tente d'établir automatiquement une connexion en utilisant la connexion par numérotation que vous avez indiquée.
- **Rester connecté après le filtrage** : votre ordinateur reste connecté à Internet une fois le filtrage terminé.

6 Cliquez sur **OK**.

Ajout d'utilisateurs

SpamKiller peut configurer plusieurs utilisateurs, à savoir ceux qui sont définis dans votre système d'exploitation Windows 2000 ou Windows XP.

Lors de l'installation de SpamKiller sur votre ordinateur, un profil d'administrateur est automatiquement créé pour l'utilisateur Windows connecté à ce moment-là. Si vous ajoutez des comptes de messagerie à SpamKiller au cours de l'installation, ceux-ci sont ajoutés à ce profil d'administrateur.

Avant d'ajouter d'autres comptes de messagerie à SpamKiller, déterminez si vous avez besoin d'ajouter d'autres utilisateurs SpamKiller. Ceci peut être utile si votre ordinateur est utilisé par plusieurs personnes qui disposent chacune de leur propre compte de messagerie. Le compte de messagerie de chaque utilisateur est ajouté à son profil, ce qui lui permet de le gérer et de définir ses paramètres, ses filtres, ainsi que sa liste d'amis personnels.

Le type attribué à un utilisateur définit les tâches qu'il est autorisé à effectuer dans SpamKiller. Le tableau suivant résume les autorisations accordées à chaque type d'utilisateur. Les administrateurs sont autorisés à effectuer toutes les tâches sans exception, alors que les utilisateurs, qui disposent de droits restreints, ne peuvent effectuer que les tâches en rapport avec leur profil personnel. Les administrateurs peuvent par exemple consulter l'ensemble du contenu des messages bloqués, alors que les utilisateurs ne peuvent en consulter que l'objet.

Tâches	Administrateur	Utilisateur avec des droits restreints
Gérer les comptes de messagerie personnels, les filtres personnels, la liste personnelle des amis et les paramètres sonores personnels	X	X
Gérer les pages personnelles E-mail bloqué et E-mail accepté	X	X
Consulter le texte des messages bloqués	X	
Consulter le texte des messages acceptés	X	X
Gérer les filtres généraux et la liste complète des amis	X	
Signaler les spams à McAfee	X	X
Envoyer des réclamations et des messages d'erreur	X	X
Gérer les réclamations et les messages d'erreur (créer, modifier et supprimer des modèles de message)	X	
Gérer les utilisateurs (créer, modifier et supprimer des utilisateurs)	X	
Sauvegarder et restaurer SpamKiller	X	
Consulter la page Résumé des spams reçus	X	X

Lorsqu'un utilisateur qui vient d'être ajouté se connecte à votre ordinateur, il est invité à ajouter un compte de messagerie à son profil utilisateur.

Pour pouvoir ajouter et gérer des utilisateurs, vous devez respecter les conditions suivantes :

- Vous devez être connecté à SpamKiller en tant qu'administrateur.
- Vous devez disposer de Windows 2000 ou Windows XP.
- Les utilisateurs que vous souhaitez ajouter ou gérer doivent posséder des comptes utilisateur Windows.

Mots de passe utilisateur et protection des enfants contre les spams

Le fait de créer un mot de passe utilisateur augmente le niveau de confidentialité. Sans ce mot de passe, personne ne peut accéder aux paramètres personnels, à la liste d'amis et à la liste des e-mails acceptés d'un utilisateur. Cette démarche permet également d'éviter que les enfants n'accèdent à SpamKiller et ne consultent le contenu des spams.

Pour créer un mot de passe pour un utilisateur SpamKiller existant :

1. Cliquez sur l'onglet **Paramètres**, puis sur **Utilisateurs**.
2. Sélectionnez un utilisateur, puis cliquez sur **Modifier**.
3. Entrez un mot de passe dans le champ **Mot de passe**. Lorsque l'utilisateur accède à SpamKiller, il doit entrer le mot de passe pour se connecter.

   IMPORTANT
   Si vous l'oubliez, il vous sera impossible de le récupérer. Seul un administrateur SpamKiller pourra vous attribuer un nouveau mot de passe.

Pour ajouter un utilisateur à SpamKiller :

1. Cliquez sur l'onglet **Paramètres**, puis sur **Utilisateurs**.
2. Cliquez sur **Ajouter**.

   La liste des utilisateurs Windows s'affiche. Pour ajouter un utilisateur qui n'apparaît pas dans la liste, vous devez créer un compte utilisateur Windows pour cette personne. Celle-ci doit ensuite se connecter au moins une fois à votre ordinateur. Ajoutez ensuite l'utilisateur à SpamKiller.

