McAfee®

Internet Security Suite 2008

Guide de l'utilisateur

Table des matières

McAfee Internet Security 3

McAfee SecurityCenter 5
Fonctions de SecurityCenter 6
Utilisation de SecurityCenter 7
Mise à jour de SecurityCenter 13
Résoudre ou ignorer des problèmes de protection 17
Utilisation des alertes 23
Affichage des événements 29
McAfee VirusScan 31
Fonctions de VirusScan 32
Démarrage de la protection antivirus en temps réel 33
Démarrage de la protection supplémentaire 35
Configuration de la protection antivirus 39
Analyse de votre ordinateur 57
Exploitation des résultats d'analyse 61
McAfee Personal Firewall 65
Fonctions de Personal Firewall 66
Démarrage du pare-feu 69
Utilisation des alertes 71
Gestion des alertes de type Informations 75
Configuration de la protection par pare-feu 77
Gestion des programmes et des autorisations 91
Gestion des services système 103
Gestion des connexions informatiques 109
Consignation, surveillance et analyse 117
Obtention d'informations sur la sécurité Internet 127
McAfee Anti-Spam 129
Fonctionnalités d'Anti-Spam 131
Configuration des comptes Webmail 133
Configuration des amis 139
Configuration de la détection de spam 147
Filtrage des e-mails 155
Traitement du e-mails filtrés 159
Configuration de la protection antiphishing 161
McAfee Privacy Service 165
Fonctionnalités de Privacy Service 166
Configuration du contrôle parental 167
Protection d'informations sur le Web 183
Protection des mots de passe 185
McAfee Data Backup 191
Caractéristiques 192
Archivage de fichiers 193
Utilisation des fichiers archivés 201
McAfee QuickClean 207
Fonctions de QuickClean 208
Nettoyage de votre ordinateur 209
Défragmentation de votre ordinateur 212

Programmation d'une tâche 213
McAfee Shredder 219
Fonctions de Shredder 220
Broyage de fichiers, dossiers et disques 221
McAfee Network Manager 223
Fonctionnalités de Network Manager 224
Présentation des icônes de Network Manager 225
Configuration d'un réseau géré 227
Gestion à distance du réseau 235
McAfee EasyNetwork 241
Fonctionnalités d'EasyNetwork 242
Configuration de EasyNetwork 243
Partage et envoi des fichiers 249
Partage d'imprimantes 255
Référence 258

Glossaire 259

A propos de McAfee 275

Copyright 275
Licence 276
Service clientèle et support technique 277
Utilisation de McAfee Virtual Technician 278
Assistance et téléchargements 279

Index 288

CHAPITRE 1

McAfee Internet Security

McAfee Internet Security Suite avec SiteAdvisor est une offre groupée de sécurité proactive 10 en 1 mise à jour en continu, qui protège ce qui est important pour vous, votre identité et votre ordinateur, contre les virus, les logiciels espions, les courriers électroniques et les messages instantanés frauduleux. Naviguez sur Internet, effectuez des achats et des opérations bancaires, envoyez et recevez des courriers électroniques et des messages instantanés et téléchargez des fichiers en toute confiance. McAfee SiteAdvisor et le contrôle parental vous aident, vous et votre famille, à éviter les sites Web à risque. Le service de sécurité de McAfee fournit, automatiquement et en continu, les fonctionnalités, améliorations et données les plus récentes en matière de menaces. En outre, la fonction d'optimisation automatique du PC supprime les fichiers indésirables, pour des performances informatiques optimales.

Contenu de ce chapitre

McAfee SecurityCenter 5
McAfee VirusScan 31
McAfee Personal Firewall 65
McAfee Anti-Spam 129
McAfee Privacy Service 165
McAfee Data Backup 191
McAfee QuickClean 207
McAfee Shredder 219
McAfee Network Manager 223
McAfee EasyNetwork 241
Référence 258
A propos de McAfee 275
Service clientèle et support technique 277

CHAPITRE 2

McAfee SecurityCenter

McAfee SecurityCenter vous permet de surveiller l'état de la sécurité de votre ordinateur, de savoir instantanément si vos services de protection contre les virus, logiciels espions et messages électroniques et de protection par pare-feu sont à jour et d'agir sur certaines failles de sécurité. Il fournit les outils de navigation et commandes nécessaires et contrôle votre besoin de coordonner et gérer tous les secteurs de la protection de votre ordinateur.

Avant de commencer à configurer et gérer la protection de votre ordinateur, étudiez l'interface de SecurityCenter et veillez à bien distinguer état de protection, catégories de protection et services de protection. Ensuite, mettez à jour SecurityCenter pour disposer de la protection McAfee la plus récente disponible.

Après la configuration initiale, vous utilisez SecurityCenter pour surveiller l'état de protection de votre ordinateur. Si SecurityCenter détecte un problème de protection, il vous alerte pour que vous puissiez corriger ou ignorer le problème (selon sa gravité). Vous pouvez aussi analyser les événements liés à SecurityCenter, comme les changements de configuration de l'analyse antivirus, dans un journal des événements.

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctions de SecurityCenter 6
Utilisation de SecurityCenter 7
Mise à jour de SecurityCenter 13
Résoudre ou ignorer des problèmes de protection ..17
Utilisation des alertes 23
Affichage des événements 29

Fonctions de SecurityCenter

SecurityCenter propose les fonctionnalités suivantes :

État de protection simplifié

Consultez facilement le niveau de protection de votre ordinateur, vérifiez la présence de mises à jour et réglez les problèmes de protection potentiels.

Mises à jour et mises à niveau automatisées

Téléchargez et installez automatiquement les mises à jour de vos programmes enregistrés. Lorsqu'une nouvelle version d'un programme McAfee enregistré est disponible, vous l'obtenez sans frais pendant toute la durée de votre abonnement. Vous bénéficiez ainsi d'une protection à jour en permanence.

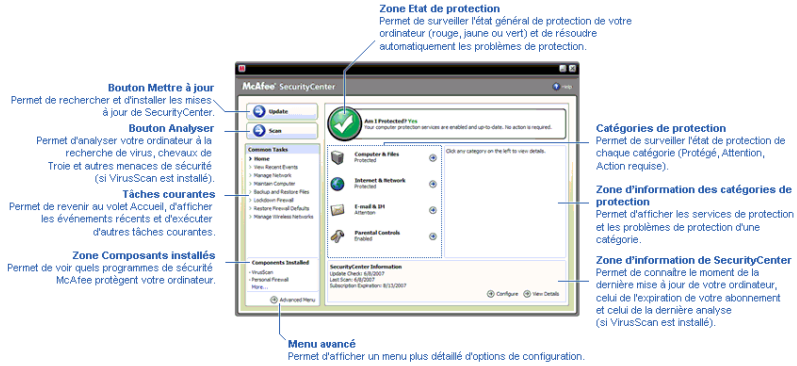
Alertes en temps réel

Les alertes de sécurité vous avertissent des nouvelles épidémies virales et des menaces de sécurité, et permettent de supprimer, neutraliser ou mieux connaître la menace.

CHAPITRE 3

Utilisation de SecurityCenter

Avant de commencer à utiliser SecurityCenter, passez en revue les composants et domaines de configuration que vous allez utiliser pour gérer l'état de protection de votre ordinateur. Pour plus d'informations sur la terminologie utilisée dans cette image, consultez Explications sur l'état de protection (page 8) et Explications sur les catégories de protection (page 9). Ensuite, vous pouvez contrôler les données de votre compte McAfee et vérifier la validité de votre abonnement.



Contenu de ce chapitre

Explications sur l'état de protection 8
Explications sur les catégories de protection 9
Explications sur les services de protection 10
Gestion de votre compte McAfee 11

Explications sur l'état de protection

L'état de protection de votre ordinateur s'affiche dans la zone d'état de protection dans le volet Accueil de SecurityCenter. Il indique si votre ordinateur est entièrement protégé contre les menaces les plus récentes et peut être influencé par des attaques externes, d'autres programmes de sécurité et des programmes accédant à Internet.

L'état de protection de votre ordinateur peut être rouge, jaune ou vert.

Etat de protection	Description
Rouge	Votre ordinateur n'est pas protégé. La zone d'état de protection du volet Accueil de SecurityCenter est rouge et indique que vous n'êtes pas protégé. SecurityCenter rapporte au moins un problème de sécurité critique. Pour obtenir une protection complète, vous devez corriger tous les problèmes de sécurité critiques dans chaque catégorie de protection (l'état de la catégorie de problèmes est mis à **Action requise**, également en rouge). Pour plus d'informations sur la correction des problèmes de protection, consultez Résolution des problèmes de protection (page 18).
Jaune	Votre ordinateur est partiellement protégé. La zone d'état de protection du volet Accueil de SecurityCenter est jaune et indique que vous n'êtes pas protégé. SecurityCenter rapporte au moins un problème de sécurité non critique. Pour obtenir une protection complète, vous devez corriger ou ignorer les problèmes de sécurité non critiques associés à chaque catégorie de protection. Pour plus d'informations sur la façon de corriger ou ignorer des problèmes de protection, consultez Résoudre ou ignorer des problèmes de protection (page 17).
Vert	Votre ordinateur est entièrement protégé. La zone d'état de protection du volet Accueil de SecurityCenter est verte et indique que vous êtes protégé. SecurityCenter ne rapporte aucun problème de sécurité, critique ou non critique. Chaque catégorie de protection énumère les services qui protègent votre ordinateur.

Explications sur les catégories de protection

Les services de protection de SecurityCenter sont divisés en quatre catégories : ordinateur & fichiers, internet & réseau, e-mail & messagerie instantanée et contrôle parental. Ces catégories vous aident à parcourir et configurer les services de sécurité qui protègent votre ordinateur.

Cliquez sur le nom d'une catégorie pour en configurer les services de protection et voir les problèmes de sécurité éventuels détectés pour ces services. Si l'état de protection de votre ordinateur est rouge ou jaune, une ou plusieurs catégories affichent un message *Action requise* ou *Attention*, indiquant que SecurityCenter a détecté un problème dans les catégories en question. Pour plus d'informations sur l'état de protection, consultez Explications sur l'état de protection (page 8).

Catégorie de protection	Description
Ordinateur & fichiers	La catégorie Ordinateur & fichiers permet de configurer les services de protection suivants : ▪ Protection antivirus ▪ Protection PUP ▪ Moniteurs système ▪ Protection Windows
Réseau & Internet	La catégorie Réseau & Internet permet de configurer les services de protection suivants : ▪ Protection par pare-feu ▪ Protection des données personnelles
E-mail & IM	La catégorie E-mail & IM permet de configurer les services de protection suivants : ▪ Protection des e-mails ▪ Protection antispam
Contrôle parental	La catégorie Contrôle parental permet de configurer les services de protection suivants : ▪ Blocage de contenu

Explications sur les services de protection

Les services de protection sont les composants essentiels de SecurityCenter que vous configurez pour protéger votre ordinateur. Les services de protection correspondent directement à des programmes McAfee. Par exemple, lorsque vous installez VirusScan, les services de protection suivants deviennent disponibles : Protection antivirus, Protection PUP, Moniteurs système et Protection Windows. Pour des informations détaillées sur ces services de protection particuliers, consultez l'aide de VirusScan.

Par défaut, tous les services de protection associés à un programme sont activés lorsque vous installez ce programme ; cependant, vous pouvez désactiver un service de protection à tout moment. Par exemple, si vous installez Privacy Service, les services Blocage de contenu et Protection des données personnelles sont tous deux activés. Si vous ne souhaitez pas utiliser le service de protection Blocage de contenu, vous pouvez le désactiver entièrement. Vous pouvez aussi désactiver temporairement un service de protection pendant des tâches de configuration ou de maintenance.

Gestion de votre compte McAfee

À partir de SecurityCenter, vous pouvez facilement accéder aux données de votre compte pour les consulter et vérifier l'état actuel de votre abonnement.

Remarque : Si vous avez installé vos programmes McAfee à partir d'un CD, vous devez les enregistrer sur le site Web de McAfee pour configurer ou mettre à jour votre compte McAfee. C'est indispensable pour pouvoir bénéficier des mises à jour régulières automatiques des programmes.

Gérer votre compte McAfee

Vous pouvez facilement accéder aux données de votre compte McAfee (Mon compte) à partir de SecurityCenter.

1. Sous **Tâches courantes**, cliquez sur **Mon compte**.
2. Connectez-vous à votre compte McAfee.

Vérifier votre abonnement

Vous pouvez vérifier votre abonnement pour vous assurer qu'il n'a pas encore expiré.

- Cliquez avec le bouton droit sur l'icône de SecurityCenter dans la zone de notification à l'extrême droite de la barre des tâches, puis cliquez sur **Vérifier l'abonnement**.

CHAPITRE 4

Mise à jour de SecurityCenter

SecurityCenter garantit la mise à jour permanente de vos programmes McAfee enregistrés en vérifiant toutes les quatre heures si des mises à jour sont disponibles en ligne et en les installant le cas échéant. Selon les programmes installés et enregistrés, les mises à jour en ligne peuvent inclure les définitions de virus les plus récentes ainsi que les mises à jour des protections contre les pirates, le spam et les logiciels espions et la protection de votre confidentialité. Si vous souhaitez vérifier l'existence de mises à jour avant l'échéance de l'intervalle par défaut, vous pouvez le faire à tout moment. Pendant que SecurityCenter recherche des mises à jour, vous pouvez continuer à travailler.

Bien que cela ne soit pas recommandé, vous pouvez modifier la façon dont SecurityCenter recherche et installe les mises à jour. Par exemple, vous pouvez configurer SecurityCenter pour qu'il télécharge les mises à jour sans les installer ou qu'il vous avertisse avant de télécharger ou d'installer des mises à jour. Vous pouvez aussi désactiver la mise à jour automatique.

Remarque : Si vous avez installé vos programmes McAfee à partir d'un CD, vous ne pourrez bénéficier des mises à jour régulières automatiques de ces programmes que lorsque vous les aurez enregistrés sur le site Web de McAfee.

Contenu de ce chapitre

Rechercher des mises à jour 14
Configurer les mises à jour automatiques 14
Désactiver les mises à jour automatiques 15

Rechercher des mises à jour

Par défaut, SecurityCenter recherche automatiquement des mises à jour toutes les quatre heures lorsque votre ordinateur est connecté à Internet ; cependant, si vous souhaitez rechercher des mises à jour avant que les quatre heures soient écoulées, vous pouvez le faire. Si vous avez désactivé les mises à jour automatiques, il vous incombe de vérifier régulièrement si des mises à jour sont disponibles.

- Dans le volet Accueil de SecurityCenter, cliquez sur **Mettre à jour**.

Conseil : Vous pouvez rechercher des mises à jour sans lancer SecurityCenter en cliquant avec le bouton droit sur l'icône de SecurityCenter dans la zone de notification à l'extrême droite de la barre des tâches, puis en cliquant sur **Mises à jour**.

Configurer les mises à jour automatiques

Par défaut, SecurityCenter vérifie et installe automatiquement les mises à jour à intervalles de quatre heures lorsque vous êtes connecté à Internet. Si vous souhaitez modifier ce comportement par défaut, vous pouvez configurer SecurityCenter pour qu"il télécharge automatiquement les mises à jour puis vous avertisse lorsqu'elles sont prêtes à être installées ou pour qu'il vous avertisse avant de télécharger les mises à jour.

Remarque : SecurityCenter vous avertit par des alertes lorsque des mises à jour sont prêtes à être téléchargées ou installées. Ces alertes vous permettent de télécharger ou installer les mises à jour, ou de les postposer. Lorsque vous mettez à jour vos programmes à partir d'une alerte, vous serez peut-être invité à vérifier votre abonnement avant de télécharger et installer les mises à jour. Pour plus d'informations, consultez Utilisation des alertes (page 23).

1. Ouvrez le volet de configuration SecurityCenter.

   Comment ?

   1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
   2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.

2. Dans le volet Configuration de SecurityCenter, sous **Des mises à jour automatiques sont désactivées**, cliquez sur **Activé**, puis sur **Avancé**.
3. Selon le cas, cliquez sur l'un des boutons suivants :
   - **Installer automatiquement les mises à jour de mes services et m'avertir de l'opération une fois terminée (recommandé)**

- **Télécharger automatiquement les mises à jour et m'avertir de la possibilité de les installer**
- **M'avertir avant de télécharger une mise à jour**

4 Cliquez sur **OK**.

Désactiver les mises à jour automatiques

Si vous désactivez les mises à jour automatiques, il vous incombe de vérifier régulièrement si des mises à jour sont disponibles, faute de quoi votre ordinateur ne disposera pas de la protection la plus récente. Pour plus d'informations sur la recherche manuelle de mises à jour, consultez Rechercher des mises à jour (page 14).

1 Ouvrez le volet de configuration SecurityCenter.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.

2 Dans le volet Configuration de SecurityCenter, sous **Des mises à jour automatiques sont activées**, cliquez sur **Désactivé**.

Conseil : Pour activer les mises à jour automatiques, cliquez sur le bouton **Activé** ou désélectionnez **Désactiver les mises à jour automatiques et me laisser les vérifier manuellement** dans le volet Options de mise à jour.

CHAPITRE 5

Résoudre ou ignorer des problèmes de protection

SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Les problèmes de protection critiques exigent une action immédiate et compromettent votre état de protection (qui passe au rouge). Les problèmes de protection non critiques n'exigent pas d'action immédiate et peuvent ou non compromettre votre état de protection (selon le type de problème). Pour obtenir un état de protection vert, vous devez corriger tous les problèmes critiques et résoudre ou ignorer tous les problèmes non critiques. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician. Pour plus d'informations sur McAfee Virtual Technician, consultez l'aide de McAfee Virtual Technician.

Contenu de ce chapitre

Résolution des problèmes de protection.....18
Ignorer des problèmes de protection 20

Résolution des problèmes de protection

La plupart des problèmes de sécurité peuvent être corrigés automatiquement ; cependant, certains problèmes peuvent exiger une action de votre part. Par exemple, si le programme Protection par pare-feu est désactivé, SecurityCenter peut l'activer automatiquement ; en revanche, s'il n'est pas installé, c'est vous qui devez l'installer. Le tableau qui suit décrit certaines autres actions que vous pouvez entreprendre lors de la résolution manuelle de problèmes de protection :

Problème	Action
L'analyse complète de votre ordinateur n'a pas été exécutée depuis au moins 30 jours.	Analysez manuellement votre ordinateur. Pour plus d'informations, consultez l'aide de VirusScan.
Vos fichiers de signatures de détection ne sont pas à jour.	Actualisez manuellement votre protection. Pour plus d'informations, consultez l'aide de VirusScan.
Un programme n'est pas installé.	Installez le programme à partir du site Web ou du CD de McAfee.
Des composants d'un programme sont manquants.	Réinstallez le programme à partir du site Web ou du CD de McAfee.
Un programme n'est pas enregistré et ne peut pas bénéficier d'une protection complète.	Enregistrez le programme sur le site Web de McAfee.
Un programme a expiré.	Vérifiez l'état de votre compte sur le site Web de McAfee.

Remarque : Souvent, un même problème de protection affecte plusieurs catégories de protection. Dans ce cas, sa résolution dans une catégorie résout le problème dans toutes les autres catégories.

Résolution automatique des problèmes de protection

SecurityCenter peut résoudre automatiquement la plupart des problèmes de protection. Les changements de configuration effectués par SecurityCenter lors de la résolution automatique de problèmes de protection ne sont pas enregistrés dans le journal des événements. Pour plus d'informations sur les événements, consultez Affichage des événements (page 29).

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, dans la zone d'état de protection, cliquez sur **Corriger**.

Résolution manuelle des problèmes de protection

Si un ou plusieurs problèmes de protection persistent après une tentative de correction automatique, vous pouvez les résoudre manuellement.

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur la catégorie de protection où SecurityCenter a rapporté le problème.
3. Cliquez sur le lien qui suit la description du problème.

Ignorer des problèmes de protection

Si SecurityCenter détecte un problème non critique, vous pouvez le corriger ou l'ignorer. D'autres problèmes non critiques (par exemple, si Antispam ou Privacy Service ne sont pas installés) sont automatiquement ignorés. Les problèmes ignorés n'apparaissent dans la zone d'information des catégories de protection dans le volet Accueil de SecurityCenter que si l'état de protection de votre ordinateur est vert. Si vous ignorez un problème, mais décidez ensuite de l'afficher dans la zone d'information des catégories de problème alors que l'état de protection de votre ordinateur n'est pas vert, vous pouvez l'y faire apparaître.

Ignorer un problème de protection

Si SecurityCenter détecte un problème non critique que vous ne souhaitez pas corriger, vous pouvez l'ignorer. Un problème ignoré est supprimé de la zone d'information des catégories de protection dans SecurityCenter.

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur la catégorie de protection où est rapporté le problème.
3. Cliquez sur le lien **Ignorer** face au problème de protection.

Afficher ou masquer des problèmes ignorés

Selon sa gravité, vous pouvez afficher ou masquer un problème de protection ignoré.

1. Ouvrez le volet Options d'alerte.

   Comment ?

   1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
   2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
   3. Sous **Alertes**, cliquez sur **Avancé**.
2. Dans le volet Configuration de SecurityCenter, cliquez sur **Problèmes ignorés**.
3. Dans le volet Problèmes ignorés, effectuez l'une des opérations suivantes :
   - Pour ignorer un problème, activez sa case à cocher.
   - Pour faire apparaître un problème dans la zone d'information des catégories de protection, désactivez sa case à cocher.

4 Cliquez sur **OK**.

Conseil : Vous pouvez aussi ignorer un problème en cliquant sur le lien **Ignorer** face au problème en question dans la zone d'information des catégories de protection.

CHAPITRE 6

Utilisation des alertes

Les alertes sont des petites boîtes de dialogue en superposition qui apparaissent dans l'angle inférieur droit de l'écran lorsque certains événements se produisent dans SecurityCenter. Une alerte fournit des informations détaillées sur un événement ainsi que des recommandations et des options de résolution des problèmes éventuellement associés à l'événement. Certaines alertes contiennent également des liens vers des informations complémentaires sur l'événement. Ces liens permettent d'ouvrir le site Web global de McAfee ou d'envoyer des informations à McAfee à des fins de dépannage.

Il y a trois types d'alertes : rouge, jaune et verte.

Type d'alerte	Description
Rouge	Une alerte rouge constitue une indication critique qui nécessite une réponse de votre part. Elle se produit lorsque SecurityCenter ne peut pas déterminer comment résoudre automatiquement un problème de protection.
Jaune	Une alerte jaune constitue une indication non critique qui nécessite généralement une réponse de votre part.
Verte	Une alerte verte constitue une indication non critique qui ne nécessite pas de réponse de votre part. Les alertes vertes fournissent des informations de base sur un événement.

Les alertes jouent un rôle important dans la surveillance et la gestion de votre état de protection ; c'est pourquoi vous ne pouvez pas les désactiver. En revanche, vous pouvez définir si certains types d'alertes d'information doivent apparaître et configurer d'autres options d'alerte (par exemple l'émission ou non d'un son lorsque SecurityCenter produit une alerte ou l'affichage ou non de l'écran d'accueil de McAfee au démarrage).

Contenu de ce chapitre

Affichage et masquage d'alertes d'information 24
Configuration des options d'alerte 26

Affichage et masquage d'alertes d'information

Les alertes d'information font état d'événements qui ne menacent pas la sécurité de l'ordinateur. Par exemple, si vous avez configuré la Protection par pare-feu, une alerte d'information s'affiche par défaut lorsqu'un programme installé sur votre ordinateur reçoit l'autorisation d'accéder à Internet. Si vous ne voulez pas afficher un type d'alerte d'information spécifique, vous pouvez la masquer. Si vous ne voulez afficher aucune alerte d'information, vous pouvez les masquer toutes. Vous pouvez aussi masquer toutes les alertes d'information lorsque vous jouez à un jeu en plein écran sur votre ordinateur. Lorsque vous avez terminé de jouer et quittez le mode plein écran, SecurityCenter recommence à afficher les alertes d'information.

Si vous masquez involontairement une alerte d'information, vous pouvez la réafficher à tout moment. Par défaut, SecurityCenter affiche toutes les alertes d'information.

Afficher ou masquer des alertes d'information

Vous pouvez configurer SecurityCenter pour qu'il affiche certaines alertes d'information et pas d'autres, ou pour qu'il masque toutes les alertes d'information.

1 Ouvrez le volet Options d'alerte.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
3. Sous **Alertes**, cliquez sur **Avancé**.

2 Dans le volet Configuration de SecurityCenter, cliquez sur **Alertes d'information**.

3 Dans le volet Alertes d'information, effectuez l'une des opérations suivantes :

- Pour afficher une alerte d'information, désactivez sa case à cocher.
- Pour masquer une alerte d'information, activez sa case à cocher.
- Pour masquer toutes les alertes d'information, activez la case à cocher **Ne pas afficher les alertes d'information**.

4 Cliquez sur **OK**.

Conseil : Vous pouvez également masquer une alerte d'information en activant la case **Ne plus afficher cette alerte** dans l'alerte même. Dans ce cas, vous pouvez réafficher l'alerte d'information en désactivant la case à cocher appropriée dans le volet Alertes d'information.

Afficher ou masquer des alertes d'information pendant un jeu

Vous pouvez masquer les alertes d'information lorsque vous jouez à un jeu en plein écran sur votre ordinateur. Lorsque vous avez terminé de jouer et quittez le mode plein écran, SecurityCenter recommence à afficher les alertes d'information.

1 Ouvrez le volet Options d'alerte.

   Comment ?

   1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
   2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
   3. Sous **Alertes**, cliquez sur **Avancé**.

2 Dans le volet Options d'alerte, activez ou désactivez la case **Afficher les alertes d'information en mode jeu**.

3 Cliquez sur **OK**.

Configuration des options d'alerte

L'apparence et la fréquence des alertes sont configurées par SecurityCenter ; cependant, vous pouvez régler certaines options de base des alertes. Par exemple, vous pouvez activer l'émission d'un son lorsqu'une alerte est produite ou masquer l'écran d'accueil au démarrage de Windows. Vous pouvez aussi masquer les alertes qui vous avertissent des épidémies virales et des autres menaces pour la sécurité dans la communauté en ligne.

Emettre un son en cas d'alerte

Si vous souhaitez recevoir une indication audible qu'une alerte s'est produite, vous pouvez configurer SecurityCenter pour qu'il produise un son à chaque alerte.

1 Ouvrez le volet Options d'alerte.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
3. Sous **Alertes**, cliquez sur **Avancé**.

2 Dans le volet Options d'alerte, sous **Son**, activez la case à cocher **Emettre un son en cas d'alerte**.

Masquer l'écran d'accueil au démarrage

Par défaut, l'écran d'accueil de McAfee apparaît brièvement au démarrage de Windows, vous indiquant que SecurityCenter protège votre ordinateur. Cependant, vous pouvez masquer l'écran d'accueil si vous ne voulez pas qu'il apparaisse.

1 Ouvrez le volet Options d'alerte.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
3. Sous **Alertes**, cliquez sur **Avancé**.

2 Dans le volet Options d'alerte, sous **Écran d'accueil**, désactivez la case à cocher **Afficher l'écran d'accueil McAfee au démarrage de Windows**.

Conseil : Vous pouvez réafficher l'écran d'accueil à tout moment en activant la case à cocher **Afficher l'écran d'accueil McAfee au démarrage de Windows**.

Masquer les alertes d'attaque virale

Vous pouvez masquer les alertes qui vous avertissent des épidémies virales et des autres menaces pour la sécurité dans la communauté en ligne.

1 Ouvrez le volet Options d'alerte.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
3. Sous **Alertes**, cliquez sur **Avancé**.

2 Dans le volet Options d'alerte, désactivez la case **M'avertir en cas d'apparition d'un virus ou d'une menace informatique**.

Conseil : Vous pouvez afficher les alertes d'attaque virale à tout moment en activant la case **M'avertir en cas d'apparition d'un virus ou d'une menace informatique**.

CHAPITRE 7

Affichage des événements

Un événement est une action ou un changement de configuration qui se produit dans une catégorie de protection et les services de protection correspondants. Différents services de protection enregistrent différents types d'événements. Par exemple, SecurityCenter enregistre un événement si un service de protection est activé ou désactivé ; Virus Protection enregistre un événement chaque fois qu'un virus est détecté et supprimé ; et Firewall Protection enregistre un événement chaque fois qu'une tentative de connexion à Internet est bloquée. Pour plus d'informations sur les catégories de protection, consultez Explications des catégories de protection (page 9).

Vous pouvez afficher les événements lorsque vous tentez de résoudre des problèmes de configuration et analysez les opérations effectuées par les autres utilisateurs. Nombre de parents utilisent le journal des événements pour surveiller le comportement de leurs enfants sur Internet. Vous affichez les événements récents si vous ne souhaitez examiner que les 30 derniers événements survenus. Vous affichez tous les événements si vous souhaitez examiner une liste complète des événements survenus. Lorsque vous visualisez tous les événements, SecurityCenter lance le journal des événements, qui trie les événements selon la catégorie de protection dans laquelle ils se sont produits.

Contenu de ce chapitre

Afficher les événements récents.....29
Afficher tous les événements.....30

Afficher les événements récents

Vous affichez les événements récents si vous ne souhaitez examiner que les 30 derniers événements survenus.

- Sous **Tâches courantes**, cliquez sur **Afficher les événements récents**.

Afficher tous les événements

Vous affichez tous les événements si vous souhaitez examiner une liste complète des événements survenus.

1. Sous **Tâches courantes**, cliquez sur **Afficher les événements récents**.
2. Dans le volet Evénements récents, cliquez sur **Afficher le fichier journal**.
3. Dans le volet gauche du journal des événements, cliquez sur le type d'événements à afficher.

CHAPITRE 8

McAfee VirusScan

VirusScan offre des services avancés de détection et de protection défendant votre ordinateur contre les menaces les plus récentes contre la sécurité : virus, chevaux de Troie, cookies de suivi, logiciels espions, logiciels publicitaires et autres programmes potentiellement indésirables. La protection s'étend au-delà des fichiers et dossiers de votre ordinateur de bureau, pour contrer les menaces provenant de différents points d'entrée, dont le courrier électronique, la messagerie instantanée et le Web.

Avec VirusScan, la protection de votre ordinateur est immédiate et constante (pas d'administration fastidieuse). Pendant que vous travaillez, jouez, naviguez sur le Web ou contrôlez votre courrier électronique, la protection s'exécute à l'arrière-plan pour surveiller, analyser et détecter des risques en temps réel. Des analyses complètes sont exécutées à intervalles programmés pour vérifier votre ordinateur avec un ensemble plus sophistiqué d'options. VirusScan vous offre la possibilité de personnaliser ce comportement si vous le souhaitez ; dans le cas contraire, votre ordinateur reste protégé.

Utilisé normalement, votre ordinateur est exposé aux virus, vers et autres menaces potentielles. Si une menace se présente, VirusScan vous en avertit, mais y fait normalement face pour vous en nettoyant ou en mettant en quarantaine les éléments infectés avant que votre ordinateur puisse subir un quelconque dommage. Dans de rare cas, une action complémentaire de votre part peut être exigée. Dans ces cas, VirusScan vous laisse décider que faire (réanalyser au prochain démarrage de l'ordinateur, conserver l'élément détecté ou le supprimer).

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctions de VirusScan 32
Démarrage de la protection antivirus en temps réel 33
Démarrage de la protection supplémentaire.....35
Configuration de la protection antivirus.....39
Analyse de votre ordinateur 57
Exploitation des résultats d'analyse 61

Fonctions de VirusScan

VirusScan propose les fonctionnalités suivantes.

Protection complète anti-virus

VirusScan offre des services avancés de détection et de protection défendant votre ordinateur contre les menaces les plus récentes contre la sécurité : virus, chevaux de Troie, cookies de suivi, logiciels espions, logiciels publicitaires et autres programmes potentiellement indésirables. La protection s'étend au-delà des fichiers et dossiers de votre ordinateur de bureau, pour contrer les menaces provenant de différents points d'entrée, dont le courrier électronique, la messagerie instantanée et le Web. Aucune administration fastidieuse.

