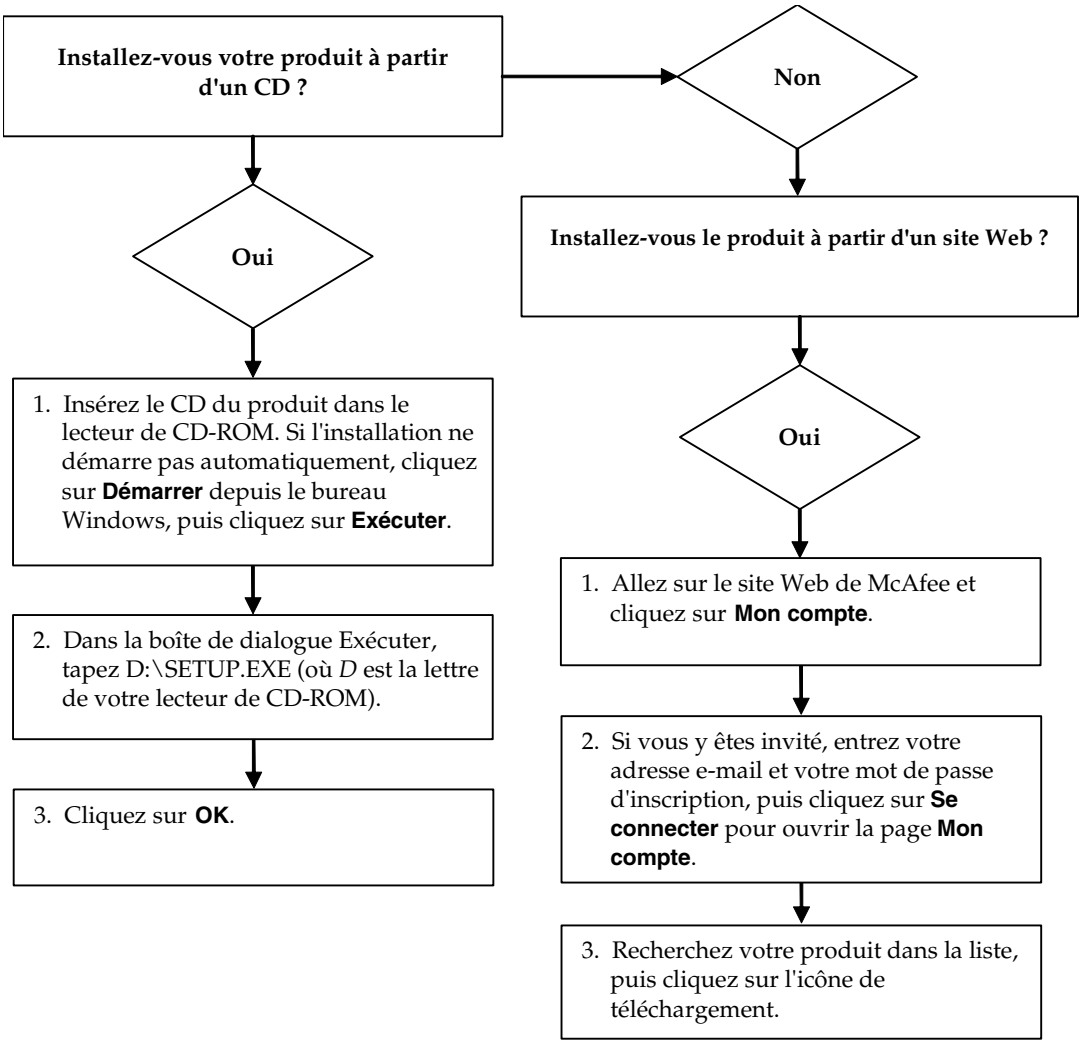
McAfee
virusscan®

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-ROM du produit, assurez-vous qu'Acrobat Reader est installé sur votre ordinateur ; sinon, installez-le depuis le CD-ROM du produit McAfee.

1. Insérez le CD-ROM 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

McAfee vous conseille de suivre les instructions fournies avec le produit pour vous enregistrer directement. 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 si vous achetez le logiciel VirusScan.

  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 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.

Support technique

Pour toute question relative au support technique, consultez notre site

http://www.mcafeeaide.com/.

Notre site de support offre, 24 heures sur 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 à l'options gratuite 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 nos services d'assistance téléphonique sur notre site

http://www.mcafeeaide.com/.

Table des matières

Mise en route 1

Bienvenue dans McAfee VirusScan.

McAfee VirusScan est un service d'abonnement offrant une protection antivirus complète, fiable et à jour. Géré par notre moteur d'analyse McAfee à la pointe de la technologie, VirusScan protège votre ordinateur contre les virus, vers, chevaux de Troie, scripts suspects, attaques hybrides et autres menaces.

Il vous offre les fonctionnalités suivantes :

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

Analyse : recherche des virus et d'autres menaces sur les disques durs et les disquettes, ainsi que dans des fichiers et dossiers individuels.

Quarantaine : chiffre et isole temporairement les fichiers suspects dans le répertoire de quarantaine jusqu'à ce que vous puissiez entreprendre l'action appropriée.

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

Nouvelles fonctions

Cette version de VirusScan vous offre les nouvelles fonctions suivantes :

- **Détection et suppression des logiciels espions et publicitaires**
  VirusScan identifie et supprime les logiciels espions et publicitaires ainsi que tous les programmes mettant en péril votre confidentialité ou ralentissent les performances de votre ordinateur.
- **Mises à jour quotidiennes automatiques**
  Les mises à jour quotidiennes automatiques de VirusScan vous protègent contre les dernières menaces informatiques, identifiées ou non.
- **Analyse rapide en arrière-plan**
  Les analyses discrètes et rapides permettent d'identifier et de détruire les virus, chevaux de Troie, vers, logiciels espions et publicitaires, programmes de numérotation téléphonique et autres menaces sans interrompre votre travail.
- **Alertes de sécurité en temps réel**
  Les alertes de sécurité vous avertissent des épidémies de virus et des menaces de sécurité, tout en vous fournissant des possibilités de réponse pour supprimer, neutraliser ou mieux connaître la menace.

- **Détection et nettoyage à de multiples points d'entrée**
  VirusScan contrôle et nettoie les principaux points d'entrée de votre ordinateur : e-mail, pièces jointes contenues dans les messages instantanés et fichiers Internet téléchargés.

- **Surveillance des e-mails contre les activités de type ver**
  La technologie WormStopper™ contrôle les activités de diffusion massive identifiées comme étant suspectes, et empêche les virus et les vers de se propager vers d'autres ordinateurs par l'intermédiaire des e-mails.

- **Surveillance des scripts contre les activités de type ver**
  La technologie ScriptStopper™ contrôle les exécutions des scripts identifiées comme étant suspectes, et empêche les virus et les vers de se propager vers d'autres ordinateurs par l'intermédiaire des e-mails.

- **Support technique gratuit par messages instantanés et e-mail**
  Le support technique fournit en direct une assistance rapide et simple par message instantané ou par e-mail.

