McAfee®

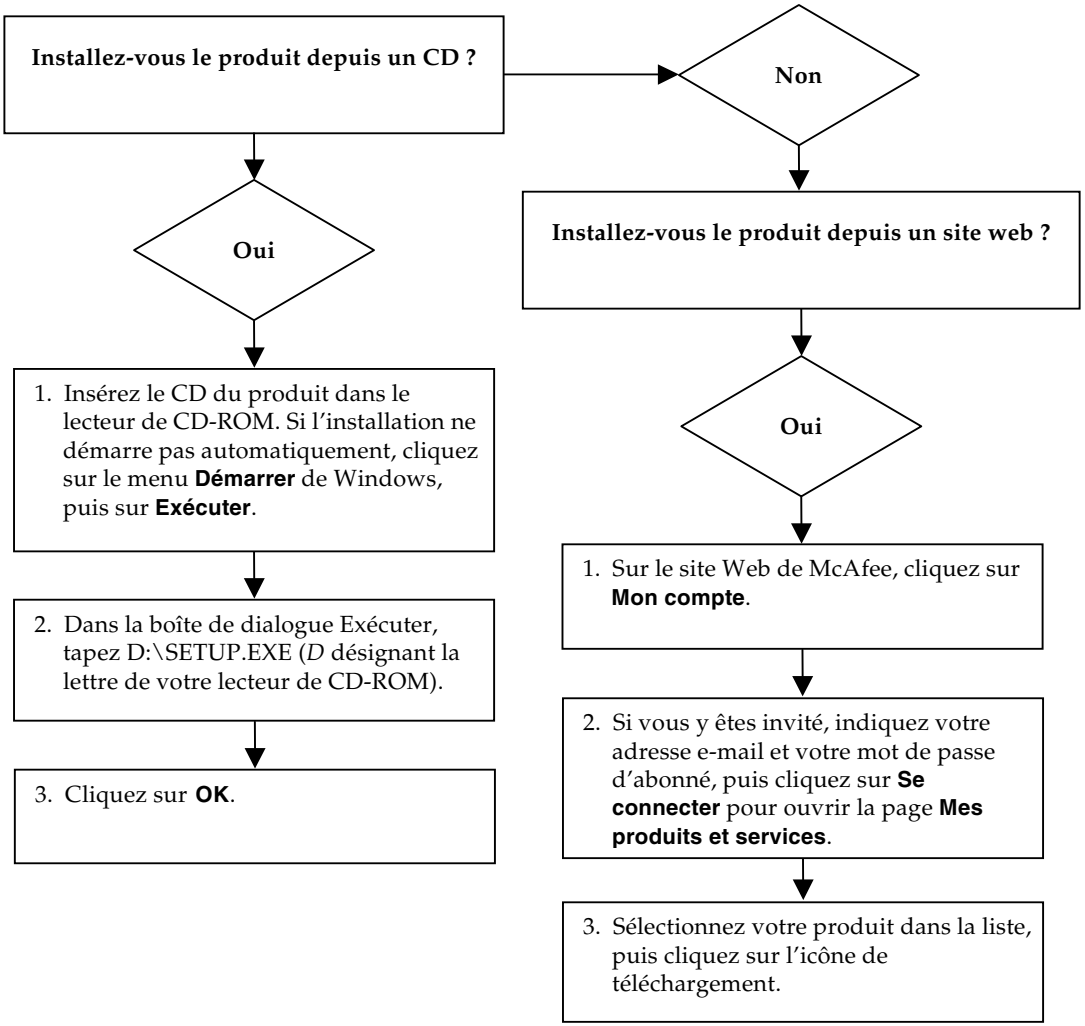
virusscan®

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/.

Sommaire

Prise en main 1

Bienvenue dans McAfee VirusScan.

McAfee VirusScan est un service d'abonnement offrant une protection antivirus complète, fiable et à jour. Fonctionnant avec notre moteur d'analyse McAfee reconnu pour son efficacité, VirusScan protège votre ordinateur contre les virus, vers, chevaux de Troie, scripts malveillants et attaques hybrides.

Il fournit les fonctions suivantes :

ActiveShield : analyse les fichiers lorsque vous ou votre ordinateur y accédez.

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

Mise en quarantaine : chiffre et isole temporairement les fichiers infectés ou suspects dans le répertoire 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 une activité de ver.

Nouvelles fonctionnalités

Cette version de VirusScan vous offre les nouvelles fonctionnalités suivantes :

- **Recherche de programmes potentiellement indésirables**
  VirusScan recherche des programmes potentiellement indésirables (parmi lesquels des programmes espions, des logiciels publicitaires et des composeurs téléphoniques) à l'aide d'analyses manuelles, d'analyses des courriers électroniques sortants, de la messagerie instantanée, via le menu raccourci de l'Explorateur Windows et l'icône de la barre d'outils de Microsoft Outlook.

- **Analyse de pièces jointes sortantes de grande taille**
  Pour traiter l'utilisation croissante de connexions Internet à haut débit, la plus grande capacité de stockage des e-mails et les tailles plus importantes des transmissions accordées par les fournisseurs, VirusScan est à présent optimisé pour analyser des pièces jointes de grande taille sans interférer avec les valeurs de temporisation du programme d'e-mail.

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

- **Analyse de Instant Messenger**
  VirusScan analyse automatiquement les transferts de fichiers entrants pour les clients de messagerie instantanée les plus couramment utilisés, notamment Yahoo Messenger, AOL Instant Messenger et MSN Messenger.

- **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.

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

- **Analyse programmée**
  Vous pouvez à présent planifier une analyse automatique à intervalles définis pour lancer une recherche complète de virus sur l'ordinateur.

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

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

- **Notification Virus Map**
  Vous pouvez à présent envoyer des informations de suivi de virus de manière anonyme afin d'enrichir notre World Virus Map. Vous pouvez vous enregistrer automatiquement à ce service gratuit et sécurisé afin de connaître les taux d'infection mondiaux les plus récents via McAfee SecurityCenter.

Configuration système requise

- Microsoft® Windows 98, Me, 2000 ou XP
- Ordinateur personnel avec processeur Windows 98 ou Me : Pentium 150 MHz ou supérieur Windows 2000 ou XP : Pentium 233 MHz ou supérieur
- Mémoire vive Windows 98 : 32 Mo (64 Mo recommandés)
  Windows Me, 2000 ou XP : 64 Mo (128 Mo recommandés)
- 40 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.

Test de VirusScan

Avant la première l'utilisation de VirusScan, il est judicieux de tester votre installation. Suivez les étapes ci-après pour tester séparément les fonctionnalités ActiveShield et Analyser.

Test de ActiveShield

Pour tester ActiveShield :

1. Allez sur le site http://www.eicar.com/ à l'aide de votre navigateur Web.
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)**, vous verrez quatre liens.
4. Cliquez sur **eicar.com**.