   REMARQUE
   Les utilisateurs Windows disposant de droits d'administrateur possèdent également des droits d'administrateur dans SpamKiller.
3. Sélectionnez un utilisateur à ajouter, puis cliquez sur **OK**. L'utilisateur est ajouté à SpamKiller et son nom apparaît dans la liste des utilisateurs SpamKiller.
4. Cliquez sur **Fermer** lorsque vous avez terminé d'ajouter des utilisateurs.

Pour créer un mot de passe pour un utilisateur, consultez la section *Pour créer un mot de passe pour un utilisateur SpamKiller existant :* à la page 108.

Lors de sa prochaine connexion à votre ordinateur, l'utilisateur est invité à ajouter un compte de messagerie à son profil utilisateur SpamKiller. Vous pouvez ajouter des comptes de messagerie au profil utilisateur si vous êtes connecté avec ce profil et que vous disposez des informations de connexion nécessaires. Pour plus d'informations, consultez la section *Ajout de comptes de messagerie* à la page 99.

Pour modifier un profil d'utilisateur SpamKiller :

1. Cliquez sur l'onglet **Paramètres**, puis sur **Utilisateurs**. La liste des utilisateurs SpamKiller s'affiche.
2. Sélectionnez un utilisateur, puis cliquez sur **Modifier**.
3. Entrez un nouveau nom et un mot de passe.

Pour supprimer un profil d'utilisateur SpamKiller :

> **AVERTISSEMENT**
> Lorsque vous supprimez un profil utilisateur, vous supprimez également les comptes de messagerie de cet utilisateur dans SpamKiller.

1. Cliquez sur l'onglet **Paramètres**, puis sur **Utilisateurs**. La liste des utilisateurs SpamKiller s'affiche.
2. Sélectionnez un utilisateur dans la liste, puis cliquez sur **Supprimer**.

Connexion à SpamKiller dans un environnement multi-utilisateur

Lorsque les utilisateurs se connectent à votre ordinateur et ouvrent SpamKiller, ils sont automatiquement connectés sous leur profil utilisateur. Si des mots de passe SpamKiller leur ont été attribués, ils doivent les saisir dans la boîte de dialogue **Connexion** qui s'affiche.

Pour changer d'utilisateur :

Vous devez être connecté à SpamKiller en tant qu'administrateur.

1. Cliquez sur **Changer d'utilisateur** en haut de la page. La boîte de dialogue correspondante apparaît.
2. Sélectionnez un utilisateur, puis cliquez sur **OK**. Si l'utilisateur dispose d'un mot de passe, la boîte de dialogue **Connexion** s'affiche. Saisissez le mot de passe de l'utilisateur dans la zone **Mot de passe**, puis cliquez sur **OK**.

Utilisation de la liste d'amis

Nous vous conseillons d'intégrer les noms et adresses e-mail de vos amis dans une liste d'amis. SpamKiller ne bloque pas les messages dont les expéditeurs figurent dans la liste. Par conséquent, ajouter des contacts à la liste d'amis permet de s'assurer que les messages de source fiable parviennent à destination.

SpamKillller vous permet d'ajouter des noms, des adresses e-mail, des domaines et des listes de diffusion à la liste d'amis. Vous pouvez ajouter les adresses une à une ou en une seule fois en important un carnet d'adresses depuis votre programme de messagerie.

SpamKiller comporte deux types de liste :

- **Liste complète des amis** : cette liste s'applique à l'ensemble des comptes de messagerie de tous les utilisateurs SpamKiller. Si vous avez ajouté plusieurs utilisateurs, vous devez être connecté à SpamKiller en tant qu'administrateur pour pouvoir la gérer.
- **Liste personnelle des amis** : cette liste s'applique à l'ensemble des comptes de messagerie associés à un utilisateur donné. Si vous avez ajouté plusieurs utilisateurs, vous devez être connecté à SpamKiller en tant qu'utilisateur pour pouvoir la gérer.

Vous pouvez ajouter des contacts à une liste d'amis afin que leurs e-mails ne soient pas bloqués. La page Amis affiche les noms et adresses ajoutés à la liste d'amis. Cette page indique également la date de l'ajout et le nombre total de messages reçus de cet ami.

Cliquez sur l'onglet **Adresses e-mail** pour afficher les adresses e-mail de la liste d'amis. Cliquez sur l'onglet **Domaines** pour afficher les adresses de domaine de la liste. Cliquez sur l'onglet **Listes de diffusion** pour afficher les listes de diffusion de la liste d'amis.

Pour basculer entre la liste complète et la liste personnelle, cliquez sur la flèche vers le bas de l'onglet **Adresses e-mail**, **Domaines** ou **Listes de diffusion**, puis sélectionnez **Liste personnelle des amis**.