Options d'analyse économes en ressources

Si l'analyse est lente, vous pouvez désactiver l'option afin de minimiser l'utilisation des ressources de l'ordinateur, mais sachez qu'une plus haute priorité sera accordée à la protection anti-virus qu'aux autres tâches. VirusScan vous offre la possibilité de personnaliser les options d'analyse en temps réel et manuelle si vous le souhaitez ; dans le cas contraire, votre ordinateur reste protégé.

Réparations automatiques

Si VirusScan détecte une menace lors d'une analyse en temps réel ou d'une analyse manuelle, il tente de la traiter automatiquement en fonction du type de menace. De cette façon, la plupart des menaces peuvent être détectées et neutralisées sans que vous deviez intervenir. Dans de rares cas, VirusScan ne pourra peut-être pas neutraliser lui-même une menace. Dans ces cas, VirusScan vous laisse décider que faire (réanalyser au prochain démarrage de l'ordinateur, conserver l'élément détecté ou le supprimer).

Suspension de tâches en mode plein écran

Lorsque vous regardez un film, jouez ou effectuez toute autre activité sur votre ordinateur qui occupe la totalité de l'écran, VirusScan suspend un certain nombre de tâches, y compris les mises à jour automatiques et les analyses manuelles.

Démarrage de la protection antivirus en temps réel

VirusScan offre deux types de protection antivirus : en temps réel et manuelle La protection antivirus en temps réel surveille en permanence votre ordinateur pour déceler toute activité virale, en analysant les fichiers chaque fois que vous ou votre ordinateur y accédez. La protection antivirus manuelle vous permet d'analyser des fichiers à la demande. Pour garantir que votre ordinateur reste protégé contre les menaces les plus récentes, laissez la protection antivirus en temps réel activée et programmez des analyses manuelles régulières plus complètes. Par défaut, VirusScan effectue une analyse programmée une fois par semaine. Pour en savoir plus sur l'analyse en temps réel et l'analyse manuelle, consultez Analyse de votre ordinateur (page 57).

Exceptionnellement, vous voudrez suspendre temporairement l'analyse en temps réel (par exemple, pour changer certaines options d'analyse ou résoudre un problème de performance). Lorsque la protection antivirus en temps réel est désactivée, votre ordinateur n'est pas protégé et votre état de protection SecurityCenter passe au rouge. Pour plus d'informations sur l'état de protection, consultez « Explications sur l'état de protection » dans l'aide de SecurityCenter.

Démarrer la protection antivirus en temps réel

Par défaut, la protection antivirus en temps réel est activée et protège votre ordinateur contre les virus, chevaux de Troie et autres menaces pour la sécurité. Si vous désactivez la protection antivirus en temps réel, vous devez la réactiver pour rester protégé.

1 Ouvrez le volet Configuration Ordinateur & fichiers.

   Comment ?

   1. Dans le volet gauche, cliquez sur **Menu Avancé**.
   2. Cliquez sur **Configurer**.
   3. Dans la fenêtre de configuration, cliquez sur **Ordinateur & fichiers**.

2 Sous **Protection anti-virus**, cliquez sur **Activé**.

Arrêter la protection antivirus en temps réel

Vous pouvez désactiver temporairement la protection antivirus en temps réel et spécifier quand elle doit reprendre. La protection peut être automatiquement réactivée après 15, 30, 45 ou 60 minutes, au redémarrage de l'ordinateur ou jamais.

1 Ouvrez le volet Configuration Ordinateur & fichiers.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans la fenêtre de configuration, cliquez sur **Ordinateur & fichiers**.

2 Sous **Protection anti-virus**, cliquez sur **Désactivé**.

3 Dans la boîte de dialogue, sélectionnez l'option de reprise de l'analyse en temps réel.

4 Cliquez sur **OK**.

CHAPITRE 9

Démarrage de la protection supplémentaire

Outre la protection antivirus en temps réel, VirusScan offre une protection avancée contre les scripts, logiciels espions et les pièces jointes potentiellement nocives dans le courrier électronique et la messagerie instantanée. Par défaut, l'analyse de scripts, la protection contre les logiciels espions et la protection du courrier électronique et des messages instantanés sont activées et protègent votre ordinateur.

Analyse de scripts

L'analyse de scripts détecte les scripts potentiellement nocifs et les empêche de s'exécuter sur votre ordinateur. Elle surveille votre ordinateur pour déceler toute activité suspecte de scripts, comme les scripts qui créent, copient ou suppriment des fichiers ou qui ouvrent votre registre Windows, et vous avertit avant que votre ordinateur puisse subir un quelconque dommage.

Protection contre les logiciels espions

La protection contre les logiciels espions détecte les logiciels espions, logiciels publicitaires et autres applications potentiellement indésirables. Les logiciels espions sont des logiciels qui peuvent être installés à votre insu sur votre ordinateur pour surveiller votre comportement, collecter des informations personnelles et même interférer dans le contrôle de l'ordinateur en installant d'autres logiciels ou en redirigeant l'activité du navigateur.

Protection des e-mails

La protection des e-mails détecte toute activité suspecte dans les e-mails et les pièces jointes que vous envoyez et recevez.

Protection de la messagerie instantanée

La protection de la messagerie instantanée détecte des menaces potentielles pour la sécurité provenant de pièces jointes à des messages instantanés que vous recevez. Elle empêche aussi les programmes de messagerie instantanée de partager des informations personnelles.

Contenu de ce chapitre

Lancer l'analyse de scripts.....36
Démarrer la protection contre les logiciels espions .36
Démarrer la protection des e-mails.....37
Démarrer la protection de la messagerie instantanée 37

Lancer l'analyse de scripts

Activez la protection par analyse de scripts pour détecter les scripts potentiellement nocifs et les empêcher de s'exécuter sur votre ordinateur. Cette protection vous avertit lorsqu'un script tente de créer, copier ou supprimer des fichiers sur votre ordinateur, ou d'effectuer des modifications dans le registre de Windows.

1 Ouvrez le volet Configuration Ordinateur & fichiers.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans la fenêtre de configuration, cliquez sur **Ordinateur & fichiers**.

2 Sous **Protection des analyses de scripts**, cliquez sur **Activé**.

Remarque : Bien que vous puissiez désactiver l'analyse des scripts à tout moment, cela laisse l'ordinateur vulnérable aux scripts nuisibles.

Démarrer la protection contre les logiciels espions

Activez la protection contre les logiciels espions pour détecter et supprimer les logiciels espions et publicitaires ainsi que tout programme potentiellement indésirable qui collecte et transmet des informations à votre insu ou sans votre autorisation.

1 Ouvrez le volet Configuration Ordinateur & fichiers.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans la fenêtre de configuration, cliquez sur **Ordinateur & fichiers**.

2 Sous **Protection des analyses de scripts**, cliquez sur **Activé**.

Remarque : Bien que vous puissiez désactiver la protection contre les logiciels espions à tout moment, cela laisse l'ordinateur vulnérable aux programmes potentiellement indésirables.

Démarrer la protection des e-mails

Activez la protection des e-mails pour détecter les vers ainsi que les menaces potentielles dans les messages électroniques sortants (SMTP) et entrants (POP3) et leurs pièces jointes.

1 Ouvrez le volet Configuration E-mail & IM.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans la fenêtre de configuration, cliquez sur **E-mail & IM**.

2 Sous **Protection de la messagerie**, cliquez sur **Activé**.

Remarque : Bien que vous puissiez désactiver la protection des e-mails à tout moment, cela laisse l'ordinateur vulnérable aux menaces par e-mail.

Démarrer la protection de la messagerie instantanée

Activez la protection de la messagerie instantanée pour détecter les menaces pour la sécurité se cachant dans les pièces jointes aux messages instantanés.

1 Ouvrez le volet Configuration E-mail & IM.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans la fenêtre de configuration, cliquez sur **E-mail & IM**.

2 Sous **Protection de la messagerie instantanée**, cliquez sur **Activé**.

Remarque : Bien que vous puissiez désactiver la protection de la messagerie instantanée à tout moment, cela laisse l'ordinateur vulnérable aux pièces jointes nuisibles des messages instantanés.

CHAPITRE 10

Configuration de la protection antivirus

VirusScan offre deux types de protection antivirus : en temps réel et manuelle La protection antivirus en temps réel analyse les fichiers à chaque fois que vous ou votre ordinateur y accédez. La protection antivirus manuelle vous permet d'analyser des fichiers à la demande. Vous pouvez définir différentes options pour chaque type de protection. Par exemple, puisque la protection en temps réel surveille en permanence votre ordinateur, vous pourriez sélectionner un certain ensemble d'options d'analyse de base et garder un choix d'options plus complet pour la protection manuelle à la demande.

Contenu de ce chapitre

Configuration des options d'analyse en temps réel .40
Configuration des options d'analyse manuelle 42
Utilisation des options SystemGuards 46
Utilisation des listes approuvées 53

Configuration des options d'analyse en temps réel

Lorsque vous activez la protection antivirus en temps réel, VirusScan utilise un ensemble d'options par défaut pour analyser les fichiers ; cependant, vous pouvez changer les options par défaut pour les adapter à vos besoins.

Pour changer les options d'analyse en temps réel, vous devez prendre des décisions concernant la cible des contrôles effectués par VirusScan, ainsi que l'emplacement et les types de fichiers analysés. Par exemple, vous pouvez déterminer si VirusScan doit vérifier les virus inconnus ou les cookies que les sites Web peuvent utiliser pour suivre vos activités, et s'il doit analyser les disques réseau mappés sur votre ordinateur ou uniquement les disques locaux. Vous pouvez aussi définir les types de fichiers à analyser (tous les fichiers ou uniquement les fichiers programmes et les documents, car c'est là que se trouvent la plupart des virus).

Lorsque vous changez les options d'analyse en temps réel, vous devez aussi spécifier s'il est important de protéger votre ordinateur contre les débordements de mémoire tampon. Une mémoire tampon est une section de mémoire utilisée pour stocker temporairement des informations. Les débordements de mémoire tampon peuvent survenir lorsque la masse d'informations que des processus ou programmes suspects stockent dans une mémoire tampon dépasse la capacité de la mémoire. Lorsque cela se produit, l'ordinateur devient plus vulnérable aux attaques.

Configurer les options d'analyse en temps réel

Vous configurez les options d'analyse en temps réel pour personnaliser la cible des contrôles effectués par VirusScan lors d'une analyse en temps réel, ainsi que l'emplacement et les types de fichiers à analyser. Les options comprennent l'analyse des virus inconnus et des cookies ainsi que la protection contre les débordements de mémoire tampon. Vous pouvez aussi configurer l'analyse en temps réel pour vérifier les disque réseau mappés sur votre ordinateur.

1 Ouvrez le volet Analyse en temps réel.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Ordinateur & fichiers**.
3. Dans la zone d'informations Ordinateurs & Fichiers, cliquez sur **Configurer**.
4. Dans le volet Configuration Ordinateur & fichiers, vérifiez que la protection antivirus est activée, puis cliquez sur **Avancé**.

2 Spécifiez les options d'analyse en temps réel, puis cliquez sur **OK**.

Pour...	Opération à exécuter...
Détecter les virus inconnus et les nouvelles variantes de virus connus	Activez la case à cocher **Recherche heuristique de virus inconnus**.
Détecter les cookies	Activez la case à cocher **Rechercher et supprimer les cookies de suivi**.
Détecter les virus et autres menaces potentielles sur les disques connectés à votre réseau	Activez la case à cocher **Analyser les lecteurs réseau**.
Protéger votre ordinateur contre les débordements de mémoire tampon	Activez la case à cocher **Activer la protection contre le débordement de tampon**.
Préciser les types de fichiers à analyser	Cliquez sur **Tous les fichiers (recommandé)** ou sur **Fichiers programme et documents uniquement**.

Configuration des options d'analyse manuelle

La protection antivirus manuelle vous permet d'analyser des fichiers à la demande. Lorsque vous lancez une analyse manuelle, VirusScan cherche sur votre ordinateur les virus et autres éléments potentiellement nuisibles en utilisant une palette d'options d'analyse plus complète. Pour changer les options d'analyse manuelle, vous devez décider ce que VirusScan doit rechercher lors d'une analyse. Par exemple, vous pouvez déterminer si VirusScan doit rechercher les virus inconnus, les programmes potentiellement indésirables tels que les logiciels espions ou publicitaires, les programmes furtifs tels que les rootkits qui peuvent octroyer un accès non autorisé à votre ordinateur, et les cookies que les sites Web peuvent utiliser pour suivre vos activités. Vous devez aussi spécifier les types de fichiers à vérifier. Par exemple, vous pouvez spécifier si VirusScan doit vérifier tous les fichiers ou uniquement les fichiers programmes et les documents (car c'est là que se trouvent la plupart des virus). Vous pouvez aussi déterminer si l'analyse doit inclure les fichiers d'archive (par exemple les fichiers .zip).

Par défaut, VirusScan analyse tous les disques et dossiers de votre ordinateur chaque fois qu'il effectue une analyse manuelle ; vous pouvez cependant modifier les emplacements par défaut pour les adapter à vos besoins. Par exemple, vous pouvez limiter l'analyse aux fichiers système critiques, aux éléments placés sur votre bureau ou à ceux de votre dossier Program Files. À moins de vouloir lancer vous-même chaque analyse manuelle, vous pouvez programmer des analyses régulières. Les analyses programmées vérifient toujours la totalité de l'ordinateur avec les options d'analyse par défaut. Par défaut, VirusScan effectue une analyse programmée une fois par semaine.

Si vous trouvez que l'analyse est lente, vous pouvez envisager de désactiver l'option afin de minimiser l'utilisation des ressources de l'ordinateur, mais sachez qu'une plus haute priorité sera accordée à la protection antivirus qu'aux autres tâches.

Remarque : Lorsque vous regardez un film, jouez ou effectuez toute autre activité sur votre ordinateur qui occupe la totalité de l'écran, VirusScan suspend un certain nombre de tâches, y compris les mises à jour automatiques et les analyses manuelles.

Configurer les options d'analyse manuelle

Vous configurez les options d'analyse manuelle pour personnaliser la cible des contrôles effectués par VirusScan lors d'une analyse manuelle, ainsi que l'emplacement et les types de fichiers à analyser. Les options comprennent la recherche de virus inconnus, l'analyse des fichiers d'archive, la recherche de logiciels espions, de programmes potentiellement indésirables, de cookies de suivi, de rootkits et de programmes furtifs.

1 Ouvrez le volet Analyse manuelle.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Ordinateur & fichiers**.
3. Dans la zone d'informations Ordinateurs & Fichiers, cliquez sur **Configurer**.
4. Dans le volet Configuration Ordinateur & fichiers, vérifiez que la protection antivirus est activée, puis cliquez sur **Avancé**.
5. Dans la fenêtre Protection antivirus, cliquez sur **Analyse manuelle**.

2 Spécifiez les options d'analyse manuelle, puis cliquez sur **OK**.

Pour...	Opération à exécuter...
Détecter les virus inconnus et les nouvelles variantes de virus connus	Activez la case à cocher **Recherche heuristique de virus inconnus**.
Détecter et supprimer les virus dans les fichiers .zip et autres fichiers d'archive	Activez la case à cocher **Analyse des fichiers .zip et autres fichiers d'archive**.
Détecter les logiciels espions, logiciels publicitaires et autres applications potentiellement indésirables.	Activez la case à cocher **Rechercher les logiciels espions et les programmes potentiellement indésirables**.
Détecter les cookies	Activez la case à cocher **Rechercher et supprimer les cookies de suivi**.
Détecter les rootkits et les programmes furtifs pouvant altérer et exploiter les fichiers système Windows existants	Activez la case à cocher **Rechercher les rootkits et autres programmes furtifs**.

Réduire l'utilisation du processeur pour les analyses tout en donnant une plus haute priorité aux autres tâches (comme la navigation Web ou l'ouverture de documents)	Activez la case à cocher **Analyser en utilisant un minimum de ressources informatiques**.
Préciser les types de fichiers à analyser	Cliquez sur **Tous les fichiers (recommandé)** ou sur **Fichiers programme et documents uniquement**.

Configurer l'emplacement de l'analyse manuelle

Vous définissez l'emplacement de l'analyse manuelle pour spécifier où VirusScan doit rechercher des virus et autres éléments nuisibles lors d'une analyse manuelle. Vous pouvez analyser tous les fichiers, dossiers et disques de votre ordinateur ou limiter l'analyse à des dossiers et disques spécifiques.

1 Ouvrez le volet Analyse manuelle.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Ordinateur & fichiers**.
3. Dans la zone d'informations Ordinateurs & Fichiers, cliquez sur **Configurer**.
4. Dans le volet Configuration Ordinateur & fichiers, vérifiez que la protection antivirus est activée, puis cliquez sur **Avancé**.
5. Dans la fenêtre Protection antivirus, cliquez sur **Analyse manuelle**.

2 Cliquez sur **Emplacement par défaut à analyser**.

3 Spécifiez l'emplacement d'analyse manuelle, puis cliquez sur **OK**.

Pour...	Opération à exécuter...
Analyser tous les fichiers et dossiers de votre ordinateur	Activez la case à cocher **Poste de travail**.
Analyser des fichiers, dossiers et disques spécifiques sur votre ordinateur	Désactivez la case à cocher **Poste de travail** et sélectionnez un ou plusieurs dossiers ou disques.

Analyser les fichiers système critiques	Désactivez la case à cocher **Poste de travail** et activez la case à cocher **Fichiers système critiques**.

Programmer une analyse

Programmez des analyses pour procéder à une analyse approfondie de votre ordinateur à la recherche de virus et d'autres menaces à tout moment de la semaine. Les analyses programmées vérifient toujours la totalité de l'ordinateur avec les options d'analyse par défaut. Par défaut, VirusScan effectue une analyse programmée une fois par semaine. Si vous trouvez que l'analyse est lente, vous pouvez envisager de désactiver l'option afin de minimiser l'utilisation des ressources de l'ordinateur, mais sachez qu'une plus haute priorité sera accordée à la protection antivirus qu'aux autres tâches.

1 Ouvrez le volet Analyse programmée.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Ordinateur & fichiers**.
3. Dans la zone d'informations Ordinateurs & Fichiers, cliquez sur **Configurer**.
4. Dans le volet Configuration Ordinateur & fichiers, vérifiez que la protection antivirus est activée, puis cliquez sur **Avancé**.
5. Dans le volet Protection antivirus, cliquez sur **Analyse programmée**.

2 Sélectionnez **Autoriser une analyse programmée**.

3 Pour réduire la puissance de calcul normalement utilisée pour une analyse, sélectionnez **Analyser en utilisant un minimum de ressources informatiques**.

4 Sélectionnez un ou plusieurs jours.

5 Spécifiez une heure de début.

6 Cliquez sur **OK**.

Conseil : Vous pouvez rétablir le programme par défaut en cliquant sur **Réinitialiser**.

Utilisation des options SystemGuards

SystemGuards permet de surveiller, consigner, rapporter et gérer les modifications potentiellement non autorisées apportées au registre de Windows ou à des fichiers système critiques sur votre ordinateur. Les modifications non autorisées apportées au registre et aux fichiers risquent de nuire à votre ordinateur, de compromettre la sécurité informatique et d'endommager de précieux fichiers système.

Les modifications du registre et des fichiers sont courantes et se produisent fréquemment sur votre ordinateur. La plupart de ces modifications étant inoffensives, les réglages par défaut de SystemGuards sont configurés pour offrir une protection fiable, intelligente et réaliste contre les modifications non autorisées présentant un risque significatif. Par exemple, lorsque SystemGuards détecte des changements inhabituels et présentant une menace potentiellement importante, cette activité est immédiatement signalée et consignée. Les modifications plus courantes mais constituant néanmoins un risque potentiel sont uniquement consignées. En revanche, la surveillance des changements standard à faible risque est désactivée par défaut. La technologie SystemGuards peut être configurée pour étendre sa protection à tout environnement que vous souhaitez.

Il y a trois types de SystemGuards : SystemGuards Programme, SystemGuards Windows et SystemGuards Navigateur.

SystemGuard Programme

Les SystemGuards Programme détectent les modifications potentiellement non autorisées apportées au registre de votre ordinateur et à d'autres fichiers critiques essentiels pour Windows. Ces éléments du registre et fichiers importants comprennent les installations ActiveX, les éléments de démarrage, les shell execute hooks de Windows et les shell service object delay loads. En surveillant ces éléments, la technologie SystemGuards Programme bloque les programmes ActiveX suspects (téléchargés depuis Internet) en plus des logiciels espions et des applications potentiellement indésirables pouvant se lancer automatiquement au démarrage de Windows.

SystemGuards Windows

Les SystemGuards Windows détectent aussi les modifications potentiellement non autorisées apportées au registre de votre ordinateur et à d'autres fichiers critiques essentiels pour Windows. Ces éléments du registre et fichiers importants comprennent les gestionnaires de menus contextuels, les DLL appInit et le fichier hosts Windows. En surveillant ces éléments, la technologie SystemGuards Windows vous aide à éviter que votre ordinateur envoie et reçoive des informations non autorisées ou personnelles via Internet. Elle peut aussi aider à bloquer les programmes suspects pouvant modifier l'apparence et le comportement des programmes importants pour vous et votre famille.

SystemGuard Navigateur

Comme les SystemGuards Programme et Windows, les SystemGuards Navigateur détectent les modifications potentiellement non autorisées apportées au registre de votre ordinateur et à d'autres fichiers critiques essentiels pour Windows. Ces SystemGuards surveillent cependant les modifications apportées à des éléments du registre et fichiers importants tels que les extensions pour Internet Explorer, les URL Internet Explorer et les zones de sécurité Internet Explorer. En surveillant ces éléments, la technologie SystemGuards Navigateur aide à empêcher les activités non autorisées dans le navigateur, comme la redirection vers des sites Web suspects, les modifications des paramètres et options du navigateur à votre insu, et l'approbation indésirable de sites Web suspects.

Activer la protection SystemGuards

Activez la protection SystemGuards pour détecter et signaler les modifications potentiellement non autorisées du registre Windows et des fichiers système sur votre ordinateur. Les modifications non autorisées apportées au registre et aux fichiers risquent de nuire à votre ordinateur, de compromettre la sécurité informatique et d'endommager de précieux fichiers système.

1 Ouvrez le volet Configuration Ordinateur & fichiers.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans la fenêtre de configuration, cliquez sur **Ordinateur & fichiers**.

2 Sous **Protection SystemGuard**, cliquez sur **Activé**.

Remarque : Vous pouvez désactiver la protection SystemGuards en cliquant sur **Désactivé**.

Configuration des options SystemGuards

Utilisez le volet SystemGuards pour configurer les options de protection, consignation et alerte contre les modifications non autorisées du registre et des fichiers liées aux fichiers et programmes Windows ainsi qu'à Internet Explorer. Les modifications non autorisées apportées au registre et aux fichiers risquent de nuire à votre ordinateur, de compromettre la sécurité informatique et d'endommager de précieux fichiers système.

1 Ouvrez le volet SystemGuards.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Ordinateur & fichiers**.
3. Dans la zone d'informations Ordinateurs & Fichiers, cliquez sur **Configurer**.
4. Dans le volet Configuration Ordinateur & fichiers, vérifiez que la protection SystemGuard est activée, puis cliquez sur **Avancé**.

2 Sélectionnez un type de protection SystemGuards dans la liste.

- **SystemGuard Programme**
- **SystemGuards Windows**
- **SystemGuard Navigateur**

3 Sous **Je souhaite**, effectuez l'une des actions suivantes :

- Pour détecter, consigner et signaler les modifications non autorisées du registre et des fichiers liées aux SystemGuards Programme, Windows et Navigateur, cliquez sur **Afficher les alertes.**
- Pour détecter et consigner les modifications non autorisées du registre et des fichiers liées aux SystemGuards Programme, Windows et Navigateur, cliquez sur **Consigner uniquement les modifications.**
- Pour désactiver la détection de modifications non autorisées du registre et des fichiers liées aux SystemGuards Programme, Windows et Navigateur, cliquez sur **Désactiver SystemGuard.**

Remarque : Pour plus d'informations sur les types de SystemGuards, consultez À propos des types de SystemGuards (page 49).

À propos des types de SystemGuards

Les SystemGuards détectent les modifications potentiellement non autorisées apportées au registre de votre ordinateur et à d'autres fichiers critiques essentiels pour Windows. Il y a trois types de SystemGuards : SystemGuards Programme, SystemGuards Windows et SystemGuards Navigateur

SystemGuard Programme

La technologie SystemGuards Programme bloque les programmes ActiveX suspects (téléchargés depuis Internet) en plus des logiciels espions et des applications potentiellement indésirables pouvant se lancer automatiquement au démarrage de Windows.

SystemGuard	Détection
Installations ActiveX	Les modifications non autorisées apportées au registre des installations ActiveX risquent de nuire à votre ordinateur, de compromettre la sécurité informatique et d'endommager de précieux fichiers système.
Éléments de démarrage	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant apporter des modifications de fichiers dans les éléments de démarrage pour permettre à des programmes suspects de s'exécuter au démarrage de votre ordinateur.
Shell Execute Hooks de Windows	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant installer des programmes dans le Shell Windows (Shell Execute Hooks) pour empêcher le bon fonctionnement des programmes de sécurité.
Shell Service Object Delay Load	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant apporter des modification de registre à la charge de retard de l'objet de service du Shell pour permettre à des fichiers nuisibles de s'exécuter au démarrage de votre ordinateur.

SystemGuards Windows

La technologie SystemGuards Windows vous aide à éviter que votre ordinateur envoie et reçoive des informations non autorisées ou personnelles via Internet. Elle peut aussi aider à bloquer les programmes suspects pouvant modifier l'apparence et le comportement des programmes importants pour vous et votre famille.

SystemGuard	Détection
Gestionnaires de menus contextuels	Modifications de registre non autorisées apportées aux gestionnaires de menus contextuels et pouvant affecter l'apparence et le comportement des menus Windows. Les menus contextuels permettent d'effectuer diverses actions sur votre ordinateur, comme un clic droit sur un fichier.
DLL AppInit	Modifications de registre non autorisées apportées aux DLL AppInit de Windows et pouvant entraîner l'exécution de fichiers potentiellement nuisibles au démarrage de votre ordinateur.
Fichier Hosts Windows	Logiciels espions, publicitaires et programmes potentiellement indésirables pouvant apporter des modifications non autorisées à votre fichier Hosts Windows pour permettre la redirection de votre navigateur vers des sites Web suspects et bloquer les mises à jour de logiciels.
Shell Winlogon	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre du Shell Winlogon pour permettre à d'autres programmes de se substituer à l'Explorateur Windows.
Clé UserInit de Winlogon	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre de Winlogon User Init pour permettre à des programmes suspects de s'exécuter lorsque vous vous connectez à Windows.
Protocoles Windows	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre des protocoles Windows et affecter ainsi la manière dont votre ordinateur envoie et reçoit des informations sur Internet.
Fournisseurs de services en couche (Layered Service Providers ou LSP) Winsock	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre des fournisseurs de services en couche (Winsock Layered Service Providers - LSP) pour intercepter et modifier les informations envoyées et reçues sur Internet.

Commandes Open Shell Windows	Modifications non autorisées aux commandes Open Shell de Windows pouvant entraîner l'exécution de vers ou d'autres programmes nuisibles sur votre ordinateur.
Gestionnaire de tâches programmées	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant apporter des modifications au registre et aux fichiers du gestionnaire de tâches partagées pour autoriser des fichiers nuisibles à s'exécuter au démarrage de votre ordinateur.
Windows Messenger Service	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre de Windows Messenger Service et ouvrir la voie aux publicités intempestives et aux programmes exécutés à distance.
Fichier Windows Win.ini	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le fichier Win.ini et permettre à des programmes suspects de s'exécuter au démarrage de votre ordinateur.

SystemGuard Navigateur

La technologie SystemGuards Navigateur aide à empêcher les activités non autorisées dans le navigateur, comme la redirection vers des sites Web suspects, les modifications des paramètres et options du navigateur à votre insu, et l'approbation indésirable de sites Web suspects.

SystemGuard	Détection
Browser Helper Objects (BHO)	Logiciels espions, publicitaires ou autres programmes potentiellement indésirables pouvant utiliser les "browser helper objects" pour suivre les actions de navigation et afficher des publicités de manière intempestive.
Barres Internet Explorer	Modifications non autorisées apportées au registre des programmes de la barre Internet Explorer, tels que Rechercher et Favoris, pouvant affecter l'apparence et le comportement d'Internet Explorer.
Modules Internet Explorer complémentaires	Logiciels espions, publicitaires ou autres programmes potentiellement indésirables pouvant installer des modules Internet Explorer complémentaires pour suivre les actions de navigation et afficher des publicités de manière intempestive.
ShellBrowser Internet Explorer	Modifications non autorisées apportées au registre du ShellBrowser Internet Explorer et pouvant affecter l'apparence et le comportement de votre navigateur Web.

WebBrowser Internet Explorer	Modifications non autorisées apportées au registre du navigateur Web Internet Explorer et pouvant affecter l'apparence et le comportement de votre navigateur Web.
URL Search Hooks Internet Explorer	Logiciels espions, publicitaires ou programmes potentiellement indésirables pouvant modifier le registre des "Internet Explorer URL Search Hooks" et autoriser ainsi la redirection de votre navigateur vers des sites Web suspects lorsque vous effectuez des recherches sur Internet.
URL Internet Explorer	Logiciels espions, publicitaires et autres programmes potentiellement nuisibles pouvant modifier le registre des URL d'Internet Explorer et affecter ainsi les paramètres du navigateur.
Restrictions Internet Explorer	Logiciels espions, publicitaires et autres programmes potentiellement nuisibles pouvant modifier le registre des restrictions d'Internet Explorer et affecter ainsi les paramètres et options du navigateur.
Zones de sécurité Internet Explorer	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre des zones de sécurité d'Internet Explorer et permettre à des fichiers nuisibles de s'exécuter au démarrage de votre ordinateur.
Sites de confiance d'Internet Explorer	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre des sites autorisés d'Internet Explorer pour permettre à votre navigateur d'afficher des sites Web suspects.
Stratégie Internet Explorer	Logiciels espions, publicitaires et autres programmes potentiellement nuisibles pouvant modifier le registre des stratégies d'Internet Explorer et affecter ainsi l'apparence et le comportement du navigateur.

Utilisation des listes approuvées

Si VirusScan détecte une modification de fichier ou de registre (SystemGuard), un programme suspect ou un débordement de mémoire tampon, il vous invite à l'approuver ou à le supprimer. Si vous approuvez l'élément et indiquez que vous ne voulez plus être alerté de son activité, l'élément est ajouté à une liste approuvée et VirusScan ne le détecte plus ou ne vous avertit plus de son activité. Si un élément a été ajouté à une liste approuvée, mais que vous décidez d'en bloquer les activités, vous pouvez le faire. Le blocage de l'élément l'empêche de s'exécuter ou de modifier votre ordinateur sans que vous soyez averti de chaque tentative. Vous pouvez aussi supprimer un élément d'une liste approuvée. La suppression d'un élément permet à VirusScan de détecter à nouveau les activités de cet élément.

Gestion des listes approuvées.

Utilisez le volet Listes approuvées pour approuver ou bloquer des éléments qui ont été précédemment détectés et approuvés. Vous pouvez aussi supprimer un élément d'une liste approuvée afin que VirusScan le détecte à nouveau.

1 Ouvrez le volet Listes approuvées.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Ordinateur & fichiers**.
3. Dans la zone d'informations Ordinateurs & Fichiers, cliquez sur **Configurer**.
4. Dans le volet Configuration Ordinateur & fichiers, vérifiez que la protection antivirus est activée, puis cliquez sur **Avancé**.
5. Dans le volet Protection antivirus, cliquez sur **Listes approuvées**.