Si ActiveShield fonctionne correctement, il détecte le fichier eicar.com dès que vous cliquez sur ce lien. Vous pouvez tenter de supprimer ou de mettre en quarantaine les fichiers infectés pour voir comment ActiveShield traite les virus. Pour plus d'informations, consultez la rubrique *Si ActiveShield trouve un virus* à la page 23.

Test de la fonction Analyser

Avant de tester la fonction Analyser, vous devez désactiver ActiveShield (sinon, il détectera les fichiers infectés avant la fonction Analyser) ; téléchargez ensuite les fichiers de test.

Pour télécharger les fichiers de test :

1. Désactivez ActiveShield : cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis cliquez sur **Désactiver**.
2. Téléchargez les fichiers de test EICAR à partir du site Web EICAR :
   a. Allez sur le 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)**, vous verrez les liens suivants :

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

      eicar.com.txt (facultatif) est le même fichier sous un autre nom pour les utilisateurs qui ont des difficultés à télécharger le premier lien. Il vous suffit de renommer le fichier "eicar.com" une fois téléchargé.

      eicar_com.zip est une copie du virus de test à l'intérieur d'un fichier compressé .ZIP (une 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. Cliquez sur chaque lien pour télécharger le fichier correspondant. Pour chacun d'eux, une boîte de dialogue **Téléchargement de fichier** s'affiche.
   e. Cliquez sur **Enregistrer**, sur le bouton **Créer un nouveau dossier**, puis renommez le **Dossier VSO Scan**.
   f. Double-cliquez sur le **Dossier VSO Scan**, puis cliquez sur **Enregistrer** dans chacune des boîtes de dialogue **Enregistrer sous**.
3. Une fois les fichiers téléchargés, quittez Internet Explorer.
4. Activez ActiveShield : Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis cliquez sur **Activer**.

Pour tester la fonction Analyser :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis cliquez sur **Analyse antivirus**.
2. À l'aide de l'arborescence de répertoires dans le panneau de gauche de la boîte de dialogue, allez dans le **Dossier VSO Scan** où vous avez enregistré les fichiers :
   a. Cliquez sur le signe **+** en regard de l'icône du lecteur C.
   b. Cliquez sur **Dossier VSO Scan** afin de le mettre en surbrillance (ne cliquez pas sur le signe **+** situé en regard).

      Ainsi, vous indiquez à la fonction Analyser de ne rechercher des virus que dans ce dossier. Vous pouvez également placer les fichiers dans des emplacements aléatoires sur votre disque dur afin d'obtenir une démonstration encore plus probante des capacités de cette fonction.
3. Dans la zone **Options d'analyse** de la boîte de dialogue **Recherche de virus**, assurez-vous que toutes les options sont sélectionnées.
4. Cliquez sur **Analyser** en bas à droite de la boîte de dialogue.

   VirusScan analyse le dossier **Dossier VSO Scan**. Les fichiers de test que vous avez enregistrés dans ce dossier s'affichent dans la **Liste des fichiers détectés**. Si tel est le cas, la fonction Analyser fonctionne correctement.

Vous pouvez tenter de supprimer ou de mettre en quarantaine les fichiers infectés pour voir comment elle traite les virus. Pour plus d'informations, consultez la section *Si la fonction Analyser trouve un virus ou un programme potentiellement indésirable* à la page 31.

Utilisation de McAfee SecurityCenter

McAfee SecurityCenter est votre centre de sécurité unifié, accessible à partir de son icône dans la barre d'état système Windows ou de votre bureau Windows. Il vous 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 actualités produits 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 ses fonctions, 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 une fonction de VirusScan :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee.
2. Pointez sur **VirusScan**, puis cliquez sur la fonction à utiliser.

Utilisation de McAfee VirusScan 2

Utilisation d'ActiveShield

Une fois démarré (chargé dans la mémoire de l'ordinateur) et activé, ActiveShield protège votre ordinateur en permanence. ActiveShield analyse les fichiers lorsque vous ou votre ordinateur y accédez. Quand ActiveShield trouve un fichier infecté, il tente automatiquement de le nettoyer. S'il ne peut pas éradiquer le virus, vous pouvez supprimer ou placer le fichier en quarantaine.

Activation ou désactivation de ActiveShield

ActiveShield est démarré (chargé dans la mémoire de votre ordinateur) et activé (signalé par l'icône rouge dans votre barre d'état système Windows) par défaut dès que vous redémarrez votre ordinateur à la suite du processus d'installation.

Si ActiveShield est arrêté (non chargé) ou désactivé (signalé en noir par l'icône), vous pouvez l'exécuter manuellement et le configurer pour qu'il se lance automatiquement au démarrage de Windows.

Activation de 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 cliquez sur **Activer**. L'icône de McAfee devient rouge .

Si ActiveShield est toujours configuré pour être lancé automatiquement au démarrage de Windows, un message vous indique que vous êtes maintenant protégé contre les virus. Dans le cas contraire, une boîte de dialogue s'affiche pour vous permettre de configurer ActiveShield de manière à ce qu'il démarre en même temps que Windows (Figure 2-1 à la page 14).

Désactivation de 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 cliquez sur **Désactiver**.
2. Cliquez sur **Oui** pour confirmer.

   L'icône de McAfee devient noire .

Si ActiveShield est toujours configuré pour être lancé automatiquement au démarrage de Windows, votre ordinateur est à nouveau protégé contre les virus lorsque vous le redémarrez.

Configuration des options de ActiveShield

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

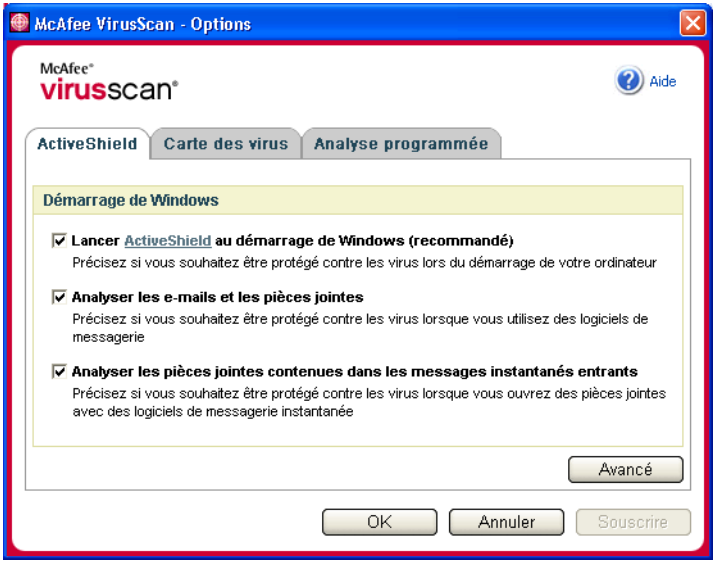


Figure 2-1. Options ActiveShield

Démarrage de ActiveShield

ActiveShield est démarré (chargé dans la mémoire de votre ordinateur) et activé (signalé par un  rouge) par défaut dès que vous redémarrez votre ordinateur à la suite du processus d'installation.