Configuration système requise

- Microsoft® Windows 98, Windows Me, Windows 2000 ou Windows XP
- Ordinateur personnel avec processeur compatible Pentium
  Windows 98, 2000 : 133 MHz minimum
  Windows Me : 150 MHz ou supérieur
  Windows XP (Édition familiale et Professionnelle) : 300 MHz minimum
- RAM
  Windows 98, Me, 2000 : 64 Mo
  Windows XP (Édition familiale et Professionnelle) : 128 Mo
- 40 Mo disponibles sur le disque dur
- Microsoft® Internet Explorer 5.5 ou ultérieur

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

Programmes de messagerie pris en charge

- POP3 (Outlook Express, Outlook, Eudora, Netscape)

Programmes de messagerie instantanée pris en charge :

- AOL Instant Messenger version 2.1 ou ultérieure
- Yahoo Messenger version 4.1 ou ultérieure
- Microsoft Windows Messenger version 3.6 ou ultérieure
- MSN Messenger version 6.0 ou ultérieure

Test de VirusScan

Avant de commencer à utiliser VirusScan, il est judicieux de tester votre installation. Pour tester séparément ActiveShield et la fonction d'analyse, suivez les étapes ci-après.

Test d'ActiveShield

REMARQUE
Pour tester ActiveShield à partir de l'onglet VirusScan dans SecurityCenter, cliquez sur **Tester VirusScan** pour afficher les FAQ de l'assistance en ligne où ces étapes sont définies.

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. Faites défiler la page jusqu'en bas. Dans la zone **Download**, (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 détectés pour voir comment ActiveShield traite les menaces potentielles. Pour plus d'informations, consultez la section *Mieux comprendre les alertes de sécurité* à la page 25.

Test de la fonction d'analyse

Avant de tester la fonction d'analyse, vous devez désactiver ActiveShield (sinon, il détectera les fichiers de test avant que la fonction d'analyse ne le fasse) ; 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 d'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 Faites défiler la page jusqu'en bas. Dans la zone **Download** (télécharger), les liens suivants apparaissent :

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 éprouvent des difficultés à télécharger le premier lien. Il vous suffit de le renommer 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 dans un fichier compressé .ZIP, qui se trouve lui-même dans 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**, puis sur le bouton **Créer un nouveau dossier**, puis renommez le dossier créé **Dossier Analyse VSO**.

f Double-cliquez sur le **Dossier Analyse VSO**, 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 d'analyse :

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

2 À l'aide de l'arborescence de répertoires dans le volet gauche de la boîte de dialogue, allez dans le **Dossier Analyse VSO** où vous avez enregistré les fichiers :

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

b Cliquez sur le **Dossier Analyse VSO** afin de le mettre en surbrillance (ne cliquez pas sur le signe **+** situé en regard).

Ainsi, vous indiquez à la fonction d'analyse de vérifier ce dossier uniquement. 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 la fonction d'analyse.

3 Dans la zone **Options d'analyse** de la boîte de dialogue **Analyse**, assurez-vous que toutes les options sont sélectionnées.

4 Cliquez sur **Analyser** dans la partie inférieure droite de la boîte de dialogue.

VirusScan analyse le **Dossier analyse VSO**. Si les fichiers de test EICAR que vous avez enregistrés dans ce dossier apparaissent dans la **Liste des fichiers détectés**, alors, l'analyse fonctionne correctement.

Vous pouvez tenter de supprimer ou de mettre en quarantaine les fichiers détectés pour voir comment la fonction d'analyse traite les menaces potentielles. Pour plus d'informations, consultez la section *Mieux comprendre les détections de menace* à la page 36.

Utilisation de McAfee SecurityCenter

McAfee SecurityCenter est votre centre de sécurité unique, 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 continuellement mises à jour et les informations les plus récentes sur les produits.
- 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 fonctions 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 sur l'icône McAfee avec le bouton droit de la souris.

2 Cliquez sur **Ouvrir SecurityCenter**.

Pour accéder à une fonction de VirusScan :

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

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. Il analyse les fichiers lorsque vous ou votre ordinateur y accédez. Lorsqu'il détecte un fichier, il tente automatiquement de le désinfecter. S'il n'y parvient pas, vous pouvez placer le fichier en quarantaine ou le supprimer.

Activation ou désactivation d'ActiveShield

ActiveShield est démarré (chargé dans la mémoire de l'ordinateur) et activé (signalé par l'icône rouge dans la 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 par l'icône noire), vous pouvez l'exécuter manuellement et le configurer pour qu'il se lance 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 cliquez sur **Activer** L'icône 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 menaces. Dans le cas contraire, le programme affiche une boîte de dialogue vous permettant de configurer le système pour lancer ActiveShield au démarrage de Windows (figure 2-1 à la page 14).

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 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 menaces lorsque vous le redémarrez.

Configuration des options d'ActiveShield

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

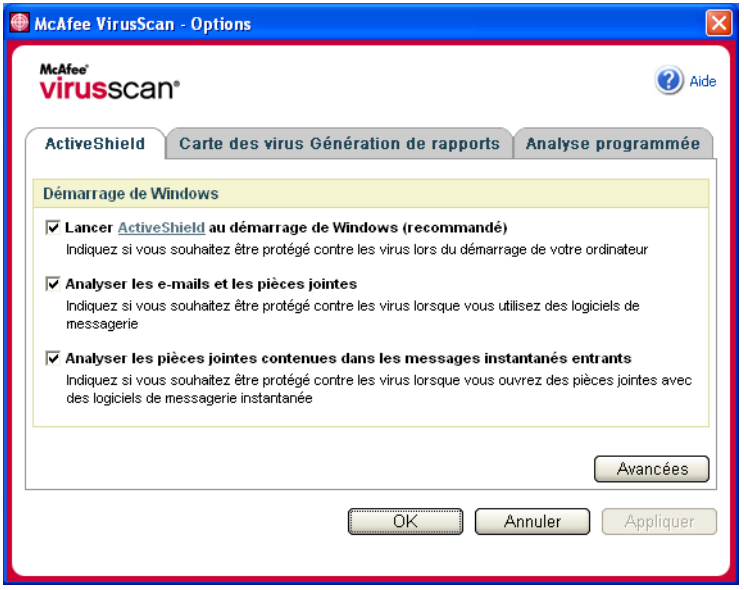


Figure 2-1. Options d'ActiveShield

Démarrage d'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 les nouveaux fichiers. Lorsque l'**Assistant de mise à jour** vous invite à cliquer sur **Terminer**, ActiveShield redémarre.

Pour lancer 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 **Options VirusScan** apparaît (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 de nouveau sur **OK**.

Arrêt d'ActiveShield

> **AVERTISSEMENT**
> Si vous arrêtez ActiveShield, votre ordinateur n'est plus protégé contre les menaces. 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 **Options VirusScan** apparaît (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 de nouveau sur **OK**.

Analyse des e-mails et des pièces jointes

Par défaut, l'analyse et la désinfection automatique des e-mails sont activées via l'option **Analyser les e-mails et les pièces jointes** (figure 2-1 à la page 14).

Lorsque cette option est activée, ActiveShield analyse automatiquement les e-mails et les pièces jointes détectés, entrants (POP3) comme sortants (SMTP), et tente de les désinfecter, 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 prise en charge pour les clients de messagerie suivants : ceux basés sur le Web, IMAP, AOL, POP3 SSL et Lotus Notes. Toutefois, ActiveShield analyse les pièces jointes aux e-mails dès leur ouverture.