2 Sélectionnez un des types de listes approuvées suivants :

- **SystemGuard Programme**
- **SystemGuards Windows**
- **SystemGuard Navigateur**
- **Programmes autorisés**
- **Débordements de mémoire tampon approuvés**

3 Sous **Je souhaite**, effectuez l'une des actions suivantes :

- Pour autoriser l'élément détecté à modifier le registre de Windows ou des fichiers système critiques sur votre ordinateur sans que vous en soyez averti, cliquez sur **Autoriser**.

- Pour bloquer l'élément détecté et l'empêcher de modifier le registre de Windows ou des fichiers système critiques sur votre ordinateur sans que vous en soyez averti, cliquez sur **Bloquer**.
- Pour supprimer l'élément des listes approuvées, cliquez sur **Supprimer**.

4 Cliquez sur **OK**.

Remarque : Pour plus d'informations sur les types de listes approuvées, consultez À propos des types de listes approuvées (page 54).

À propos des types de listes approuvées

Les SystemGuards dans le volet Listes approuvées représentent des modifications non autorisées au registre et aux fichiers que VirusScan a détectées précédemment, mais que vous avez choisi d'autoriser à partir d'une alerte ou du volet Résultats de l'analyse. Il y a cinq types de listes approuvées que vous pouvez gérer dans le volet Listes approuvées : SystemGuards Programme, SystemGuards Windows, SystemGuards Navigateur, Programmes approuvés et Débordements de mémoire tampon approuvés.

Option	Description
SystemGuard Programme	Les SystemGuards Programme dans le volet Listes approuvées représentent des modifications non autorisées au registre et aux fichiers que VirusScan a détectées précédemment, mais que vous avez choisi d'autoriser à partir d'une alerte ou du volet Résultats de l'analyse. Les SystemGuards Programme détectent les modifications du registre et des fichiers système associées aux installations ActiveX, éléments de démarrage, shell execute hooks de Windows et shell service object delay loads. Ces types de modifications non autorisées du registre et des fichiers système risquent de nuire à votre ordinateur, de compromettre la sécurité informatique et d'endommager de précieux fichiers système.

SystemGuards Windows	Les SystemGuards Windows dans le volet Listes approuvées représentent des modifications non autorisées au registre et aux fichiers que VirusScan a détectées précédemment, mais que vous avez choisi d'autoriser à partir d'une alerte ou du volet Résultats de l'analyse. Les SystemGuards Windows détectent les les modifications du registre et des fichiers système associées aux gestionnaires de menus contextuels, aux DLL appInit, au fichier Hosts de Windows, au shell Winlogon, aux Winsock Layered Service Providers (LSP), etc. Ces types de modifications non autorisées du registre et des fichiers système peuvent affecter la façon dont votre ordinateur envoie et reçoit des informations via Internet, changer l'apparence et le comportement de programmes et autoriser des programmes suspects à s'exécuter sur votre ordinateur.
SystemGuard Navigateur	Les SystemGuards Navigateur dans le volet Listes approuvées représentent des modifications non autorisées au registre et aux fichiers que VirusScan a détectées précédemment, mais que vous avez choisi d'autoriser à partir d'une alerte ou du volet Résultats de l'analyse. Les SystemGuards Navigateur détectent les modifications non autorisées du registre et autres comportements indésirables associés aux Browser Helper Objects, aux extensions Internet Explorer, aux URL Internet Explorer, aux zones de sécurité Internet Explorer, etc. Ces types de modifications non autorisées peuvent entraîner des activités indésirables dans le navigateur, comme la redirection vers des sites Web suspects, les modifications des paramètres et options du navigateur, et l'approbation de sites Web suspects.
Programmes autorisés	Les programmes approuvés sont des programmes potentiellement indésirables que VirusScan a détectés précédemment, mais que vous avez choisi d'autoriser à partir d'une alerte ou du volet Résultats de l'analyse.

Débordements de mémoire tampon approuvés	Les débordements de mémoire tampon approuvés représentent des activités indésirables que VirusScan a détectées précédemment, mais que vous avez choisi d'autoriser à partir d'une alerte ou du volet Résultats de l'analyse. Les débordements de mémoire tampon peuvent nuire à votre ordinateur et endommager des fichiers. Les débordements de mémoire tampon surviennent lorsque la masse d'informations que des processus ou programmes suspects stockent dans une mémoire tampon dépasse la capacité de la mémoire.

CHAPITRE 11

Analyse de votre ordinateur

Lorsque vous lancez SecurityCenter pour la première fois, la protection antivirus en temps réel de VirusScan commence à protéger votre ordinateur contre les virus, chevaux de Troie et autres menaces potentiellement nuisibles. À moins que vous désactiviez la protection antivirus en temps réel, VirusScan surveille en permanence votre ordinateur pour déceler toute activité virale, en analysant les fichiers chaque fois que vous ou votre ordinateur y accédez, en utilisant les options d'analyse en temps réel que vous avez définies. Pour garantir que votre ordinateur reste protégé contre les menaces les plus récentes, laissez la protection antivirus en temps réel activée et programmez des analyses manuelles régulières plus complètes. Pour en savoir plus sur la configuration des options d'analyse en temps réel et d'analyse manuelle, consultez Configuration de la protection antivirus (page 39).

VirusScan offre une palette plus détaillée d'options d'analyse pour la protection antivirus manuelle, vous permettant ainsi d'exécuter périodiquement des analyses plus poussées. Vous pouvez lancer des analyses manuelles à partir de SecurityCenter, en ciblant des emplacement spécifiques selon un programme défini. Cependant, vous pouvez aussi exécuter des analyses manuelles en cours de travail directement dans l'Explorateur Windows. L'analyse dans SecurityCenter offre l'avantage de permettre de changer les options d'analyse sur le moment. L'analyse à partir de l'Explorateur Windows, en revanche, offre une approche pratique de la sécurité informatique.

Que vous lanciez une analyse manuelle à partir de SecurityCenter ou de l'Explorateur Windows, vous pouvez consulter les résultats de l'analyse une fois celle-ci terminée. Vous pouvez consulter les résultats d'une analyse pour déterminer si VirusScan a détecté, réparé ou mis en quarantaine des virus, chevaux de Troie, logiciels espions, logiciels publicitaires, cookies et autres programmes potentiellement indésirables. Les résultats d'une analyse peuvent s'afficher de différentes manières. Par exemple, vous pouvez afficher un résumé des résultats ou des informations détaillées telles que le statut et le type de l'infection. Vous pouvez aussi afficher des statistiques générales d'analyse et de détection.

Contenu de ce chapitre

Analyser votre ordinateur.....58
Afficher les résultats de l'analyse 59

Analyser votre ordinateur

Vous pouvez exécuter une analyse manuelle à partir du menu Avancé ou du menu de base de SecurityCenter. Si vous lancez une analyse à partir du menu Avancé, vous pouvez confirmer les options d'analyse manuelle avant de commencer. Si vous lancez une analyse à partir du menu de base, VirusScan lance immédiatement l'analyse, en utilisant les options d'analyse existantes. Vous pouvez aussi exécuter une analyse dans l'Explorateur Windows en utilisant les options d'analyse existantes.

- Effectuez l'une des opérations suivantes :

  Analyser dans SecurityCenter

Pour...	Opération à exécuter...
Analyser avec les paramètres existants	Cliquez sur **Analyser** dans le menu de base.
Analyser avec des paramètres différents	Cliquez sur **Analyser** dans le menu Avancé, sélectionnez les emplacements à analyser, sélectionnez les options d'analyse et cliquez sur **Analyser maintenant**.

  Analyser dans l'Explorateur Windows

  1. Ouvrez l'Explorateur Windows.
  2. Cliquez avec le bouton droit sur un fichier, dossier ou disque, puis cliquez sur **Analyser**.

Remarque : Les résultats d'analyse apparaissent dans l'alerte Analyse terminée. Ces résultats comprennent le nombre d'éléments analysés, détectés, réparés, mis en quarantaine et supprimés. Cliquez sur **Afficher les détails de l'analyse** pour en savoir plus sur les résultats d'analyse ou gérer les éléments infectés.

Afficher les résultats de l'analyse

Lorsqu'une analyse manuelle se termine, vous pouvez en afficher les résultats pour déterminer ce que l'analyse a décelé et connaître l'état de protection actuel de votre ordinateur. Les résultats d'analyse indiquent si VirusScan a détecté, réparé ou mis en quarantaine des virus, chevaux de Troie, logiciels espions, logiciels publicitaires, cookies et autres programmes potentiellement indésirables.

- Dans le menu de base ou le menu avancé, cliquez sur **Analyser**, puis effectuez l'une des opérations suivantes :

Pour...	Opération à exécuter...
Afficher les résultats d'analyse dans l'alerte	Affichez les résultats d'analyse dans l'alerte Analyse terminée.
Afficher davantage d'informations sur les résultats d'analyse	Cliquez sur **Afficher les détails de l'analyse** dans l'alerte Analyse terminée.
Afficher un bref résumé des résultats d'analyse	Pointez sur l'icône **Analyse terminée** dans la zone de notification de votre barre des tâches.
Afficher des statistiques d'analyse et de détection	Double-cliquez sur l'icône **Analyse terminée** dans la zone de notification de votre barre des tâches.
Afficher des détails sur les éléments détectés, l'état d'infection et le type d'infection.	Double-cliquez sur l'icône **Analyse terminée** dans la zone de notification de votre barre des tâches, puis cliquez sur **Afficher les résultats** dans le volet Progression de l'analyse : Analyse manuelle.

CHAPITRE 12

Exploitation des résultats d'analyse

Si VirusScan détecte une menace lors d'une analyse en temps réel ou d'une analyse manuelle, il tente de la traiter automatiquement en fonction du type de menace. Par exemple, si VirusScan détecte un virus, un cheval de Troie ou un cookie de suivi sur votre ordinateur, il tente de nettoyer le fichier infecté. S'il n'y parvient pas, il le met en quarantaine.

Pour certaines menaces, il se peut que VirusScan ne réussisse pas à nettoyer ni à mettre en quarantaine un fichier. Dans ce cas, VirusScan vous invite à gérer la menace en question. Vous avez le choix entre différentes actions selon le type de menace. Par exemple, si un virus est détecté dans un fichier, mais que VirusScan ne parvient pas à nettoyer ce fichier ni à le mettre en quarantaine, il y refuse tout accès. Si des cookies de suivi sont détectés, mais que VirusScan ne réussit pas à nettoyer ou mettre en quarantaine les cookies, vous pouvez décider de les supprimer ou de les autoriser. Si des programmes potentiellement indésirables sont détectés, VirusScan n'effectue aucune action automatique ; il vous laisse décider de les mettre en quarantaine ou de les autoriser.

Lorsque VirusScan met des éléments en quarantaine, il les chiffre et les isole dans un dossier pour empêcher les fichiers, programmes ou cookies de nuire à votre ordinateur. Vous pouvez restaurer ou supprimer les éléments mis en quarantaine. Dans la plupart des cas, vous pouvez supprimer un cookie en quarantaine sans affecter votre système ; en revanche, si VirusScan a mis en quarantaine un programme que vous connaissez et utilisez, envisagez de le restaurer.

Contenu de ce chapitre

Gérer les virus et chevaux de Troie 62
Gérer les programmes potentiellement indésirables 62
Gérer des fichiers en quarantaine.....63
Gérer des programmes et cookies en quarantaine ...63

Gérer les virus et chevaux de Troie

Si VirusScan détecte un virus ou un cheval de Troie sur votre ordinateur lors d'une analyse en temps réel ou d'une analyse manuelle, il tente de nettoyer le fichier. S'il n'y parvient pas, VirusScan tente de le mettre en quarantaine. Si cette tentative échoue également, il bloque l'accès au fichier (uniquement lors d'une analyse en temps réel).

1 Ouvrez le volet Résultats de l'analyse.

   Comment ?

   1. Double-cliquez sur l'icône **Analyse terminée** dans la zone de notification à l'extrême droite de votre barre des tâches.
   2. Dans le volet Progression de l'analyse : Analyse manuelle, cliquez sur **Afficher les résultats**.

2 Dans la liste des résultats d'analyse, cliquez sur **Virus et chevaux de Troie**.

Remarque : Pour gérer les fichiers mis en quarantaine par VirusScan, consultez Gérer les fichiers mis en quarantaine (page 63).

Gérer les programmes potentiellement indésirables

Si VirusScan détecte un programme potentiellement indésirable sur votre ordinateur lors d'une analyse en temps réel ou manuelle, vous avez le choix de supprimer ou d'autoriser le programme. La suppression du programme potentiellement indésirable ne l'efface pas de votre système. Elle met le programme en quarantaine pour l'empêcher d'endommager votre ordinateur ou vos fichiers.

1 Ouvrez le volet Résultats de l'analyse.

   Comment ?

   1. Double-cliquez sur l'icône **Analyse terminée** dans la zone de notification à l'extrême droite de votre barre des tâches.
   2. Dans le volet Progression de l'analyse : Analyse manuelle, cliquez sur **Afficher les résultats**.

2 Dans la liste des résultats d'analyse, cliquez sur **Programmes potentiellement indésirables**.

3 Sélectionnez un programme potentiellement indésirable.

4 Sous **Je souhaite**, cliquez sur **Supprimer** ou **Autoriser**.

5 Confirmez votre choix.

Gérer des fichiers en quarantaine

Lorsque VirusScan met en quarantaine des fichiers infectés, il les chiffre et les isole dans un dossier pour empêcher les fichiers de nuire à votre ordinateur. Vous pouvez ensuite choisir de restaurer ou de supprimer les fichiers en quarantaine.

1 Ouvrez le volet Fichiers mis en quarantaine.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Restaurer**.
3. Cliquez sur **Fichiers**.

2 Sélectionnez un fichier en quarantaine.

3 Effectuez l'une des opérations suivantes :

- Pour réparer le fichier infecté et le remettre à son emplacement d'origine sur votre ordinateur, cliquez sur **Restaurer**.
- Pour supprimer le fichier infecté de votre ordinateur, cliquez sur **Supprimer**.

4 Cliquez sur **Oui** pour confirmer votre choix.

Conseil : Vous pouvez restaurer ou supprimer plusieurs fichiers à la fois.

Gérer des programmes et cookies en quarantaine

Lorsque VirusScan met en quarantaine des programmes potentiellement indésirables ou des cookies de suivi, il les chiffre et les isole dans un dossier protégé pour empêcher ces programmes ou cookies de nuire à votre ordinateur. Vous pouvez ensuite choisir de restaurer ou de supprimer les éléments mis en quarantaine. Le plus souvent, vous pouvez supprimer un élément en quarantaine sans affecter votre système.

1 Ouvrez le volet Programmes mis en quarantaine et cookies de suivi.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Restaurer**.
3. Cliquez sur **Programmes et cookies**.

2 Sélectionnez un programme ou cookie en quarantaine.

3 Effectuez l'une des opérations suivantes :

- Pour réparer le fichier infecté et le remettre à son emplacement d'origine sur votre ordinateur, cliquez sur **Restaurer**.
- Pour supprimer le fichier infecté de votre ordinateur, cliquez sur **Supprimer**.

4 Cliquez sur **Oui** pour confirmer l'opération.

Conseil : Vous pouvez restaurer ou supprimer plusieurs programmes et cookies à la fois.

CHAPITRE 13

McAfee Personal Firewall

Personal Firewall offre à votre ordinateur et à vos données personnelles une protection avancée. Personal Firewall établit une barrière entre votre ordinateur et Internet. Il surveille silencieusement le trafic Internet et signale toute activité suspecte.

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctions de Personal Firewall 66
Démarrage du pare-feu 69
Utilisation des alertes 71
Gestion des alertes de type Informations 75
Configuration de la protection par pare-feu 77
Gestion des programmes et des autorisations 91
Gestion des services système 103
Gestion des connexions informatiques 109
Consignation, surveillance et analyse 117
Obtention d'informations sur la sécurité Internet ... 127

Fonctions de Personal Firewall

Personal Firewall propose les fonctionnalités suivantes :

Niveaux de protection standard et personnalisés

Protégez-vous contre les intrusions et activités suspectes avec les paramètres de protection par défaut ou personnalisables du pare-feu.

Recommandations en temps réel

Recevez des recommandations, de manière dynamique, pour vous aider à déterminer si vous devez autoriser l'accès de certains programmes à Internet ou si vous pouvez faire confiance au trafic réseau.

Gestion intelligente de l'accès des programmes

Gérez l'accès à Internet des programmes, via un système d'alertes et de journaux d'événements, et configurez des autorisations d'accès pour des programmes spécifiques dans le volet Autorisations des programmes du pare-feu.

Protection de vos séances de jeu

Empêchez les alertes concernant les tentatives d'intrusion et les activités suspectes de vous distraire au cours de vos séances de jeu en plein écran.

Protection au démarrage de l'ordinateur

Dès que Windows® s'ouvre, le pare-feu protège votre ordinateur contre les tentatives d'intrusion ainsi que contre les programmes et le trafic réseau indésirables.

Contrôle du port de service système

Gérez les ports de service système ouverts et fermés requis par certains programmes.

Gestion des connexions informatiques

Autorisez et bloquez les connexions à distance entre d'autres ordinateurs et le vôtre.

Intégration des informations de HackerWatch

Enregistrez les schémas de piratage et d'intrusion généraux via le site Web de HackerWatch, qui fournit également des informations de sécurité récentes sur les programmes installés sur votre ordinateur, ainsi que des statistiques globales sur les événements de sécurité et les ports Internet.

Verrouillage du pare-feu

Bloquez instantanément tout le trafic entrant et sortant entre votre ordinateur et Internet.

Rétablissement des paramètres du pare-feu

Rétablissez instantanément les paramètres de protection d'origine du pare-feu

Détection avancée des chevaux de Troie

Détectez et empêchez les applications potentiellement nuisibles, telles que les chevaux de Troie, de transmettre vos données personnelles sur Internet.

Consignation des événements

Enregistrez les événements récents en matière de trafic entrant et sortant et d'intrusions.

Surveillance du trafic Internet

Consultez des cartes mondiales indiquant la source des attaques et du trafic malveillants. Obtenez également des informations détaillées sur le propriétaire, ainsi que des données géographiques sur les adresses IP émettrices. Vous pouvez en outre analyser le trafic entrant et sortant, et surveiller la bande passante et l'activité des programmes.

Prévention des intrusions

Protégez votre confidentialité des menaces venant d'Internet Grâce à cette fonctionnalité de type heuristique, McAfee apporte un troisième niveau de protection en bloquant les éléments qui présentent des symptômes d'attaques ou des caractéristiques de tentatives de piratage.

Analyse du trafic améliorée

Analysez aussi bien le trafic Internet entrant et sortant que les connexions des programmes, y compris ceux qui écoutent activement les connexions ouvertes. Vous saurez ainsi quels sont les programmes vulnérables et vous pourrez prendre les mesures nécessaires.

CHAPITRE 14

Démarrage du pare-feu

Dès que vous installez le pare-feu, votre ordinateur est protégé contre les intrusions et contre le trafic réseau indésirable. De plus, vous êtes prêt à traiter les alertes et à gérer les accès Internet entrants et sortants des programmes connus et inconnus. Les recommandations intelligentes et le niveau de sécurité Fiable (avec l'option sélectionnée pour ne permettre aux programmes qu'un accès sortant à Internet) sont automatiquement activés.

Vous pouvez désactiver le pare-feu depuis le volet Internet & Configuration réseau mais, dans ce cas, votre ordinateur n'est plus protégé contre les intrusions et le trafic réseau indésirable, et vous ne pouvez plus gérer efficacement les connexions Internet entrantes et sortantes. La désactivation de la protection par pare-feu doit être provisoire et exceptionnelle. Vous pouvez aussi activer le pare-feu depuis le volet Internet & Configuration réseau.

Le pare-feu désactive automatiquement le pare-feu Windows® pour devenir le pare-feu par défaut.

Remarque : pour configurer le pare-feu, ouvrez le volet Internet et Configuration réseau.

Contenu de ce chapitre

Activation de la protection par pare-feu 69
Désactivation de la protection par pare-feu 70

Activation de la protection par pare-feu

Vous pouvez activer le pare-feu pour protéger votre ordinateur contre les intrusions et contre le trafic réseau indésirable, ainsi que pour gérer les connexions Internet entrantes et sortantes.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est désactivée**, cliquez sur **Activer**.

Désactivation de la protection par pare-feu

Vous pouvez désactiver le pare-feu si vous ne souhaitez plus protéger votre ordinateur contre les intrusions et le trafic réseau indésirable. Lorsque le pare-feu est désactivé, vous ne pouvez pas gérer les connexions Internet entrantes et sortantes.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Désactiver**.

CHAPITRE 15

Utilisation des alertes

Le pare-feu utilise un ensemble d'alertes pour vous aider à gérer votre sécurité. Ces alertes peuvent être classées en trois catégories principales :

- Alerte rouge
- Alerte jaune
- Alerte verte

Les alertes peuvent aussi contenir les informations nécessaires pour vous aider à décider comment traiter les alertes ou à s'informer sur les programmes exécutés sur votre ordinateur.

Contenu de ce chapitre

A propos des alertes 72

A propos des alertes

Le pare-feu dispose de trois types d'alertes de base. De même, certaines alertes incluent des informations qui vous aideront à en savoir plus ou à obtenir des informations sur les programmes qui s'exécutent sur votre ordinateur.

Alerte rouge

Une alerte rouge s'affiche si le pare-feu détecte, puis bloque, un cheval de Troie sur votre ordinateur et vous recommande d'effectuer une recherche d'autres menaces éventuelles. Un cheval de Troie semble être un programme légitime. Toutefois, il peut interrompre, endommager ou permettre un accès non autorisé à votre ordinateur. Cette alerte se produit à tous les niveaux de sécurité, sauf Ouvrir.

Alerte jaune

Le type d'alerte le plus courant est l'alerte jaune, qui vous informe d'une activité d'un programme ou d'un événement de réseau détecté par le pare-feu. L'alerte décrit l'activité de programme ou l'événement de réseau, puis propose une ou deux options qui exigent votre réponse. Par exemple, l'alerte **Nouveau réseau détecté** s'affiche lorsqu'un ordinateur équipé du pare-feu est connecté à un nouveau réseau. Vous pouvez choisir d'autoriser ou non le réseau. Si vous l'autorisez, le pare-feu autorise le trafic émanant de tout ordinateur se trouvant sur le réseau et l'adresse de celui-ci est ajoutée à la liste Adresses IP autorisées. Si les recommandations intelligentes sont activées, des programmes sont ajoutés dans le volet Autorisations de programme.

Alerte verte

Dans la plupart des cas, les alertes vertes fournissent des informations de base concernant un événement et ne requièrent aucune réponse. Les alertes vertes sont désactivées par défaut et se produisent généralement lorsque les niveaux de sécurité Standard, Fiable, Elevé et Furtif sont définis.

Assistance utilisateur

Les alertes du pare-feu contiennent généralement des informations complémentaires pour vous aider à gérer la sécurité de votre ordinateur, comme par exemple :

- **En savoir plus sur ce programme** : ouvre le site Web de sécurité de McAfee pour vous permettre d'obtenir des informations sur un programme que le pare-feu a détecté sur votre ordinateur.

- **Informer McAfee de ce programme** : envoie à McAfee des informations sur un fichier inconnu que le pare-feu a détecté sur votre ordinateur.
- **McAfee vous recommande de** : affiche des informations concernant le traitement des alertes. Par exemple, une alerte peut vous recommander d'autoriser l'accès à Internet d'un programme.

CHAPITRE 16

Gestion des alertes de type Informations

Le pare-feu vous permet d'afficher ou de masquer des alertes d'information lorsqu'il détecte des tentatives d'intrusion ou une activité suspecte lors de certains événements, par exemple pendant un jeu en plein écran.

Contenu de ce chapitre

Afficher des alertes durant une session de jeu 75
Masquer les alertes de type Informations 76

Afficher des alertes durant une session de jeu

Vous pouvez autoriser l'affichage des alertes d'information du pare-feu lorsque celui-ci détecte des tentatives d'intrusion ou une activité suspecte pendant un jeu en plein écran.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans le volet Configuration de SecurityCenter, sous **Alertes**, cliquez sur **Avancé**.
4. Dans le volet Options d'alerte, sélectionnez **Afficher les alertes d'information en mode jeu**.
5. Cliquez sur **OK**.

Masquer les alertes de type Informations

Vous pouvez empêcher l'affichage des alertes d'information du pare-feu lorsque celui-ci détecte des tentatives d'intrusion ou une activité suspecte.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans le volet Configuration de SecurityCenter, sous **Alertes**, cliquez sur **Avancé**.
4. Dans le volet Configuration de SecurityCenter, cliquez sur **Alertes d'information**.
5. Dans le volet Alertes d'information, vous pouvez soit :
   - Sélectionner **Ne pas afficher les alertes d'information** pour masquer les alertes d'information.
   - Désélectionner une alerte à masquer.
6. Cliquez sur **OK**.

CHAPITRE 17

Configuration de la protection par pare-feu

Le pare-feu offre diverses méthodes pour gérer votre sécurité et pour personnaliser la manière dont vous souhaitez réagir aux événements et alertes de sécurité.

Après l'installation initiale du pare-feu, le niveau de sécurité de l'ordinateur est défini à Fiable et vos programmes ne bénéficient que d'un accès sortant à Internet. Cependant, le pare-feu propose d'autres niveaux, du plus restrictif au plus permissif.

Le pare-feu vous donne en outre la possibilité de recevoir des recommandations concernant les alertes et l'accès à Internet des programmes.

Contenu de ce chapitre

Gestion des niveaux de sécurité du pare-feu 78
Configuration des recommandations intelligentes pour les alertes 83
Optimisation de la sécurité du pare-feu.....85
Verrouillage et restauration du pare-feu 88

Gestion des niveaux de sécurité du pare-feu

Les niveaux de sécurité du pare-feu déterminent dans quelle mesure vous voulez gérer et répondre aux alertes. Ces alertes apparaissent lorsque le pare-feu détecte un trafic réseau et des connexions Internet entrantes et sortantes indésirables. Par défaut, le niveau de sécurité du pare-feu est défini à Fiable, n'autorisant qu'un accès sortant.

Lorsque le niveau de sécurité Fiable est configuré et que les recommandations intelligentes sont activées, des alertes jaunes offrent le choix d'autoriser ou d'interdire l'accès aux programmes inconnus qui demandent un accès entrant. Lorsque des programmes connus sont détectés, des alertes vertes apparaissent à titre informatif et l'accès à ces programmes est automatiquement autorisé. Lorsqu'un programme bénéficie d'une autorisation d'accès, il peut créer des connexions sortantes et être à l'écoute des connexions entrantes non sollicitées.

D'une manière générale, plus un niveau de sécurité est restrictif (Furtif et Elevé), plus le nombre d'options et d'alertes affichées, et donc le nombre d'interventions de votre part, est important.

Le tableau qui suit décrit les six niveaux de sécurité du pare-feu, du plus restrictif au plus laxiste :

Niveau	Description
Verrouiller	Bloque toutes les connexions réseau entrantes et sortantes, notamment l'accès à des sites Web, des e-mails et des mises à jour de sécurité. Cette opération équivaut à vous déconnecter d'Internet. Vous pouvez utiliser ce paramètre pour bloquer des ports que vous avez configurés comme ouverts dans le volet Services système.
Furtif	Bloque toutes les connexions Internet entrantes, à l'exception des ports ouverts, masquant ainsi la présence de votre ordinateur sur Internet. Le pare-feu vous avertit lorsque de nouveaux programmes tentent des connexions Internet sortantes ou reçoivent des demandes de connexion entrantes. Les programmes bloqués et ajoutés s'affichent dans le volet Autorisations de programme.
Elevé	Vous avertit lorsque de nouveaux programmes tentent des connexions Internet sortantes ou reçoivent des demandes de connexion entrantes. Les programmes bloqués et ajoutés s'affichent dans le volet Autorisations de programme. Lorsque le niveau de sécurité Elevé est activé, un programme ne demande que le type d'accès dont il a besoin à ce moment précis (accès uniquement sortant, par exemple), que vous pouvez alors autoriser ou interdire. Ultérieurement, si le programme demande une connexion à la fois entrante et sortante, vous pouvez lui accorder un accès complet depuis le volet Autorisations de programme.

Standard	Surveille les connexions entrantes et sortantes et vous envoie une alerte lorsque de nouveaux programmes tentent d'accéder à Internet. Les programmes bloqués et ajoutés s'affichent dans le volet Autorisations de programme.
Fiable	Octroie aux programmes des accès Internet soit entrants et sortants (complets) ou sortants uniquement. Le niveau de sécurité par défaut est Fiable, avec l'option sélectionnée pour n'autoriser qu'un accès sortant. Si un programme bénéficie d'un accès complet, le pare-feu le considère automatiquement comme fiable et l'ajoute à la liste des programmes autorisés dans le volet Autorisations de programme. Si un programme ne bénéficie que d'un accès sortant, le pare-feu le considère automatiquement comme fiable uniquement lorsqu'il établit une connexion Internet sortante. Une connexion entrante n'est pas automatiquement approuvée.
Ouvert	Autorise toutes les connexions Internet entrantes et sortantes.

Le pare-feu vous permet également de rétablir immédiatement le niveau de sécurité Fiable (et autoriser les accès sortants uniquement) depuis le volet Restaurer les paramètres de protection par défaut du pare-feu.

Activation du niveau de sécurité Verrouillage

Vous pouvez définir le niveau de sécurité du pare-feu à Verrouillage pour bloquer toutes les connexions réseau entrantes et sortantes.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Niveau de sécurité, faites glisser le curseur jusqu'à ce que le niveau actuel affiché soit **Verrouillage**.
4. Cliquez sur **OK**.

Activation du niveau de sécurité Furtif

Vous pouvez définir le niveau de sécurité du pare-feu à Furtif pour bloquer toutes les connexions réseau entrantes, à l'exception des ports ouverts, de manière à masquer la présence de votre ordinateur sur Internet.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Niveau de sécurité, faites glisser le curseur jusqu'à ce que le niveau actuel affiché soit **Furtif**.
4. Cliquez sur **OK**.

Remarque : En mode Furtif, le pare-feu vous avertit lorsque de nouveaux programmes demandent une connexion Internet sortante ou reçoivent des demandes de connexion entrantes.

Activation du niveau de sécurité Elevé

Vous pouvez définir le niveau de sécurité à Elevé pour être averti lorsque de nouveaux programmes tentent des connexions Internet sortantes ou reçoivent des demandes de connexion entrantes.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Niveau de sécurité, faites glisser le curseur jusqu'à ce que le niveau actuel affiché soit **Elevé**.
4. Cliquez sur **OK**.

Remarque : En mode Elevé, un programme ne demande que le type d'accès dont il a besoin à ce moment précis (accès uniquement sortant, par exemple), que vous pouvez alors autoriser ou interdire. Ultérieurement, si le programme demande une connexion à la fois entrante et sortante, vous pouvez lui accorder un accès complet depuis le volet Autorisations de programme.

Activation du niveau de sécurité Standard

Vous pouvez définir le niveau de sécurité à Standard pour surveiller les connexions entrantes et sortantes et être averti lorsque de nouveaux programmes tentent d'accéder à Internet.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Niveau de sécurité, faites glisser le curseur jusqu'à ce que le niveau actuel affiché soit **Standard**.
4. Cliquez sur **OK**.

Activation du niveau de sécurité Faible

Vous pouvez définir le niveau de sécurité du pare-feu à Fiable pour autoriser soit un accès complet soit un accès réseau sortant uniquement.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Niveau de sécurité, faites glisser le curseur jusqu'à ce que le niveau actuel affiché soit **Faible**.
4. Effectuez l'une des opérations suivantes :
   - Pour autoriser un accès réseau complet entrant et sortant, sélectionnez **Autoriser l'accès total**.
   - Pour autoriser un accès réseau sortant uniquement, sélectionnez **Autoriser l'accès sortant uniquement**.
5. Cliquez sur **OK**.

Remarque : L'option **Autoriser l'accès sortant uniquement** est l'option par défaut.