Si ActiveShield est arrêté (signalé par un  noir), vous pouvez le configurer pour qu'il démarre automatiquement au démarrage de Windows (recommandé).

> **REMARQUE**
> Durant les mises à jour de VirusScan, l'**Assistant de mise à jour** peut quitter temporairement ActiveShield afin d'installer de nouveaux fichiers. Lorsque l'**Assistant de mise à jour** vous invite à cliquer sur **Terminer**, 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 cliquez sur **Options**.

   La boîte de dialogue **McAfee VirusScan - Options** s'affiche (Figure 2-1 à la page 14).

2. Cochez la case **Lancer ActiveShield au démarrage de Windows (recommandé)**, puis cliquez sur **Appliquer** pour enregistrer vos modifications.

3. Cliquez sur **OK** pour confirmer, puis sur **OK**.

Arrêt de ActiveShield

> **AVERTISSEMENT**
> Si vous arrêtez ActiveShield, votre ordinateur ne sera plus protégé contre les virus. Si vous devez arrêter ActiveShield pour une autre raison que la mise à jour de VirusScan, assurez-vous 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 cliquez sur **Options**.

   La boîte de dialogue **McAfee VirusScan - Options** s'affiche (Figure 2-1 à la page 14).

2. Décochez la case **Lancer ActiveShield au démarrage de Windows (recommandé)**, puis cliquez sur **Appliquer** pour enregistrer vos modifications.

3. Cliquez sur **OK** pour confirmer, puis sur **OK**.

Analyse des e-mails et des pièces jointes

Par défaut, l'analyse des e-mails et le nettoyage automatique sont activés via l'option **Analyser les e-mails et les pièces jointes** (Figure 2-1 à la page 14) et l'option **Nettoyer automatiquement les pièces jointes infectées (recommandé)** (Figure 2-2 à la page 18).

Lorsque ces deux options sont activées, ActiveShield analyse automatiquement les e-mails et les pièces jointes infectés, qu'ils soient entrants (POP3) ou sortants (SMTP), et tente de les nettoyer, pour les clients de messagerie électronique les plus couramment utilisés, notamment :

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

REMARQUE

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

Si vous désactivez l'option **Analyser les e-mails et les pièces jointes**, les options de Analyse e-mails (Figure 2-2 à la page 18) et celles de WormStopper (Figure 2-5 à la page 22) sont automatiquement désactivées. Si vous désactivez l'analyse des e-mails sortants, les options de WormStopper sont automatiquement désactivées.

Si vous modifiez vos options d'analyse d'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 entrants, ActiveShield procède aux opérations suivantes :

- Il tente de nettoyer l'e-mail infecté.
- Il tente de mettre en quarantaine ou de supprimer un e-mail qui ne peut pas être nettoyé.
- Il intègre un fichier d'alerte dans l'e-mail entrant qui précise les actions réalisées pour supprimer l'infection.

E-mails sortants

En cas d'infection d'un e-mail ou d'une pièce jointe sortants, ActiveShield procède aux opérations suivantes :

- Il tente de nettoyer l'e-mail infecté.
- Il tente de mettre en quarantaine ou de supprimer un e-mail qui ne peut pas être nettoyé.

> **REMARQUE**
> Pour plus d'informations sur les erreurs d'analyse des e-mails sortants, reportez-vous à l'aide en ligne.
>
> Par défaut, l'option d'**affichage de l'état d'analyse des e-mails sortants** est désactivée. Dans ce cas, la fenêtre d'état n'apparaît qu'en cas d'erreur. Pour toujours l'afficher, sélectionnez l'option mentionnée (dans l'onglet Analyse e-mails de la boîte de dialogue d'options avancées ActiveShield).

Désactivation de l'analyse des e-mails

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 n'analyse que 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 cliquez sur **Options**.
2. Cliquez sur **Avancé**, puis sur l'onglet **Analyse e-mails** (Figure 2-2 à la page 18).
3. Désélectionnez **E-mails entrants** ou **E-mails sortants**, puis cliquez sur **OK**.

Si votre serveur de messagerie est paramétré de manière à n'envoyer et ne recevoir des e-mails que lorsque vous êtes à votre poste, vous pouvez choisir de recevoir des alertes pour vous avertir de nettoyer les e-mails en désactivant le nettoyage automatique. Procédez aux opérations suivantes pour désactiver le nettoyage automatique, puis reportez-vous à la section *Gestion des e-mails infectés* à la page 24 pour obtenir plus d'informations sur la réponse aux alertes.

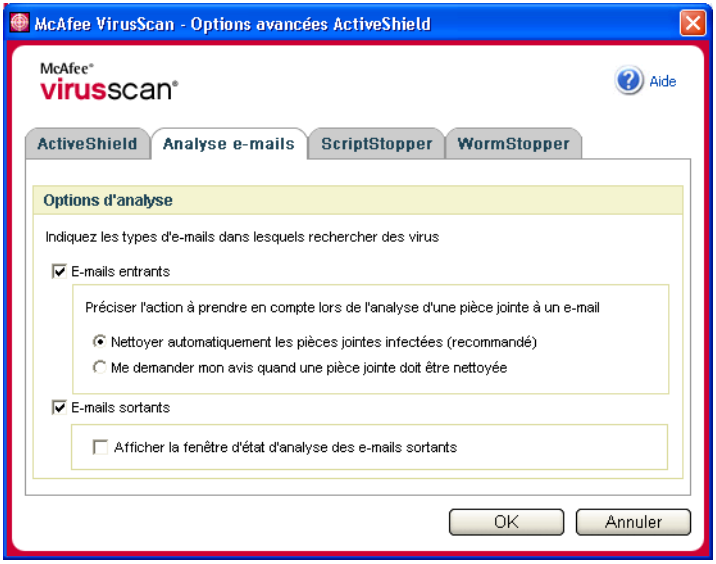


Figure 2-2. Options d'analyse des e-mails

Désactivation de la désinfection automatique 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 cliquez sur **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 contenues dans les messages instantanés entrants

Par défaut, l'analyse des pièces jointes contenues dans les messages instantanés est activée via l'option **Analyser les pièces jointes contenues dans les messages instantanés entrants** (Figure 2-1 à la page 14).