Ouverture d'une liste d'amis

1. Pour ouvrir une liste d'amis, cliquez sur l'onglet **Amis**.
2. Cliquez sur l'onglet **Adresses e-mail**, **Domaines** ou **Listes de diffusion**. La liste complète des amis apparaît. Pour afficher la liste personnelle des amis, cliquez sur la flèche vers le bas de l'un des onglets, puis sélectionnez **Liste personnelle des amis**.

REMARQUE
Si votre ordinateur fonctionne sous Windows 2000 ou Windows XP et que vous avez ajouté plusieurs utilisateurs à SpamKiller, les utilisateurs avec des droits restreints peuvent uniquement afficher leur liste personnelle d'amis.

Importation de carnets d'adresses

Vous pouvez importer manuellement ou automatiquement des carnets d'adresses dans une liste d'amis. Si vous choisissez l'importation automatique, SpamKiller contrôle régulièrement la présence de nouveaux contacts dans vos carnets d'adresses et les importe automatiquement dans une liste d'amis.

Vous pouvez importer des carnets d'adresses à partir des programmes de messagerie suivants :

- Microsoft Outlook (version 98 ou ultérieure)
- Microsoft Outlook Express (toutes les versions)
- Netscape Communicator (version 6 et versions précédentes si le carnet d'adresses a été exporté sous forme de fichier LDIF)
- Qualcomm Eudora (version 5 ou ultérieure)
- IncrediMail Xe
- MSN/Hotmail
- Tous les programmes capables d'exporter leur carnet d'adresses sous forme de fichier texte

Pour importer un carnet d'adresses automatiquement :

Il est possible de mettre à jour régulièrement votre liste personnelle d'amis en créant un calendrier d'importation d'adresses à partir des carnets.

1. Cliquez sur l'onglet **Paramètres**, puis sur **Carnets d'adresses**. La boîte de dialogue **Importer des carnets d'adresses** apparaît. Elle contient la liste des carnets d'adresses que SpamKiller contrôle régulièrement et à partir desquels il importe de nouvelles adresses.
2. Cliquez sur **Ajouter**. La boîte de dialogue **Planifier l'importation** apparaît.
3. Sélectionnez le **Type** et la **Source** du carnet d'adresses à importer.
4. Dans le champ **Planification**, indiquez la fréquence selon laquelle SpamKiller doit rechercher les nouvelles adresses dans le carnet.
5. Cliquez sur **OK**. Après une mise à jour, les nouvelles adresses apparaissent dans votre liste personnelle d'amis.

Pour importer un carnet d'adresses manuellement :

Il est possible d'importer manuellement des carnets d'adresses dans vos listes complète et personnelle d'amis.

> **REMARQUE**
> Si votre ordinateur fonctionne sous Windows 2000 ou Windows XP et que vous avez ajouté plusieurs utilisateurs à SpamKiller, vous devez vous connecter en tant qu'administrateur pour pouvoir ajouter des contacts à la liste complète des amis.

1. Cliquez sur l'onglet **Amis**, puis sur **Importer carnet d'adr**.

   La boîte de dialogue **Importer un carnet d'adresses** apparaît. Elle contient la liste des types de carnet d'adresses que vous pouvez importer.

2. Sélectionnez un type de carnet d'adresses à importer ou cliquez sur **Parcourir** pour importer des adresses stockées dans un fichier.

   Pour importer le carnet d'adresses uniquement dans la liste personnelle des amis, vérifiez que la case **Ajouter à la Liste personnelle des amis** est bien cochée. Pour importer le carnet d'adresses uniquement dans la liste complète des amis, assurez-vous que cette case n'est *pas* cochée.

3. Cliquez sur **Suivant**. Une page de confirmation indique le nombre d'adresses que SpamKiller a ajouté.

4. Cliquez sur **Terminer**. Les adresses apparaissent alors dans la liste complète ou personnelle des amis.

Pour modifier les informations d'un carnet d'adresses :

Modifiez les informations d'un carnet d'adresses importé automatiquement.

1. Cliquez sur l'onglet **Paramètres**, puis sur **Carnets d'adresses**.
2. Sélectionnez un carnet d'adresses, puis cliquez sur **Modifier**.
3. Modifiez les informations du carnet d'adresses, puis cliquez sur **OK**.

Pour supprimer un carnet d'adresses de la liste d'importation automatique :

Pour que SpamKiller n'importe plus automatiquement les adresses d'un carnet d'adresses, supprimez ce carnet.

1. Cliquez sur l'onglet **Paramètres**, puis sur **Carnets d'adresses**.
2. Sélectionnez un carnet d'adresses, puis cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'ouvre.
3. Cliquez sur **Oui** pour supprimer le carnet d'adresses de la liste.

Ajout de contacts

Pour être certain de recevoir tous les e-mails envoyés par vos amis, ajoutez leurs noms et adresses à une liste d'amis. Vous pouvez le faire à partir des pages Amis, E-mail bloqué et E-mail accepté et de Microsoft Outlook et Outlook Express.