Si vous désactivez l'option **Analyser les e-mails et les pièces jointes**, les options d'analyse e-mail et celles de WormStopper (figure 2-2 à la page 17) 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 e-mail, vous devez redémarrer votre programme de messagerie pour appliquer les modifications.

E-mails entrants

S'il détecte un e-mail ou une pièce jointe entrants, ActiveShield procède comme suit :

- Il tente de désinfecter l'e-mail détecté.
- Il tente de mettre en quarantaine ou de supprimer tout e-mail qui ne peut pas être désinfecté.
- Il intègre, dans l'e-mail entrant, un fichier d'alerte qui décrit les actions réalisées pour supprimer la menace potentielle.

E-mails sortants

S'il détecte un e-mail ou une pièce jointe sortants, ActiveShield procède comme suit :

- Il tente de désinfecter l'e-mail détecté.
- Il tente de mettre en quarantaine ou de supprimer tout e-mail qui ne peut pas être désinfecté.

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

Désactivation de l'analyse des e-mails

Par défaut, ActiveShield analyse les e-mails entrants et sortants. Si vous souhaitez bénéficier d'un meilleur contrôle, vous pouvez toutefois configurer ActiveShield pour 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 cliquez sur **Options**.
2. Cliquez sur **Avancé**, puis sur l'onglet **Analyse e-mails** (Figure 2-2).
3. Désélectionnez l'option **E-mails entrants** ou **E-mails sortants**, puis cliquez sur **OK**.

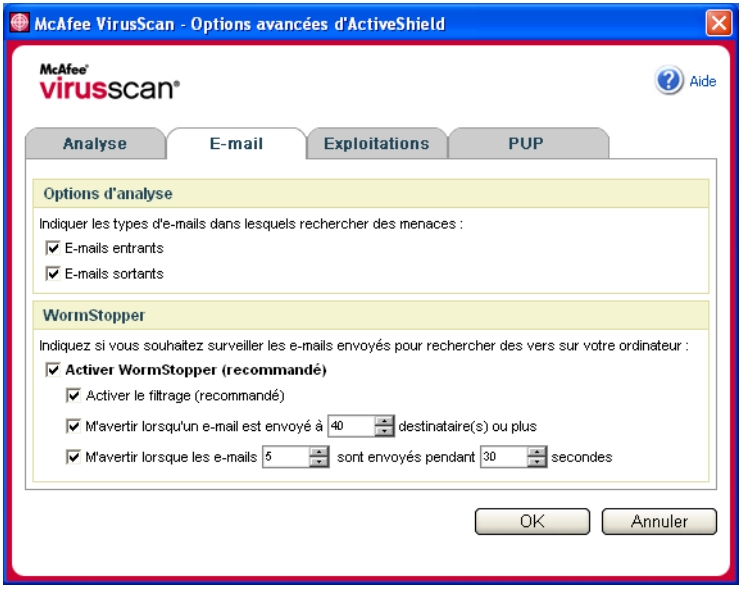


Figure 2-2. Options avancées d'ActiveShield - Onglet E-mail

Recherche des vers

VirusScan surveille votre ordinateur à la recherche de toute activité suspecte qui pourrait signaler la présence d'une menace virale. Tandis que VirusScan permet d'éradiquer les virus et d'autres menaces, WormStopper™ empêche la propagation des virus et des vers.

Un « ver » informatique est un virus qui se propage automatiquement et qui se fixe dans la mémoire active et peut utiliser les e-mails pour envoyer des copies de lui-même. Sans WormStopper, les vers sont uniquement détectables lorsque leur réplication non contrôlée puise dans les ressources du système en venant ralentir ses performances ou en interrompant les tâches.

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

- 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 l'option par défaut **Activer WormStopper (recommandé)** de la boîte de dialogue **Options avancées**, WormStopper surveille l'activité des courriers électroniques à la recherche de schémas suspects et vous alerte lorsqu'un nombre spécifié de courriers électroniques ou de destinataires est dépassé au cours d'un intervalle donné.

Pour configurer ActiveShield de manière à ce qu'il recherche les activités de ver dans les messages e-mails envoyés :

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 **E-mail**.

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

Par défaut, les options détaillées ci-dessous sont activées :

- recherche de schémas indiquant une activité suspecte
- émission d'un avertissement quand un e-mail est envoyé à 40 destinataires ou plus
- émission d'un avertissement quand 5 e-mails ou plus sont envoyés en moins de 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 27) :

- Blocage automatique des e-mails sortants suspects

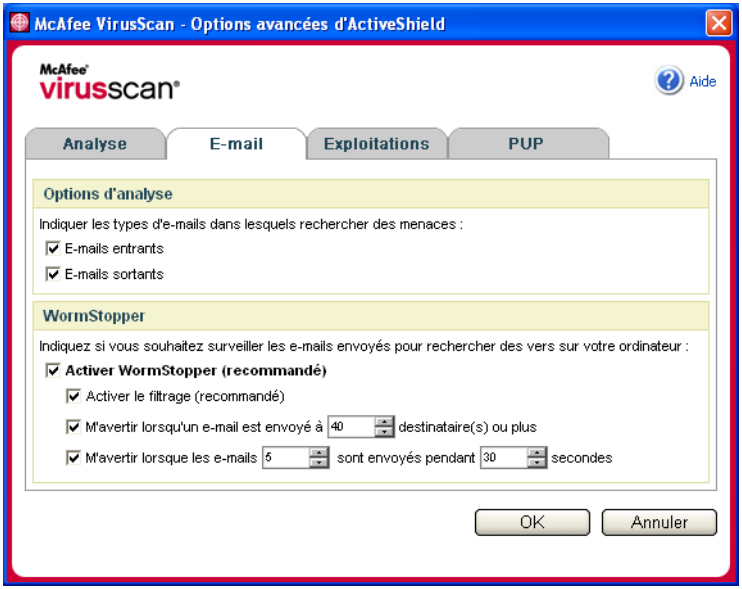


Figure 2-3. Options avancées d'ActiveShield - Onglet E-mail

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 détectés pour les programmes de messagerie instantanée les plus souvent utilisés, dont :

- 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 la désinfection automatique des pièces jointes contenues dans les messages instantanés.

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

- Il tente de désinfecter le message détecté.
- Il vous demande de mettre en quarantaine ou de supprimer tout message qui ne peut pas être désinfecté.

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 fichiers utilisés par votre ordinateur lorsque celui-ci tente de les utiliser. Cette option fournit l'analyse la plus complète possible.

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

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis cliquez sur **Options**.
2. Cliquez sur **Avancée**, puis sur l'onglet **Analyse** (figure 2-4 à la page 21).
3. Cliquez sur **Tous les fichiers (recommandé)**, puis sur **OK**.