Lorsque cette option est activée, VirusScan analyse et essaie automatiquement de nettoyer les pièces jointes des messages instantanés entrants infectés pour les clients de messagerie instantanée les plus couramment utilisés, notamment :

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

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

Lorsqu'une pièce jointe contenue dans un message instantané entrant est infectée, VirusScan procède comme suit :

- Il tente de nettoyer le message infecté.
- Il vous demande de mettre en quarantaine ou de supprimer un message qui ne peut pas être nettoyé.

Analyse de tous les fichiers

Si vous configurez ActiveShield pour qu'il utilise l'option par défaut **Tous les fichiers (recommandé)**, il analyse tous les types de fichier lorsque votre ordinateur tente de les utiliser. Utilisez cette option pour obtenir l'analyse la plus complète possible.

Pour configurer ActiveShield afin d'analyser tous les types de fichier :

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

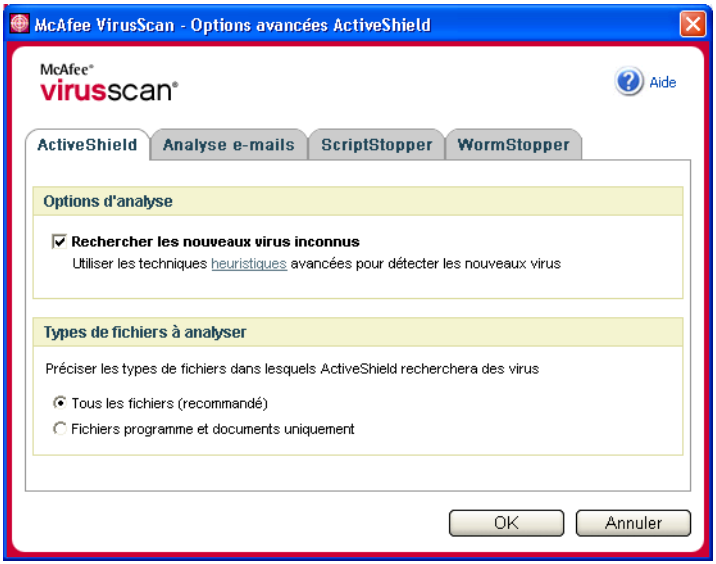


Figure 2-3. Options ActiveShield avancées

Analyse des fichiers programme et des documents uniquement

Si vous configurez ActiveShield pour qu'il utilise l'option **Fichiers programme et documents uniquement**, il analyse les fichiers programme et les documents, mais aucun des autres fichiers utilisés par votre ordinateur. Le dernier fichier de signature de virus (fichier .DAT) détermine les types de fichier qu'analysera ActiveShield. Pour configurer ActiveShield afin d'analyser les fichiers programme et les documents uniquement, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis cliquez sur **Options**.
2. Cliquez sur **Avancé**, puis sur l'onglet **ActiveShield** (Figure 2-3 à la page 19).
3. Cliquez sur **Fichiers programme et documents uniquement**, puis sur **OK**.

Recherche de virus nouveaux et inconnus

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

Pour configurer ActiveShield pour qu'il recherche les virus nouveaux et inconnus :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis cliquez sur **Options**.
2. Cliquez sur **Avancé**, puis sur l'onglet **ActiveShield** (Figure 2-3 à la page 19).
3. Cliquez sur **Rechercher les nouveaux virus inconnus** (recommandé), puis sur **OK**.

Recherche des scripts et des vers

VirusScan surveille votre ordinateur à la recherche de toute activité suspecte qui pourrait indiquer la présence d'une menace virale. Tandis que VirusScan permet d'éradiquer les virus, ScriptStopper™ et WormStopper™ empêchent virus, vers et chevaux de Troie de se répandre.

Les mécanismes de protection de ScriptStopper et de WormStopper détectent, signalent et bloquent les activités malveillantes, notamment :

- Une exécution de script qui entraîne la création, la copie/suppression de fichiers ou l'ouverture de votre registre Windows
- Une tentative de faire suivre des e-mails à une grande partie de votre carnet d'adresses
- Des tentatives de faire suivre plusieurs e-mails à intervalles rapprochés

Si vous configurez ActiveShield afin qu'il utilise les options par défaut **Activer ScriptStopper (recommandé)** et **Activer WormStopper (recommandé)** de la boîte de dialogue **Options avancées**, ScriptStopper et WormStopper surveillent l'exécution des scripts et l'activité des e-mails à la recherche de schémas suspects et vous alertent lorsqu'un nombre spécifié d'e-mails ou de destinataires est dépassé au cours d'un intervalle donné.

Pour configurer ActiveShield de manière à ce qu'il recherche les scripts malveillants et les activités de ver :

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

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

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

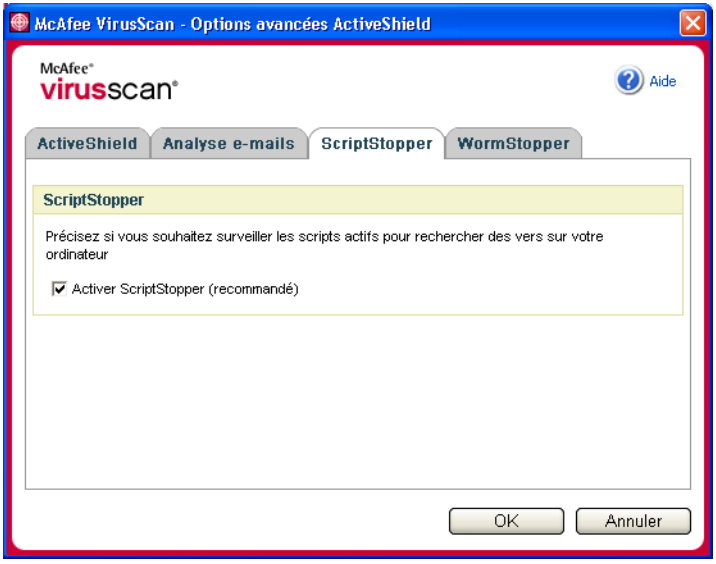


Figure 2-4. Options de ScriptStopper

4 Cliquez sur l'onglet **WormStopper**, sur **Activer WormStopper (recommandé)**, puis sur **OK** (Figure 2-5 à la page 22).

Par défaut, les options détaillées 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 la durée en secondes de la surveillance des e-mails envoyés, des détections erronées risquent de se produire. McAfee recommande de choisir l'option **Non** pour conserver les valeurs par défaut. Vous pouvez néanmoins cliquer sur **Oui** pour modifier la valeur applicable.