Activation du niveau de sécurité Ouvert

Vous pouvez définir le niveau de sécurité du pare-feu à Ouvert pour autoriser toutes les connexions réseau entrantes et sortantes.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Niveau de sécurité, faites glisser le curseur jusqu'à ce que le niveau actuel affiché soit **Ouvert**.
4. Cliquez sur **OK**.

Configuration des recommandations intelligentes pour les alertes

Vous pouvez configurer le pare-feu pour inclure, exclure ou afficher les recommandations sous forme d'alertes lorsque des programmes tentent d'accéder à Internet. Les recommandations intelligentes vous aident à savoir comment traiter une alerte.

Lorsque les recommandations intelligentes sont activées (et que le niveau de sécurité Elevé est activé, avec accès sortant uniquement), le pare-feu autorise ou bloque automatiquement les programmes connus et affiche dans l'alerte une recommandation lorsqu'il détecte des programmes potentiellement dangereux.

Lorsque les recommandations intelligentes sont désactivées, le pare-feu n'autorise ni ne bloque l'accès à Internet et ne suggère pas non plus la conduite à tenir.

Lorsque les recommandations intelligentes sont définies à Afficher uniquement, une alerte vous invite à autoriser ou bloquer l'accès, mais recommande un plan d'action.

Activation des recommandations intelligentes

Vous pouvez activer les recommandations intelligentes pour que le pare-feu autorise ou bloque automatiquement les programmes et vous avertisse concernant les programmes non reconnus et potentiellement dangereux.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Niveau de sécurité, sous **Recommandations intelligentes**, sélectionnez **Activer les recommandations intelligentes**.
4. Cliquez sur **OK**.

Désactivation des recommandations intelligentes

Vous pouvez désactiver les recommandations intelligentes pour que le pare-feu autorise ou bloque les programmes et vous avertisse concernant les programmes non reconnus et potentiellement dangereux. Dans ce cas, cependant, les alertes ne contiennent aucune recommandation quant au traitement de l'accès des programmes. Si le pare-feu détecte un nouveau programme suspect ou connu comme étant une menace possible, il bloque automatiquement l'accès à Internet du programme.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Niveau de sécurité, sous **Recommandations intelligentes**, sélectionnez **Désactiver les recommandations intelligentes**.
4. Cliquez sur **OK**.

Affichage des recommandations intelligentes uniquement

Vous pouvez afficher les recommandations intelligentes de sorte que les alertes ne fassent que suggérer une conduite à tenir et vous laissent décider d'autoriser ou non l'accès aux programmes non reconnus et potentiellement dangereux.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Niveau de sécurité, sous **Recommandations intelligentes**, sélectionnez **Afficher uniquement**.
4. Cliquez sur **OK**.

Optimisation de la sécurité du pare-feu

La sécurité de votre ordinateur peut être mise en péril de différentes manières. Par exemple, certains programmes peuvent tenter de se connecter à Internet avant le lancement de Windows®. En outre, des utilisateurs expérimentés peuvent envoyer une requête ping à votre ordinateur pour savoir s'il est connecté à un réseau. Le pare-feu vous protège contre ces deux types d'intrusions en permettant d'activer la protection au démarrage et de bloquer les requêtes ping ICMP. Le premier paramètre interdit aux programmes d'accéder à Internet au démarrage de Windows, et le second bloque les requêtes ping grâce auxquelles d'autres utilisateurs peuvent détecter votre ordinateur sur un réseau.

Les paramètres d'installation standard incluent la détection automatique des tentatives d'intrusion les plus courantes, comme les attaques par déni de service ou l'utilisation des failles. L'utilisation des paramètres d'installation standard garantit une protection contre les attaques et les accès indésirables. Toutefois, vous pouvez désactiver la détection automatique de certains types d'attaques ou d'accès dans le volet Détection des intrusions.

Protection de votre ordinateur au démarrage

Vous pouvez protéger votre ordinateur au démarrage de Windows de manière à bloquer les nouveaux programmes qui ne bénéficiaient pas de l'accès à Internet et le demandent maintenant. Le pare-feu affiche des alertes appropriées pour les programmes ayant demandé l'accès, que vous pouvez alors autoriser ou bloquer. Pour pouvoir utiliser cette option, votre niveau de sécurité ne doit pas être défini sur Ouvert ou sur Verrouillage.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Niveau de sécurité, sous **Paramètres de sécurité**, sélectionnez **Activer la protection au démarrage**.
4. Cliquez sur **OK**.

Remarque : les connexions et les intrusions bloquées ne sont pas consignées lorsque la protection au démarrage est activée.

Configuration des paramètres de requête ping

Vous pouvez autoriser ou empêcher la détection de votre ordinateur sur le réseau par d'autres utilisateurs.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Niveau de sécurité, sous **Paramètres de sécurité**, effectuez l'une des actions suivantes :
   - Sélectionnez **Autoriser les requêtes ping ICMP** pour autoriser la détection de votre ordinateur sur le réseau à l'aide de requêtes ping.
   - Décochez la case **Autoriser les requêtes ping ICMP** pour empêcher la détection de votre ordinateur sur le réseau à l'aide de requêtes ping.
4. Cliquez sur **OK**.

Configuration de la détection des intrusions

Vous pouvez détecter les tentatives d'intrusion afin de protéger votre ordinateur contre les attaques et les recherches non autorisées. Les paramètres d'installation standard incluent la détection automatique des tentatives d'intrusion les plus courantes, comme les attaques par déni de service ou l'utilisation des failles ; toutefois, vous pouvez désactiver la détection automatique de certains types d'attaques ou d'accès.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Pare-feu, cliquez sur **Détection des intrusions**.
4. Sous **Détecter les tentatives d'intrusion**, effectuez l'une des actions suivantes :
   - Sélectionnez un nom pour détecter automatiquement l'attaque ou effectuer une analyse.
   - Désélectionnez un nom pour désactiver la détection ou l'analyse automatique.
5. Cliquez sur **OK.**

Configurer les paramètres relatifs à l'état de la protection par pare-feu.

Vous pouvez configurer le pare-feu pour ignorer que des problèmes spécifiques à votre ordinateur ne sont pas signalés à SecurityCenter.

1. Dans le volet McAfee SecurityCenter, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Dans le volet Configuration de SecurityCenter, sous **Etat de protection**, cliquez sur **Avancé**.
3. Dans le volet Problèmes ignorés, sélectionnez une ou plusieurs des options suivantes :
   - **La protection par pare-feu est désactivée.**
   - **Le pare-feu est configuré sur le niveau de sécurité Ouvert.**
   - **Le service de pare-feu ne fonctionne pas.**
   - **La protection par pare-feu n'est pas installée sur votre ordinateur.**
   - **Votre pare-feu Windows est désactivé.**
   - **Le pare-feu en sortie n'est pas installé sur votre ordinateur.**
4. Cliquez sur **OK**.

Verrouillage et restauration du pare-feu

Le Verrouillage bloque instantanément tout le trafic réseau entrant et sortant pour vous aider à isoler et résoudre un problème sur votre ordinateur.

Verrouillage instantané du pare-feu

Vous pouvez verrouiller le pare-feu pour qu'il bloque instantanément tout le trafic réseau entre votre ordinateur et Internet.

1. Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Verrouiller le pare-feu**.
2. Dans le volet Verrouiller le pare-feu, cliquez sur **Verrouillage**.
3. Cliquez sur **Oui** pour confirmer.

Conseil : Vous pouvez aussi verrouiller le pare-feu en cliquant avec le bouton droit sur l'icône de SecurityCenter dans la zone de notification à l'extrême droite de la barre des tâches, puis en cliquant sur **Liens rapides** et sur **Verrouiller le pare-feu**.

Déverrouillage instantané du pare-feu

Vous pouvez déverrouiller le pare-feu pour qu'il autorise instantanément tout le trafic réseau entre votre ordinateur et Internet.

1. Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Verrouiller le pare-feu**.
2. Dans le volet Verrouillage activé, cliquez sur **Déverrouiller**.
3. Cliquez sur **Oui** pour confirmer.

Restaurer les paramètres du pare-feu

Vous pouvez restaurer rapidement les paramètres de protection définis à l'origine pour le pare-feu. Cette opération rétablit le niveau de sécurité Fiable et autorise un accès réseau sortant uniquement, active les recommandations intelligentes, rétablit la liste des programmes et de leurs autorisations par défaut dans le volet Autorisations de programme, supprime les adresses IP approuvées et interdites, et restaure les services système, les paramètres de consignation des événements et la détection des intrusions.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Restaurer les paramètres par défaut du pare-feu**.
2. Dans le volet Restaurer les paramètres de protection par défaut du pare-feu, cliquez sur **Paramètres par défaut**.
3. Cliquez sur **Oui** pour confirmer.

Conseil : Vous pouvez aussi restaurer les paramètres par défaut du pare-feu en cliquant avec le bouton droit sur l'icône de SecurityCenter dans la zone de notification à l'extrême droite de la barre des tâches, puis en cliquant sur **Liens rapides** et sur **Restaurer les paramètres par défaut du pare-feu**.

CHAPITRE 18

Gestion des programmes et des autorisations

Le pare-feu vous permet de gérer et de créer des autorisations d'accès pour les programmes (nouveaux et existants) nécessitant des accès Internet entrants et sortants. Le pare-feu vous permet d'accorder aux programmes un accès total ou sortant uniquement. Vous pouvez également bloquer l'accès des programmes.

Contenu de ce chapitre

Autorisation de l'accès Internet des programmes 92
Autorisation de l'accès sortant uniquement des programmes 95
Blocage de l'accès Internet des programmes 97
Suppression des autorisations d'accès de certains programmes 99
En savoir plus sur les programmes 100

Autorisation de l'accès Internet des programmes

Certains programmes, comme les navigateurs Internet, doivent accéder à Internet pour fonctionner correctement.

Le pare-feu vous permet d'utiliser la page Autorisations de programme pour :

- Autoriser l'accès des programmes
- Autoriser l'accès sortant uniquement des programmes
- Bloquer l'accès des programmes

Vous pouvez également autoriser un accès complet ou un accès sortant uniquement d'un programme depuis le journal des événements sortants ou des événements récents.

Autoriser l'accès total d'un programme

Vous pouvez octroyer à un programme actuellement bloqué sur votre ordinateur un accès à Internet complet, entrant et sortant.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Firewall, cliquez sur **Autorisations de programme**.
4. Sous **Autorisations de programme**, sélectionnez un programme défini sur **Bloqué** ou sur **Accès sortant uniquement**.
5. Sous **Action**, cliquez sur **Autoriser l'accès**.
6. Cliquez sur **OK**.

Autoriser l'accès total d'un nouveau programme

Vous pouvez octroyer à un nouveau programme sur votre ordinateur un accès à Internet complet, entrant et sortant.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Firewall, cliquez sur **Autorisations de programme**.
4. Sous **Autorisations de programme**, cliquez sur **Ajouter un programme autorisé**.
5. Dans la boîte de dialogue d'**Ajout de programmes**, recherchez et sélectionnez le programme à ajouter, puis cliquez sur **Ouvrir**.

Remarque : Vous pouvez modifier les autorisations définies pour un programme récemment ajouté comme vous le feriez pour un autre programme, en sélectionnant le programme voulu puis en cliquant sur **Autoriser l'accès sortant uniquement** ou sur **Bloquer l'accès** sous **Action**.

Autoriser un accès total depuis le journal des événements récents

Vous pouvez octroyer à un programme actuellement bloqué apparaissant dans le journal des événements récents un accès à Internet complet, entrant et sortant.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Menu Avancé**.
2. Cliquez sur **Rapports & journaux**.
3. Sous **Evénements récents**, sélectionnez la description de l'événement, puis cliquez sur **Autoriser l'accès**.
4. Dans la boîte de dialogue Autorisations de programme, cliquez sur **Oui** pour confirmer.

Rubriques connexes

- Afficher les événements sortants (page 119)

Autoriser un accès total depuis le journal des événements sortants

Vous pouvez octroyer à un programme actuellement bloqué apparaissant dans le journal des événements sortants un accès à Internet complet, entrant et sortant.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Menu Avancé**.
2. Cliquez sur **Rapports & journaux**.
3. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
4. Cliquez sur **Réseau & Internet**, puis sur **Evénements sortants**.
5. Sélectionnez un programme et, sous **Je souhaite**, cliquez sur **Autoriser l'accès**.
6. Dans la boîte de dialogue Autorisations de programme, cliquez sur **Oui** pour confirmer.

Autorisation de l'accès sortant uniquement des programmes

Certains programmes se trouvant sur votre ordinateur nécessitent un accès sortant à Internet. Le pare-feu vous permet de configurer les autorisations de programme pour autoriser l'accès Internet sortant uniquement.

Autoriser l'accès sortant uniquement d'un programme

Vous pouvez accorder à un programme un accès Internet sortant uniquement.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Firewall, cliquez sur **Autorisations de programme**.
4. Sous **Autorisations de programme**, sélectionnez un programme défini sur **Bloqué** ou sur **Accès total**.
5. Sous **Action**, cliquez sur **Autoriser l'accès sortant uniquement**.
6. Cliquez sur **OK**.

Autoriser un accès sortant uniquement depuis le journal des événements récents

Vous pouvez octroyer à un programme actuellement bloqué apparaissant dans le journal des événements récents un accès à Internet sortant uniquement.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Menu Avancé**.
2. Cliquez sur **Rapports & journaux**.
3. Sous **Evénements récents**, sélectionnez la description de l'événement, puis cliquez sur **Autoriser l'accès sortant uniquement**.
4. Dans la boîte de dialogue Autorisations de programme, cliquez sur **Oui** pour confirmer.

Autoriser un accès sortant uniquement depuis le journal des événements sortants

Vous pouvez octroyer à un programme actuellement bloqué apparaissant dans le journal des événements sortants un accès à Internet sortant uniquement.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Menu Avancé**.
2. Cliquez sur **Rapports & journaux**.
3. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
4. Cliquez sur **Réseau & Internet**, puis sur **Evénements sortants**.
5. Sélectionnez un programme et, sous **Je souhaite**, cliquez sur **Autoriser l'accès sortant uniquement**.
6. Dans la boîte de dialogue Autorisations de programme, cliquez sur **Oui** pour confirmer.

Blocage de l'accès Internet des programmes

Le pare-feu vous permet d'empêcher les programmes d'accéder à Internet. Assurez-vous que le blocage de l'accès d'un programme n'interrompe pas votre connexion réseau ou un autre programme devant accéder à Internet pour pouvoir fonctionner correctement.

Blocage de l'accès d'un programme

Vous pouvez interdire à un programme tout accès Internet entrant et sortant.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Firewall, cliquez sur **Autorisations de programme**.
4. Sous **Autorisations de programme**, sélectionnez un programme défini sur **Accès total** ou sur **Accès sortant uniquement**.
5. Sous **Action**, cliquez sur **Bloquer l'accès**.
6. Cliquez sur **OK**.

Blocage de l'accès d'un nouveau programme

Vous pouvez interdire à un nouveau programme tout accès Internet entrant et sortant.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Firewall, cliquez sur **Autorisations de programme**.
4. Sous **Autorisations de programme**, cliquez sur **Ajouter un programme bloqué**.
5. Dans la boîte de dialogue d'ajout de programmes, recherchez et sélectionnez le programme à ajouter, puis cliquez sur **Ouvrir**.

Remarque : Vous pouvez modifier les autorisations définies pour un nouveau programme en sélectionnant le programme voulu puis en cliquant sur **Autoriser l'accès sortant uniquement** ou sur **Autoriser l'accès** sous **Action**.

Bloquer l'accès depuis le journal des événements récents

Vous pouvez empêcher un programme apparaissant dans le journal des événements récents d'accéder à Internet, tant en entrée qu'en sortie.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Menu Avancé**.
2. Cliquez sur **Rapports & journaux**.
3. Sous **Evénements récents**, sélectionnez la description de l'événement, puis cliquez sur **Bloquer l'accès**.
4. Dans la boîte de dialogue Autorisations de programme, cliquez sur **Oui** pour confirmer.

Suppression des autorisations d'accès de certains programmes

Avant de retirer l'autorisation d'accès d'un programme, assurez-vous que cela n'affecte pas le fonctionnement de votre ordinateur ou de votre connexion réseau.

Suppression des autorisations d'un programme

Vous pouvez empêcher tout accès Internet entrant et sortant d'un programme.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Firewall, cliquez sur **Autorisations de programme**.
4. Sous **Autorisations de programme**, sélectionnez un programme.
5. Sous **Action**, cliquez sur **Supprimer l'autorisation de programme**.
6. Cliquez sur **OK**.

Remarque : le pare-feu vous empêche de modifier certains programmes (certaines actions sont alors désactivées ou apparaissent en grisé).

En savoir plus sur les programmes

Si vous savez pas quelles autorisations définir pour un programme, vous pouvez obtenir des informations sur le programme concerné sur le site Web HackerWatch de McAfee

Obtention d'informations sur un programme

Vous pouvez obtenir des informations sur un programme sur le site Web HackerWatch de McAfee pour décider d'autoriser ou non l'accès Internet entrant et sortant.

Remarque : Assurez-vous que vous êtes bien connecté à Internet afin que votre navigateur puisse se connecter au site Web HackerWatch de McAfee, où vous trouverez des informations à jour sur les programmes, les conditions d'accès à Internet et les menaces potentielles en termes de sécurité.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Firewall, cliquez sur **Autorisations de programme**.
4. Sous **Autorisations de programme**, sélectionnez un programme.
5. Sous **Action**, cliquez sur **Plus d'informations**.

Obtenir des informations sur un programme depuis le journal des événements sortants

Dans le journal des événements sortants, vous pouvez obtenir des informations sur un programme sur le site Web HackerWatch de McAfee pour décider d'autoriser ou non l'accès Internet entrant et sortant à des programmes spécifiques.

Remarque : Assurez-vous que vous êtes bien connecté à Internet afin que votre navigateur puisse se connecter au site Web HackerWatch de McAfee, où vous trouverez des informations à jour sur les programmes, les conditions d'accès à Internet et les menaces potentielles en termes de sécurité.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Menu Avancé**.
2. Cliquez sur **Rapports & journaux**.
3. Sous Evénements récents, sélectionnez un événement, puis cliquez sur **Afficher le journal**.
4. Cliquez sur **Réseau & Internet**, puis sur **Evénements sortants**.
5. Sélectionnez une adresse IP, puis cliquez sur **Plus d'informations**.

CHAPITRE 19

Gestion des services système

Certaines applications, notamment les programmes de serveur Web ou de partage de fichiers, doivent pouvoir accepter les connexions non sollicitées d'autres ordinateurs via les ports de service système désignés. En général, Firewall ferme ces ports de service système car ils constituent la source la plus probable de menaces pour la sécurité de votre système. Cependant, pour que les demandes de connexion émises par des ordinateurs distants puissent être acceptées, il est nécessaire que les ports de service système soient ouverts.

Contenu de ce chapitre

Configuration des ports de service système.....104

Configuration des ports de service système

Les ports de service système peuvent être configurés pour autoriser ou refuser l'accès réseau distant à un service sur votre ordinateur.

La liste ci-dessous répertorie les services système courants et les ports y associés :

- Ports 20-21 de protocole de transfert de fichiers (FTP)
- Port 143 de serveur de messagerie (IMAP)
- Port 110 de serveur de messagerie (POP3)
- Port 25 de serveur de messagerie (SMTP)
- Port 445 de serveur d'annuaires Microsoft (MSFT DS)
- Port 1433 de Microsoft SQL Server (MSFT SQL)
- Port 123 de NTP (Network Time Protocol)
- Port 3389 Remote Desktop / Assistance à distance / Terminal Server (RDP)
- Port 135 d'appel de procédure à distance (RPC)
- Port 443 de serveur Web sécurisé (HTTPS)
- Port 5000 Universal Plug and Play (UPNP)
- Port 80 de serveur Web (HTTP)
- Ports 137-139 de partage de fichiers Windows (NETBIOS)

Les ports de service système peuvent aussi être configurés pour permettre à un ordinateur de partager sa connexion Internet avec d'autres ordinateurs connectés via le même réseau. Cette connexion, connue sous le nom d'Internet Connection Sharing (ICS), permet à l'ordinateur qui partage sa connexion d'agir comme une passerelle entre Internet et l'autre ordinateur du réseau.

Remarque : Si votre ordinateur possède une application qui accepte les connexions de serveurs Web ou FTP, l'ordinateur qui partage la connexion devra peut-être ouvrir le port de service système associé et autoriser le transfert de connexions entrantes pour ce port.

Autoriser l'accès à un port de service système existant

Vous pouvez ouvrir un port existant pour autoriser l'accès distant à un service réseau de votre ordinateur.

Remarque : Un port ouvert de service système peut rendre votre ordinateur vulnérable aux menaces Internet. Par conséquent, n'ouvrez un port que si c'est vraiment indispensable.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Pare-feu, cliquez sur **Services système**.
4. Sous **Port ouvert de service système**, sélectionnez un service système pour ouvrir le port correspondant.
5. Cliquez sur **OK**.

Blocage de l'accès à un port de service système

Vous pouvez fermer un port existant pour bloquer l'accès réseau distant à un service de votre ordinateur.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Pare-feu, cliquez sur **Services système**.
4. Sous **Port ouvert de service système**, décochez un service système pour fermer le port correspondant.
5. Cliquez sur **OK**.

Configurer un nouveau port de service système

Vous pouvez configurer sur votre ordinateur un nouveau port de service réseau que vous pouvez ouvrir ou fermer pour autoriser ou bloquer l'accès distant sur votre ordinateur.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Pare-feu, cliquez sur **Services système**.
4. Cliquez sur **Ajouter**.
5. Dans le volet Services système, sous **Ports et services système**, entrez les informations suivantes :
   - Nom du programme
   - Ports TCP/IP entrants

- Ports TCP/IP sortants
- Ports UDP entrants
- Ports UDP sortants

6 Si vous souhaitez envoyer les données d'activité de ce port à un autre ordinateur Windows en réseau partageant votre connexion Internet, sélectionnez **Réacheminez l'activité réseau de ce port vers les utilisateurs réseau utilisant le Partage de connexion Internet**.

7 Eventuellement, décrivez la nouvelle configuration.

8 Cliquez sur **OK**.

Remarque : Si votre ordinateur possède une application qui accepte les connexions de serveurs Web ou FTP, l'ordinateur qui partage la connexion devra peut-être ouvrir le port de service système associé et autoriser le transfert de connexions entrantes pour ce port. Si vous utilisez ICS (Internet Connection Sharing), vous devez également ajouter une connexion fiable à un ordinateur à la liste Adresses IP autorisées. Pour plus d'informations, consultez Ajouter une connexion fiable à un ordinateur.

Modification d'un port de service système

Vous pouvez modifier les informations d'accès réseau entrant et sortant concernant un port de service système existant.

Remarque : Si vous saisissez les informations du port de manière erronée, le service système échouera.

1 Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.

2 Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.

3 Dans le volet Pare-feu, cliquez sur **Services système**.

4 Sélectionnez un service système, puis cliquez sur **Modifier**.

5 Dans le volet Services système, sous **Ports et services système**, entrez les informations suivantes :

- Nom du programme
- Ports TCP/IP entrants
- Ports TCP/IP sortants
- Ports UDP entrants
- Ports UDP sortants

6 Si vous souhaitez envoyer les données d'activité de ce port à un autre ordinateur Windows en réseau partageant votre connexion Internet, sélectionnez **Réacheminez l'activité**

réseau de ce port vers les utilisateurs réseau utilisant le Partage de connexion Internet.

7 Eventuellement, décrivez la configuration modifiée.

8 Cliquez sur **OK**.

Suppression d'un port de service système

Vous pouvez supprimer un port de service système existant de votre ordinateur. Une fois ce port supprimé, les ordinateurs distants ne peuvent plus accéder au service réseau sur votre ordinateur.

1 Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.

2 Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.

3 Dans le volet Pare-feu, cliquez sur **Services système**.

4 Sélectionnez un service système, puis cliquez sur **Supprimer**.

5 A l'invite, cliquez sur **Oui** pour confirmer.

CHAPITRE 20

Gestion des connexions informatiques

Vous pouvez configurer le pare-feu pour gérer des connexions distantes à votre ordinateur en créant des règles basées sur des adresses IP (Internet Protocol) et associées à des ordinateurs distants. Les ordinateurs associés à des adresses IP autorisées sont considérés comme fiables pour se connecter à votre ordinateur, et vous pouvez interdire aux IP inconnues, suspectes ou non fiables de se connecter à celui-ci.

Lorsque vous autorisez une connexion, assurez-vous que l'ordinateur que vous autorisez n'est pas infecté. Si celui-ci est infecté par un ver ou un autre mécanisme, votre ordinateur sera exposé au même risque. En outre, McAfee recommande que les ordinateurs que vous autorisez soient également protégés par un firewall et par un antivirus à jour. Le pare-feu ne consigne pas le trafic et ne génère aucune alerte pour les adresses de la liste Adresses IP autorisées.

Vous pouvez faire en sorte que les ordinateurs associés à des adresses IP inconnues, suspectes ou non fiables ne puissent pas se connecter à votre ordinateur.

Firewall bloquant tout le trafic indésirable, l'interdiction d'une adresse IP n'est en règle générale pas nécessaire. Vous ne devez interdire une adresse IP que si vous êtes certain que cette connexion Internet représente une menace. Assurez-vous de ne bloquer aucune adresse IP importante, comme votre serveur DNS ou DHCP, ou d'autres serveurs de votre fournisseur d'accès Internet. En fonction des paramètres de sécurité définis sur votre ordinateur, Firewall peut vous prévenir s'il détecte un événement provenant d'une adresse IP interdite.

Contenu de ce chapitre

Fiabilité des connexions informatiques 110
Interdiction de connexions informatiques 113

Fiabilité des connexions informatiques

Vous pouvez ajouter, modifier ou supprimer des adresses IP fiables dans le volet Adresses IP autorisées et interdites, sous **Adresses IP autorisées**.

La liste **Adresses IP autorisées** du volet Adresses IP autorisées et interdites permet d'autoriser tout le trafic provenant d'un ordinateur donné à accéder à votre ordinateur. Firewall ne consigne pas le trafic et ne génère aucune alerte pour les adresses qui figurent dans la liste **Adresses IP autorisées**.

Le pare-feu autorise toutes les adresses IP vérifiées de cette liste et permet toujours au trafic provenant d'une adresse IP fiable de franchir le pare-feu, quels que soient les ports concernés. L'activité entre l'ordinateur associé à une adresse IP fiable et votre ordinateur n'est pas filtrée ou analysée par le pare-feu. Par défaut, la liste Adresses IP autorisées indique le premier réseau privé que le pare-feu trouve.

Lorsque vous autorisez une connexion, assurez-vous que l'ordinateur que vous autorisez n'est pas infecté. Si celui-ci est infecté par un ver ou un autre mécanisme, votre ordinateur sera exposé au même risque. En outre, McAfee recommande que les ordinateurs que vous autorisez soient également protégés par un firewall et par un antivirus à jour.

Ajout d'une connexion fiable à un ordinateur

Vous pouvez ajouter une connexion fiable à un ordinateur et l'adresse IP qui lui est associée.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Pare-feu, cliquez sur **Adresses IP autorisées et interdites**.
4. Dans le volet Adresses IP autorisées et interdites, sélectionnez **Adresses IP autorisées**, puis cliquez sur **Ajouter**.
5. Sous **Ajouter une règle d'adresse IP autorisée**, vous pouvez soit :
   - Sélectionner **Une seule adresse IP**, puis entrer l'adresse IP voulue.
   - Sélectionner un **Intervalle d'adresses IP**, puis entrer les adresses IP de début et de fin dans les champs **De l'adresse IP** et **A l'adresse IP**.

6 Si un service système utilise ICS (Internet Connection Sharing), vous pouvez ajouter l'intervalle d'adresses IP suivant : 192.168.0.1 à 192.168.0.255.

7 Eventuellement, sélectionnez **La règle expire dans**, puis entrez le nombre de jours où la règle doit être appliquée.

8 Eventuellement, entrez une description de cette règle.

9 Cliquez sur **OK**.

10 Dans la boîte de dialogue **Adresses IP autorisées et interdites**, cliquez sur **Oui** pour confirmer.

Remarque : Pour plus d'informations sur ICS (Internet Connection Sharing), consultez Configurer un nouveau service système.

Ajouter un ordinateur autorisé depuis le journal des événements entrants

Vous pouvez ajouter la connexion d'un ordinateur autorisé et l'adresse IP associée depuis le journal des événements entrants.

1 Dans le volet McAfee SecurityCenter, sous Tâches courantes, cliquez sur **Menu Avancé**.

2 Cliquez sur **Rapports & journaux**.

3 Sous **Evénements récents**, cliquez sur **Afficher le journal**.

4 Cliquez sur **Réseau & Internet**, puis sur **Evénements entrants**.

5 Sélectionnez une adresse IP source et, sous **Je souhaite**, cliquez sur **Autoriser cette adresse**.

6 Cliquez sur **Oui** pour confirmer.

Modification d'une connexion fiable à un ordinateur

Vous pouvez modifier une connexion fiable à un ordinateur et l'adresse IP qui lui est associée.

1 Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.

2 Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.

3 Dans le volet Pare-feu, cliquez sur **Adresses IP autorisées et interdites**.

4 Dans le volet Adresses IP autorisées et interdites, sélectionnez **Adresses IP autorisées**.

5 Sélectionnez une adresse IP, puis cliquez sur **Modifier**.

6 Sous **Modifier une adresse IP autorisée**, vous pouvez soit :

- Sélectionner **Une seule adresse IP**, puis entrer l'adresse IP voulue.

- Sélectionner un **Intervalle d'adresses IP**, puis entrer les adresses IP de début et de fin dans les champs **De l'adresse IP** et **A l'adresse IP**.

7 Le cas échéant, cochez la case **La règle expire dans**, puis entrez le nombre de jours pendant lesquels la règle doit être appliquée.

8 Eventuellement, entrez une description de cette règle.

9 Cliquez sur **OK**.

Remarque : Vous ne pouvez pas modifier les connexions par défaut que le pare-feu a automatiquement ajoutées à partir d'un réseau privé fiable.

Suppression d'une connexion fiable à un ordinateur

Vous pouvez supprimer une connexion fiable à un ordinateur et l'adresse IP qui lui est associée.

1 Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.

2 Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.

3 Dans le volet Pare-feu, cliquez sur **Adresses IP autorisées et interdites**.

4 Dans le volet Adresses IP autorisées et interdites, sélectionnez **Adresses IP autorisées**.

5 Sélectionnez une adresse IP, puis cliquez sur **Supprimer**.

6 Dans la boîte de dialogue **Adresses IP autorisées et interdites**, cliquez sur **Oui** pour confirmer.

Interdiction de connexions informatiques

Vous pouvez ajouter, modifier ou supprimer des adresses IP interdites dans le volet Adresses IP autorisées et interdites, sous **Adresses IP interdites**.

Vous pouvez faire en sorte que les ordinateurs associés à des adresses IP inconnues, suspectes ou non fiables ne puissent pas se connecter à votre ordinateur.

Firewall bloquant tout le trafic indésirable, l'interdiction d'une adresse IP n'est en règle générale pas nécessaire. Vous ne devez interdire une adresse IP que si vous êtes certain que cette connexion Internet représente une menace. Assurez-vous de ne bloquer aucune adresse IP importante, comme votre serveur DNS ou DHCP, ou d'autres serveurs de votre fournisseur d'accès Internet. En fonction des paramètres de sécurité définis sur votre ordinateur, Firewall peut vous prévenir s'il détecte un événement provenant d'une adresse IP interdite.

Ajout d'une connexion interdite à un ordinateur

Vous pouvez ajouter une connexion interdite à un ordinateur et l'adresse IP qui lui est associée.