REMARQUE
Si votre ordinateur fonctionne sous Windows 2000 ou Windows XP et que vous avez ajouté plusieurs utilisateurs à SpamKiller, vous devez vous connecter en tant qu'administrateur pour pouvoir ajouter des contacts à la liste complète des amis.

Pour ajouter un contact à partir de la page E-mail bloqué ou E-Mail accepté :

1. Cliquez sur l'onglet **Messages**, puis sur **E-mail bloqué** ou **E-mail accepté**.

   - Ou -

   Dans Microsoft Outlook ou Outlook Express, cliquez sur  pour ouvrir la page E-mail bloqué du compte.

   La page E-mail bloqué ou E-mail accepté s'ouvre.

2. Sélectionnez un message provenant d'un expéditeur que vous souhaitez ajouter à une liste d'amis, puis cliquez sur **Ajouter un ami**.

3. Dans le champ **Adresse**, entrez l'adresse à ajouter à la liste d'amis. Ce champ contient peut-être déjà l'adresse figurant dans le message sélectionné.

4. Dans le champ **Nom**, entrez le nom de votre ami.

5. Dans le champ **Type d'ami**, sélectionnez le type d'adresse à ajouter :

   - **Une seule adresse e-mail** : l'adresse e-mail de l'expéditeur est ajoutée à l'onglet Adresses e-mail de la liste d'amis.
   - **Tous les utilisateurs du domaine** : le nom du domaine est ajouté à l'onglet **Domaines** de la liste d'amis. SpamKiller accepte tous les e-mails provenant du domaine.
   - **Liste de diffusion** : l'adresse est ajoutée à l'onglet **Listes de diffusion** de la liste d'amis.

   Pour ajouter l'adresse uniquement à la liste personnelle des amis, vérifiez que la case **Ajouter à la Liste personnelle des amis** est bien cochée. Pour ajouter l'adresse uniquement à la liste complète des amis, assurez-vous que cette case n'est *pas* cochée.

6. Cliquez sur **OK**. Tous les messages provenant de ce contact sont identifiés comme des messages provenant d'un ami et figurent dans la page E-mail accepté.

Pour ajouter un contact à partir de la page Amis :

1. Cliquez sur l'onglet **Amis**, puis sur **Ajouter un ami**. La boîte de dialogue **Propriétés des amis** s'affiche.
2. Dans le champ **Adresse**, entrez l'adresse à ajouter à la liste d'amis.
3. Dans le champ **Nom**, entrez le nom de votre ami.
4. Dans le champ **Type d'ami**, sélectionnez le type d'adresse à ajouter :
   - **Une seule adresse e-mail** : l'adresse e-mail de l'expéditeur est ajoutée à la liste d'amis.
   - **Tous les utilisateurs du domaine** : le nom du domaine est ajouté à l'onglet Domaines de la liste d'amis. SpamKiller accepte tous les e-mails provenant du domaine.
   - **Liste de diffusion** : l'adresse est ajoutée à l'onglet Listes de diffusion de la liste d'amis.

   Pour ajouter l'adresse uniquement à la liste personnelle des amis, vérifiez que la case **Ajouter à la Liste personnelle des amis** est bien cochée. Pour ajouter l'adresse uniquement à la liste complète des amis, assurez-vous que cette case n'est *pas* cochée.
5. Cliquez sur **OK**. Tous les messages provenant de ce contact sont identifiés comme des messages provenant d'un ami et figurent dans la page E-mail accepté.

Pour ajouter un contact à partir de Microsoft Outlook :

1. Ouvrez votre compte de messagerie dans Microsoft Outlook ou Outlook Express.
2. Sélectionnez un message envoyé par un expéditeur que vous souhaitez ajouter à une liste d'amis.
3. Cliquez sur  dans la barre d'outils de Microsoft Outlook. Tous les messages provenant de ce contact sont identifiés comme des messages provenant d'un ami et figurent dans la page E-mail accepté.

Modification des contacts d'une liste d'amis

1 Cliquez sur l'onglet **Amis**, puis sur **Adresses e-mail**, **Domaines** ou **Listes de diffusion**.

La liste complète des amis apparaît. Pour afficher la liste personnelle des amis, cliquez sur la flèche vers le bas de l'un des onglets, puis sélectionnez **Liste personnelle des amis**.

REMARQUE
Si votre ordinateur fonctionne sous Windows 2000 ou Windows XP et que vous avez ajouté plusieurs utilisateurs à SpamKiller, seuls les administrateurs peuvent accéder à la liste complète des amis.

2 Sélectionnez l'adresse à modifier, puis cliquez sur **Modifier cet ami**.

3 Modifiez les informations souhaitées, puis cliquez sur **OK**.

Suppression de contacts dans la liste d'amis

Supprimez les adresses que vous ne souhaitez plus voir figurer dans la liste d'amis.