Cette option 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 24) :

- Blocage automatique des e-mails suspects sortants

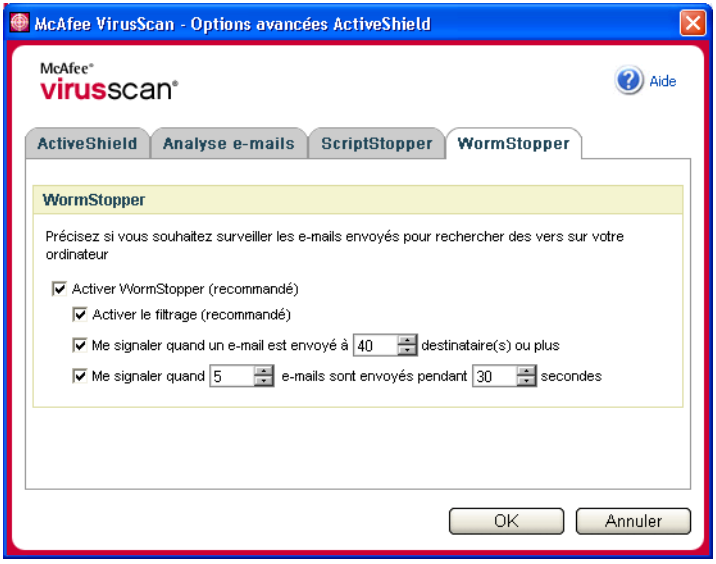


Figure 2-5. Options de WormStopper

Si ActiveShield trouve un virus

Si ActiveShield trouve un virus, une alerte de virus similaire à celle de la Figure 2-6 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 fichiers infectés, des e-mails infectés, des scripts suspects et des vers potentiels et décider de soumettre ou non les fichiers infectés aux laboratoires de McAfee AVERT pour analyse.

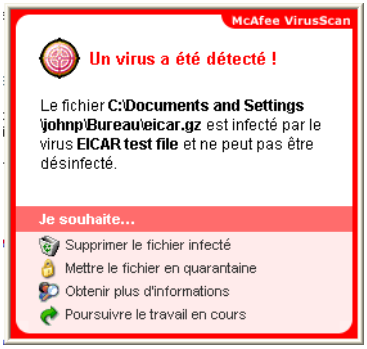


Figure 2-6. Alerte de virus

Gestion des fichiers infectés

1. Si ActiveShield peut éradiquer le virus, vous pouvez en savoir plus ou ignorer l'alerte :

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

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

   Un message de confirmation s'affiche et vous invite à effectuer une analyse antivirus de votre ordinateur. Cliquez sur **Analyser** pour exécuter le processus de mise en quarantaine.

3. Si ActiveShield ne parvient pas à mettre le fichier en quarantaine, cliquez sur **Supprimer le fichier infecté** pour tenter de supprimer le fichier.

Gestion des e-mails infectés

1. Si vous avez désactivé le nettoyage automatique des e-mails, vous avez la possibilité d'en savoir plus et de nettoyer l'e-mail :
   a. Cliquez sur **Obtenir plus d'informations** pour afficher le nom du fichier, le nom du virus, l'état de l'infection, l'expéditeur et l'objet de l'e-mail infecté.
   b. Cliquez sur **Nettoyer les pièces jointes infectées**.
2. Si ActiveShield ne parvient pas à nettoyer l'e-mail, cliquez sur **Mettre en quarantaine les pièces jointes infectées** pour chiffrer et isoler temporairement les fichiers infectés et suspects dans le répertoire de quarantaine jusqu'à ce qu'une action appropriée puisse être entreprise.

   Un message de confirmation s'affiche et vous invite à effectuer une analyse antivirus de votre ordinateur. Cliquez sur **Analyser** pour exécuter le processus de mise en quarantaine.
3. Si ActiveShield ne parvient pas à mettre l'e-mail en quarantaine, cliquez sur **Supprimer les pièces jointes infectées** pour tenter de supprimer le fichier.

Gestion des scripts suspects

1. Si ActiveShield détecte un script suspect, vous avez la possibilité d'en savoir plus à ce sujet mais vous pouvez aussi l'arrêter si vous n'aviez pas l'intention de le lancer :
   a. Cliquez sur **Obtenir plus d'informations** pour afficher le nom, l'emplacement et la description de l'activité associée au script suspect.
   b. Cliquez sur **Arrêter ce script** pour empêcher l'exécution du script suspect.
2. Si vous êtes certain de pouvoir faire confiance au script, vous pouvez autoriser son exécution :
   a. Cliquez sur **Autoriser cette fois ce script** pour autoriser une exécution unique de tous les scripts contenus dans un seul fichier.
   b. Cliquez sur **Poursuivre ce que je faisais** pour ignorer l'alerte et permettre l'exécution du script.

Gestion des vers potentiels

1. Si ActiveShield détecte un risque de ver, vous avez la possibilité d'en savoir plus à ce sujet, mais vous pouvez aussi arrêter l'e-mail si vous n'aviez pas l'intention de le lancer :
   a. Cliquez sur **Obtenir plus d'informations** 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.
   b. Cliquez sur **Arrêter cet e-mail** pour annuler l'envoi de l'e-mail suspect et l'effacer de votre file d'attente.
2. Si vous êtes certain de pouvoir faire confiance à l'activité d'e-mail en cours, cliquez sur **Poursuivre ce que je faisais** pour ignorer l'alerte et permettre l'envoi du message.

Analyse manuelle de votre ordinateur

La fonction Analyser vous 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 essaie automatiquement de le nettoyer, sauf s'il s'agit d'un programme potentiellement indésirable. Si elle ne peut pas nettoyer le fichier, vous pouvez supprimer ce dernier ou le mettre en quarantaine.

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 cliquez sur **Recherche de virus**.

La boîte de dialogue **Analyse antivirus** s'ouvre (Figure 2-7).

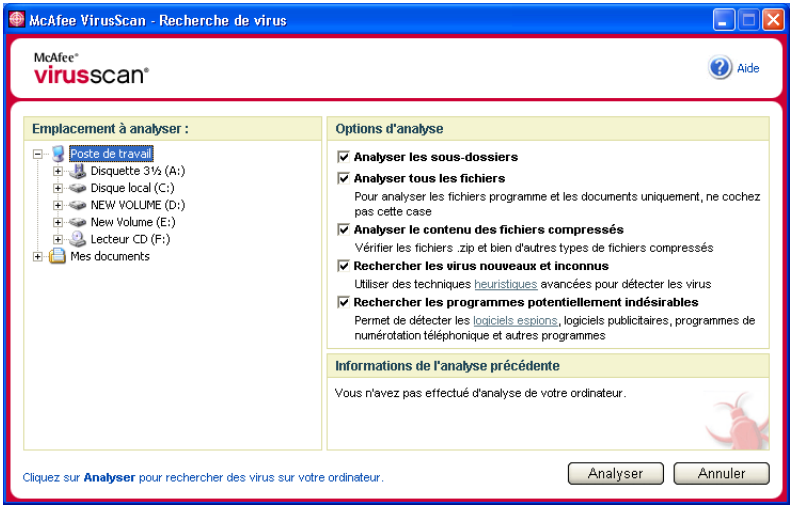


Figure 2-7. Recherche de virus

2 Cliquez sur le lecteur, le dossier ou le fichier que vous voulez 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 cette case pour limiter l'analyse aux seuls fichiers visibles lorsque vous ouvrez un dossier ou un lecteur.