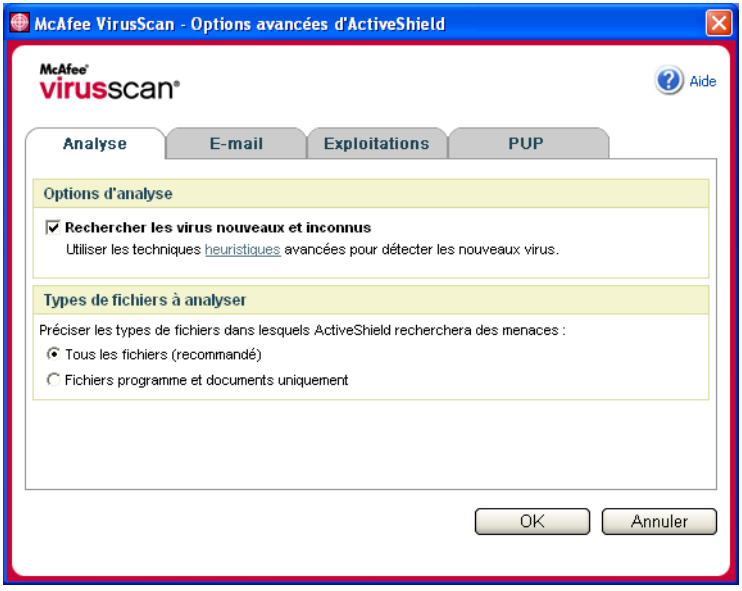


Figure 2-4. Options avancées d'ActiveShield - Onglet Analyse

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 fichiers 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 **Avancée**, puis sur l'onglet **Analyse** (Figure 2-4).
3. Cliquez sur **Fichiers programme et documents uniquement**, puis sur **OK**.

Recherche des virus nouveaux et inconnus

Si vous définissez ActiveShield sur l'option par défaut **Rechercher les nouveaux virus inconnus**, il utilise des techniques heuristiques avancées pour tenter 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, 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 **Avancée**, puis sur l'onglet **Analyse** (Figure 2-4).
3. Cliquez sur **Rechercher les virus nouveaux et inconnus (recommandé)**, puis sur **OK**.

Recherche des scripts

VirusScan surveille votre ordinateur à la recherche de toute activité suspecte qui pourrait signaler la présence d'une menace virale. Tandis que VirusScan permet d'éradiquer les virus et d'autres menaces, ScriptStopper™ empêche les chevaux de Troie d'exécuter des scripts et de propager davantage les virus.

Un « cheval de Troie » est un programme suspect qui se fait passer pour une application anodine. Les chevaux de Troie ne sont pas des virus, car ils ne se répliquent pas, mais ils sont tout aussi ravageurs.

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

- l'exécution d'un script qui entraîne la création/copie/suppression de fichiers ou l'ouverture de votre registre Windows,

Si vous configurez ActiveShield afin qu'il utilise l'option par défaut **Activer ScriptStopper (recommandé)** de la boîte de dialogue **Options avancées**, ScriptStopper surveille l'exécution des scripts à la recherche de schémas suspects et vous alerte lorsqu'un nombre spécifié de courriers électroniques ou de destinataires est dépassé au cours d'un intervalle donné.

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

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis cliquez sur **Options**.
2. Cliquez sur **Avancée**, puis sur l'onglet **Exploitations** (Figure 2-5).
3. Cliquez sur **Activer ScriptStopper (recommandé)**, puis sur **OK**.

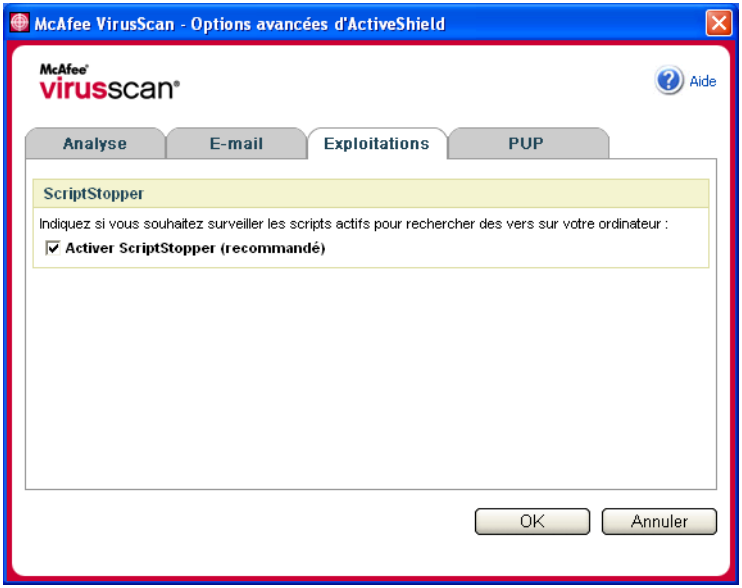


Figure 2-5. Options avancées d'ActiveShield - Onglet Exploitations

Recherche des programmes potentiellement indésirables (PUP)

REMARQUE
Si McAfee AntiSpyware est installé sur votre ordinateur, il gère les activités de tous les programmes potentiellement indésirables. Ouvrez McAfee AntiSpyware pour configurer vos options.

Si vous configurez ActiveShield pour qu'il utilise par défaut l'option **Rechercher les programmes potentiellement indésirables (recommandé)** dans la boîte de dialogue **Options avancées**, la protection contre les programmes potentiellement indésirables (PUP) détecte, bloque et élimine rapidement les logiciels espions et publicitaires, ainsi que tous les autres programmes qui accèdent à vos données personnelles et les transmettent sans votre autorisation.

Pour configurer ActiveShield afin qu'il recherche tous les PUP :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis cliquez sur **Options**.
2. Cliquez sur **Avancée**, puis sur l'onglet **PUP** (Figure 2-6).
3. Cliquez sur **Rechercher les programmes potentiellement indésirables (recommandé)**, puis sur **OK**.

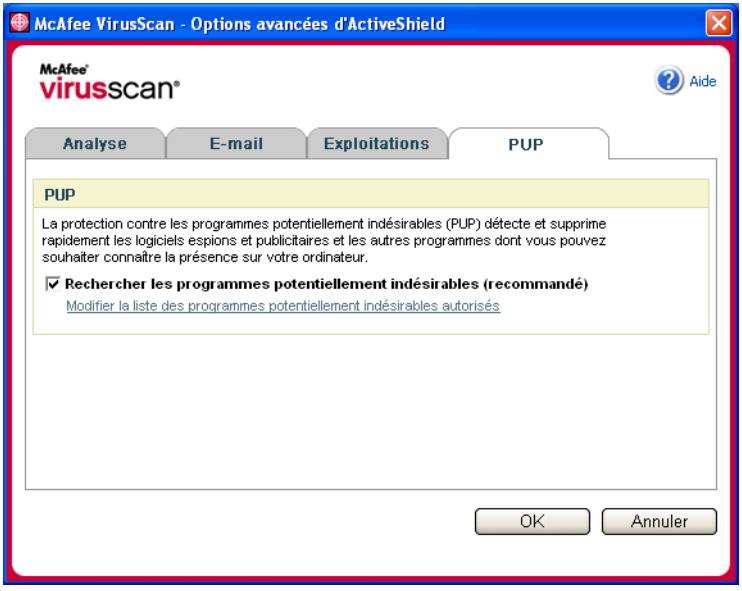


Figure 2-6. Options avancées d'ActiveShield - Onglet PUP

Mieux comprendre les alertes de sécurité

Si ActiveShield trouve un virus, une alerte similaire à celle de la Figure 2-7 s'affiche. Pour la plupart des virus, des chevaux de Troie et des vers, ActiveShield tente automatiquement de désinfecter le fichier et vous avertit. Pour les programmes potentiellement indésirables (PUP), ActiveShield détecte le fichier, le bloque automatiquement et vous avertit.