Remarque : Assurez-vous de ne bloquer aucune adresse IP importante, comme votre serveur DNS ou DHCP, ou d'autres serveurs de votre fournisseur d'accès Internet.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.
2. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
3. Dans le volet Pare-feu, cliquez sur **Adresses IP autorisées et interdites**.
4. Dans le volet Adresses IP autorisées et interdites, sélectionnez **Adresses IP interdites**, puis cliquez sur **Ajouter**.
5. Sous **Ajouter une règle d'adresse IP interdite**, vous pouvez soit :
   - Sélectionner **Une seule adresse IP**, puis entrer l'adresse IP voulue.
   - Sélectionner un **Intervalle d'adresses IP**, puis entrer les adresses IP de début et de fin dans les champs **De l'adresse IP** et **A l'adresse IP**.

6 Eventuellement, sélectionnez **La règle expire dans**, puis entrez le nombre de jours où la règle doit être appliquée.

7 Eventuellement, entrez une description de cette règle.

8 Cliquez sur **OK**.

9 Dans la boîte de dialogue **Adresses IP autorisées et interdites**, cliquez sur **Oui** pour confirmer.

Modification d'une connexion interdite à un ordinateur

Vous pouvez modifier une connexion interdite à un ordinateur et l'adresse IP qui lui est associée.

1 Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.

2 Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.

3 Dans le volet Pare-feu, cliquez sur **Adresses IP autorisées et interdites**.

4 Dans le volet Adresses IP autorisées et interdites, sélectionnez **Adresses IP interdites**, puis cliquez sur **Modifier**.

5 Sous **Modifier une adresse IP interdite**, vous pouvez soit :

- Sélectionner **Une seule adresse IP**, puis entrer l'adresse IP voulue.
- Sélectionner un **Intervalle d'adresses IP**, puis entrer les adresses IP de début et de fin dans les champs **De l'adresse IP** et **A l'adresse IP**.

6 Eventuellement, sélectionnez **La règle expire dans**, puis entrez le nombre de jours où la règle doit être appliquée.

7 Eventuellement, entrez une description de cette règle.

8 Cliquez sur **OK**.

Suppression d'une connexion interdite à un ordinateur

Vous pouvez supprimer une connexion interdite à un ordinateur et l'adresse IP qui lui est associée.

1 Dans le volet McAfee SecurityCenter, cliquez sur **Réseau & Internet**, puis cliquez sur **Configurer**.

2 Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.

3 Dans le volet Pare-feu, cliquez sur **Adresses IP autorisées et interdites**.

4 Dans le volet Adresses IP autorisées et interdites, sélectionnez **Adresses IP interdites**.

5 Sélectionnez une adresse IP, puis cliquez sur **Supprimer**.

6 Dans la boîte de dialogue **Adresses IP autorisées et interdites**, cliquez sur **Oui** pour confirmer.

Interdiction d'un ordinateur depuis le journal des événements entrants

Vous pouvez interdire la connexion d'un ordinateur et l'adresse IP associée dans le journal des événements entrants.

Les adresses IP figurant dans le journal des événements entrants sont bloquées. Par conséquent, l'interdiction d'une adresse ne vous apporte aucune protection supplémentaire, sauf si votre ordinateur utilise des ports délibérément ouverts ou comporte un programme autorisé à accéder à Internet.

Ajoutez une adresse IP à votre liste **Adresses IP interdites** uniquement si un ou plusieurs ports sont délibérément ouverts et que vous avez de bonnes raisons pour souhaiter empêcher cette adresse d'accéder aux ports ouverts.

Vous pouvez utiliser la page Événements entrants, qui répertorie les adresses IP de l'ensemble du trafic Internet entrant, pour interdire une adresse IP que vous suspectez être la source d'activités Internet suspectes ou indésirables.

1. Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Menu Avancé**.
2. Cliquez sur **Rapports & journaux**.
3. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
4. Cliquez sur **Réseau & Internet**, puis sur **Evénements entrants**.
5. Sélectionnez une adresse IP source et, sous **Je souhaite**, cliquez sur **Interdire cette adresse**.
6. Dans la boîte de dialogue **Ajouter une règle d'adresse IP interdite**, cliquez sur **Oui** pour confirmer.

Interdiction d'un ordinateur depuis le journal des événements de détection des intrusions

Vous pouvez interdire la connexion d'un ordinateur et l'adresse IP associée depuis le journal des événements de détection des intrusions.

1. Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Menu Avancé**.
2. Cliquez sur **Rapports & journaux**.
3. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
4. Cliquez sur **Réseau & Internet**, puis sur **Evénements de détection des intrusions**.
5. Sélectionnez une adresse IP source et, sous **Je souhaite**, cliquez sur **Interdire cette adresse**.
6. Dans la boîte de dialogue **Ajouter une règle d'adresse IP interdite**, cliquez sur **Oui** pour confirmer.

CHAPITRE 21

Consignation, surveillance et analyse

Firewall fournit des informations abondantes et faciles à consulter concernant la consignation, la surveillance et l'analyse des événements et du trafic Internet. Mieux vous comprendrez le trafic et les événements Internet, mieux vous pourrez gérer vos connexions Internet.

Contenu de ce chapitre

Journalisation des événements 118
Utilisation des statistiques 120
Suivi du trafic Internet 121
Surveillance du trafic Internet 124

Journalisation des événements

Le pare-feu vous permet d'activer ou de désactiver la consignation des événements et, lorsque cette fonction est activée, les types d'événements à consigner. La consignation des événements permet de visualiser les événements entrants et sortants et les intrusions qui se sont produits récemment.

Configuration des paramètres du journal d'événements

Vous pouvez spécifier et configurer les types d'événements du pare-feu à consigner. Par défaut, la consignation des événements est activée pour tous les événements et toutes les activités.

1. Dans le volet Internet & Configuration réseau, sous **La protection par pare-feu est activée**, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Paramètres du journal d'événements**.
3. Si cette option n'est pas encore sélectionnée, sélectionnez **Activer la consignation des événements** .
4. Sous **Activer la consignation des événements**, sélectionnez ou désélectionnez les types d'événements à consigner ou non. Les types d'événement sont les suivants :
   - Programmes bloqués
   - Requêtes ping ICMP
   - Trafic en provenance des adresses IP interdites
   - Evénements sur des ports de service système
   - Evénements sur des ports inconnus
   - Evénements de détection des intrusions (IDS)
5. Pour empêcher la consignation sur des ports spécifiques, sélectionnez **Ne pas consigner les événements sur les ports suivants**, puis entrez des numéros de port séparés par des virgules ou bien des plages de ports en les séparant par des tirets. Exemple : `137-139, 445, 400-5000`.
6. Cliquez sur **OK**.

Afficher les événements récents

Si la consignation est activée, vous pouvez afficher les événements récents. Le volet Evénements récents présente la date et la description de l'événement. Il affiche uniquement l'activité des programmes dont l'accès à Internet est explicitement bloqué.

- Dans **Menu avancé**, sous le volet Tâches courantes, cliquez sur **Rapports & journaux** ou **Afficher les événements récents**. Vous pouvez également cliquer sur **Afficher les événements récents** sous le volet Tâches courantes du Menu de base.

Afficher les événements entrants

Si la consignation est activée, vous pouvez afficher les événements entrants. La page Evénements entrants inclut la date et l'heure, l'adresse IP source, le nom d'hôte ainsi que le type d'information et d'événement.

1. Vérifiez que l'onglet du menu Avancé est activé. Dans le volet Tâches courantes, cliquez sur **Rapports & journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Cliquez sur **Réseau & Internet**, puis sur **Evénements entrants**.

Remarque : depuis le journal des événements entrants, vous pouvez autoriser, interdire et suivre une adresse IP.

Afficher les événements sortants

Si la consignation est activée, vous pouvez afficher les événements sortants. Les événements sortants comprennent le nom du programme à l'origine d'une tentative d'accès sortant, la date et l'heure de l'événement et l'emplacement du programme sur votre ordinateur.

1. Dans le volet Tâches courantes, cliquez sur **Rapports & journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Cliquez sur **Réseau & Internet**, puis sur **Evénements sortants**.

Remarque : vous pouvez accorder un accès total ou un accès uniquement sortant dans le journal des événements sortants. Vous pouvez également trouver des informations supplémentaires concernant le programme.

Affichage des événements de détection des intrusions

Si la consignation est activée, vous pouvez afficher les événements d'intrusion entrants. Les événements de détection d'intrusion indiquent la date et l'heure de l'événement, l'adresse IP source, le nom d'hôte et le type de l'événement.

1. Dans le volet Tâches courantes, cliquez sur **Rapports & journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Cliquez sur **Réseau & Internet**, puis sur **Evénements de détection des intrusions**.

Remarque : depuis le journal des événements de détection des intrusions, vous pouvez interdire et suivre une adresse IP.

Utilisation des statistiques

Firewall utilise HackerWatch, le site Web de sécurité de McAfee, pour obtenir et vous fournir des statistiques relatives aux événements de sécurité et à l'activité des ports sur l'ensemble d'Internet.

Afficher les statistiques générales des événements de sécurité

HackerWatch surveille les événements de sécurité Internet survenant dans le monde entier et vous permet d'en prendre connaissance sur SecurityCenter. Les informations recueillies concernent des incidents enregistrés par HackerWatch au cours des dernières 24 heures, et des 7 et 30 derniers jours.

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **HackerWatch**.
3. Sous Suivi des événements, consultez les statistiques des événements de sécurité.

Consulter l'activité générale des ports Internet

HackerWatch surveille les événements de sécurité Internet survenant dans le monde entier et vous permet d'en prendre connaissance sur SecurityCenter. Les informations affichées concernent notamment les principaux ports pour lesquels des événements ont été communiqués à HackerWatch au cours des sept derniers jours. En général, les informations affichées concernent les ports HTTP, TCP et UDP.

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **HackerWatch**.
3. Consultez les événements des principaux ports sous **Activité récente des ports**.

Suivi du trafic Internet

Firewall propose plusieurs options pour suivre le trafic Internet. Ces options vous permettent de suivre géographiquement un ordinateur en réseau, d'obtenir des informations relatives au domaine et au réseau et de retrouver des ordinateurs à partir de journaux Evénements entrants et Evénements de détection des intrusions.

Suivre géographiquement un ordinateur en réseau

Vous pouvez utiliser le traceur visuel pour localiser géographiquement un ordinateur qui se connecte ou tente de se connecter au vôtre, et ce, en utilisant son nom ou son adresse IP. Le traceur visuel vous permet également d'accéder aux informations relatives au réseau et à l'enregistrement de l'ordinateur. Lorsque vous exécutez le traceur visuel, une carte du monde s'affiche et indique l'itinéraire le plus probable des données entre l'ordinateur source et le vôtre.

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Traceur visuel**.
3. Saisissez l'adresse IP de l'ordinateur et cliquez sur **Rechercher**.
4. Sous **Traceur visuel**, sélectionnez **Vue de la carte**.

Remarque : vous ne pouvez pas effectuer le traçage d'événements sur une adresse IP en boucle, privée ou non valide.

Obtenir des informations concernant l'enregistrement d'un ordinateur

Le traceur visuel vous permet d'extraire de SecurityCenter des informations relatives à l'enregistrement d'un ordinateur. Il s'agit notamment du nom de domaine de celui-ci, des nom et adresse de l'abonné et du contact administratif.

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Traceur visuel**.
3. Saisissez l'adresse IP de l'ordinateur, puis cliquez sur **Rechercher**.
4. Sous **Traceur visuel**, sélectionnez **Vue de l'abonné**.

Obtention d'informations concernant le réseau d'un ordinateur

Le traceur visuel vous permet d'extraire de SecurityCenter des informations relatives au réseau d'un ordinateur. Il s'agit notamment d'indications sur le réseau de domiciliation du domaine.

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Traceur visuel**.
3. Saisissez l'adresse IP de l'ordinateur, puis cliquez sur **Rechercher**.
4. Sous **Traceur visuel**, sélectionnez **Vue du réseau**.

Suivi d'un ordinateur depuis le journal des événements entrants

Dans le volet Evénements entrants, vous pouvez suivre une adresse IP figurant dans le journal des événements entrants.

1. Vérifiez que l'onglet du menu Avancé est activé. Dans le volet Tâches courantes, cliquez sur **Rapports & journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Cliquez sur **Réseau & Internet**, puis sur **Evénements entrants**.
4. Dans le volet Evénements entrants, sélectionnez une adresse IP source, puis cliquez sur **Tracer cette adresse**.
5. Dans le volet Traceur visuel, effectuez l'une des actions suivantes :
   - **Vue de la carte** : localisez géographiquement un ordinateur à l'aide de l'adresse IP sélectionnée.
   - **Vue de l'abonné** : localisez les informations de domaine au moyen de l'adresse IP sélectionnée.
   - **Vue du réseau** : localisez les informations de réseau au moyen de l'adresse IP sélectionnée.
6. Lorsque vous avez fini, cliquez sur **Terminé**.

Suivre un ordinateur depuis le journal des événements de détection des intrusions

Dans le volet Evénements de détection des intrusions, vous pouvez suivre une adresse IP figurant dans le journal des événements de détection des intrusions.

1. Dans le volet Tâches courantes, cliquez sur **Rapports & journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Cliquez sur **Réseau & Internet**, puis sur **Evénements de détection des intrusions**. Dans le volet Evénements de

détection des intrusions, sélectionnez une adresse IP source, puis cliquez sur **Tracer cette adresse**.

4 Dans le volet Traceur visuel, effectuez l'une des actions suivantes :

- **Vue de la carte** : localisez géographiquement un ordinateur à l'aide de l'adresse IP sélectionnée.
- **Vue de l'abonné** : localisez les informations de domaine au moyen de l'adresse IP sélectionnée.
- **Vue du réseau** : localisez les informations de réseau au moyen de l'adresse IP sélectionnée.

5 Lorsque vous avez fini, cliquez sur **Terminé**.

Suivi d'une adresse IP surveillée

Vous pouvez suivre une adresse IP surveillée afin d'obtenir une vue géographique indiquant l'itinéraire le plus probable des données entre l'ordinateur source et le vôtre. De plus, vous pouvez obtenir des informations d'enregistrement et de réseau concernant l'adresse IP.

1 Vérifiez que le Menu avancé est activé, puis cliquez sur **Outils**.

2 Dans le volet Outils, cliquez sur **Moniteur de trafic**.

3 Sous **Moniteur de trafic**, cliquez sur **Programmes actifs**.

4 Sélectionnez un programme, puis l'adresse IP apparaissant sous le nom du programme.

5 Sous **Activité du programme**, cliquez sur **Tracer cette adresse IP**.

6 Sous **Traceur visuel**, vous pouvez voir une carte indiquant l'itinéraire le plus probable des données entre l'ordinateur source et le vôtre. De plus, vous pouvez obtenir des informations d'enregistrement et de réseau concernant l'adresse IP.

Remarque : pour consulter les statistiques les plus récentes, cliquez sur **Actualiser** sous **Traceur visuel**.

Surveillance du trafic Internet

Firewall fournit diverses méthodes pour surveiller votre trafic Internet, et notamment :

- **Graphique d'analyse du trafic** : présente le trafic Internet entrant et sortant récent.
- **Graphique d'utilisation du trafic** : indique le pourcentage de bande passante utilisé par les programmes les plus actifs au cours des dernières 24 heures.
- **Programmes actifs** : indique les programmes qui utilisent actuellement le plus de connexions réseau sur votre ordinateur, ainsi que les adresses IP auxquelles ils accèdent.

A propos du graphique d'analyse du trafic

Le graphique Analyse du trafic est une représentation graphique et numérique du trafic Internet entrant et sortant. De plus, le Moniteur de trafic indique les programmes qui utilisent le plus grand nombre de connexions réseau sur votre ordinateur, ainsi que les adresses IP auxquelles ils accèdent.

Le volet Analyse du trafic présente le trafic Internet entrant et sortant récent, ainsi que les débits de transfert actuels, moyens et maximum. Vous pouvez également consulter le volume du trafic, y compris le volume depuis que vous avez démarré Firewall et le trafic total du mois en cours et du mois précédent.

Le volet Analyse du trafic présente l'activité Internet en temps réel de votre ordinateur, y compris le volume et le débit du trafic Internet entrant et sortant récent de votre ordinateur, ainsi que la vitesse de connexion et le nombre total d'octets transférés sur Internet.

La ligne verte continue représente le débit de transfert actuel du trafic entrant. La ligne pointillée verte représente le débit de transfert moyen du trafic entrant. Si le débit actuel et le débit moyen sont identiques, la ligne pointillée ne figure pas sur le graphique. La ligne continue reflète alors les débits moyen et actuel.

La ligne continue rouge représente le débit actuel du trafic sortant. La ligne pointillée rouge représente le débit moyen du trafic sortant. Si le débit actuel et le débit moyen sont identiques, la ligne pointillée ne figure pas sur le graphique. La ligne continue reflète alors les débits moyen et actuel.

Analyser le trafic entrant et sortant

Le graphique Analyse du trafic est une représentation graphique et numérique du trafic Internet entrant et sortant. De plus, le Moniteur de trafic indique les programmes qui utilisent le plus grand nombre de connexions réseau sur votre ordinateur, ainsi que les adresses IP auxquelles ils accèdent.

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Moniteur de trafic**.
3. Sous **Moniteur de trafic**, cliquez sur **Analyse du trafic**.

Conseil : pour consulter les statistiques les plus récentes, cliquez sur **Actualiser** sous **Analyse du trafic**.

Surveillance de la bande passante utilisée par les programmes

Vous pouvez afficher le graphique à secteurs, qui présente le pourcentage approximatif de bande passante utilisé par les programmes les plus actifs sur votre ordinateur au cours des dernières vingt-quatre heures. Ce graphique à secteurs représente visuellement les quantités relatives de bande passante utilisées par les programmes.

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Moniteur de trafic**.
3. Sous **Moniteur de trafic**, cliquez sur **Utilisation du trafic**.

Conseil : pour consulter les statistiques les plus récentes, cliquez sur **Actualiser** sous **Utilisation du trafic**.

Surveillance de l'activité des programmes

Vous pouvez afficher l'activité entrante et sortante des programmes, y compris les connexions et ports des ordinateurs distants.

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Moniteur de trafic**.
3. Sous **Moniteur de trafic**, cliquez sur **Programmes actifs**.
4. Vous pouvez afficher les informations suivantes :
   - Graphique d'activité du programme : sélectionnez le programme dont vous souhaitez afficher le graphique d'activité.
   - Connexion à l'écoute : sélectionnez un élément sous le nom du programme.

- Connexion de l'ordinateur : sélectionnez une adresse IP sous le nom du programme, le processus système ou le service.

Remarque : pour consulter les statistiques les plus récentes, cliquez sur **Actualiser** sous **Programmes actifs**.

CHAPITRE 22

Obtention d'informations sur la sécurité Internet

Firewall utilise HackerWatch, le site Web de sécurité de McAfee, pour fournir des informations actualisées concernant les programmes et l'activité générale d'Internet. HackerWatch fournit également un didacticiel HTML concernant Firewall.

Contenu de ce chapitre

Lancement du didacticiel HackerWatch 128

Lancement du didacticiel HackerWatch

Pour en savoir plus sur Firewall, vous pouvez accéder au didacticiel HackerWatch depuis SecurityCenter.

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **HackerWatch**.
3. Sous **Ressources HackerWatch**, cliquez sur **Afficher le didacticiel**.

CHAPITRE 23

McAfee Anti-Spam

Anti-Spam (anciennement appelé SpamKiller) empêche les e-mails non sollicités de pénétrer dans votre boîte de réception en examinant votre courrier entrant, puis en le marquant comme du spam (un message vous invitant à acheter quelque chose) ou du phishing (message vous invitant à fournir des informations personnelles à un site Web potentiellement frauduleux). Anti-Spam filtre ensuite les messages de spam et les place dans le dossier McAfee Anti-Spam.

Si vos amis vous envoient parfois des messages légitimes qui peuvent être interprétés comme du spam, vous pouvez éviter leur filtrage en ajoutant l'adresse de ces amis à votre liste d'amis Anti-Spam. Vous pouvez aussi personnaliser la détection du spam. Par exemple, vous pouvez filtrer les messages plus radicalement, spécifier que chercher dans un message et créer vos propres filtres.

Anti-Spam vous protège aussi si vous tentez d'accéder à un site Web potentiellement frauduleux par le biais d'un lien inséré dans un e-mail. Lorsque vous cliquez sur un lien menant à un site Web potentiellement frauduleux, vous êtes redirigé vers la page du filtre antiphishing. S'il y a des sites Web que vous ne voulez pas filtrer, vous pouvez les ajouter à la liste blanche (les sites Web de cette liste ne sont pas filtrés).

Anti-Spam fonctionne avec divers programmes de messagerie tels que les comptes POP3, POP3 Webmail, Yahoo®, MSN®/Hotmail®, Windows® Live™ Mail et MAPI (Microsoft Exchange Server). Si vous utilisez un navigateur pour lire votre courrier, vous devez ajouter votre compte Webmail à Anti-Spam. Tous les autres comptes sont configurés automatiquement et vous ne devez pas les ajouter à Anti-Spam.

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctionnalités d'Anti-Spam 131
Configuration des comptes Webmail 133
Configuration des amis 139
Configuration de la détection de spam 147
Filtrage des e-mails 155
Traitement du e-mails filtrés 159
Configuration de la protection antiphishing 161

Fonctionnalités d'Anti-Spam

Anti-Spam propose les fonctionnalités suivantes :

Filtrage des spams

Les filtres avancés d'Anti-Spam empêchent les messages non sollicités de pénétrer dans votre boîte de réception et sont automatiquement mis à jour pour tous vos comptes de messagerie Internet. Vous pouvez aussi créer des filtres personnalisés pour veiller à filtrer tout le spam et signaler du spam à McAfee pour analyse.

Filtrage antiphishing

Le filtre antiphishing identifie les sites de phishing (frauduleux) potentiels qui cherchent à obtenir des informations personnelles.

Traitement personnalisé du spam

Marquez le courrier non sollicité comme du spam et déplacez-le vers votre dossier McAfee Anti-Spam ou marquez le courrier légitime comme n'étant pas du spam et déplacez-le vers votre boîte de réception.

Amis

Importez les adresses électroniques de vos amis dans la liste d'amis pour éviter que leurs messages soient filtrés.

Tri des listes par pertinence

Vous pouvez trier vos filtres personnels, amis, carnets d'adresses et comptes Webmail par pertinence (cliquez simplement sur le nom de colonne approprié).

Prise en charge supplémentaire

Anti-Spam prend en charge Mozilla® Thunderbird™ 1.5 et 2.0, et offre une prise en charge 64 bits de Windows Vista™ pour Windows Mail. Le nouveau mode Jeu arrête en outre les processus d'arrière-plan d'Anti-Spam afin que votre ordinateur ne ralentisse pas pendant que vous jouez à des jeux vidéo ou regardez des DVD. Anti-Spam filtre aussi les comptes Microsoft® Outlook®, Outlook Express ou Windows Mail sur n'importe quel port, y compris les ports SSL (Secure Socket Layer).

CHAPITRE 24

Configuration des comptes Webmail

Si vous utilisez un navigateur pour lire vos messages électroniques, vous devez configurer Anti-Spam pour qu'il se connecte à votre compte et filtre vos messages. Pour ajouter votre compte Webmail à Anti-Spam, ajoutez simplement les informations de compte fournies par votre fournisseur de messagerie.

Après avoir ajouté un compte Webmail, vous pouvez modifier les informations de votre compte et obtenir davantage d'informations sur le Webmail filtré. Si vous n'utilisez plus un compte Webmail ou ne voulez plus qu'il soit filtré, vous pouvez le supprimer.

Anti-Spam fonctionne avec divers programmes de messagerie tels que les comptes POP3, POP3 Webmail, Yahoo®, MSN/Hotmail, Windows Live Mail et MAPI. POP3 est le type de compte le plus courant. Il constitue également la norme en matière de messagerie Internet. Si vous possédez un compte POP3, Anti-Spam se connecte directement au serveur et filtre les messages avant que le programme de messagerie ne les récupère. Les comptes POP3 Webmail, Yahoo, MSN/Hotmail et Windows Mail sont basés sur le Web. Le filtrage des comptes POP3 Webmail est similaire au filtrage des comptes POP3. MAPI est un système Microsoft qui prend en charge plusieurs types de messagerie (messagerie Internet, télécopies et messagerie Exchange Server). Actuellement, seul Microsoft Outlook peut travailler directement avec des comptes MAPI.

Remarque : Bien qu'Anti-Spam puisse accéder aux comptes MAPI, il ne filtre pas vos messages tant que vous ne les avez pas récupérés avec Microsoft Outlook.

Contenu de ce chapitre

Ajouter un compte Webmail 134
Modifier un compte Webmail 134
Supprimer un compte Webmail..... 135
Explications sur les informations de compte Webmail 136

Ajouter un compte Webmail

Ajoutez un compte Webmail POP3 (par exemple, Yahoo), MSN/Hotmail ou Windows Mail (seules les versions payantes sont entièrement prises en charge) si vous souhaitez filtrer le spam parmi les messages de ce compte.

1 Ouvrez le volet Protection antispam.

   Comment ?

   1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
   2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
   3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Comptes Webmail**.

3 Dans le volet Comptes Webmail, cliquez sur **Ajouter**.

4 Spécifiez les informations du compte (page 136), puis cliquez sur **Suivant**.

5 Sous **Options de vérification**, spécifiez quand Anti-Spam doit vérifier la présence de spam sur votre compte (page 136).

6 Si vous utilisez une connexion par numérotation, spécifiez comment Anti-Spam doit se connecter à Internet (page 136).

7 Cliquez sur **Terminer**.

Modifier un compte Webmail

Vous devez modifier les informations de votre compte Webmail lorsque votre compte subit des modifications. Par exemple, modifiez votre compte Webmail si vous changez de mot de passe ou si vous souhaitez qu'Anti-Spam vérifie plus fréquemment la présence de spam.

1 Ouvrez le volet Protection antispam.

   Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Comptes Webmail**.

3 Sélectionnez le compte que vous souhaitez modifier, puis cliquez sur **Modifier**.

4 Spécifiez les informations du compte (page 136), puis cliquez sur **Suivant**.

5 Sous **Options de vérification**, spécifiez quand Anti-Spam doit vérifier la présence de spam sur votre compte (page 136).

6 Si vous utilisez une connexion par numérotation, spécifiez comment Anti-Spam doit se connecter à Internet (page 136).

7 Cliquez sur **Terminer**.

Supprimer un compte Webmail

Supprimez un compte Webmail lorsque vous ne voulez plus y filtrer le spam. Par exemple, si votre compte n'est plus actif ou en cas de problèmes, vous pouvez supprimer le compte le temps du dépannage.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Comptes Webmail**.

3 Sélectionnez le compte à supprimer, puis cliquez sur **Supprimer**.

Explications sur les informations de compte Webmail

Les tableaux qui suivent décrivent les informations que vous devez spécifier lorsque vous ajoutez ou modifiez des comptes Webmail.

Informations sur le compte

Informations	Description
Description	Décrivez le compte pour votre référence. Dans cette zone, vous pouvez saisir tout type d'information.
Adresse e-mail	Spécifiez l'adresse électronique de ce compte de messagerie.
Type de compte	Spécifiez le type du compte de messagerie que vous ajoutez (par exemple, POP3 Webmail ou MSN/Hotmail).
Serveur	Spécifiez le nom du serveur de messagerie qui héberge ce compte. Si vous ne connaissez pas le nom du serveur, reportez-vous aux informations fournies par votre fournisseur d'accès à Internet (FAI).
Nom d'utilisateur	Spécifiez le nom d'utilisateur de ce compte de messagerie. Par exemple, si votre adresse e-mail est *utilisateur*@hotmail.com, votre nom d'utilisateur est probablement *utilisateur*.
Mot de passe	Spécifiez le mot de passe de ce compte de messagerie.
Confirmer le mot de passe	Confirmez le mot de passe de ce compte de messagerie.

Options de vérification

Option	Description
Vérifier toutes les	Anti-Spam vérifie le spam sur ce compte à l'intervalle que vous spécifiez (nombre de minutes). Cet intervalle doit être compris entre 5 et 3600 minutes.
Vérifier au démarrage	Anti-Spam vérifie le compte à chaque démarrage de l'ordinateur.

Options de connexion

Option	Description
Ne jamais établir de connexion	Anti-Spam n'établit pas automatiquement la connexion. Vous devez établir manuellement votre connexion par numérotation.
Etablir une connexion si aucune n'est disponible	Lorsqu'une connexion Internet n'est pas disponible, Anti-Spam tente de se connecter en utilisant la connexion par numérotation que vous spécifiez.
Toujours établir la connexion indiquée	Anti-Spam tente de se connecter en utilisant la connexion par numérotation que vous avez indiquée. Si vous êtes actuellement connecté via une autre connexion par numérotation que celle que vous spécifiez, vous serez déconnecté.
Etablir cette connexion	Spécifiez la connexion par numérotation qu'Anti-Spam doit utiliser pour se connecter à Internet.
Rester connecté une fois le filtrage terminé	Votre ordinateur reste connecté à Internet après le filtrage.

CHAPITRE 25

Configuration des amis

Pour faire en sorte qu'Anti-Spam ne filtre pas les messages légitimes de vos amis, vous pouvez ajouter leurs adresses à votre liste d'amis Anti-Spam.

La façon la plus simple de mettre à jour votre liste d'amis est d'ajouter vos carnets d'adresses à Anti-Spam de manière à importer toutes les adresses de vos amis. Après avoir ajouté un carnet d'adresses, son contenu est automatiquement importé à intervalles planifiés (chaque jour, semaine ou mois) pour que votre liste d'amis reste à jour en permanence.

Vous pouvez aussi mettre à jour manuellement votre liste d'amis Anti-Spam ou ajouter un domaine entier si vous voulez que chaque utilisateur du domaine soit ajouté à votre liste d'amis. Par exemple, si vous ajoutez le domaine entreprise.com, aucune des adresses de cette entreprise ne sera filtrée.

Contenu de ce chapitre

Configuration automatique d'amis 140
Configuration manuelle d'amis 143

Configuration automatique d'amis

Vous pouvez mettre automatiquement à jour votre liste d'amis en ajoutant vos carnets d'adresses à Anti-Spam. L'ajout d'un carnet d'adresses permet à Anti-Spam d'importer les adresses correspondantes pour en remplir la liste d'amis.

Après avoir ajouté un carnet d'adresses, vous pouvez spécifier l'intervalle auquel son contenu doit être importé dans votre liste d'amis. Vous pouvez aussi supprimer un carnet d'adresses si vous ne voulez plus en importer le contenu.

Ajouter un carnet d'adresses

Ajoutez vos carnets d'adresses afin qu'Anti-Spam puisse importer automatiquement toutes vos adresses électroniques et mettre à jour votre liste d'amis. Votre liste d'amis sera ainsi toujours à jour.

1. Ouvrez le volet Protection antispam.

   Comment ?

   1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
   2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
   3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2. Dans le volet Protection antispam, cliquez sur **Carnets d'adresses**.
3. Dans le volet Carnets d'adresses, cliquez sur **Ajouter**.
4. Sélectionnez le type de carnet d'adresses à importer dans la liste **Type**.
5. Si la liste **Source** doit être remplie, sélectionnez la source du carnet d'adresses. Par exemple, si vous avez des carnets d'adresses Outlook, vous devez sélectionner Outlook dans cette liste.
6. Cliquez sur **Tous les jours, Toutes les semaines** ou **Tous les mois** dans la liste **Calendrier** pour déterminer quand Anti-Spam doit vérifier s'il y a de nouvelles adresses dans votre carnet d'adresses.
7. Cliquez sur **OK**.

Modifier un carnet d'adresses

Après avoir ajouté des carnets d'adresses, vous pouvez en modifier les données d'importation et le calendrier. Par exemple, modifiez vos carnets d'adresses si vous souhaitez qu'Anti-Spam vérifie plus fréquemment la présence de nouvelles adresses.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Carnets d'adresses**.

3 Sélectionnez le carnet d'adresses que vous souhaitez modifier, puis cliquez sur **Modifier**.

4 Sélectionnez le type de carnet d'adresses à importer dans la liste **Type**.

5 Si la liste **Source** doit être remplie, sélectionnez la source du carnet d'adresses. Par exemple, si vous avez des carnets d'adresses Outlook, vous devez sélectionner Outlook dans cette liste.