  Exemple : les fichiers de la Figure 2-8 sont les seuls fichiers analysés si vous décochez la case **Analyser les sous-dossiers**. Les dossiers et leur contenu ne sont pas analysés. Pour analyser ces dossiers et leur contenu, laissez cette case cochée.

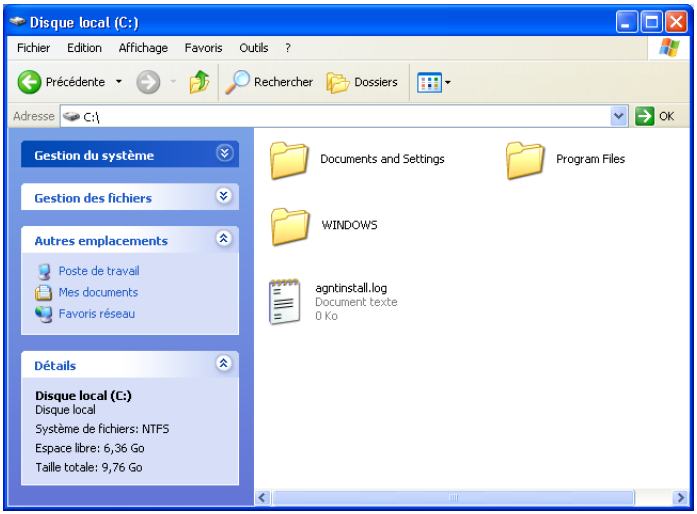


Figure 2-8. Contenu du disque local

- **Analyser tous les fichiers** — Cochez cette case pour permettre l'analyse complète de tous les types de fichier. Décochez cette case 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 cette case pour empêcher la vérification des fichiers, compressés ou non, contenus dans le fichier compressé.

  Parfois, les créateurs 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. Scan peut détecter ces virus lorsque cette option est sélectionnée.

- **Rechercher les virus nouveaux et inconnus** — Utilisez cette option pour rechercher les virus récents n'ayant peut-être pas encore de « 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 symptomatiques de virus non identifiés à l'intérieur des fichiers.

  Cette méthode d'analyse permet aussi de rechercher des caractéristiques de fichier qui, en général, écartent la présence éventuelle de virus dans le fichier. Cela minimise les risques que la fonction Analyser donne une indication erronée. Cependant, si une analyse heuristique détecte un virus, agissez avec les mêmes précautions que vous prendriez avec un fichier dont vous savez qu'il contient un virus.

  Bien qu'effectuant l'analyse la plus complète, cette option est généralement plus lente qu'une analyse normale.

- **Rechercher les programmes potentiellement indésirables** — Utilisez cette option 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 l'analyse. Plus le disque dur est volumineux et plus il contient de fichiers, plus l'analyse dure longtemps.

4 Cliquez sur **Analyser** pour commencer l'analyse des fichiers.

Lorsque l'analyse est 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 **Recherche de virus** (Figure 2-9).

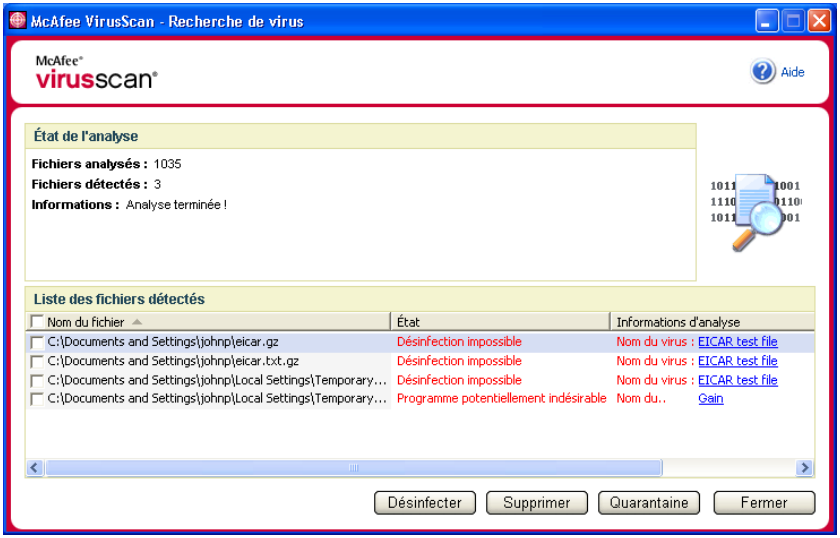


Figure 2-9. Résultats de l'analyse

REMARQUE
La fonction Analyser compte un fichier compressé (.ZIP, .CAB, etc.) comme un 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 Analyser 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. Sinon, reportez-vous à la rubrique *Si la fonction Analyser trouve un virus ou un programme potentiellement indésirable* à la page 31.

Analyse via 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 dans 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 **Recherche de virus** s'ouvre et l'analyse des fichiers démarre. Par défaut, toutes les **Options d'analyse** sont présélectionnées pour effectuer l'analyse la plus complète possible (Figure 2-7 à la page 25).

Analyse via Microsoft Outlook

VirusScan vous 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 97 ou version ultérieure.

Pour effectuer une analyse antivirus 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 effectuer l'analyse la plus complète possible (Figure 2-7 à la page 25).

Recherche automatique de virus et de programmes potentiellement indésirables

Bien que VirusScan n'analyse les fichiers que lorsque vous ou votre ordinateur y accédez, vous pouvez programmer une analyse automatique dans le planificateur de Windows afin de lancer une recherche intégrale 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 cliquez sur **Options**.