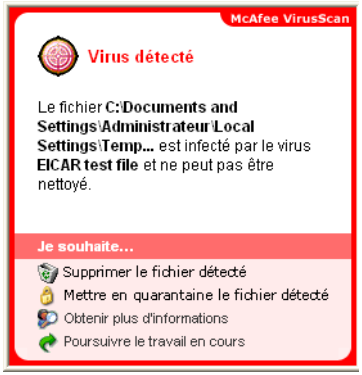


Figure 2-7. Alerte de virus

Vous pouvez alors choisir la méthode de traitement des fichiers et e-mails détectés, des scripts suspects, des vers potentiels ou des PUP, et décider de soumettre ou non les fichiers infectés aux laboratoires de McAfee AVERT pour analyse.

Pour plus de protection, vous êtes invité à analyser immédiatement l'ensemble de votre ordinateur chaque fois qu'ActiveShield détecte un fichier suspect. Cette analyse vous est rappelée de manière périodique, à moins que vous ne décidiez de masquer l'invite d'analyse.

Gestion des fichiers détectés

1. Si ActiveShield peut désinfecter le fichier, vous avez la possibilité d'en savoir plus ou d'ignorer l'alerte :
   - Cliquez sur **Obtenir des informations complémentaires** pour afficher le nom du fichier détecté, 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 désinfecter le fichier, cliquez sur **Mettre en quarantaine le fichier détecté** pour chiffrer et isoler temporairement les fichiers suspects dans le répertoire de quarantaine jusqu'à ce qu'une action appropriée puisse être entreprise.

   Un message de confirmation vous invite à effectuer une analyse de votre ordinateur. Cliquez sur **Analyser** pour mettre le fichier en quarantaine.
3. Si ActiveShield ne parvient pas à mettre le fichier en quarantaine, cliquez sur **Supprimer le fichier détecté** pour tenter de supprimer le fichier.

Gestion des e-mails détectés

Par défaut, l'analyse des e-mails tente automatiquement de désinfecter l'e-mail détecté. Un fichier d'alerte inclus dans le message sortant vous indique si l'e-mail a été nettoyé, mis en quarantaine ou supprimé.

Gestion des scripts suspects

Si ActiveShield détecte un script suspect, vous avez la possibilité d'en savoir plus à ce sujet, mais vous pouvez également arrêter le script si vous n'aviez pas l'intention de le lancer :

- Cliquez sur **Obtenir des informations complémentaires** pour afficher le nom, l'emplacement et la description de l'activité associée au script suspect.
- Cliquez sur **Arrêter ce script** pour empêcher l'exécution du script suspect.

Si vous êtes certain de pouvoir faire confiance au script, vous pouvez autoriser son exécution :

- Cliquez sur **Autoriser cette fois ce script** pour autoriser une exécution unique de tous les scripts contenus dans un même fichier.
- Cliquez sur **Poursuivre le travail en cours** pour ignorer l'alerte et permettre l'exécution du script.

Gestion des vers potentiels

Si ActiveShield détecte un ver potentiel, vous avez la possibilité d'en savoir plus à ce sujet, mais vous pouvez également arrêter l'e-mail si vous n'aviez pas l'intention de le lancer :

- Cliquez sur **Obtenir des informations complémentaires** pour afficher la liste des destinataires, l'objet, le corps du message et la description de l'activité suspecte associée à l'e-mail détecté.
- Cliquez sur **Arrêter cet e-mail** pour annuler l'envoi du message suspect et l'effacer de votre file d'attente.

Si vous êtes certain de pouvoir faire confiance à l'opération de courrier électronique en cours, cliquez sur **Poursuivre le travail en cours** pour ignorer l'alerte et permettre l'envoi du message.

Gestion des PUP

Si ActiveShield détecte et bloque un programme potentiellement indésirable (PUP), vous avez la possibilité d'en savoir plus à ce sujet, puis de supprimer ce programmes si vous n'aviez pas l'intention de l'installer :

- Cliquez sur **Obtenir des informations complémentaires** pour afficher le nom du fichier infecté, son emplacement et l'action recommandée associée au PUP.
- Cliquez sur **Supprimer ce PUP** pour supprimer le programme si vous n'aviez pas l'intention de l'installer.

  Un message de confirmation apparaît.

  - Si (a) vous ne parvenez pas à identifier le PUP, ou (b) vous ne l'avez pas installé dans le cadre d'une offre groupée et/ou avez accepté un contrat de licence associé à ces programmes, cliquez sur **OK** pour désinstaller le programme à l'aide du programme de désinstallation McAfee.

  - Sinon, cliquez sur **Annuler** pour quitter le processus de désinstallation automatique. Si vous changez d'avis ultérieurement, vous pouvez désinstaller manuellement le programme à l'aide du programme de désinstallation du fournisseur.
- Cliquez sur **Poursuivre le travail en cours** pour ignorer l'alerte et bloquer le programme cette fois-ci.

Si vous (a) parvenez à identifier le PUP ou (b) vous l'avez installé dans le cadre d'une offre groupée et/ou avez accepté un contrat de licence associé à ce programme, vous pouvez autoriser son exécution.

- Cliquez sur **Autoriser ce PUP** pour l'intégrer à votre liste blanche et toujours autoriser son exécution.

  Pour plus d'informations, consultez la section « *Gestion des PUP autorisés* ».

Gestion des PUP autorisés

Les programmes ajoutés à la liste de PUP autorisés ne sont pas détectés par McAfee VirusScan.

Si un PUP est détecté et ajouté dans la liste des PUP autorisés, vous pouvez au besoin le supprimer de la liste.

Si votre liste de PUP autorisés est pleine, vous devez supprimer certains éléments avant de pouvoir autoriser un autre PUP.

Pour supprimer un programme de votre liste de PUP autorisés :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **VirusScan**, puis cliquez sur **Options**.
2. Cliquez sur **Avancée**, puis sur l'onglet **PUP**.
3. Cliquez sur **Modifier la liste des PUP autorisés**, cochez la case en regard du nom du fichier et cliquez sur **Supprimer.** Cliquez sur **OK** lorsque vous n'avez plus d'éléments à supprimer.

Analyse manuelle de votre ordinateur

La fonction d'analyse vous permet de rechercher de manière sélective des virus et d'autres menaces sur les disques durs et les disquettes, ainsi que dans des fichiers et dossiers individuels. Quand elle détecte un fichier suspect, elle tente automatiquement de le désinfecter, sauf s'il s'agit d'un programme potentiellement indésirable. Si elle ne parvient pas à désinfecter le fichier, vous pouvez le mettre en quarantaine ou le supprimer.

Recherche manuelle des virus et d'autres menaces

Pour analyser votre ordinateur :

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

La boîte de dialogue **Analyse** s'ouvre (Figure 2-8).