6 Cliquez sur **Tous les jours, Toutes les semaines** ou **Tous les mois** dans la liste **Calendrier** pour déterminer quand Anti-Spam doit vérifier s'il y a de nouvelles adresses dans votre carnet d'adresses.

7 Cliquez sur **OK**.

Supprimer un carnet d'adresses

Supprimez un carnet d'adresses lorsque vous ne souhaitez plus qu'Anti-Spam en importe automatiquement les adresses (par exemple, si un carnet d'adresses n'est plus à jour et que vous ne voulez plus l'utiliser).

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Carnets d'adresses**.

3 Sélectionnez le carnet d’adresses à supprimer, puis cliquez sur **Supprimer**.

Configuration manuelle d'amis

Vous pouvez mettre à jour manuellement votre liste d'amis en modifiant les entrées une à une. Par exemple, si vous recevez un message d'un ami dont l'adresse ne figure pas dans votre carnet d'adresses, vous pouvez l'ajouter manuellement. Le plus simple pour ce faire est d'utiliser la barre d'outils d'Anti-Spam. Sinon, vous devez spécifier vous-même les données de votre ami.

Ajouter un ami à partir de la barre d'outils d'Anti-Spam

Si vous utilisez les programmes de messagerie Outlook, Outlook Express, Windows Mail, Eudora™ ou Thunderbird, vous pouvez ajouter des amis directement à partir de la barre d'outils d'Anti-Spam.

Pour ajouter un ami dans...	Sélectionnez un message, puis...
Outlook, Outlook Express, Windows Mail	Cliquez sur **Ajouter un ami**.
Eudora, Thunderbird	Dans le menu **Anti-Spam**, cliquez sur **Ajouter un ami**.

Ajouter manuellement un ami

Si vous ne voulez pas ajouter un ami directement à partir de la barre d'outils ou si vous avez oublié de le faire lors de la réception du message, vous pouvez encore ajouter un ami à votre liste d'amis sans devoir attendre qu'Anti-Spam importe automatiquement votre carnet d'adresses.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Amis**.

3 Dans le volet Amis, cliquez sur **Ajouter**.

4 Dans la zone **Nom**, saisissez le nom de votre ami.

5 Sélectionnez **Une seule adresse e-mail** dans la liste **Type**.

6 Saisissez l'adresse électronique de votre ami dans la zone **Adresse e-mail**.

7 Cliquez sur **OK**.

Ajouter un domaine

Ajoutez un domaine entier si vous voulez ajouter chaque utilisateur de ce domaine à votre liste d'amis. Par exemple, si vous ajoutez le domaine entreprise.com, aucune des adresses de cette entreprise ne sera filtrée.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Amis**.

3 Dans le volet Amis, cliquez sur **Ajouter**.

4 Saisissez le nom de l'organisation ou du groupe dans la zone **Nom**.

5 Sélectionnez **Domaine entier** dans la liste **Type**.

6 Tapez le nom du domaine dans la zone **Adresse e-mail**.

7 Cliquez sur **OK**.

Modifier un ami

Si les informations associées à un ami changent, vous pouvez mettre à jour votre liste d'amis afin d'être sûr qu'Anti-Spam ne marque pas ses messages comme du spam.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Amis**.

3 Sélectionnez l'ami que vous souhaitez modifier, puis cliquez sur **Modifier**.

4 Dans la zone **Nom**, modifiez le nom de votre ami.

5 Modifiez l'adresse électronique de votre ami dans la zone **Adresse e-mail**.

6 Cliquez sur **OK**.

Modifier un domaine

Si les informations associées à un domaine changent, vous pouvez mettre à jour votre liste d'amis afin d'être sûr qu'Anti-Spam ne marque pas comme du spam les messages provenant de ce domaine.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Amis**.

3 Dans le volet Amis, cliquez sur **Ajouter**.

4 Modifiez le nom de l'organisation ou du groupe dans la zone **Nom**.

5 Sélectionnez **Domaine entier** dans la liste **Type**.

6 Modifiez le nom du domaine dans la zone **Adresse e-mail**.

7 Cliquez sur **OK**.

Supprimer un ami

Si une personne ou un domaine figurant dans votre liste d'amis vous envoie du spam, supprimez-le de votre liste d'amis Anti-Spam afin que ses messages soient à nouveau filtrés.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Amis**.

3 Sélectionnez le nom de l'ami à supprimer, puis cliquez sur **Supprimer**.

CHAPITRE 26

Configuration de la détection de spam

Anti-Spam vous permet de personnaliser la façon dont le spam est détecté. Vous pouvez filtrer plus agressivement les messages, spécifier les critères à rechercher dans un message et chercher des jeux de caractères spécifiques lors de l'analyse du spam. Vous pouvez aussi créer des filtres personnels pour affiner l'identification du spam par Anti-Spam. Par exemple, si un message non sollicité contenant le mot hypothèque n'est pas filtré, vous pouvez ajouter un filtre contenant ce mot.

Si vous avez des problèmes avec votre messagerie, vous pouvez désactiver la protection antispam dans le cadre de votre stratégie de dépannage.

Contenu de ce chapitre

Désactivation de la protection antispam 147
Définition des options de filtrage.....148
Utilisation de filtres personnels 152

Désactivation de la protection antispam

Vous pouvez désactiver la protection antispam pour empêcher Anti-Spam de filtrer les e-mails.

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **E-mail & IM**.
3. Sous **Protection antispam**, cliquez sur **Désactivée**

Conseil : N'oubliez pas de cliquer sur **Activer** sous **Protection antispam** pour vous protéger contre le spam.

Définition des options de filtrage

Ajustez les options de filtrage d'Anti-Spam si vous souhaitez filtrer plus agressivement les messages, spécifier les critères à rechercher dans un message et chercher des jeux de caractères spécifiques lors de l'analyse du spam.

Niveau de filtrage

Le niveau de filtrage détermine l'agressivité avec laquelle les messages sont filtrés. Par exemple, si du spam n'est pas filtré et que votre niveau de filtrage est Moyen, vous pouvez le changer en Elevé. Cependant, si le niveau de filtrage est à Elevé, seuls sont acceptés les messages provenant d'expéditeurs répertoriés dans la liste d'amis : tous les autres messages sont filtrés.

Filtres spéciaux

Le filtre détermine les informations qu'Anti-Spam doit rechercher dans un e-mail. Des filtres spéciaux détectent les messages contenant du texte caché, des images incorporées, des erreurs de formatage HTML intentionnelles et d'autres techniques habituelles des auteurs de spam. Puisque les messages qui possèdent ces attributs sont généralement du spam, les filtres spéciaux sont activés par défaut. Par exemple, si vous souhaitez recevoir les messages qui contiennent des images incorporées, vous devrez peut-être désactiver le filtre d'images spécial.

Jeux de caractères

Anti-Spam peut chercher des jeux de caractères spécifiques lorsqu'il analyse le spam. Les jeux de caractères sont utilisés pour représenter une langue, notamment son alphabet, les chiffres et autres symboles. Si vous recevez du spam en grec, vous pouvez filtrer tous les messages contenant le jeu de caractères grec.

Veillez cependant à ne pas filtrer les jeux de caractères des langues dans lesquelles vous recevez des e-mails de sources fiables. Par exemple, si vous voulez filtrer des messages en italien, vous pourriez être tenté de sélectionner Europe de l'Ouest car l'Italie se trouve en Europe de l'Ouest. Cependant, si vous recevez des messages légitimes en anglais, un filtre basé sur l'Europe de l'Ouest filtrera aussi les messages en anglais ainsi que dans les autres langues utilisant le jeux de caractères Europe de l'Ouest. En l'occurrence, vous ne pouvez pas filtrer uniquement les messages en italien.

Remarque : le filtrage de messages contenant des caractères dans un jeu de caractères spécifique est réservé aux utilisateurs avancés.

Modifier le niveau de filtrage

Vous pouvez changer le degré de filtrage des messages. Par exemple, si des messages légitimes sont filtrés, vous pouvez diminuer le niveau de filtrage.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Options de filtrage**.

3 Sous **Options de filtrage**, déplacez le curseur sur le niveau approprié, puis cliquez sur **OK**.

Niveau	Description
Faible	La plupart des e-mails sont acceptés.
Moyennement faible	seuls les spams évidents sont bloqués.
Moyen	Le filtrage des messages s'effectue au niveau recommandé.
Moyennement élevé	Tout e-mail présentant des caractéristiques de spam est filtré.
Élevé	Seuls les messages d'expéditeurs appartenant à votre liste d'amis sont acceptés.

Désactiver un filtre spécial

Les filtres spéciaux sont activés par défaut, car ils filtrent les messages typiquement envoyés par les auteurs de spam. Par exemple, les messages qui contiennent des images incorporées sont généralement du spam ; cependant, si vous recevez fréquemment des messages légitimes contenant des images incorporées, désactivez le filtre d'images spécial.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Options de filtrage**.

3 Sous **Options de filtrage**, sélectionnez ou désélectionnez les cases voulues, puis cliquez sur **OK**.

Filtre	Description
Filtrer des messages qui contiennent du texte masqué	Ce filtre cherche du texte caché, car les auteurs de spam utilisent souvent des messages contenant du texte caché pour éviter d'être détectés.
Filtrer des messages qui contiennent une certaine proportion d'images et de texte	Ce filtre cherche des images incorporées, car les messages contenant de telles images sont généralement du spam.
Filtrer des messages qui contiennent des erreurs de mise en forme HTML intentionnelles	Ce filtre cherche les messages contenant un formatage incorrect, qui est une autre manière d'essayer d'éviter les filtres antispam.
Ne pas filtrer les messages supérieurs à	Ce filtre ignore les messages d'une taille supérieure à la taille spécifiée, car les messages volumineux ne sont probablement pas du spam. Vous pouvez augmenter ou diminuer la taille des messages (la plage valide est comprise entre 0 et 250 Ko).

Appliquer les filtres de jeux de caractères

Remarque : le filtrage de messages contenant des caractères dans un jeu de caractères spécifique est réservé aux utilisateurs avancés.

Vous pouvez filtrer des jeux de caractères spécifiques ; cependant, ne filtrez pas les jeux de caractères des langues dans lesquelles vous recevez des e-mails de sources fiables.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Jeux de caractères**.

3 Cochez les cases correspondant aux jeux de caractères que vous souhaitez filtrer.

4 Cliquez sur **OK**.

Utilisation de filtres personnels

Le filtre détermine les informations qu'Anti-Spam doit rechercher dans un e-mail. Lorsque du spam est détecté, le message est marqué comme tel et est laissé dans votre boîte de réception ou déplacé vers le dossier McAfee Anti-Spam. Pour plus d'informations sur le traitement du spam, consultez Modifier la façon dont un message est traité et marqué (page 156).

Par défaut, Anti-Spam utilise de nombreux filtres ; cependant, vous pouvez créer de nouveaux filtres ou modifier des filtres existants pour affiner l'identification du spam par Anti-Spam. Par exemple, si vous ajoutez un filtre contentant le mot hypothèque, Anti-Spam filtre les messages contenant ce mot. Ne créez pas des filtres basés sur des mot courants qui apparaissent dans des messages légitimes, car ces messages aussi seraient alors filtrés. Après avoir créé un filtre, vous pouvez le modifier s'il ne semble pas être efficace. Par exemple, si vous avez créé un filtre qui cherche le mot viagra dans l'objet du message, mais continuez à recevoir des messages contenant le mot viagra car celui-ci apparaît dans le corps du message, changez le filtre pour qu'il cherche le mot viagra dans le corps plutôt que dans l'objet du message.

Les expressions régulières (RegEx) sont des caractères spéciaux et séquences de caractères spéciales qui peuvent aussi être utilisées dans des filtres personnels ; cependant, McAfee recommande de n'utiliser les expressions régulières que si vous êtes un utilisateur avancé. Si vous n'êtes pas familiarisé avec les expressions régulières ou si vous souhaitez en savoir plus sur leur utilisation, vous pouvez rechercher des expressions régulières sur le Web (par exemple, sur http://fr.wikipedia.org/wiki/Expression_rationnelle).

Ajouter un filtre personnel

Vous pouvez ajouter des filtres pour affiner l'identification du spam par Anti-Spam.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Filtres personnels**.

3 Cliquez sur **Ajouter**.

4 Spécifiez ce que le filtre personnel doit rechercher (page 154) dans un message.

5 Cliquez sur **OK**.

Modifier un filtre personnel

Vous pouvez modifier les filtres pour affiner l'identification du spam.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Filtres personnels**.

3 Sélectionnez le filtre que vous souhaitez modifier, puis cliquez sur **Modifier**.

4 Spécifiez ce que le filtre personnel doit rechercher (page 154) dans un message.

5 Cliquez sur **OK**.

Supprimer un filtre personnel

Vous pouvez supprimer définitivement les filtres que vous ne souhaitez plus utiliser.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Filtres personnels**.

3 Sélectionnez le filtre à supprimer, puis cliquez sur **Supprimer**.

4 Cliquez sur **OK**.

Spécification d'un filtre personnel

Le tableau qui suit décrit ce qu'un filtre personnel recherche dans un message.

Informations	Description
Article	Cliquez sur une entrée pour déterminer si le filtre recherche des mots ou des expressions dans l'objet, le corps, les en-têtes ou l'expéditeur du message.
Condition	Cliquez sur une entrée pour déterminer si le filtre recherche un message contenant, ou ne contenant pas, les mots ou les expressions que vous spécifiez.
Mots ou expressions	Saisissez les mots ou expressions à rechercher dans un message. Par exemple, si vous spécifiez le mot hypothèque, tous les messages contenant ce mot seront filtrés.
Ce filtre utilise des expressions standard (RegEx)	Spécifiez les schémas de caractères utilisés dans des conditions de filtre. Pour tester un schéma de caractères, cliquez sur **Test**.

CHAPITRE 27

Filtrage des e-mails

Anti-Spam examine les messages entrants et les classe dans la catégorie spam (e-mails de démarchage) ou phishing (e-mails vous invitant à fournir des informations personnelles à un site Web potentiellement frauduleux). Par défaut, Anti-Spam marque ensuite chaque message non sollicité comme du spam ou du phishing (la balise [SPAM] ou [PHISH] apparaît dans l'objet du message) et le déplace vers le dossier McAfee Anti-Spam.

Pour personnaliser la façon dont Anti-Spam filtre vos messages, vous pouvez marquer le message comme spam ou non dans la barre d'outils Anti-Spam, changer l'emplacement où sont envoyés le messages de spam ou changer le marqueur ajouté à la ligne d'objet.

Pour changer la façon dont le spam est traité et marqué, vous pouvez personnaliser l'emplacement où sont envoyés les messages de spam et de phishing ainsi que le nom du marqueur qui apparaît dans la ligne d'objet.

Vous pouvez aussi désactiver les barres d'outils Anti-Spam dans le cadre de votre stratégie de dépannage lorsque vous rencontrez des problèmes avec votre programme de messagerie.

Contenu de ce chapitre

Marquer un message à partir de la barre d'outils Anti-Spam 155
Modifier la façon dont un message est traité et marqué 156
Désactiver la barre d'outils Anti-Spam.....157

Marquer un message à partir de la barre d'outils Anti-Spam

Lorsque vous marquez un message comme spam, le marqueur [SPAM] ou un marqueur de votre choix est ajouté à l'objet du message et le message est laissé dans votre boîte de réception ou déplacé vers le dossier Anti-Spam (Outlook, Outlook Express, Windows Mail, Thunderbird) ou le dossier Courrier indésirable (Eudora®). Lorsque vous marquez un message comme non spam, le marqueur est retiré du message et le message est replacé dans votre boîte de réception.

Pour marquer un message dans...	Sélectionnez un message, puis...
Outlook, Outlook Express, Windows Mail	Cliquez sur **Marquer comme spam** ou **Marquer comme non spam**.

Eudora, Thunderbird	Dans le menu **Anti-Spam**, cliquez sur **Marquer comme spam** ou sur **Marquer comme non spam**.

Modifier la façon dont un message est traité et marqué

Vous pouvez changer la façon dont le spam est traité et marqué. Par exemple, vous pouvez décider si le message est déposé dans la boîte de réception ou dans le dossier McAfee Anti-Spam et changer le marquer [SPAM] ou [PHISH] ajouté à la ligne d'objet du message.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Traitement**.

3 Sélectionnez ou désactivez les cases appropriées, puis cliquez sur **OK**.

Option	Description
Marquer comme spam et déplacer vers le dossier McAfee Anti-Spam	Il s'agit du paramètre par défaut. Les messages de spam sont déplacés vers votre dossier McAfee Anti-Spam.
Marquer comme spam et laisser dans la boîte de réception	Les spams restent dans votre boîte de réception.
Ajouter ce marqueur personnalisable à l'objet des spams	Le marqueur saisi est ajouté à la ligne d'objet des spams.
Ajouter ce marqueur personnalisable à l'objet des messages de type phishing	Le marqueur saisi est ajouté à la ligne d'objet des messages hameçons.

Désactiver la barre d'outils Anti-Spam

Si vous utilisez Outlook, Outlook Express, Windows Mail, Eudora ou Thunderbird, vous pouvez désactiver la barre d'outils Anti-Spam.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Barres d'outils de messagerie**.

3 Désélectionnez la case à cocher associée à la barre d'outils à désactiver.

4 Cliquez sur **OK**.

Conseil : Vous pouvez réactiver les barres d'outils Anti-Spam à tout moment en sélectionnant les cases correspondantes.

CHAPITRE 28

Traitement du e-mails filtrés

Parfois, du spam ne sera pas détecté. Vous pouvez alors signaler les spams à McAfee, qui les analysera pour créer des mises à jour pour les filtres.

Si vous utilisez un compte Webmail, vous pouvez copier, supprimer et obtenir des informations sur les messages filtrés. C'est utile lorsque vous ne savez pas si un message légitime a été filtré ou que vous désirez savoir quand le message a été filtré.

Contenu de ce chapitre

Signaler les spams à McAfee.....159
Copier ou supprimer un message Webmail filtré 160
Afficher un événement associé à un Webmail filtré .160

Signaler les spams à McAfee

Vous pouvez signaler les spams à McAfee, qui les analysera pour créer des mises à jour pour les filtres.

1 Ouvrez le volet Protection antispam.

Comment ?

1. Dans la fenêtre Accueil de SecurityCenter, cliquez sur **E-mail & IM**.
2. Dans la zone d'informations E-mail & IM, cliquez sur **Configurer**.
3. Dans le volet Configuration E-mail & IM, sous **Protection antispam**, cliquez sur **Avancé**.

2 Dans le volet Protection antispam, cliquez sur **Notification à McAfee**.

3 Sélectionnez les cases appropriées, puis cliquez sur **OK**.

Option	Description
Activer la notification en cliquant sur Marquer comme étant du spam	signale un message à McAfee lorsque vous le marquez comme étant un spam.
Activer la notification en cliquant sur Marquer comme n'étant pas du spam	signale un message à McAfee lorsque vous le marquez comme n'étant pas un spam.

Envoyer le message entier (et non les en-têtes uniquement)	envoie le message entier, et pas seulement les en-têtes, lorsque vous le signalez à McAfee.

Copier ou supprimer un message Webmail filtré

Vous pouvez copier ou supprimer des messages qui ont été filtrés dans votre compte Webmail.

1. Sous **Tâches courantes**, cliquez sur **Afficher les événements récents**.
2. Dans le volet Evénements récents, cliquez sur **Afficher le fichier journal**.
3. Dans le volet de gauche, développez la liste **E-mail & IM**, puis cliquez sur **Evénements de filtrage de la messagerie**.
4. Sélectionnez un message.
5. Sous **Je souhaite**, effectuez l'une des actions suivantes :
   - Cliquez sur **Copier** pour copier le message dans le Presse-papiers.
   - Cliquez sur **Supprimer** pour supprimer le message.

Afficher un événement associé à un Webmail filtré

Vous pouvez vérifier quand le message a été filtré et sur quel compte il a été reçu.

1. Sous **Tâches courantes**, cliquez sur **Afficher les événements récents**.
2. Dans le volet Evénements récents, cliquez sur **Afficher le fichier journal**.
3. Dans le volet de gauche, développez la liste **E-mail & IM**, puis cliquez sur **Evénements de filtrage de la messagerie**.
4. Sélectionnez le journal que vous souhaitez afficher.

CHAPITRE 29

Configuration de la protection antiphishing

Anti-Spam classe le courrier non sollicité dans la catégorie spam (e-mails de démarchage) ou phishing (e-mails vous invitant à fournir des informations personnelles à un site Web potentiellement frauduleux ou reconnu comme tel). La protection contre le Phishing vous aide à vous protéger contre les sites Web frauduleux. Si, dans un message, vous cliquez sur un lien menant à un site Web potentiellement frauduleux ou connu comme tel, Anti-Spam vous redirige vers la page du filtre antiphishing.

S'il y a des sites Web que vous ne voulez pas filtrer, ajoutez-les à la liste d'autorisation de Phishing. Vous pouvez aussi modifier ou supprimer des sites Web de la liste d'autorisation. Il n'est pas nécessaire d'ajouter des sites tels que Google®, Yahoo ou McAfee, car ces sites Web ne sont pas considérés frauduleux.

Remarque : si SiteAdvisor est installé, vous ne bénéficiez pas de la protection contre le Phishing d'Anti-Spam, car SiteAdvisor possède déjà une protection similaire.

Contenu de ce chapitre

Ajouter un site Web à la liste d'autorisation.....161
Modifier des sites dans la liste d'autorisation.....162
Supprimer un site Web de la liste d'autorisation.....162
Désactivation de la protection antiphishing.....163

Ajouter un site Web à la liste d'autorisation

S'il y a des sites Web que vous ne voulez pas filtrer, ajoutez-les à la liste d'autorisation.

1. Ouvrez le volet Protection contre le Phishing.

   Comment ?

   1. Dans le volet Accueil de SecurityCenter, cliquez sur **Réseau & Internet**.
   2. Dans la zone d'informations Réseau & Internet, cliquez sur **Configurer**.

2. Dans le volet Protection contre le Phishing, cliquez sur **Avancé**.
3. Sous **Liste d'autorisation**, cliquez sur **Ajouter**.
4. Tapez l'adresse du site Web, puis cliquez sur **OK**.

Modifier des sites dans la liste d'autorisation

Si vous avez ajouté un site Web à la liste d'autorisation et que l'adresse de ce site change, vous pouvez la mettre à jour.

1 Ouvrez le volet Protection contre le Phishing.

Comment ?

1. Dans le volet Accueil de SecurityCenter, cliquez sur **Réseau & Internet**.
2. Dans la zone d'informations Réseau & Internet, cliquez sur **Configurer**.

2 Dans le volet Protection contre le Phishing, cliquez sur **Avancé**.

3 Sous **Liste d'autorisation**, sélectionnez le site Web à mettre à jour, puis cliquez sur **Modifier.**

4 Modifiez l'adresse du site Web, puis cliquez sur **OK**.

Supprimer un site Web de la liste d'autorisation

Si vous avez ajouté un site Web à la liste d'autorisation pour pouvoir y accéder mais voulez maintenant le filtrer, supprimez-le de la liste.

1 Ouvrez le volet Protection contre le Phishing.

Comment ?

1. Dans le volet Accueil de SecurityCenter, cliquez sur **Réseau & Internet**.
2. Dans la zone d'informations Réseau & Internet, cliquez sur **Configurer**.

2 Dans le volet Protection contre le Phishing, cliquez sur **Avancé**.

3 Sous **Liste d'autorisation**, sélectionnez le site Web à supprimer, puis cliquez sur **Supprimer.**

Désactivation de la protection antiphishing

Si vous avez déjà un logiciel antiphishing autre que celui de McAfee et qu'un conflit se produit, vous pouvez désactiver la protection contre le Phishing d'Anti-Spam.

1. Dans le volet Accueil de SecurityCenter, cliquez sur **Réseau & Internet**.
2. Dans la zone d'informations Réseau & Internet, cliquez sur **Configurer**.
3. Sous **Protection contre le Phishing**, cliquez sur **Désactivé**.

Conseil : Lorsque vous avez terminé, n'oubliez pas de cliquer sur **Activé** sous **Protection contre le Phishing** pour être à nouveau protégé contre les sites Web frauduleux.

CHAPITRE 30

McAfee Privacy Service

Ce logiciel offre une protection avancée pour vous, votre famille, vos fichiers personnels et votre ordinateur. Il vous protège contre l'usurpation d'identité en ligne, bloque la transmission d'informations personnelles et filtre le contenu potentiellement choquant en ligne (y compris les images). Il propose également des fonctionnalités avancées de contrôle parental qui permettent à des adultes non seulement de surveiller, de contrôler et d'analyser certaines habitudes de navigation non autorisées, mais aussi de stocker de façon sécurisée des mots de passe personnels.

Avant de commencer à utiliser Privacy Service, nous vous conseillons de vous familiariser avec ses principales fonctionnalités. Pour plus de détails sur la configuration et l'utilisation de ces fonctionnalités, consultez l'aide de Privacy Service.

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctionnalités de Privacy Service 166
Configuration du contrôle parental 167
Protection d'informations sur le Web 183
Protection des mots de passe 185

Fonctionnalités de Privacy Service

Privacy Service propose les fonctionnalités suivantes :

- Contrôle parental
- Protection des informations personnelles
- Password Vault

Contrôle parental

La fonction de contrôle parental permet de filtrer les images potentiellement inappropriées, de configurer des groupes de classification de contenu (tranches d'âge utilisées pour restreindre l'accès à des sites Web et au contenu) et de définir des heures limites de navigation Web (période et durée de connexion autorisée à Internet) pour les utilisateurs de SecurityCenter. Le contrôle parental permet globalement de restreindre, d'accorder ou de bloquer l'accès à certains sites Web en fonction de mots clés.

Protection des informations personnelles

La protection des informations personnelles permet d'éviter que vos informations sensibles ou confidentielles (numéros de cartes de crédit, numéros de comptes bancaires, adresses, etc.) ne soient transmises sur le Web.

Password Vault

Password Vault est une zone de stockage sécurisée pour vos mots de passe personnels. Il permet de stocker des mots de passe en sécurité de sorte qu'aucun autre utilisateur (pas même un administrateur) ne puisse y accéder.

CHAPITRE 31

Configuration du contrôle parental

Si vos enfants utilisent votre ordinateur, vous pouvez y configurer un contrôle parental. Le contrôle parental permet de déterminer ce que vos enfants peuvent voir et faire sur le Web. Pour configurer le contrôle parental, vous pouvez activer ou désactiver le filtrage d'images, choisir un groupe de classification du contenu et définir des heures limites de navigation sur le Web. Le filtrage d'images empêche l'affichage d'images potentiellement inappropriées lorsqu'un enfant navigue sur le Web ; le groupe de classification du contenu détermine le type de contenu et de sites Web qui sont accessibles à un enfant d'après sa tranche d'âge ; les heures limites de navigation sur le Web définissent les jours et heures auxquels un enfant peut accéder au Web. Le contrôle parental permet également de filtrer (bloquer ou autoriser) certains sites Web pour tous les enfants.

Remarque : vous devez être administrateur pour pouvoir configurer le contrôle parental.

Contenu de ce chapitre

Configuration des utilisateurs 168
Filtrage des images Web potentiellement inappropriées 174
Configuration du groupe de classification du contenu 175
Configuration des heures limites de navigation Web 177
Filtrage de sites Web 178
Filtrage de sites Web par mots clés 181

Configuration des utilisateurs

Pour configurer le contrôle parental, vous devez attribuer des autorisations aux utilisateurs de SecurityCenter. Par défaut, les utilisateurs de SecurityCenter correspondent aux utilisateurs de Windows définis sur votre ordinateur. Cependant, si vous avez mis à niveau SecurityCenter à partir d'une ancienne version basée sur les utilisateurs de McAfee, vos utilisateurs McAfee et leurs autorisations sont conservés.

Remarque : pour configurer des utilisateurs, vous devez vous connecter à SecurityCenter en tant qu'administrateur.

Gestion des utilisateurs Windows

Pour configurer le contrôle parental, vous devez attribuer aux utilisateurs des autorisations qui déterminent ce que chacun peut voir et faire sur Internet. Par défaut, les utilisateurs de SecurityCenter correspondent aux utilisateurs de Windows définis sur votre ordinateur. L'ajout, la modification du compte et la suppression d'un utilisateur se font dans Windows, sous Gestion de l'ordinateur. Vous pouvez ensuite définir un contrôle pour ces utilisateurs dans SecurityCenter.

Si vous avez mis à niveau SecurityCenter à partir d'une ancienne version basée sur les utilisateurs McAfee, consultez Gestion des utilisateurs McAfee (page 170).

Gestion des utilisateurs McAfee

Si vous avez mis à niveau SecurityCenter à partir d'une ancienne version basée sur les utilisateurs de McAfee, vos utilisateurs McAfee et leurs autorisations sont automatiquement conservés. Vous pouvez continuer à configurer et gérer les utilisateurs McAfee ; toutefois, pour faciliter la maintenance, McAfee recommande de basculer vers des utilisateurs Windows. Une fois le passage effectué à des utilisateurs Windows, vous ne pouvez plus revenir à des utilisateurs McAfee.

Si vous continuez d'employer des utilisateurs McAfee, vous pouvez ajouter, modifier ou supprimer des utilisateurs et changer ou récupérer le mot de passe de l'administrateur McAfee.

Basculer vers des utilisateurs Windows

Pour faciliter la maintenance, McAfee recommande de basculer vers des utilisateurs Windows. Une fois le passage effectué à des utilisateurs Windows, vous ne pouvez plus revenir à des utilisateurs McAfee.

1 Ouvrez le volet Paramètres des utilisateurs.

   Comment ?

   1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
   2. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
   3. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
   4. Dans le volet Configuration du contrôle parental, cliquez sur **Avancé**.

2 Dans le volet Paramètres des utilisateurs, cliquez sur **Basculer**.

3 Confirmez l'opération.

Ajouter un utilisateur McAfee

Après avoir créé un utilisateur McAfee, vous pouvez en configurer le contrôle parental. Pour plus d'informations, consultez l'aide de Privacy Service.

1 Connectez-vous à SecurityCenter en tant qu'administrateur.

2 Ouvrez le volet Paramètres des utilisateurs.

   Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
3. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
4. Dans le volet Configuration du contrôle parental, cliquez sur **Avancé**.

3 Dans le volet Paramètres des utilisateurs, cliquez sur **Ajouter**.

4 Suivez les instructions à l'écran pour définir un nom d'utilisateur, un mot de passe, un type de compte et des contrôles parentaux.

5 Cliquez sur **Créer**.

Modifier les données d'un compte utilisateur McAfee

Vous pouvez changer le mot de passe, le type de compte ou la fonction de connexion automatique d'un utilisateur McAfee.

1 Connectez-vous à SecurityCenter en tant qu'administrateur.

2 Ouvrez le volet Paramètres des utilisateurs.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
3. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
4. Dans le volet Configuration du contrôle parental, cliquez sur **Avancé**.

3 Dans le volet Paramètres des utilisateurs, cliquez sur un nom d'utilisateur, puis sur **Modifier**.

4 Suivez les instructions à l'écran pour modifier le mot de passe, le type de compte ou les contrôles parentaux de l'utilisateur.

5 Cliquez sur **OK**.

Supprimer un utilisateur McAfee

Vous pouvez supprimer un utilisateur McAfee à tout moment.

Pour supprimer un utilisateur McAfee :

1 Connectez-vous à SecurityCenter en tant qu'administrateur.

2 Ouvrez le volet Paramètres des utilisateurs.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
3. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
4. Dans le volet Configuration du contrôle parental, cliquez sur **Avancé**.

3 Dans le volet Paramètres des utilisateurs, sous **Comptes utilisateurs McAfee**, sélectionnez un nom d'utilisateur, puis cliquez sur **Supprimer**.