1 Cliquez sur l'onglet **Amis**, puis sur **Adresses e-mail**, **Domaines** ou **Listes de diffusion**.

La liste complète des amis apparaît. Pour afficher la liste personnelle des amis, cliquez sur la flèche vers le bas de l'un des onglets, puis sélectionnez **Liste personnelle des amis**.

REMARQUE
Si votre ordinateur fonctionne sous Windows 2000 ou Windows XP et que vous avez ajouté plusieurs utilisateurs à SpamKiller, seuls les administrateurs peuvent accéder à la liste complète des amis.

2 Sélectionnez une adresse dans la liste, puis cliquez sur **Effacer cet ami**. Une boîte de dialogue de confirmation s'ouvre.

3 Cliquez sur **Oui** pour supprimer ce contact.

Utilisation des messages bloqués ou acceptés

Cliquez sur l'onglet **Messages** pour accéder à vos messages bloqués et acceptés. Les pages E-mail bloqué et E-mail accepté présentent les mêmes fonctions.

Page E-mail bloqué

Cliquez sur l'onglet **E-mail bloqué** de la page Messages pour afficher les messages bloqués.

> **REMARQUE**
> Vous pouvez également consulter les messages bloqués à partir de votre compte Microsoft Outlook en ouvrant la boîte de réception Outlook, puis en cliquant sur dans la barre d'outils de Microsoft Outlook ou Outlook Express.

Les messages bloqués sont les messages que SpamKiller a identifié comme des spams, qu'il a supprimés de la boîte de réception et qu'il a placés dans le dossier E-mail bloqué.

La page E-mail bloqué affiche tous les spams supprimés de vos comptes de messagerie. Pour consulter les e-mails bloqués d'un compte donné, cliquez sur la flèche vers le bas située dans l'onglet **E-mail bloqué**, puis sélectionnez le compte à afficher.

La sous-fenêtre de messages située en haut répertorie les spams, triés par date. Le message le plus récent apparaît en haut de la liste. La sous-fenêtre de prévisualisation située en bas contient le texte du message sélectionné.

> **REMARQUE**
> Si votre ordinateur fonctionne sous Windows 2000 ou Windows XP, que vous avez ajouté plusieurs utilisateurs à SpamKiller et que vous êtes connecté à SpamKiller en tant qu'utilisateur avec des droits restreints, le contenu des messages ne s'affiche pas dans la sous-fenêtre de prévisualisation située en bas.

La sous-fenêtre centrale affiche les détails des messages. Cliquez sur la flèche vers le bas pour développer la sous-fenêtre des détails des messages et afficher le texte et les en-têtes de message au format natif avec toutes les balises de code HTML. Cette sous-fenêtre contient les informations suivantes :

- **Action** : décrit la manière dont SpamKiller a traité le spam. Le champ Action est associé à l'action du filtre qui a bloqué le message.
- **Raison** : explique pourquoi SpamKiller a bloqué le message. Pour ouvrir l'éditeur de filtres et afficher le filtre, cliquez sur Raison. L'éditeur de filtres indique les éléments recherchés par le filtre dans les messages, ainsi que l'action effectuée par SpamKiller sur les messages retenus par le filtre.
- **De** : affiche l'expéditeur du message.
- **Date** : précise la date à laquelle le message vous a été envoyé.
- **À** : indique les destinataires du message.
- **Objet** : affiche le sujet du message figurant dans le champ Objet.

La colonne de gauche contient les icônes associées aux messages si des réclamations ou des messages d'erreur ont été envoyés manuellement.

- Réclamation envoyée : une réclamation concernant le message a été envoyée.
- Message d'erreur envoyé : un message d'erreur a été envoyé à l'adresse de réponse du spam.
- Réclamation et message d'erreur envoyés : une réclamation et un message d'erreur ont été envoyés.

Page E-mail accepté

Cliquez sur l'onglet **E-mail accepté** de la page Messages pour afficher les messages acceptés.

La page E-mail accepté affiche tous les messages de la boîte de réception de tous vos comptes de messagerie. En revanche, pour les comptes MAPI, elle ne contient pas d'e-mails internes. Pour consulter les e-mails acceptés d'un compte donné, cliquez sur la flèche vers le bas située dans l'onglet **E-mail accepté**, puis sélectionnez le compte à afficher.

> **REMARQUE**
> SpamKiller a été conçu pour accepter les messages de source fiable. Toutefois, si des messages de source fiable s'affichent dans la liste des e-mails bloqués, vous pouvez les replacer dans la boîte de réception (et dans la liste des e-mails acceptés) en les sélectionnant, puis en cliquant sur **Récupérer ce message**.