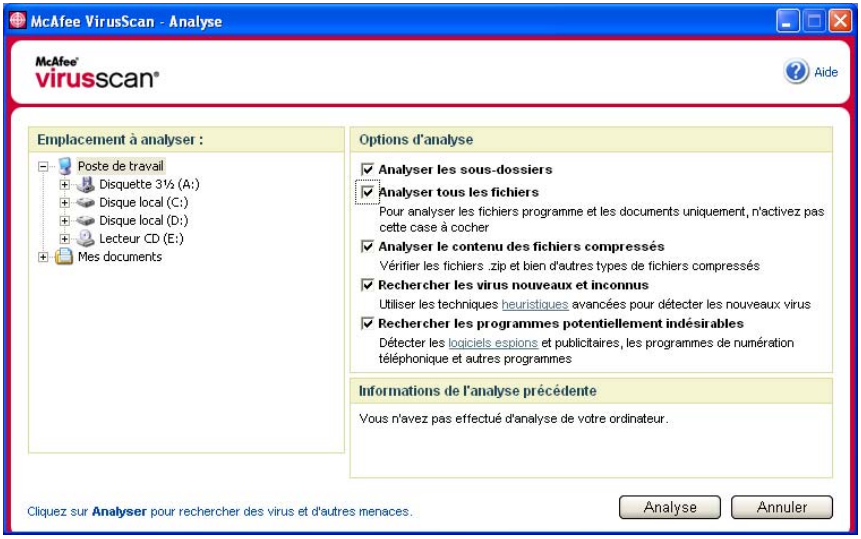


Figure 2-8. Boîte de dialogue Analyse

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 que l'analyse soit la plus complète possible (Figure 2-8) :

- **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 2-9 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.

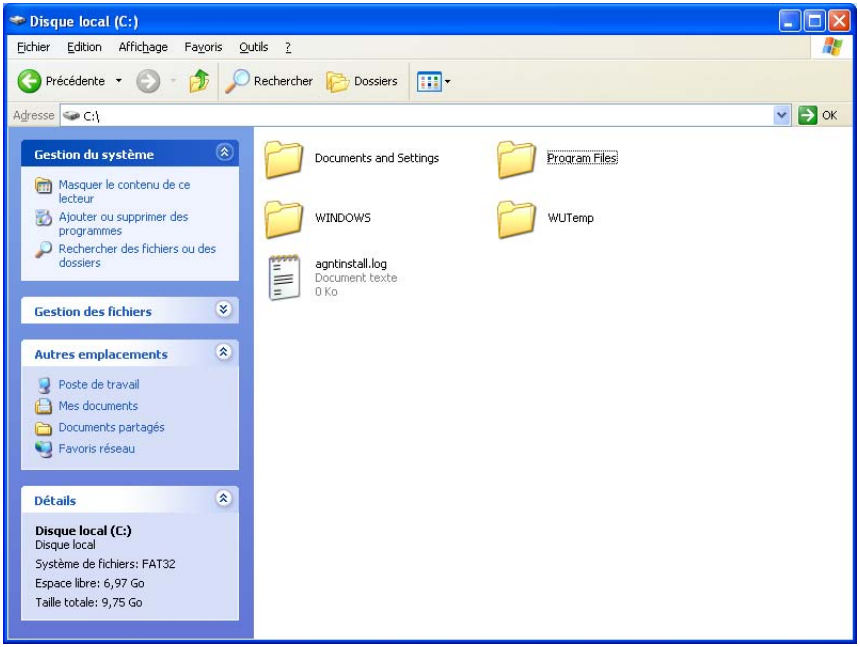


Figure 2-9. Contenu du disque local

- **Analyser tous les fichiers** : cochez cette case pour permettre l'analyse complète de tous les types de fichiers. 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 cachés dans des fichiers .ZIP et d'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 la vigilance des programmes d'analyse antivirus. La fonction d'analyse peut détecter ces virus lorsque cette case est cochée.

- **Rechercher les virus nouveaux et inconnus** : utilisez cette option pour rechercher les virus les plus récents pour lesquels il n'existe peut-être pas encore de « remède ». Cette option utilise des techniques heuristiques avancées pour tenter de faire correspondre les fichiers aux signatures des virus connus tout en recherchant des signes symptomatiques de virus non identifiés dans les fichiers.

  Cette méthode d'analyse permet également de rechercher des caractéristiques de fichier qui, en général, écartent la présence éventuelle de virus dans le fichier. Cela réduit le risque que la fonction d'analyse donne une indication erronée. Cependant, si une analyse heuristique détecte un virus, prenez les mêmes précautions que vous prendriez avec un fichier qui, à votre connaissance, 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 les logiciels espions et publicitaires et d'autres programmes qui accèdent à vos données personnelles et les transmettent sans votre autorisation.

  REMARQUE
  Laissez toutes ces options sélectionnées afin d'effectuer l'analyse la plus complète possible. Elles ont pour effet d'analyser tous les fichiers contenus sur le lecteur ou dans le dossier sélectionné ; par conséquent, 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.

À l'issue de l'analyse, le programme affiche un résumé de l'analyse (nombre de fichiers analysés et détectés, nombre de programmes potentiellement indésirables et nombre de fichiers désinfectés automatiquement).

5 Cliquez sur **OK** pour fermer la fenêtre et afficher la liste des fichiers détectés dans la boîte de dialogue **Analyse** (Figure 2-10).

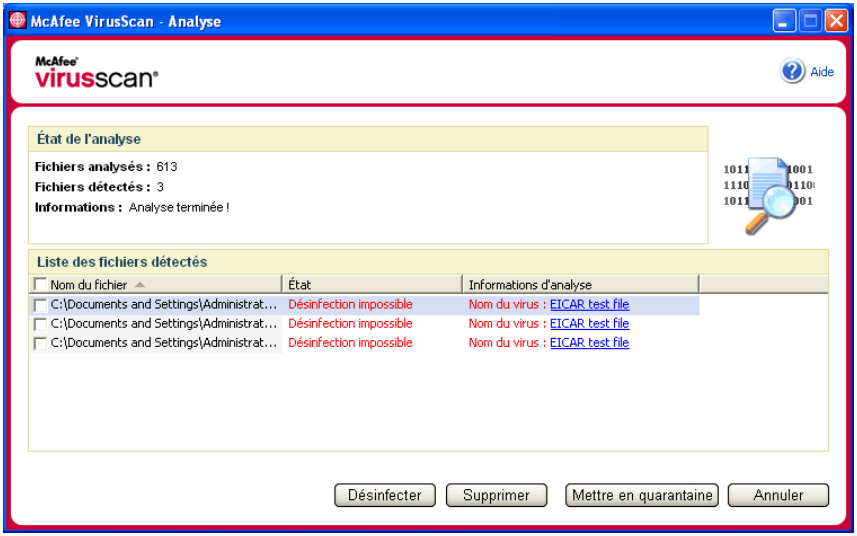


Figure 2-10. Résultats de l'analyse

REMARQUE
La fonction d'analyse compte les fichiers compressés (.ZIP, .CAB, etc.) 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 détecte pas de virus ni d'autre menace, 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, consultez la section *Mieux comprendre les détections de menace* à la page 36.