Modifier le mot de passe de l'administrateur McAfee

Si vous ne vous rappelez pas le mot de passe de l'administrateur McAfee ou si vous pensez que sa confidentialité a pu être compromise, vous pouvez le modifier.

1 Connectez-vous à SecurityCenter en tant qu'administrateur.

2 Ouvrez le volet Paramètres des utilisateurs.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
3. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
4. Dans le volet Configuration du contrôle parental, cliquez sur **Avancé**.

3 Dans le volet Paramètres des utilisateurs, sous **Comptes utilisateurs McAfee**, sélectionnez **Administrateur**, puis cliquez sur **Modifier**.

4 Dans la boîte de dialogue Modifier le compte utilisateur, tapez un nouveau mot de passe dans la zone **Nouveau mot de passe**, puis saisissez-le à nouveau dans la zone **Confirmer le mot de passe**.

5 Cliquez sur **OK**.

Récupérer le mot de passe de l'administrateur McAfee

Si vous oubliez le mot de passe administrateur, vous pouvez le récupérer.

1. Cliquez avec le bouton droit sur l'icône de SecurityCenter, puis cliquez sur **Changer d'utilisateur**.
2. Dans la liste **Nom d'utilisateur**, cliquez sur **Administrateur**, puis sur **Mot de passe oublié**.
3. Tapez la réponse à la question secrète dans la zone **Réponse**.
4. Cliquez sur **Valider**.

Filtrage des images Web potentiellement inappropriées

Selon l'âge ou le niveau de maturité d'un utilisateur, vous pouvez filtrer (bloquer ou autoriser) les images potentiellement inappropriées lorsque l'utilisateur navigue sur le Web. Par exemple, vous pouvez empêcher l'affichage des images potentiellement inappropriées lorsque vos jeunes enfants naviguent sur le Web, mais les autoriser pour les grands adolescents et les adultes de la famille. Par défaut, le filtrage d'images est désactivé pour tous les membres du groupe Adulte ; ces utilisateurs peuvent donc voir des images potentiellement inappropriées lorsqu'ils naviguent sur le Web. Pour plus d'informations sur la définition de la tranche d'âge d'un utilisateur, consultez Configuration du groupe de classification du contenu (page 175).

Filtrer les images Web potentiellement inappropriées

Par défaut, les nouveaux utilisateurs sont ajoutés au groupe Adulte et le filtrage d'images est désactivé. Si vous souhaitez empêcher l'affichage des images potentiellement inappropriées lorsqu'un utilisateur particulier navigue sur le Web, vous pouvez activer le filtrage des images. Chaque image Web potentiellement inappropriée est alors automatiquement remplacée par une image McAfee fixe.

1 Ouvrez le volet Paramètres des utilisateurs.

   Comment ?

   1. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
   2. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
   3. Dans le volet Configuration du contrôle parental, cliquez sur **Avancé**.
   4. Dans le volet Contrôle parental, cliquez sur **Paramètres des utilisateurs**.

2 Dans le volet Paramètres des utilisateurs, cliquez sur un nom d'utilisateur, puis sur **Modifier**.

3 Dans la fenêtre Modifier le compte utilisateur, sous **Filtrage d'images**, cliquez sur **Activé**.

4 Cliquez sur **OK**.

Configuration du groupe de classification du contenu

Un utilisateur peut appartenir à l'un des groupes de classification du contenu suivants :

- Jeune enfant
- Enfant
- Jeune adolescent
- Adolescent
- Adultes

Privacy Service évalue (bloque ou autorise) le contenu Web en fonction du groupe auquel appartient un utilisateur. Cela permet de bloquer ou autoriser certains sites Web pour certains utilisateurs de la famille. Par exemple, vous pourriez empêcher l'accès à un site Web pour les membres du groupe Jeune enfant, mais l'autoriser pour ceux du groupe Adolescent. Pour classifier le contenu de manière plus stricte pour un utilisateur, vous pouvez également lui limiter l'accès aux sites Web répertoriés dans la liste **Sites Web filtrés**. Pour plus d'informations, consultez Filtrage de sites Web (page 178).

Par défaut, un nouvel utilisateur est ajouté au groupe Adulte, qui permet l'accès à tout le contenu Web.

Configuration du groupe de classification du contenu pour un utilisateur

Par défaut, un nouvel utilisateur est ajouté au groupe Adulte, qui permet l'accès à tout le contenu Web. Vous pouvez ensuite ajuster le groupe de classification du contenu de l'utilisateur en fonction de son âge et de son niveau de maturité.

1 Ouvrez le volet Paramètres des utilisateurs.

Comment ?

1. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
2. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
3. Dans le volet Configuration du contrôle parental, cliquez sur **Avancé**.
4. Dans le volet Contrôle parental, cliquez sur **Paramètres des utilisateurs**.

2 Dans le volet Paramètres des utilisateurs, cliquez sur un nom d'utilisateur, puis sur **Modifier**.

3 Dans la fenêtre Modifier le compte utilisateur, sous **Contrôle d'accès au contenu**, cliquez sur la tranche d'âge à affecter à l'utilisateur.

Pour empêcher l'utilisateur d'accéder à tout site Web répertorié dans la liste **Sites Web filtrés**, activez la case **Cet utilisateur n'a accès qu'aux sites de la liste de sites Web filtrés**.

4 Cliquez sur **OK**.

Configuration des heures limites de navigation Web

Si vous craignez un usage irresponsable ou excessif d'Internet, vous pouvez définir des limites de temps appropriées pour la navigation Web de vos enfants. Lorsque vous limitez la navigation Web à des heures spécifiques pour vos enfants, vous pouvez être sûr que SecurityCenter les mettra en application, même si vous n'êtes pas à la maison.

Par défaut, un enfant est autorisé à naviguer sur le Web à n'importe quel moment du jour et de la nuit, tous les jours de la semaine ; vous pouvez cependant limiter la navigation Web à des heures ou jours spécifiques ou interdire totalement la navigation sur le Web. Si un entant tente de naviguer sur le Web à un moment où il n'y est pas autorisé, McAfee affiche un message le lui indiquant. Si vous interdisez totalement la navigation sur le Web, l'enfant peut se connecter et utiliser l'ordinateur, y compris d'autres programmes employant Internet comme le courrier électronique, la messagerie instantanée, ftp, les jeux, etc., mais il ne peut pas naviguer sur le Web.

Définir des heures limites de navigation Web

Vous pouvez utiliser la grille des heures limites de navigation Web pour limiter l'accès au Web d'un enfant à des jours et heures spécifiques.

1 Ouvrez le volet Paramètres des utilisateurs.

   Comment ?

   1. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
   2. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
   3. Dans le volet Configuration du contrôle parental, cliquez sur **Avancé**.
   4. Dans le volet Contrôle parental, cliquez sur **Paramètres des utilisateurs**.

2 Dans le volet Paramètres des utilisateurs, cliquez sur un nom d'utilisateur, puis sur **Modifier**.

3 Dans la fenêtre Modifier le compte utilisateur, sous **Périodes de connexion à Internet**, sélectionnez les jours et heures auxquels l'utilisateur ne peut pas naviguer sur le Web.

4 Cliquez sur **OK**.

Filtrage de sites Web

Vous pouvez filtrer (bloquer ou autoriser) des sites Web pour tous les utilisateurs à l'exception des membres du groupe Adulte. En bloquant un site Web, vous empêchez vos enfants d'y accéder lorsqu'ils naviguent sur le Web. Si un enfant tente d'accéder à un site Web bloqué, un message l'informe que l'accès à ce site est impossible car il est bloqué par McAfee.

Vous pouvez autoriser un site Web si McAfee l'a bloqué par défaut mais que vous voulez autoriser vos enfants à y accéder. Pour plus d'informations sur les sites Web bloqués par défaut par McAfee, consultez Filtrage de sites Web par mots clés (page 181). Vous pouvez aussi modifier ou supprimer à tout moment un site Web filtré.

Remarque : Les utilisateurs (y compris les administrateurs) membres du groupe Adulte peuvent accéder à tous les sites Web, même ceux qui ont été bloqués. Pour tester les sites Web bloqués, vous devez vous connecter en tant que non-adulte.

Blocage d'un site Web

En bloquant un site Web, vous empêchez vos enfants d'y accéder lorsqu'ils naviguent sur le Web. Si un enfant tente d'accéder à un site Web bloqué, un message l'informe que l'accès à ce site est impossible car il est bloqué par McAfee.

1 Ouvrez le volet Contrôle parental.

   Comment ?

   1. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
   2. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
   3. Dans le volet de configuration du contrôle parental, vérifiez que le contrôle parental est activé, puis cliquez sur **Avancé**.

2 Dans le volet Contrôle parental, cliquez sur **Sites Web filtrés**.

3 Dans le volet Sites Web filtrés, saisissez l'adresse d'un site Web dans le champ **http://**, puis cliquez sur **Bloquer**.

4 Cliquez sur **OK**.

Conseil : Vous pouvez bloquer un site Web précédemment autorisé en cliquant sur l'adresse du site Web dans la liste **Sites Web filtrés**, puis en cliquant sur **Bloquer**.

Autoriser un site Web

Vous pouvez autoriser un site Web pour être sûr qu'il n'est bloqué pour aucun utilisateur. Si vous autorisez un site Web que McAfee a bloqué par défaut, vous remplacez le réglage par défaut.

1 Ouvrez le volet Contrôle parental.

Comment ?

1. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
2. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
3. Dans le volet de configuration du contrôle parental, vérifiez que le contrôle parental est activé, puis cliquez sur **Avancé**.

2 Dans le volet Contrôle parental, cliquez sur **Sites Web filtrés**.

3 Dans le volet Sites Web filtrés, saisissez l'adresse d'un site Web dans le champ **http://**, puis cliquez sur **Autoriser**.

4 Cliquez sur **OK**.

Conseil : Vous pouvez autoriser un site Web précédemment bloqué en cliquant sur l'adresse du site Web dans la liste **Sites Web filtrés**, puis en cliquant sur **Autoriser**.

Mettre à jour un site Web filtré

Si l'adresse d'un site Web a changé ou si vous l'avez mal écrite lorsque vous l'avez bloquée ou autorisée, vous pouvez la modifier.

1 Ouvrez le volet Contrôle parental.

Comment ?

1. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
2. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
3. Dans le volet de configuration du contrôle parental, vérifiez que le contrôle parental est activé, puis cliquez sur **Avancé**.

2 Dans le volet Contrôle parental, cliquez sur **Sites Web filtrés**.

3 Dans le volet Sites Web filtrés, cliquez sur une entrée de la liste des **Sites Web filtrés**, modifiez l'adresse du site Web dans la zone **http://**, puis cliquez sur **Mettre à jour**.

4 Cliquez sur **OK**.

Supprimer un site Web filtré

Vous pouvez supprimer un site Web filtré si vous ne voulez plus le bloquer ou l'autoriser.

1. Ouvrez le volet Contrôle parental.

   Comment ?

   1. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
   2. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
   3. Dans le volet de configuration du contrôle parental, vérifiez que le contrôle parental est activé, puis cliquez sur **Avancé**.

2. Dans le volet Contrôle parental, cliquez sur **Sites Web filtrés**.
3. Dans le volet Sites Web filtrés, cliquez sur une entrée de la liste **Sites Web filtrés**, puis sur **Supprimer**.
4. Cliquez sur **OK**.

Filtrage de sites Web par mots clés

Le filtrage par mots clés permet d'empêcher les utilisateurs non adultes de visiter des sites Web qui contiennent des mots potentiellement inappropriés. Lorsque l'analyse par mots clés est activée, une liste par défaut de mots clés et de règles correspondantes permet de classer le contenu pour les utilisateurs en fonction de leur groupe de classification du contenu. Les utilisateurs doivent appartenir à une certaine tranche d'âge pour accéder à des sites Web qui contiennent des mots clés spécifiques. Par exemple, seuls les membres du groupe Adulte peuvent visiter les sites Web contenant le mot *porno* et seuls les membres du groupe Enfant (et plus âgés) peuvent visiter les sites Web contenant le mot *drogues*.

Vous pouvez aussi ajouter vos propres mots clés à la liste par défaut et les associer à certains groupes de classification du contenu. Les règles des mots clés que vous ajoutez remplacent celles éventuellement associées à un mot clé correspondant dans la liste par défaut.

Désactiver le filtrage par mots clés

Par défaut, le filtrage par mots clés est activé, ce qui signifie qu'une liste par défaut de mots clés et de règles correspondantes est utilisée pour classer le contenu pour les utilisateurs en fonction de leur groupe de classification du contenu. Bien que McAfee ne le recommande pas, vous pouvez désactiver le filtrage par mots clés à tout moment.

1 Ouvrez le volet Contrôle parental.

   Comment ?

   1. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
   2. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
   3. Dans le volet de configuration du contrôle parental, vérifiez que le contrôle parental est activé, puis cliquez sur **Avancé**.

2 Dans le volet Contrôle parental, cliquez sur **Mots clés**.

3 Dans le volet Mots clés, cliquez sur **Désactiver**.

4 Cliquez sur **OK**.

Blocage de sites Web en fonction de mots clés

Si vous voulez bloquer des sites Web en raison d'un contenu inapproprié mais que vous n'en connaissez pas l'adresse spécifique, vous pouvez les bloquer d'après des mots clés. Il suffit de saisir un mot clé, puis de déterminer quels groupes de classification du contenu peuvent afficher des sites Web qui contiennent ce mot clé.

1 Ouvrez le volet Contrôle parental.

Comment ?

1. Dans le volet Accueil de SecurityCenter, cliquez sur **Contrôle parental**.
2. Dans la section d'informations sur le contrôle parental, cliquez sur **Configurer**.
3. Dans le volet de configuration du contrôle parental, vérifiez que le contrôle parental est activé, puis cliquez sur **Avancé**.

2 Dans le volet Contrôle parental, cliquez sur **Mots clés** et vérifiez que le filtrage par mots clés est activé.

3 Sous **Liste de mots clés**, tapez un mot clé dans la zone **Rechercher**.

4 Faites glisser le curseur **Age minimum** afin de spécifier une tranche d'âge minimum.
Les utilisateurs de cette tranche d'âge ou plus âgés peuvent visiter les sites Web qui contiennent ce mot clé.

5 Cliquez sur **OK**.

CHAPITRE 32

Protection d'informations sur le Web

Vous pouvez protéger vos informations privées et fichiers confidentiels lorsque vous naviguez sur le Web en bloquant certaines informations. Par exemple, vous pouvez empêcher que vos informations personnelles (comme votre nom, votre adresse, votre numéro de carte de crédit ou de compte bancaire) soient transmises sur le Web en les ajoutant à la zone des informations bloquées.

Remarque : Privacy Service n'empêche pas la transmission d'informations personnelles sur des sites Web sécurisés (sites utilisant le protocole https://), comme des sites bancaires.

Contenu de ce chapitre

Protection des informations personnelles 184

Protection des informations personnelles

Empêchez la transmission de vos informations personnelles (comme votre nom, votre adresse, votre numéro de carte de crédit ou de compte bancaire) sur le Web en bloquant ces informations. Si McAfee détecte des informations personnelles dans des données (par exemple, un champ de formulaire ou un fichier) sur le point d'être envoyées via le Web, deux cas de figure peuvent se présenter.

- Si vous êtes connecté en tant qu'administrateur, vous devez confirmer ou non l'envoi des informations.
- Si vous n'êtes pas administrateur, la partie bloquée est remplacée par des astérisques (*). Par exemple, si un site Web malveillant tente d'envoyer votre numéro de carte de crédit à un autre ordinateur, le numéro lui-même est remplacé par des astérisques.

Protéger les informations personnelles

Vous pouvez bloquer les types d'informations personnelles suivantes : nom, adresse, code postal, numéro de sécurité sociale, numéro de téléphone, numéro de carte de crédit, comptes bancaires, comptes de courtage et cartes téléphoniques. Si vous voulez bloquer des informations personnelles d'un autre type, vous pouvez définir le type sur **autre**.

1 Ouvrez le volet Informations protégées.

   Comment ?

   1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
   2. Dans le volet Accueil de SecurityCenter, cliquez sur **Réseau & Internet**.
   3. Dans la section d'informations relatives à Internet et au réseau, cliquez sur **Configurer**.
   4. Dans le volet d'Internet et de configuration réseau, vérifiez que la protection des informations personnelles est activée, puis cliquez sur **Avancé**.

2 Dans le volet Informations protégées, cliquez sur **Ajouter**.

3 Sélectionnez le type d'information à bloquer dans la liste.

4 Saisissez vos informations personnelles, puis cliquez sur **OK**.

CHAPITRE 33

Protection des mots de passe

Password Vault est une zone de stockage sécurisée pour vos mots de passe personnels. Il permet de stocker des mots de passe en sécurité de sorte qu'aucun autre utilisateur (pas même un administrateur) ne puisse y accéder.

Contenu de ce chapitre

Configuration de Password Vault 186

Configuration de Password Vault

Pour pouvoir utiliser Password Vault, vous devez commencer par configurer un mot de passe pour Password Vault. Seuls les utilisateurs qui connaissent ce mot de passe peuvent accéder à Password Vault. Si vous oubliez votre mot de passe Password Vault, vous pouvez le réinitialiser. Notez toutefois que, dans ce cas, tous les mots de passe précédemment enregistrés dans Password Vault sont supprimés.

Une fois que vous avez configuré votre mot de passe Password Vault, vous pouvez y ajouter, modifier et supprimer des mots de passe. Vous pouvez aussi modifier votre mot de passe Password Vault à tout moment.

Ajouter un mot de passe

Si vous avez des problèmes à vous souvenir des mots de passe, vous pouvez les ajouter dans Password Vault. Password Vault est un endroit sécurisé auquel n'ont accès que les utilisateurs qui connaissent votre mot de passe Password Vault.

1 Ouvrez le volet Password Vault.

   Comment ?

   1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
   2. Dans le volet Accueil de SecurityCenter, cliquez sur **Réseau & Internet**.
   3. Dans la section d'informations relatives à Internet et au réseau, cliquez sur **Configurer**.
   4. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé** sous **Password Vault**.

2 Saisissez votre mot de passe Password Vault dans la zone de texte **Mot de passe**, puis saisissez-le à nouveau dans la zone **Confirmer le mot de passe**.

3 Cliquez sur **Ouvrir**.

4 Dans le volet Gérer Password Vault, cliquez sur **Ajouter**.

5 Saisissez une description du mot de passe (par exemple, sa fonction) dans la zone de texte **Description**, puis saisissez le mot de passe dans la zone de texte **Mot de passe**.

6 Cliquez sur **OK**.

Modifier un mot de passe

Pour garantir que les entrées de Password Vault sont fiables et à jour, vous devez les mettre à jour lorsque les mots de passe changent.

1 Ouvrez le volet Password Vault.

   Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Réseau & Internet**.
3. Dans la section d'informations relatives à Internet et au réseau, cliquez sur **Configurer**.
4. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé** sous **Password Vault**.

2 Saisissez votre mot de passe Password Vault dans le champ **Mot de passe**.

3 Cliquez sur **Ouvrir**.

4 Dans le volet Gérer Password Vault, cliquez sur une entrée de mot de passe, puis sur **Modifier**.

5 Modifiez la description du mot de passe (par exemple, sa fonction) dans la zone de texte **Description** ou modifiez le mot de passe dans la zone de texte **Mot de passe**.

6 Cliquez sur **OK**.

Supprimer un mot de passe

Vous pouvez supprimer un mot de passe Password Vault à tout moment. Il est impossible de récupérer un mot de passe supprimé.

1 Ouvrez le volet Password Vault.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Réseau & Internet**.
3. Dans la section d'informations relatives à Internet et au réseau, cliquez sur **Configurer**.
4. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé** sous **Password Vault**.

2 Saisissez votre mot de passe Password Vault dans le champ **Mot de passe**.

3 Cliquez sur **Ouvrir**.

4 Dans le volet Gérer Password Vault, cliquez sur une entrée de mot de passe, puis sur **Supprimer**.

5 Cliquez sur **Oui** dans la boîte de dialogue Confirmation de suppression.

Modifier le mot de passe Password Vault

Vous pouvez modifier votre mot de passe Password Vault à tout moment.

1 Ouvrez le volet Password Vault.

   Comment ?

   1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
   2. Dans le volet Accueil de SecurityCenter, cliquez sur **Réseau & Internet**.
   3. Dans la section d'informations relatives à Internet et au réseau, cliquez sur **Configurer**.
   4. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé** sous **Password Vault**.

2 Dans le volet Password Vault, saisissez le mot de passe actuel dans la zone **Mot de passe**, puis cliquez sur **Ouvrir**.

3 Dans le volet Gérer Password Vault, cliquez sur **Modifier le mot de passe**.

4 Entrez un nouveau mot de passe dans la zone **Choisir un mot de passe**, puis saisissez-le à nouveau dans la zone **Confirmer le mot de passe**.

5 Cliquez sur **OK**.

6 Dans la boîte de dialogue Le mot de passe de Password Vault a été modifié, cliquez sur **OK**.

Réinitialiser le mot de passe Password Vault

Si vous oubliez votre mot de passe Password Vault, vous pouvez le réinitialiser. Notez toutefois que, dans ce cas, tous les mots de passe précédemment enregistrés dans Password Vault sont supprimés.

1 Ouvrez le volet Password Vault.

   Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Réseau & Internet**.
3. Dans la section d'informations relatives à Internet et au réseau, cliquez sur **Configurer**.
4. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé** sous **Password Vault**.

2 Sous **Réinitialiser Password Vault**, saisissez un nouveau mot de passe dans la zone **Mot de passe**, puis saisissez-le à nouveau dans la zone **Confirmer le mot de passe**.

3 Cliquez sur **Rétablir**.

4 Cliquez sur **Oui** dans la boîte de dialogue Confirmation de la réinitialisation du mot de passe.

CHAPITRE 34

McAfee Data Backup

Grâce à Data Backup, plus de perte accidentelle de données avec l'archivage des fichiers sur un CD, un DVD, une clé USB, un disque dur externe ou un lecteur réseau. L'archivage local permet d'archiver (sauvegarder) vos données personnelles sur CD, DVD, lecteur USB, disque dur externe ou disque réseau. En cas de perte accidentelle, vous possédez ainsi une copie locale de vos enregistrements, documents et autres données importantes.

Avant de commencer à utiliser Data Backup, vous pouvez vous familiariser avec ses fonctions les plus importantes. Pour en savoir plus sur la configuration et l'utilisation de ces fonctions, consultez l'aide de Data Backup. Après avoir parcouru les fonctions du programme, vérifiez que vous disposez de supports d'archivage adéquats prêts pour l'exécution d'archives locales.

Contenu de ce chapitre

Caractéristiques 192
Archivage de fichiers 193
Utilisation des fichiers archivés 201

Caractéristiques

Data Backup propose les fonctionnalités suivantes pour enregistrer et restaurer vos photos, fichiers audio et autres fichiers importants.

Archivage prévu en local

Protégez vos données en archivant vos fichiers et dossiers sur un lecteur CD, DVD, USB, un disque dur externe ou un lecteur réseau. Une fois que vous avez effectué une première opération d'archivage, l'archivage incrémentiel se fait automatiquement.

Restauration d'un simple clic de souris

Si des fichiers et des dossiers sont supprimés de votre ordinateur ou corrompus par erreur, vous pourrez restaurer les dernières versions archivées à partir du support d'archivage utilisé.

Compression et chiffrement

Par défaut, vos fichiers archivés sont compressés, ce qui permet d'économiser de l'espace sur votre support d'archivage. Par mesure de sécurité supplémentaire, vos archives sont chiffrées par défaut.

CHAPITRE 35

Archivage de fichiers

Vous pouvez utiliser McAfee Data Backup pour archiver une copie de vos fichiers sur un CD, un DVD, une clé USB, un disque dur externe ou un lecteur réseau. Ce type d'archivage facilite la récupération d'informations en cas de pertes ou de dommages accidentels.

Avant de commencer à archiver vos fichiers, vous devez choisir leur emplacement d'archivage par défaut (CD, DVD, clé USB, disque dur externe ou lecteur réseau). McAfee a présélectionné d'autres paramètres, comme les dossiers et types de fichiers à archiver, que vous pouvez toutefois modifier.

Après avoir défini les options d'archivage local, vous pouvez modifier la fréquence par défaut à laquelle Data Backup exécute des archivages rapides ou complets. Vous pouvez également lancer des archivages manuels à tout moment.

Contenu de ce chapitre

Réglage des options d'archivage 194
Lancement d'archivages complets et rapides 199

Réglage des options d'archivage

Avant de commencer à archiver vos données, vous devez définir quelques options d'archives locales. Par exemple, vous devez configurer les types de fichiers de surveillance et d'emplacements surveillés. Les emplacements surveillés sont les dossiers sur votre ordinateur dans lesquels Data Backup surveille l'apparition de nouveaux fichiers ou les changements de fichiers. Les types de fichiers de surveillance sont les types de fichiers (par exemple, .doc, .xls, etc.) que Data Backup archive dans les emplacements surveillés. Par défaut, Data Backup surveille tous les types de fichiers mémorisés dans vos emplacements surveillés.

Vous pouvez définir deux types d'emplacements surveillés : des emplacements de surveillance approfondie et des emplacements de surveillance de premier niveau. Si vous définissez un emplacement de surveillance approfondie, Data Backup archive les types de fichiers de surveillance dans ce dossier ou ses sous-dossiers. Si vous définissez un emplacement surveillé de premier niveau, Data Backup archive les types de fichiers de surveillance dans ce dossier uniquement (non ses sous-dossiers). Vous pouvez aussi identifier les emplacements que vous voulez exclure des archives locales. Par défaut, les emplacements Windows Poste de travail ou Mes documents sont configurés comme emplacements de surveillance approfondie.

Après avoir configuré les types et les emplacements de fichiers de surveillance, vous devez configurer l'emplacement d'archivage (le CD, le DVD, la clé USB, le disque dur externe ou le lecteur réseau où les données archivées seront mémorisées). Vous pouvez changer l'emplacement d'archivage à tout moment.

Pour des raisons de sécurité ou des questions de taille, le chiffrement ou la compression sont activés par défaut pour vos fichiers archivés. Le contenu des fichiers chiffrés est transformé de texte à code, masquant les informations qui deviennent illisibles pour les personnes qui ne savent pas les déchiffrer. Les fichiers comprimés sont comprimés sous une forme qui minimise l'espace requis pour les stocker ou les transmettre. Bien que McAfee le déconseille, vous pouvez désactiver le chiffrement ou la compression à tout moment.

Inclusion d'un emplacement dans les archives

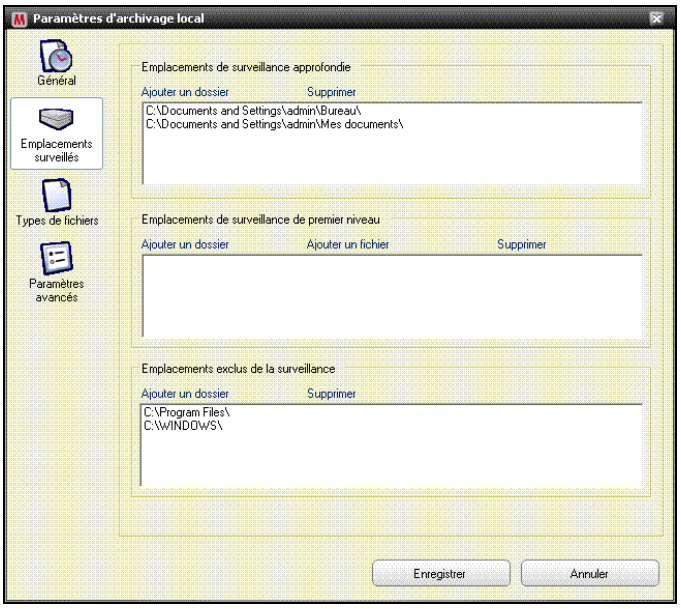
Vous pouvez définir deux types d'emplacements surveillés pour l'archivage : approfondi et de surface. Si vous configurez un emplacement de surveillance approfondie, Data Backup surveille les changements apportés au dossier et à ses sous-dossiers. Si vous configurez un emplacement de surveillance de premier niveau, Data Backup surveille le contenu du dossier uniquement, et ne surveille pas ses sous-dossiers.

Pour inclure un emplacement dans l'archive :

1 Cliquez sur l'onglet **Archives locales**.

2 Dans le volet gauche, cliquez sur **Paramètres**.

3 Dans la boîte de dialogue Paramètres d'archivage local, cliquez sur **Emplacements surveillés**.



4 Effectuez l'une des opérations suivantes :

- Pour archiver le contenu d'un dossier, sous-dossiers compris, cliquez sur **Ajouter un dossier** sous **Emplacements de surveillance approfondie**.
- Pour archiver le contenu d'un dossier, sans inclure les sous-dossiers, cliquez sur **Ajouter un dossier** sous **Emplacements de surveillance de premier niveau**.

5 Dans la boîte de dialogue de recherche d'un dossier, naviguez jusqu'au dossier à surveiller, puis cliquez sur **OK**.

6 Cliquez sur **Enregistrer**.

Conseil : pour que Data Backup surveille un dossier qui n'a pas encore été créé, cliquez sur **Créer un dossier** dans la boîte de dialogue de recherche d'un dossier. Le dossier est simultanément créé et paramétré comme emplacement de surveillance.

Définition des types de fichiers archivés

Vous pouvez spécifier les types de fichiers qui seront archivés dans vos emplacements de surveillance approfondie ou de premier niveau. Vous pouvez choisir dans une liste existante de types de fichiers ou ajouter un nouveau type à la liste.

Pour définir les types de fichiers archivés :

1. Cliquez sur l'onglet **Archives locales**.
2. Dans le volet gauche, cliquez sur **Paramètres**.
3. Dans la boîte de dialogue Paramètres d'archives locales, cliquez sur **Types de fichiers**.
4. Développez les listes de types de fichiers et cochez les cases en regard des types de fichiers que vous voulez archiver.
5. Cliquez sur **Enregistrer**.

Conseil : pour ajouter un nouveau type de fichier dans la liste **Types de fichiers sélectionnés**, saisissez l'extension de fichier dans la zone **Ajouter un type de fichier personnalisé à la liste Autres**, puis cliquez sur **Ajouter**. Le nouveau type de fichier devient automatiquement un type de fichier de surveillance.

Exclusion d'un emplacement des archives

L'exclusion d'un emplacement permet d'empêcher l'archivage de cet emplacement (ce dossier) et de son contenu.

Pour exclure un emplacement des archives :

1. Cliquez sur l'onglet **Archives locales**.
2. Dans le volet gauche, cliquez sur **Paramètres**.
3. Dans la boîte de dialogue Paramètres d'archivage local, cliquez sur **Dossiers surveillés**.
4. Sous **Emplacements exclus de la surveillance**, cliquez sur **Ajouter un dossier**.
5. Dans la boîte de dialogue de recherche d'un dossier, naviguez jusqu'au dossier à exclure, sélectionnez-le et cliquez sur **OK**.
6. Cliquez sur **Enregistrer**.

Conseil : pour que Data Backup exclue un dossier qui n'a pas encore été créé, cliquez sur **Créer un dossier** dans la boîte de dialogue de recherche d'un dossier. Le dossier est simultanément créé et exclu.

Modification de l'emplacement d'archivage

Lorsque vous modifiez l'emplacement de l'archivage, les fichiers précédemment archivés à un autre endroit sont recensés comme *Jamais archivé*.