Tout comme la page E-mail bloqué, la sous-fenêtre de messages située en haut répertorie les messages, triés par date. La sous-fenêtre de prévisualisation située en bas contient le texte du message sélectionné.

La sous-fenêtre centrale indique si un message a été envoyé par un contact de la liste d'amis ou si le message répond aux critères d'un filtre, mais l'action du filtre a été définie sur **Accepter** ou **Marquer comme courrier indés. possible**. Cliquez sur la flèche vers le bas pour développer la sous-fenêtre des détails des messages et afficher le texte et les en-têtes de message au format natif avec toutes les balises de code HTML.

Cette sous-fenêtre contient les informations suivantes :

- **Action** : décrit la manière dont SpamKiller a traité le message.
- **Raison** : si un message a été marqué, explique pourquoi SpamKiller a marqué le message.
- **De** : affiche l'expéditeur du message.
- **Date** : précise la date à laquelle le message vous a été envoyé.
- **À** : indique les destinataires du message.
- **Objet** : affiche le sujet du message figurant dans le champ Objet.

L'une des icônes suivantes peut apparaître en regard d'un message.

- Message d'un ami : SpamKiller a détecté que l'expéditeur du message figure dans une liste d'amis. C'est un message que vous souhaitez conserver.
- Message indésirable potentiel : le message correspond à un filtre dont l'action est définie sur Marquer comme courrier indésirable potentiel.
- Réclamation envoyée : une réclamation concernant le message a été envoyée.
- Message d'erreur envoyé : un message d'erreur a été envoyé à l'adresse de réponse du spam.
- Réclamation et message d'erreur envoyés : une réclamation et un message d'erreur ont été envoyés.

Tâches relatives aux e-mails bloqués ou acceptés

Le panneau de droite des pages E-mail bloqué et E-mail accepté répertorie les tâches que vous pouvez effectuer.

- Bloquer ce message : supprime un message de la boîte de réception et le place dans le dossier E-mail bloqué de SpamKiller (cette option apparaît uniquement sur la page E-mail accepté).
- Récupérer ce message : replace un message dans votre boîte de réception (cette option apparaît uniquement sur la page E-mail bloqué) et ouvre la boîte de dialogue **Options de secours**. Vous pouvez ajouter automatiquement l'expéditeur à votre liste d'amis et récupérer tous les messages provenant de cet expéditeur.
- Effacer ce message : supprime le message sélectionné.
- Ajouter un ami : ajoute le nom de l'expéditeur, l'adresse e-mail, le domaine ou la liste de diffusion à une liste d'amis.
- Ajouter un filtre : crée un filtre.

- Signaler à McAfee : informe McAfee de certains spams reçus.
- Envoyer une réclamation : envoie une réclamation relative aux spams à l'administrateur du domaine de l'expéditeur ou à une adresse e-mail de votre choix.
- Envoyer une erreur : envoie un message d'erreur à l'adresse de réponse du spam.

Récupération de messages

Si la page E-mail bloqué contient des e-mails de source fiable, vous pouvez les replacer dans votre boîte de réception.

Pour récupérer un message :

1 Cliquez sur l'onglet **Messages**, puis sur **E-mail bloqué**.

- Ou -

Dans la boîte de réception Microsoft Outlook ou Outlook Express, cliquez sur  pour ouvrir la page E-mail bloqué du compte.

La page E-mail bloqué s'affiche.

2 Sélectionnez un message et cliquez sur **Récupérer ce message**. La boîte de dialogue **Options de secours** apparaît.

- **Ajouter un ami** : ajoute l'expéditeur à votre liste d'amis.
- **Récupérer tout d'un même expéditeur** : récupère tous les messages bloqués de l'expéditeur du message sélectionné.

3 Cliquez sur **OK**. Le message est alors replacé dans votre boîte de réception et dans le dossier E-mail accepté.

Blocage de messages

Vous pouvez bloquer les spams figurant actuellement dans votre boîte de réception. Lorsque vous bloquez un message, SpamKiller crée automatiquement un filtre pour le supprimer de la boîte de réception. Vous pouvez bloquer les messages de la boîte de réception à partir de la page E-mail accepté ou de Microsoft Outlook ou Outlook Express.

Pour bloquer un message depuis la page E-mail accepté :

1 Cliquez sur l'onglet **Messages**, puis sur **E-mail accepté**. La page E-mail accepté affiche les messages se trouvant actuellement dans votre boîte de réception.

2 Sélectionnez un message, puis cliquez sur **Bloquer ce message**. Le message, qui est alors supprimé à la fois de la boîte de réception et de la page E-mail accepté, est copié dans le dossier E-mail bloqué.

Pour bloquer un message à partir de Microsoft Outlook :

Seuls les messages externes peuvent être bloqués (messages provenant d'un serveur Internet).