Analyse via l'Explorateur Windows

VirusScan propose un menu contextuel pour rechercher des virus et d'autres menaces dans les fichiers, les dossiers ou les lecteurs sélectionnés dans l'Explorateur Windows.

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 **Analyser**.

   La boîte de dialogue **Analyse** s'ouvre et l'analyse des fichiers démarre. Par défaut, toutes les **Options d'analyse** sont présélectionnées pour que l'analyse soit la plus complète possible (figure 2-8 à la page 29).

Analyse via Microsoft Outlook

Dans Microsoft Outlook 97 et les versions ultérieures, VirusScan vous permet d'utiliser une icône de la barre d'outils pour rechercher des virus et d'autres menaces dans des banques de messages sélectionnées et leurs sous-dossiers, des dossiers de boîte aux lettres ou des e-mails contenant des pièces jointes.

Pour effectuer une analyse 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 sur l'icône de l'analyseur de messagerie dans la barre d'outils  .

   L'analyseur de messagerie s'ouvre et commence à analyser les fichiers. Par défaut, toutes les **Options d'analyse** sont présélectionnées pour que l'analyse soit la plus complète possible (figure 2-8 à la page 29).

Recherche automatique des virus et d'autres menaces

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 tâches Windows afin de lancer une recherche intégrale de virus et d'autres menaces sur votre ordinateur à la fréquence indiquée.

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 **Options VirusScan** s'affiche.

2 Cliquez sur l'onglet **Analyse programmée** (figure 2-11 à la page 34).

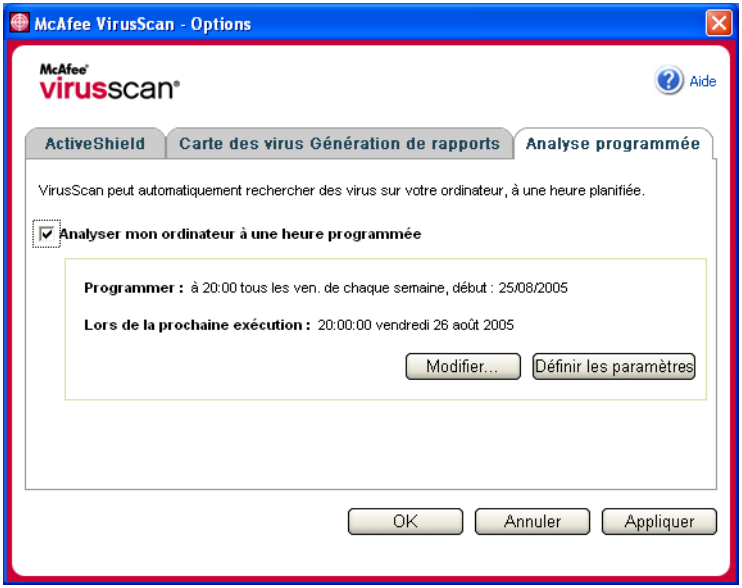


Figure 2-11. Options d'analyse programmée

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

4 Choisissez une fréquence d'analyse automatique :

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

  a. Cliquez sur **Modifier**.

  b. Sélectionnez la fréquence d'analyse de votre ordinateur dans la liste **Tâche planifiée**, puis sélectionnez des options supplémentaires dans la zone dynamique située en dessous :

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

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

  Tous les mois : indiquez le jour de l'analyse. Cliquez sur **Sélectionner les mois** pour indiquer les mois concernés par l'analyse, puis sur **OK**.

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

  REMARQUE
  Les options suivantes du Planificateur de tâches Windows ne sont pas prises en charge :
  Au démarrage du système, **Si inactif** ou **Afficher les différents horaires**. La dernière fréquence prise en charge restera activée 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** apparaît.

  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 **Définir les paramètres par défaut**. Sinon, cliquez sur **OK**.

Mieux comprendre les détections de menace

Pour la plupart des virus, des chevaux de Troie et des vers, la fonction d'analyse tente automatiquement de désinfecter 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 d'analyse détecte un programme potentiellement indésirable, vous pouvez tenter de le désinfecter, le mettre en quarantaine ou le supprimer manuellement (soumission AVERT indisponible).

Pour traiter un virus ou un programme potentiellement indésirable :

1. Si un fichier apparaît dans la **Liste des fichiers détectés**, cochez la case située en regard 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. Il vous est également possible de 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 tenter de le désinfecter.

3. Si la fonction d'analyse ne parvient pas à désinfecter le fichier, cliquez sur **Mettre en quarantaine** pour chiffrer et isoler temporairement les fichiers suspects dans le répertoire 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* à la page 37.

4. Si la fonction d'analyse ne parvient pas à désinfecter le fichier ni à le mettre en quarantaine, vous pouvez exécuter l'une des actions suivantes :

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

Si la fonction d'analyse ne parvient pas à désinfecter ni 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 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 détecté. Pour plus d'informations, consultez la section *Création d'une disquette de secours* à la page 38.

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 quarantaine chiffre et isole temporairement les fichiers suspects dans le répertoire de quarantaine jusqu'à ce que vous puissiez entreprendre l'action appropriée. 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 cliquez sur **Gestion des fichiers mis en quarantaine**.

La liste des fichiers mis en quarantaine apparaît (Figure 2-12).

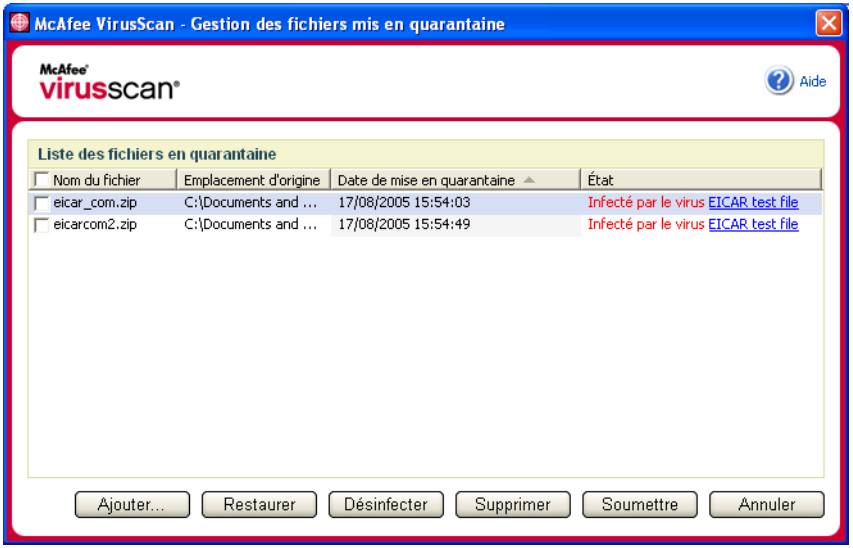


Figure 2-12. Boîte de dialogue Gestion des fichiers mis en quarantaine

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

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. Il vous est également possible de cliquer sur le nom du virus dans la liste **État** pour afficher des détails provenant de la bibliothèque d'informations sur les virus.

Enfin, vous pouvez cliquer sur **Ajouter**, sélectionner un fichier suspect à ajouter dans la liste des fichiers en quarantaine, cliquer sur **Ouvrir**, puis le sélectionner dans la liste des fichiers en quarantaine.