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

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

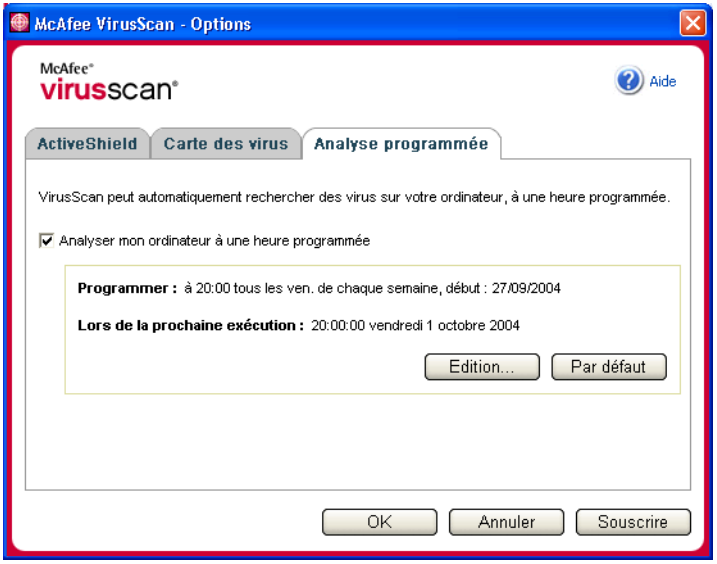


Figure 2-10. Options d'analyse programmée

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) jour(s) 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
Ces options ne sont pas prises en charge dans le planificateur de Windows : **Au démarrage du système**, **Si inactif** et **Afficher les différents horaires**. Le dernier calendrier pris en charge restera activé tant que vous n'aurez pas sélectionné l'une des options correctes.

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**. Sinon, cliquez sur **OK**.

Si la fonction Analyser trouve un virus ou un programme potentiellement indésirable

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

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 de 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 désinfecter.

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

4 Si la fonction Analyser ne peut pas nettoyer ou mettre le fichier en quarantaine, vous pouvez exécuter l'une des actions suivantes :

- Cliquez sur **Supprimer** pour supprimer le fichier.
- Cliquez sur **Fermer** pour fermer la boîte de dialogue.

Si la fonction Analyser ne peut pas nettoyer le fichier ou éradiquer le virus, consultez la bibliothèque d'informations sur les virus à l'adresse http://fr.mcafee.com/virusInfo/default.asp pour obtenir des instructions sur l'éradication manuelle du virus.

Si un fichier détecté vous empêche de vous connecter à Internet ou d'utiliser votre ordinateur, tentez d'utiliser une disquette de secours pour démarrer votre ordinateur. La disquette de secours permet généralement de démarrer un ordinateur paralysé par un fichier infecté. Pour plus d'informations, reportez-vous à la section *Création d'une disquette de secours* à la page 34.

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 fonctionnalité Mise en quarantaine chiffre et isole temporairement les fichiers infectés et suspects dans le répertoire de quarantaine jusqu'à ce qu'une action appropriée puisse être entreprise. Une fois nettoyé, 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 cliquez sur **Gestion des fichiers mis en quarantaine**.

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

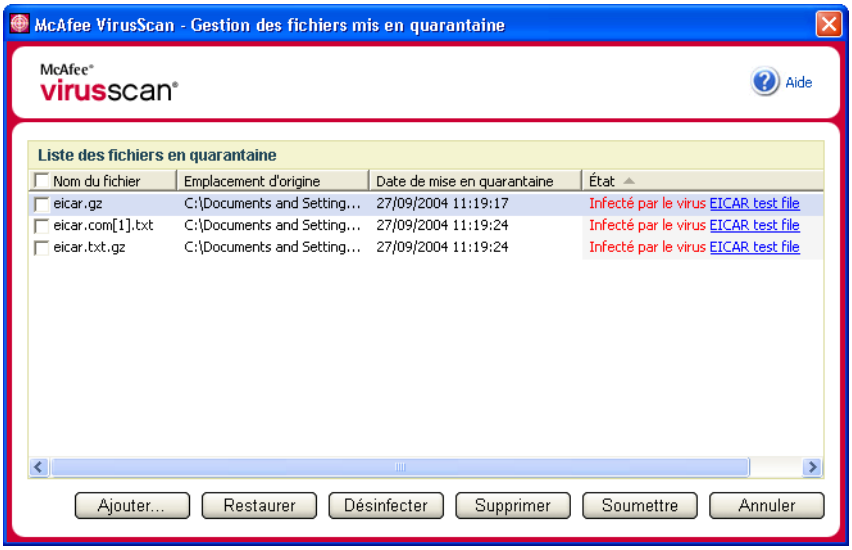


Figure 2-11. Gestion des fichiers mis en quarantaine

2 Cochez la case située en regard 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 **État** pour afficher des détails provenant de la bibliothèque d'informations sur les virus.
>
> Vous pouvez aussi cliquer sur **Ajouter**, sélectionner un fichier suspect à ajouter dans la liste des fichiers mis en quarantaine, cliquer sur **Ouvrir**, puis le sélectionner dans la liste des fichiers mis en quarantaine.

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 peut pas éradiquer le virus, cliquez sur **Supprimer** pour supprimer le fichier.

6 Si VirusScan ne parvient pas à nettoyer ou supprimer le fichier et s'il ne s'agit pas d'un programme potentiellement indésirable, vous pouvez le soumettre à McAfee AntiVirus Emergency Response Team (AVERT™) pour analyse :

   a Actualisez 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 contenant votre adresse électronique, votre pays, la version de votre logiciel, le nom de votre système d'exploitation ainsi que le nom d'origine et l'emplacement du fichier. La taille maximum de l'envoi est celle d'un fichier de 1,5 Mo par jour.

7 Cliquez sur **Fermer** pour fermer la boîte de dialogue.

Création d'une disquette de secours

L'utilitaire Rescue Disk crée une disquette de démarrage qui vous permet d'initialiser et d'analyser votre ordinateur si un virus vous 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 n'est disponible que pour les ordinateurs à partitions de disque dur FAT (FAT 16 et FAT 32). Elle est facultative 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 Analyser pour vous assurer que ni votre ordinateur, ni la disquette ne contiennent de virus Pour plus d'informations, reportez-vous à la section *Recherche manuelle de virus et de programmes potentiellement indésirables* à la page 25.

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

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

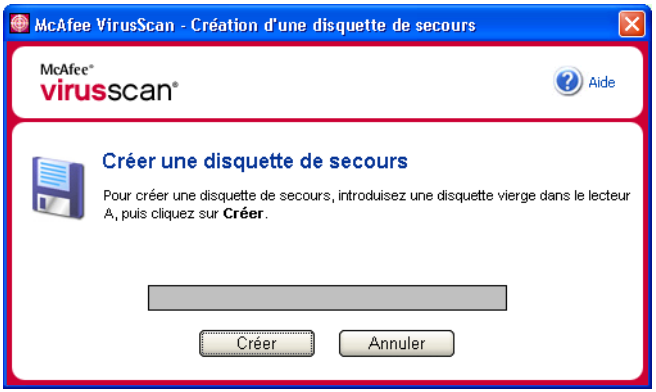


Figure 2-12. Création d'une disquette de secours

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

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

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.

L'état de la création s'affiche dans la boîte de dialogue **Création d'une disquette de secours**.

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. Éteignez l'ordinateur infecté.
2. Insérez la disquette de secours dans le lecteur.
3. Allumez l'ordinateur.