1 Ouvrez votre boîte de réception Microsoft Outlook ou Outlook Express.

2 Sélectionnez un message, puis cliquez sur  . Une copie du message est placée dans le dossier E-mail bloqué.

Suppression de messages

SpamKiller supprime automatiquement les messages du dossier E-mail bloqué 15 jours après leur suppression de la boîte de réception. Vous pouvez modifier le délai de suppression des messages ou les supprimer manuellement.

SpamKiller ne supprime pas automatiquement les messages du dossier E-mail accepté, puisque ce dernier contient les messages figurant actuellement dans votre boîte de réception.

Pour modifier les paramètres de suppression automatique des messages bloqués :

Par défaut, SpamKiller supprime les spams qu'il trouve dans la boîte de réception et les place dans le dossier E-mail bloqué. Il supprime automatiquement tous les messages du dossier E-mail bloqué au bout de 15 jours. Vous avez la possibilité de modifier la fréquence à laquelle SpamKiller supprime les messages bloqués.

Au lieu de déplacer les spams vers le dossier E-mail bloqué, SpamKiller peut indiquer « [spam] » ou tout autre marqueur de votre choix dans la ligne d'objet de l'e-mail et le conserver dans la boîte de réception. Le marquage des messages peut s'avérer utile lorsque vous déplacez les messages marqués vers un autre dossier de votre client de messagerie tel que le dossier « messages indésirables ». Vous pouvez déplacer les messages marqués en créant une règle dans votre client de messagerie afin qu'il recherche les messages contenant le marqueur « [spam] » et les place dans le dossier de votre choix.

1 Cliquez sur l'onglet **Paramètres**, puis sur l'icône **Options de filtrage**.

2 Sélectionnez la manière dont SpamKiller doit traiter les messages :

- **Placer le courrier indésirable dans la boîte E-mails bloqués** : les spams sont supprimés de la boîte de réception et placés dans le dossier E-mail bloqué de SpamKiller.
- **Conserver e-mails bloqués pendant ____ jours** : les messages bloqués restent dans le dossier E-mail bloqué pendant la durée indiquée.
- **Marquer le courrier indésirable et garder dans boîte de réception** : les spams restent dans la boîte de réception, mais le marqueur « [spam] » ou tout autre marqueur de votre choix sera indiqué dans la ligne d'objet du message.

3 Cliquez sur **OK**.

Pour supprimer un message manuellement :

1 Cliquez sur l'onglet **Messages**, puis sur **E-mail bloqué**.

- Ou -

Dans la boîte de réception Microsoft Outlook ou Outlook Express, cliquez sur pour ouvrir la page E-mail bloqué du compte.

2 Sélectionnez le message à supprimer.

3 Cliquez sur **Effacer ce message**. Une boîte de dialogue de confirmation s'ouvre.

4 Cliquez sur **Oui** pour supprimer le message.

Ajout de contacts à une liste d'amis

Consultez la section *Pour ajouter un contact à partir de la page E-mail bloqué ou E-Mail accepté :* à la page 113.

Ajout de filtres

Pour plus d'informations sur les filtres, consultez la rubrique *Utilisation des filtres* de l'aide en ligne.

1. Cliquez sur l'onglet **Messages**.
2. Cliquez sur l'onglet **E-mail bloqué** ou **E-mail accepté**, puis sur **Ajouter un filtre**. La boîte de dialogue **Éditeur de filtres** s'ouvre.
3. Cliquez sur **Ajouter** pour lancer la création d'une condition de filtre. La boîte de dialogue **Condition du filtre** s'ouvre.
4. Pour créer une condition de filtre, procédez de la manière suivante.

   Une condition de filtre est un énoncé qui indique à SpamKiller les éléments à rechercher dans un message, par exemple, « Le texte du message contient prêt hypothécaire ». Dans cet exemple, le filtre recherche les messages contenant les mots « prêt hypothécaire ». Pour plus d'informations, consultez la rubrique *Conditions du filtre* de l'aide en ligne.

   a. Sélectionnez un type de condition dans le premier champ.

   b. Sélectionnez ou entrez les valeurs appropriées dans les zones suivantes.

   c. Si les options ci-après apparaissent, sélectionnez-les pour affiner la condition de filtre.

      Rechercher également dans les codes de mise en forme : cette option apparaît uniquement si la condition de filtre est destinée à effectuer une recherche dans le texte du message. Si vous cochez cette case, SpamKiller lance une recherche sur le texte spécifié, non seulement dans le texte du message, mais également dans ses codes de mise en forme.

      Sensible à la casse : cette option apparaît uniquement pour les conditions dans lesquelles vous avez saisi une valeur de condition. Si vous cochez cette case, SpamKiller différencie les lettres majuscules et minuscules contenues dans la valeur saisie.