3 Cliquez sur **Désinfecter**.

4 Si la désinfection réussit, cliquez sur **Restaurer** pour replacer le fichier à son emplacement d'origine.

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

6 Si VirusScan ne parvient pas à désinfecter ni à supprimer le fichier et qu'il ne s'agit pas d'un programme potentiellement indésirable, vous pouvez le soumettre à McAfee AntiVirus Emergency Response Team (AVERT™) pour 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 l'envoyer à AVERT.

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

7 Cliquez sur **Annuler** 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, consultez la section *Recherche manuelle des virus et d'autres menaces* à la page 29.

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 **Créer une disquette de secours** s'affiche (Figure 2-13).

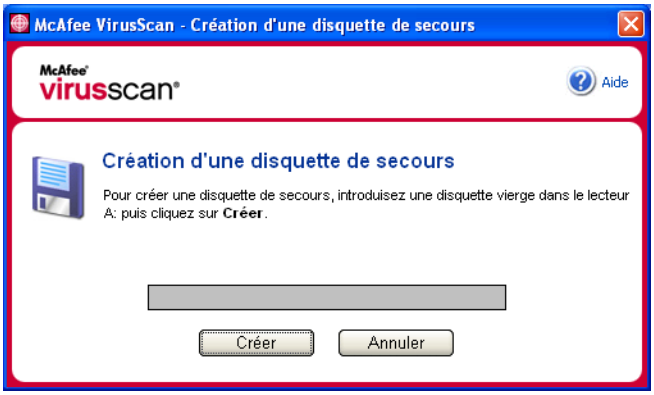


Figure 2-13. Boîte de dialogue Création d'une disquette de secours

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 **Créer une disquette de secours**.

5 Lorsque le message « Disquette de secours créée » 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 ce faire, suivez les mêmes instructions que pour 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 **Options VirusScan**.

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 **Options VirusScan** s'affiche.

2 Cliquez sur l'onglet **Carte des virus** (Figure 2-14).

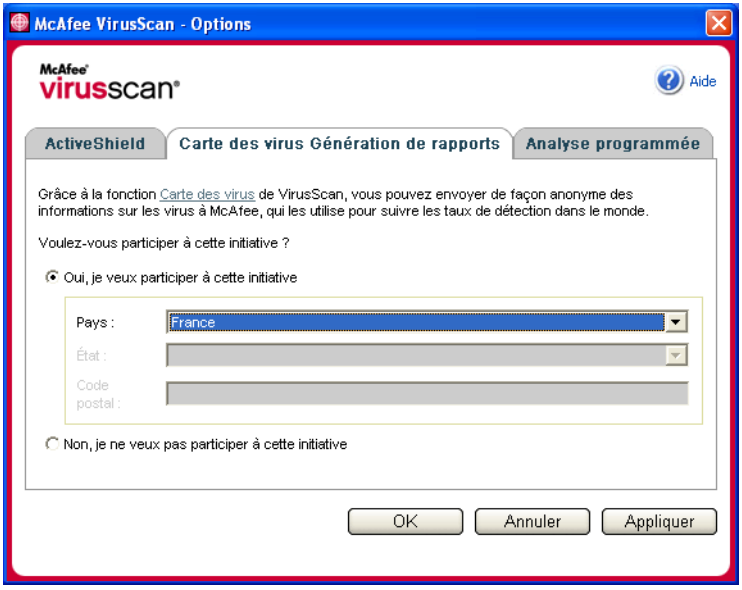


Figure 2-14. Options de Carte des virus

3 Acceptez l'option par défaut **Oui, je veux participer à cette initiative** pour envoyer de manière anonyme vos informations sur les virus à World Virus Map, le baromètre des taux de détection mondiaux de McAfee. Autrement, sélectionnez **Non, je ne veux pas participer à cette initiative** 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 de détection 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 2-15).

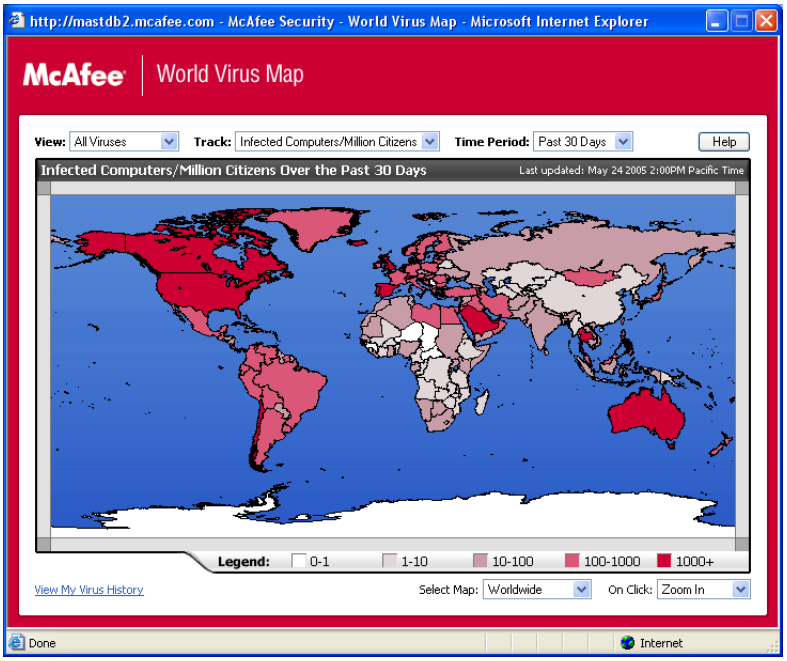


Figure 2-15. World Virus Map

Par défaut, World Virus Map indique le nombre d'ordinateurs qui ont été détectés dans le monde au cours des 30 derniers 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 détectés ou changer la période de temps afin d'afficher uniquement les résultats pour les 7 jours précédents ou les dernières 24 heures.

La section **Suivi de virus** présente les nombres totaux cumulés de fichiers analysés, de fichiers détectés et d'ordinateurs détectés 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 SecurityCenter** s'ouvre.

3 Cliquez sur **Vérifier maintenant**.

Si une mise à jour existe, la boîte de dialogue **Mises à jour de VirusScan** s'affiche (consultez la figure 2-16 à la page 44). 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.

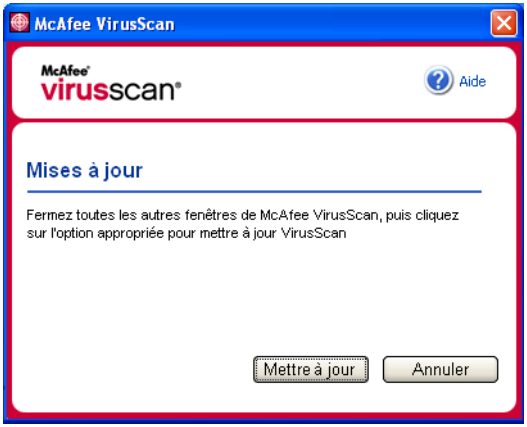


Figure 2-16. Boîte de dialogue des mises à jour

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

A

C

D

E

I

L

M

N

O

P

R

S

T

U

V

W