   Une fenêtre grise à choix multiple s'affiche.
4. Choisissez l'option qui répond le mieux 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

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

Notification à World Virus Map

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

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

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

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

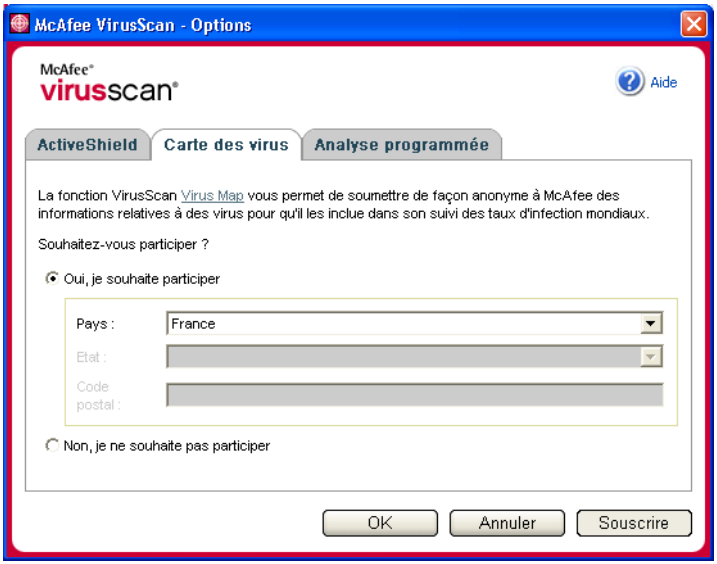


Figure 2-13. Options de Carte des virus

3 Acceptez l'option par défaut **Oui, je souhaite participer** pour envoyer de manière anonyme vos informations sur les virus à World Virus Map, le baromètre des taux d'infection mondiaux de McAfee. Sinon, sélectionnez **Non, je ne souhaites pas participer** pour ne pas envoyer vos informations.

4 Si vous résidez aux États-Unis, sélectionnez l'état et entrez le code postal de la localité où se trouve votre ordinateur. Dans le cas contraire, VirusScan tente automatiquement de sélectionner le pays dans lequel 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 taux d'infection mondiaux les plus récents via l'icône McAfee de votre 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 cliquez sur **World Virus Map**.

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

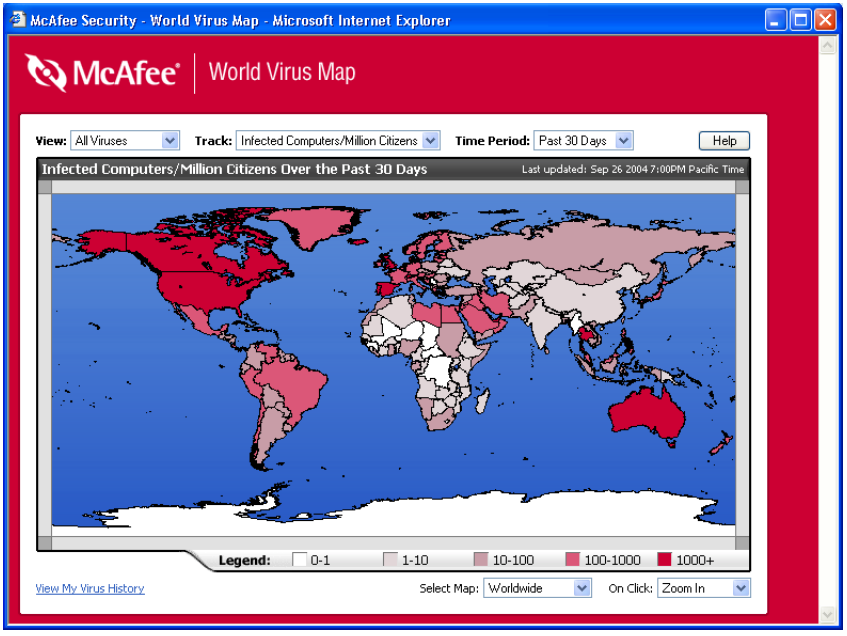


Figure 2-14. World Virus Map

Par défaut, World Virus Map indique le nombre d'ordinateurs qui ont été infectés dans le monde au cours des derniers 30 jours, ainsi que la date de la dernière mise à jour des données de notification. Vous pouvez changer l'affichage de la carte afin de connaître le nombre de fichiers infectés ou changer la période de temps afin d'afficher uniquement les résultats pour les 7 jours précédents ou les dernières 24 heures.

La section **Virus Tracking (Suivi de virus)** présente les nombres totaux cumulés de fichiers analysés, de fichiers infectés et d'ordinateurs infectés signalés depuis 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 des définitions de virus, sans interrompre votre travail.

Les fichiers de définition de virus font environ 100 Ko et ont donc un impact minimal 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 toute menace d'attaque virale.

Recherche automatique de mises à jour

McAfee SecurityCenter est automatiquement configuré pour vérifier toutes les quatre heures les mises à jour de tous vos services McAfee lorsque vous êtes connecté à Internet et pour vous en informer à l'aide de messages d'alerte et 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 achever la mise à jour. Assurez-vous d'enregistrer tous vos travaux et de fermer toutes les applications avant de redémarrer.

Recherche manuelle de mises à jour

Parallèlement à la recherche automatique de mises à jour toutes les quatre heures lorsque vous êtes connecté à Internet, vous pouvez également rechercher manuellement des mises à jour à tout moment.

Pour rechercher manuellement des mises à jour de VirusScan :

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

   La boîte de dialogue **Mises à jour de McAfee SecurityCenter** s'ouvre.

3 Cliquez sur **Vérifier**.

Si une mise à jour existe, la boîte de dialogue **Mises à jour de VirusScan** s'affiche (voir Figure 2-15). Cliquez sur **Mettre à jour** pour continuer.

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

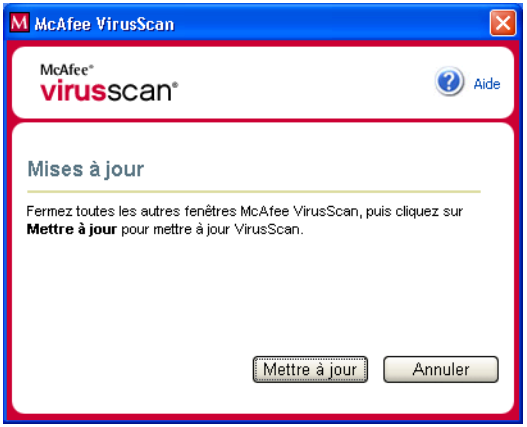


Figure 2-15. Boîte de dialogue des mises à jour

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

5 Cliquez sur **Terminer** une fois l'installation de la mise à jour terminée.

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

Index

D

E

L

M

N

O

P

S

T

U

V

W