      Rechercher variations : permet à SpamKiller de détecter les fautes d'orthographe intentionnelles que les spammeurs font le plus souvent. Par exemple, le mot « mortgage » peut être orthographié « mortg@g3 » pour échapper aux filtres.

   d. Cliquez sur **OK**.

5 Créez une autre condition de filtre en suivant les étapes ci-dessous ou passez à l'Étape 6 pour sélectionner une action de filtre.

   a Cliquez sur **Ajouter**, puis créez la condition de filtre. Cliquez sur **OK** lorsque vous avez terminé.

   Les deux conditions de filtre apparaissent dans la liste correspondante et sont réunies par **et**. L'opérateur **et** indique que la recherche de SpamKiller porte sur les messages qui répondent aux *deux* conditions de filtre. Pour que SpamKiller recherche les messages qui répondent à l'une ou l'autre des conditions, remplacez **et** par **ou** en cliquant sur **et**, puis en sélectionnant **ou** dans le champ.

   b Cliquez sur **Ajouter** pour créer une nouvelle condition ou passez à l'Étape 6 pour sélectionner une action de filtre.

   Si vous avez créé trois conditions ou plus, vous pouvez les regrouper pour créer des clauses. Pour obtenir des exemples de regroupement, consultez la rubrique *Groupement de filtres* de l'aide en ligne.

   Pour regrouper des conditions de filtre, sélectionnez une condition, puis cliquez sur **Grouper**.

   Les conditions regroupées sont surlignées en bleu.

   REMARQUE
   Pour dissocier des conditions de filtre, sélectionnez une condition regroupée, puis cliquez sur **Dissocier**.

6 Sélectionnez une action de filtre dans le champ **Action**. Cette action indique à SpamKiller comment traiter les messages trouvés par le filtre. Pour plus d'informations, consultez la rubrique *Actions du filtre* de l'aide en ligne.

7 Cliquez sur **Avancé** pour sélectionner les options de filtre avancées (la sélection d'options avancées est facultative). Pour plus d'informations, consultez la rubrique *Options avancées du filtre* de l'aide en ligne.

8 Cliquez sur **OK** lorsque vous avez terminé de créer le filtre.

   REMARQUE
   Pour modifier une condition, sélectionnez-la et modifiez-la. Pour supprimer une condition, sélectionnez-la et cliquez sur **Supprimer**.

Notification de spams à McAfee

Vous pouvez signaler les spams reçus à McAfee, qui les analysera en vue de mettre à jour les filtres.

Pour signaler des spams à McAfee :

1. Cliquez sur l'onglet **Messages**, puis sur **E-mail bloqué** ou **E-mail accepté**. La page E-mail bloqué ou E-mail accepté s'ouvre.
2. Sélectionnez un message, puis cliquez sur **Signaler à McAfee**. Une boîte de dialogue de confirmation s'ouvre.
3. Cliquez sur **Oui**. Le message est envoyé automatiquement à McAfee.

Envoi de réclamations manuellement

Envoyez une réclamation pour empêcher un expéditeur de vous inonder de spams. Pour plus d'informations sur l'envoi de réclamations, consultez la rubrique *Envoi de réclamations et de messages d'erreur* de l'aide en ligne.

Pour envoyer une réclamation manuellement :

1. Cliquez sur l'onglet **Messages**, puis sur **E-mail bloqué** ou **E-mail accepté**. Une liste de messages s'affiche.
2. Sélectionnez le message pour lequel vous souhaitez envoyer une réclamation, puis cliquez sur **Envoyer une réclamation**. La boîte de dialogue **Envoyer une réclamation** s'ouvre.
3. Sélectionnez le destinataire de la réclamation.

   AVERTISSEMENT
   Dans la plupart des cas, ne sélectionnez pas **L'expéditeur (non recommandé)**. En envoyant une réclamation à l'expéditeur du spam, vous validez votre adresse e-mail et risquez de recevoir un nombre de spams encore plus important de cet expéditeur.

4. Cliquez sur **Suivant**, puis suivez les instructions des boîtes de dialogue.

Envoi de messages d'erreur

Pour plus d'informations sur l'envoi de messages d'erreur, consultez la rubrique *Envoi de réclamations et de messages d'erreur* de l'aide en ligne.

Envoyez un message d'erreur pour empêcher un expéditeur de vous inonder de spams.

Pour envoyer un message d'erreur manuellement :

1. Cliquez sur l'onglet **Messages**, puis sur **E-mail bloqué** ou **E-mail accepté**. Une liste de messages s'affiche.
2. Pour envoyer un message d'erreur concernant un spam donné, sélectionnez le message, puis cliquez sur **Envoyer une erreur**. Un message d'erreur est envoyé à l'adresse de réponse du spam.

Index

A

B

C

D

E

W