Pour modifier l'emplacement d'archivage :

1. Cliquez sur l'onglet **Archives locales**.
2. Dans le volet gauche, cliquez sur **Paramètres**.
3. Cliquez sur **Changer d'emplacement d'archivage**.
4. Dans la boîte de dialogue Emplacement d'archivage, sélectionnez l'une des options suivantes :
   - Cliquez sur **Sélectionner le lecteur de CD/DVD**, cliquez sur le lecteur de CD ou de DVD de votre ordinateur dans la liste **Lecteur**, puis sur **Enregistrer**.
   - Cliquez sur **Sélectionner un emplacement de lecteur**, naviguez jusqu'à un lecteur USB, un disque local ou un disque dur externe, sélectionnez-le, puis cliquez sur **OK**.
   - Cliquez sur **Sélectionner un emplacement réseau**, naviguez jusqu'à un dossier réseau, sélectionnez-le, puis cliquez sur **OK**.
5. Vérifiez le nouvel emplacement d'archivage sous **Emplacement d'archivage sélectionné**, puis cliquez sur **OK**.
6. Dans la boîte de dialogue de confirmation, cliquez sur **OK**.
7. Cliquez sur **Enregistrer**.

Désactivation du chiffrement et la compression des archives

Le chiffrement des fichiers archivés permet d'assurer la confidentialité de vos informations en masquant le contenu des fichiers qui deviennent illisibles. La compression des fichiers archivés, quant à elle, permet de réduire leur taille. Le chiffrement et la compression sont activés par défaut, mais vous pouvez les désactiver à tout moment.

Pour désactiver le chiffrement et la compression des archives :

1. Cliquez sur l'onglet **Archives locales**.
2. Dans le volet gauche, cliquez sur **Paramètres**.
3. Dans la boîte de dialogue Paramètres d'archivage local, cliquez sur **Paramètres avancés**.
4. Annulez la sélection de la case **Activer le chiffrement pour améliorer la sécurité**.
5. Annulez la sélection de la case **Activer la compression pour réduire le volume des données à stocker**.
6. Cliquez sur **Enregistrer**.

Remarque : McAfee recommande de ne pas désactiver le chiffrement ou la compression lors de l'archivage des fichiers.

Lancement d'archivages complets et rapides

Vous pouvez lancer deux types d'archivages : complet ou rapide. Lorsque vous lancez un archivage complet, vous archivez un jeu complet de données en fonction des types et des emplacements de fichiers surveillés que vous avez configurés. Lorsque vous lancez un archivage rapide, vous n'archivez que les fichiers qui ont changé depuis le dernier archivage rapide ou complet.

Par défaut, Data Backup est programmé pour lancer un archivage complet des types de fichiers surveillés dans vos emplacements surveillés tous les lundis à 9 heures et un archivage rapide toutes les 48 heures après le dernier archivage complet ou rapide. Cette planification assure une sauvegarde actualisée de vos fichiers à tout moment. Toutefois, si vous ne voulez pas archiver toutes les 48 heures, vous pouvez configurer le programme pour l'adapter à vos besoins.

Si vous voulez archiver le contenu de vos emplacements surveillés sur demande, vous pouvez le faire à tout moment. Par exemple, si vous modifiez un fichier que vous voulez archiver, mais si Data Backup n'est configuré que pour lancer un archivage rapide au bout de plusieurs heures, vous pouvez archiver manuellement ce fichier. Lorsque vous archivez manuellement les fichiers, l'intervalle que vous aviez défini pour les archivages automatiques est redéfini.

Vous pouvez aussi interrompre un archivage automatique ou manuel s'il intervient à un moment qui ne vous convient pas. Par exemple, si vous effectuez une tâche gourmande en ressources et si un archivage automatique démarre, vous pouvez l'arrêter. Lorsque vous arrêtez un archivage automatique, l'intervalle que vous aviez défini pour les archivages automatiques est redéfini.

Planification d'archivages automatiques

Vous pouvez régler la fréquence des archivages rapides et complets pour garantir la protection constante de vos données.

Pour planifier des archivages automatiques :

1. Cliquez sur l'onglet **Archives locales**.
2. Dans le volet gauche, cliquez sur **Paramètres**.
3. Dans la boîte de dialogue Paramètres d'archives locales, cliquez sur **Général**.
4. Pour lancer un archivage complet chaque jour, semaine ou mois, cliquez sur une des options suivantes sous **Fréquence de l'archivage complet** :
   - **Jours**
   - **Semaines**

- **Mois**

5 Cochez la case à côté du jour où vous voulez lancer l'archivage complet.

6 Cliquez sur une valeur dans la liste **A** pour spécifier l'heure à laquelle vous voulez lancer l'archivage complet.

7 Pour lancer un archivage rapide tous les jours ou toutes les heures, cliquez sur une des options suivantes dans **Archivage rapide** :

- **Heures**
- **Jours**

8 Saisissez un nombre représentant la fréquence dans la zone **Fréquence de l'archivage rapide**.

9 Cliquez sur **Enregistrer**.

Interruption d'un archivage automatique

Data Backup archive automatiquement les fichiers dans vos emplacements surveillés en fonction du programme que vous définissez. Vous pouvez toutefois interrompre à tout moment un archivage automatique en cours.

Pour interrompre un archivage automatique :

1 Dans le volet de gauche, cliquez sur **Arrêter l'archivage**.

2 Cliquez sur **Oui** dans la boîte de dialogue de confirmation.

Remarque : le lien **Arrêter l'archivage** n'apparaît qu'au cours d'une opération d'archivage.

Lancement manuel de l'archivage

Des archivages automatiques s'exécutent selon un programme prédéfini, mais vous pouvez aussi à tout moment lancer un archivage rapide ou complet. Un archivage rapide n'archive que les fichiers qui ont changé depuis le dernier archivage rapide ou complet. Un archivage complet archive les types de fichiers surveillés dans tous les emplacements surveillés.

Pour lancer manuellement un archivage rapide ou complet :

1 Cliquez sur l'onglet **Archives locales**.

2 Pour lancer un archivage rapide, cliquez sur **Archivage rapide** dans le volet de gauche.

3 Pour lancer un archivage complet, cliquez sur **Archivage complet** dans le volet de gauche.

4 Dans la boîte de dialogue Prêt à commencer l'archivage, vérifiez votre espace et vos paramètres de stockage, puis cliquez sur **Continuer**.

CHAPITRE 36

Utilisation des fichiers archivés

Lorsque vous avez archivé des fichiers, vous pouvez utiliser Data Backup pour travailler avec eux. Vos fichiers archivés sont présentés dans un affichage explorateur traditionnel qui permet de les repérer facilement. Au fur et à mesure de l'extension de votre archive, vous voudrez sûrement trier les fichiers ou les rechercher. Vous pouvez aussi ouvrir des fichiers directement dans la vue explorateur pour en examiner le contenu sans avoir à les récupérer.

Vous récupérez les fichiers d'une archive si votre copie locale du fichier est périmée ou manquante, ou si elle a été corrompue. Data Backup vous fournit aussi les informations dont vous avez besoin pour gérer vos archives locales et vos supports de stockage.

Contenu de ce chapitre

Utilisation de l'explorateur d'archives locales 202
Restauration de fichiers archivés 204
Gestion des archives 206

Utilisation de l'explorateur d'archives locales

L'explorateur d'archives locales permet d'afficher et de manipuler les fichiers que vous voulez archiver localement. Vous pouvez afficher le nom de chaque ficher, le type, l'emplacement, l'état (archivé, non archivé ou archive en cours) et la date à laquelle chaque fichier a été archivé pour la dernière fois. Vous pouvez aussi trier les fichiers selon un de ces critères.

Si vous disposez d'un archivage important, vous pouvez trouver rapidement un fichier en le recherchant. Vous pouvez rechercher tout ou partie du nom ou du chemin du fichier, puis affiner votre recherche en précisant la taille de fichier approximative et la date à laquelle il a été archivé pour la dernière fois.

Lorsque vous avez repéré un fichier, vous pouvez l'ouvrir directement dans l'explorateur d'archives locales. Data Backup ouvre le fichier dans son programme natif, ce qui permet d'effectuer des changements sans quitter l'explorateur d'archives locales. Le fichier est enregistré dans son emplacement surveillé original sur votre ordinateur et est archivé automatiquement selon le programme d'archivage que vous aurez défini.

Tri des fichiers archivés

Vous pouvez trier vos fichiers et dossiers archivés selon les critères suivants : nom, type de fichier, taille, état (archivé, non archivé, ou archive en cours), la date à laquelle les fichiers ont été archivés pour la dernière fois ou l'emplacement des fichiers sur votre ordinateur (chemin).

Pour trier les fichiers archivés :

1. Cliquez sur l'onglet **Archives locales**.
2. Dans le volet droit, cliquez sur un nom de colonne.

Recherche d'un fichier archivé

Si vous disposez d'un référentiel important de fichiers archivés, vous pouvez trouver rapidement un fichier en le recherchant. Vous pouvez rechercher tout ou partie du nom ou du chemin du fichier, puis affiner votre recherche en précisant la taille de fichier approximative et la date à laquelle il a été archivé pour la dernière fois.

Pour rechercher un fichier archivé :

1. Saisissez tout ou partie du nom du fichier dans la zone **Recherche** en haut de l'écran, puis appuyez sur la touche Entrée.
2. Saisissez tout ou partie du chemin dans la boîte **Tout ou partie du chemin**.
3. Spécifiez la taille approximative du fichier que vous recherchez en effectuant l'une des procédures suivantes :
   - Cliquez sur **<100 Ko**, **<1 Mo** ou **>1 Mo**.
   - Cliquez sur **Taille en Ko**, puis indiquez les valeurs de taille appropriées dans les champs correspondants.
4. Spécifiez la date approximative de la dernière sauvegarde en ligne du fichier en effectuant l'une des procédures suivantes :
   - Cliquez sur **Cette semaine**, **Ce mois** ou **Cette année**.
   - Cliquez sur **Spécifier dates**, sur **Archivés** dans la liste, puis sur les valeurs de date appropriées dans les listes de dates.
5. Cliquez sur **Rechercher**.

Remarque : si vous ne connaissez pas la taille approximative ou la date du dernier archivage, cliquez sur **Inconnu**.

Ouvrir un fichier archivé

Vous pouvez consulter le contenu d'un fichier archivé en l'ouvrant directement dans l'explorateur d'archivage local.

Pour ouvrir un fichier archivé :

1. Cliquez sur l'onglet **Archives locales**.
2. Dans le volet de droite, cliquez sur le nom d'un fichier, puis sur **Ouvrir**.

Conseil : pour ouvrir un fichier archivé, vous pouvez également double-cliquer sur son nom.

Restauration de fichiers archivés

En cas d'endommagement, d'absence ou de suppression malencontreuse d'un fichier surveillé, vous pouvez en restaurer une copie à partir de l'archive locale. Il est donc important d'archiver régulièrement vos fichiers. Vous pouvez également restaurer d'anciennes versions d'un fichier à partir des archives locales. Si, par exemple, vous archivez régulièrement un fichier sans souhaiter remonter à une version précédente, vous pouvez le faire en localisant le fichier à l'emplacement d'archivage. Si l'emplacement d'archivage est un disque local ou réseau, vous pouvez naviguer jusqu'au fichier. S'il s'agit d'un disque dur externe ou d'une clé USB, vous devez connecter ce périphérique à l'ordinateur, puis rechercher le fichier. Si l'emplacement est un CD ou un DVD, vous devez l'insérer dans l'ordinateur, puis naviguer jusqu'au fichier.

Vous pouvez également restaurer les fichiers archivés sur un ordinateur à partir d'un autre ordinateur. Ainsi, si vous archivez un ensemble de fichiers sur le disque dur externe d'un ordinateur A, vous pouvez restaurer ces fichiers sur un ordinateur B. Pour ce faire, installez McAfee Data Backup sur l'ordinateur B et connectez le disque dur externe. Dans Data Backup, recherchez ensuite les fichiers, qui sont ajoutés à la liste **Fichiers manquants** à des fins de restauration.

Pour plus d'informations sur l'archivage des fichiers, reportez-vous à la rubrique Archivage de fichiers. Si vous supprimez intentionnellement un fichier surveillé de vos archives, vous pouvez aussi effacer son entrée de la liste des **fichiers manquants**.

Restauration des fichiers manquants à partir d'une archive locale

L'archive locale de Data Backup permet de récupérer des données manquantes dans un dossier de surveillance sur votre ordinateur local. Ainsi, par exemple, si un fichier est retiré d'un dossier de surveillance ou supprimé et s'il a déjà été archivé, vous pouvez le restaurer à partir de l'archive locale.

Pour récupérer un fichier manquant à partir d'une archive locale :

1. Cliquez sur l'onglet **Archives locales**.
2. Dans l'onglet **Fichiers manquants** au bas de l'écran, cochez la case en regard du nom du fichier à restaurer.
3. Cliquez sur **Restaurer**.

Conseil : pour restaurer tous les fichiers de la liste **Fichiers manquants**, vous pouvez également cliquer sur **Tout restaurer**.

Restauration d'une ancienne version d'un fichier à partir des archives locales

Pour restaurer une ancienne version d'un fichier archivé, recherchez-le et ajoutez-le à la liste **Fichiers manquants**. Vous pouvez ensuite restaurer le fichier, comme pour tout autre fichier de la liste **Fichiers manquants**.

Pour restaurer une ancienne version d'un fichier à partir des archives locales :

1. Cliquez sur l'onglet **Archives locales**.
2. Dans l'onglet **Fichiers manquants** au bas de l'écran, cliquez sur **Parcourir**, puis accédez à l'emplacement de stockage de l'archive.

   Les noms de dossiers archivés ont le format suivant : `cre jjmmaa_hh-mm-ss_***`, où `jjmmaa` correspond à la date d'archivage des fichiers, `hh-mm-ss` correspond à l'heure d'archivage des fichiers et `***` correspond à `Complet` ou à `Inc`, selon si l'archivage a été rapide ou complet.
3. Sélectionnez l'emplacement, puis cliquez sur **OK**.

   Les fichiers contenus à l'emplacement sélectionné apparaissent dans la liste **Fichiers manquants** ; ils sont prêts à être restaurés. Pour en savoir plus, reportez-vous à Restauration des fichiers manquants à partir d'une archive locale.

Supprimer les fichiers de la liste des fichiers manquants

Lorsqu'un fichier archivé est retiré d'un dossier surveillé ou effacé, il apparaît automatiquement dans la liste **Fichiers manquants**. Vous êtes ainsi averti qu'il existe une incohérence entre les fichiers archivés et les fichiers contenus dans les dossiers surveillés. Si le fichier a été intentionnellement retiré du dossier surveillé ou supprimé, vous pouvez l'effacer de la liste **Fichiers manquants**.

Pour supprimer un fichier de la liste des fichiers manquants :

1. Cliquez sur l'onglet **Archives locales**.
2. Dans l'onglet **Fichiers manquants** au bas de l'écran, cochez la case en regard du nom du fichier à supprimer.
3. Cliquez sur **Supprimer**.

Conseil : pour supprimer tous les fichiers de la liste **Fichiers manquants**, vous pouvez également cliquer sur **Supprimer tout**.

Gestion des archives

Vous pouvez consulter un résumé de vos archives complètes et rapides à tout moment. Vous pouvez par exemple connaître la quantité de données surveillées, de données archivées et de données actuellement surveillées mais non encore archivées. Vous pouvez également parcourir votre programme d'archivage et obtenir la date de la dernière archive et des prochaines.

Afficher un résumé de votre activité d'archivage

Vous pouvez à tout moment afficher des informations sur votre activité d'archivage. Par exemple, vous pouvez afficher le pourcentage de fichiers que vous avez archivé, la taille des données surveillées, la taille des données qui ont été archivées et la taille des données qui sont surveillées mais qui n'ont pas encore été archivées. Vous pouvez aussi afficher les dates à laquelle les dernières archives et les archives suivantes sont intervenues.

Pour afficher un résumé de votre activité de sauvegarde :

1. Cliquez sur l'onglet **Archives locales**.
2. En haut de l'écran, cliquez sur **Résumé du compte**.

CHAPITRE 37

McAfee QuickClean

QuickClean améliore les performances de votre ordinateur en supprimant des fichiers qui peuvent l'encombrer. Il vide votre Corbeille et supprime les fichiers temporaires, raccourcis, fragments de fichiers perdus, fichiers de registre, fichiers en mémoire cache, cookies, fichiers d'historique du navigateur, messages envoyés et supprimés, fichiers récemment utilisés, fichiers Active-X et fichiers de point de restauration système. QuickClean protège également votre confidentialité en utilisant le composant McAfee Shredder pour supprimer en toute sécurité et de manière définitive des éléments pouvant contenir des informations personnelles confidentielles telles que vos nom et adresse. Pour des informations sur le broyage de fichiers, voir McAfee Shredder.

Defragmenteur de disques organise les fichiers et dossiers de votre ordinateur de manière à éviter leur éparpillement (fragmentation) lors de leur enregistrement sur le disque dur de votre ordinateur. En défragmentant périodiquement votre disque dur, vous garantissez le regroupement des fichiers et dossiers fragmentés, ce qui permet de les récupérer plus rapidement ensuite.

Si vous ne souhaitez pas effectuer manuellement la maintenant de votre ordinateur, vous pouvez demander l'exécution automatique programmée de QuickClean et Défragmenteur de disques, indépendamment et à la fréquence de votre choix.

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctions de QuickClean 208
Nettoyage de votre ordinateur 209
Défragmentation de votre ordinateur 212
Programmation d'une tâche 213

Fonctions de QuickClean

QuickClean fournit différents outils de nettoyage qui suppriment les fichiers inutiles de manière sûre et efficace. En supprimant ces fichiers, vous augmentez l'espace disponible sur le disque dur de votre ordinateur et en améliorez les performances.

Nettoyage de votre ordinateur

QuickClean supprime les fichiers susceptibles d'encombrer votre ordinateur. Il vide votre Corbeille et supprime les fichiers temporaires, raccourcis, fragments de fichiers perdus, fichiers de registre, fichiers en mémoire cache, cookies, fichiers d'historique du navigateur, messages envoyés et supprimés, fichiers récemment utilisés, fichiers Active-X et fichiers de point de restauration système. QuickClean supprime ces éléments sans toucher aux autres informations essentielles.

Vous pouvez utiliser les nettoyeurs de QuickClean pour supprimer des fichiers inutiles de votre ordinateur. Le tableau suivant décrit les nettoyeurs QuickClean :

Nom	Fonction
Nettoyeur de la Corbeille	supprime les fichiers contenus dans la Corbeille.
Nettoyeur de fichiers temporaires	supprime les fichiers stockés dans des dossiers temporaires.
Nettoyeur de raccourcis	supprime les raccourcis inutilisables et les raccourcis auxquels aucun programme n'est associé.
Nettoyeur de fragments de fichiers perdus	supprime de l'ordinateur les fragments de fichiers perdus.
Nettoyeur du registre	supprime du registre Windows® les informations correspondant à des programmes désormais inexistants. Le registre est une base de données dans laquelle Windows stocke ses données de configuration. Il contient des profils pour chaque utilisateur de l'ordinateur ainsi que des informations sur le matériel du système, les programmes installés et les paramètres des propriétés. Windows se réfère continuellement à ces informations en cours de travail.
Nettoyeur du cache	supprime les fichiers mis en cache qui s'accumulent lorsque vous naviguez sur des pages Web. Ces fichiers sont habituellement des fichiers temporaires stockés dans un dossier cache. Un dossier cache est une zone de stockage temporaire de votre ordinateur. Pour augmenter la vitesse et l'efficacité de la navigation sur le Web, votre navigateur peut extraire une page Web de son cache (plutôt que d'un serveur distant) lorsque vous souhaitez la revoir.

Cookie Cleaner (Nettoyeur de cookies)	supprime les cookies. Ces fichiers prennent généralement la forme de fichiers temporaires. Un cookie est un petit fichier contenant des informations, dont généralement un nom d'utilisateur et les date et heures du moment, stocké sur l'ordinateur d'une personne naviguant sur le Web. Les cookies sont essentiellement utilisés par des sites Web pour identifier des utilisateurs qui se sont déjà enregistrés ou ont déjà visité le site ; toutefois, ils peuvent aussi être une source d'informations pour les hackers.
Nettoyeur de l'historique du navigateur	supprime l'historique de votre navigateur Web.
Nettoyeur d'e-mails Outlook Express et Outlook (éléments envoyés et supprimés)	supprime les messages envoyés et supprimés d'Outlook® et Outlook Express.
Nettoyeur récemment utilisé	supprime les fichiers récemment utilisés créés avec l'un des programmes suivants : ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Historique de Windows ▪ Lecteur Windows Media ▪ WinRAR® ▪ WinZip®
Nettoyeur de contrôles ActiveX	supprime les contrôles ActiveX. ActiveX est un composant logiciel utilisé par des programmes ou des pages Web pour ajouter des fonctionnalités qui se fondent dans le programme ou la page Web et y apparaissent comme des éléments normaux. Les plupart des contrôles ActiveX sont inoffensifs ; toutefois, certains peuvent subtiliser des informations sur votre ordinateur.
Nettoyeur de points de restauration système	supprime les anciens points de restauration système (hormis le plus récent) de votre ordinateur. Les points de restauration système sont créés par Windows pour noter les modifications apportées à votre ordinateur afin que vous puissiez revenir à une situation antérieure en cas de problème.

Nettoyage de votre ordinateur

Vous pouvez utiliser les nettoyeurs de QuickClean pour supprimer des fichiers inutiles de votre ordinateur. Lorsque vous avez terminé, sous **Résumé QuickClean**, vous pouvez voir la quantité d'espace disque récupérée après le nettoyage, le nombre de fichiers supprimés, et les date et heure de dernière exécution de QuickClean sur votre ordinateur.

1. Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **McAfee QuickClean**, cliquez sur **Démarrer**.
3. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Suivant** pour utiliser les nettoyeurs par défaut de la liste.
   - Sélectionnez ou désactivez les nettoyeurs appropriés, puis cliquez sur **Suivant**. Si vous sélectionnez Nettoyeur récemment utilisé, vous pouvez cliquer sur **Propriétés** pour sélectionner ou désélectionner les fichiers qui ont été récemment créés par les programmes de la liste, puis cliquer sur **OK**.
   - Cliquez sur **Paramètres par défaut** pour rétablir les nettoyeurs par défaut, puis cliquez sur **Suivant**.
4. Lorsque l'analyse est terminée, cliquez sur **Suivant**.
5. Cliquez sur **Suivant** pour confirmer la suppression des fichiers.
6. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Suivant** si vous acceptez l'option par défaut **Non, je souhaite supprimer les fichiers à l'aide de la fonction Windows standard**.
   - Cliquez sur **Oui, je souhaite procéder à la suppression sécurisée de mes fichiers à l'aide de Shredder**, spécifiez le nombre de passages (jusqu'à 10) et cliquez sur **Suivant**. Le broyage de fichiers peut être long s'il y a beaucoup d'informations à effacer.
7. Si des fichiers ou éléments ont été verrouillés pendant le nettoyage, vous pouvez être invité à faire redémarrer l'ordinateur. Cliquez sur **OK** pour fermer le message.
8. Cliquez sur **Terminer**.

Remarque : Les fichiers supprimés à l'aide de Shredder ne peuvent pas être récupérés. Pour des informations sur le broyage de fichiers, voir McAfee Shredder.

Défragmentation de votre ordinateur

Defragmenteur de disques organise les fichiers et dossiers de votre ordinateur de manière à éviter leur éparpillement (fragmentation) lors de leur enregistrement sur le disque dur de votre ordinateur. En défragmentant périodiquement votre disque dur, vous garantissez le regroupement des fichiers et dossiers fragmentés, ce qui permet de les récupérer plus rapidement ensuite.

Défragmenter votre ordinateur

Vous pouvez défragmenter votre ordinateur pour améliorer l'accès aux fichiers et dossiers et leur récupération.

1. Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Défragmenteur de disque**, cliquez sur **Analyse**.
3. Suivez les instructions à l'écran.

Remarque : pour plus d'informations sur Défragmenteur de disque, consultez l'aide de Windows.

Programmation d'une tâche

Le Planificateur de tâches automatise l'exécution régulière de QuickClean ou de Défragmenteur de disque sur votre ordinateur. Par exemple, vous pouvez programmer une tâche QuickClean qui vide la Corbeille tous les dimanches à 21h00 ou une tâche Défragmenteur de disque qui défragmente le disque dur de votre ordinateur le dernier jour de chaque mois. Vous pouvez créer, modifier ou supprimer une tâche à tout moment. Vous devez être connecté à l'ordinateur pour qu'une tâche programmée puisse s'exécuter. Si une tâche n'est pas exécutée pour une raison quelconque, elle sera reprogrammée cinq minutes après votre reconnexion.

Programmer une tâche QuickClean

Vous pouvez programmer une tâche QuickClean qui nettoie automatiquement votre ordinateur à l'aide d'un ou plusieurs nettoyeurs. Lorsque l'opération est terminée, sous **Résumé QuickClean**, vous pouvez voir les date et heure auxquelles l'exécution de la tâche est à nouveau programmée.

1. Ouvrez le volet Planificateur de tâches.

   Comment ?

   1. Dans McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
   2. Sous **Planificateur de tâches**, cliquez sur **Démarrer**.

2. Dans la liste **Sélectionner une opération à planifier**, cliquez sur **McAfee QuickClean**.
3. Entrez le nom à donner à la tâche dans la zone **Nom de la tâche**, puis cliquez sur **Créer**.
4. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Suivant** pour utiliser les nettoyeurs de la liste.
   - Sélectionnez ou désactivez les nettoyeurs appropriés, puis cliquez sur **Suivant**. Si vous sélectionnez Nettoyeur récemment utilisé, vous pouvez cliquer sur **Propriétés** pour sélectionner ou désélectionner les fichiers qui ont été récemment créés par les programmes de la liste, puis cliquer sur **OK**.
   - Cliquez sur **Paramètres par défaut** pour rétablir les nettoyeurs par défaut, puis cliquez sur **Suivant**.
5. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Planification** pour accepter l'option par défaut **Non, je souhaite supprimer les fichiers à l'aide de la fonction Windows standard**.

- Cliquez sur **Oui, je souhaite procéder à la suppression sécurisée de mes fichiers à l'aide de Shredder**, spécifiez le nombre de passages (jusqu'à 10) et cliquez sur **Planification**.

6 Dans la boîte de dialogue **Planification**, sélectionnez la fréquence à laquelle la tâche doit être exécutée, puis cliquez sur **OK**.

7 Si vous avez apporté des modifications aux propriétés du Nettoyeur récemment utilisé, vous serez peut-être invité à faire redémarrer votre ordinateur. Cliquez sur **OK** pour fermer le message.

8 Cliquez sur **Terminer**.

Remarque : Les fichiers supprimés à l'aide de Shredder ne peuvent pas être récupérés. Pour des informations sur le broyage de fichiers, voir McAfee Shredder.

Modifier une tâche QuickClean

Vous pouvez modifier une tâche QuickClean programmée pour changer les nettoyeurs utilisés ou sa fréquence d'exécution automatique sur votre ordinateur. Lorsque l'opération est terminée, sous **Résumé QuickClean**, vous pouvez voir les date et heure auxquelles l'exécution de la tâche est à nouveau programmée.

1 Ouvrez le volet Planificateur de tâches.

Comment ?

1. Dans McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Planificateur de tâches**, cliquez sur **Démarrer**.

2 Dans la liste **Sélectionner une opération à planifier**, cliquez sur **McAfee QuickClean**.

3 Sélectionnez la tâche dans la liste **Sélectionner une tâche existante**, puis cliquez sur **Modifier**.

4 Effectuez l'une des opérations suivantes :

- Cliquez sur **Suivant** pour utiliser les nettoyeurs sélectionnés pour la tâche.
- Sélectionnez ou désactivez les nettoyeurs appropriés, puis cliquez sur **Suivant**. Si vous sélectionnez Nettoyeur récemment utilisé, vous pouvez cliquer sur **Propriétés** pour sélectionner ou désélectionner les fichiers qui ont été récemment créés par les programmes de la liste, puis cliquer sur **OK**.
- Cliquez sur **Paramètres par défaut** pour rétablir les nettoyeurs par défaut, puis cliquez sur **Suivant**.

5 Effectuez l'une des opérations suivantes :

- Cliquez sur **Planification** pour accepter l'option par défaut **Non, je souhaite supprimer les fichiers à l'aide de la fonction Windows standard**.
- Cliquez sur **Oui, je souhaite procéder à la suppression sécurisée de mes fichiers à l'aide de Shredder**, spécifiez le nombre de passages (jusqu'à 10) et cliquez sur **Planification**.

6 Dans la boîte de dialogue **Planification**, sélectionnez la fréquence à laquelle la tâche doit être exécutée, puis cliquez sur **OK**.

7 Si vous avez apporté des modifications aux propriétés du Nettoyeur récemment utilisé, vous serez peut-être invité à faire redémarrer votre ordinateur. Cliquez sur **OK** pour fermer le message.

8 Cliquez sur **Terminer**.

Remarque : Les fichiers supprimés à l'aide de Shredder ne peuvent pas être récupérés. Pour des informations sur le broyage de fichiers, voir McAfee Shredder.

Supprimer une tâche QuickClean

Vous pouvez supprimer une tâche QuickClean programmée si vous ne souhaitez plus son exécution automatique.

1 Ouvrez le volet Planificateur de tâches.

Comment ?

1. Dans McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Planificateur de tâches**, cliquez sur **Démarrer**.

2 Dans la liste **Sélectionner une opération à planifier**, cliquez sur **McAfee QuickClean**.

3 Sélectionnez la tâche dans la liste **Sélectionner une tâche existante**.

4 Cliquez sur **Supprimer**, puis sur **Oui** pour confirmer la suppression.

5 Cliquez sur **Terminer**.

Programmer une tâche Défragmenteur de disque

Vous pouvez programmer une tâche Défragmenteur de disque pour planifier la fréquence à laquelle le disque dur de votre ordinateur doit être automatiquement défragmenté. Lorsque l'opération est terminée, sous **Défragmenteur de disque**, vous pouvez voir les date et heure auxquelles l'exécution de la tâche est à nouveau programmée.

1 Ouvrez le volet Planificateur de tâches.

   Comment ?

   1. Dans McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
   2. Sous **Planificateur de tâches**, cliquez sur **Démarrer**.

2 Dans la liste **Sélectionner une opération à planifier**, cliquez sur **Défragmenteur de disque**.

3 Entrez le nom à donner à la tâche dans la zone **Nom de la tâche**, puis cliquez sur **Créer**.

4 Effectuez l'une des opérations suivantes :

   - Cliquez sur **Planification** pour accepter l'option par défaut **Procéder à la défragmentation même si l'espace disque est insuffisant**.
   - Désélectionnez **Procéder à la défragmentation même si l'espace disque est insuffisant**, puis cliquez sur **Planification**.

5 Dans la boîte de dialogue **Planification**, sélectionnez la fréquence à laquelle la tâche doit être exécutée, puis cliquez sur **OK**.

6 Cliquez sur **Terminer**.

Modifier une tâche Défragmenteur de disque

Vous pouvez modifier une tâche Défragmenteur de disque programmée pour changer sa fréquence d'exécution automatique sur votre ordinateur. Lorsque l'opération est terminée, sous **Défragmenteur de disque**, vous pouvez voir les date et heure auxquelles l'exécution de la tâche est à nouveau programmée.

1 Ouvrez le volet Planificateur de tâches.

   Comment ?

1. Dans McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Planificateur de tâches**, cliquez sur **Démarrer**.

2 Dans la liste **Sélectionner une opération à planifier**, cliquez sur **Défragmenteur de disque**.

3 Sélectionnez la tâche dans la liste **Sélectionner une tâche existante**, puis cliquez sur **Modifier**.

4 Effectuez l'une des opérations suivantes :

- Cliquez sur **Planification** pour accepter l'option par défaut **Procéder à la défragmentation même si l'espace disque est insuffisant**.
- Désélectionnez **Procéder à la défragmentation même si l'espace disque est insuffisant**, puis cliquez sur **Planification**.

5 Dans la boîte de dialogue **Planification**, sélectionnez la fréquence à laquelle la tâche doit être exécutée, puis cliquez sur **OK**.

6 Cliquez sur **Terminer**.

Supprimer une tâche Défragmenteur de disque

Vous pouvez supprimer une tâche Défragmenteur de disque programmée si vous ne souhaitez plus son exécution automatique.

1 Ouvrez le volet Planificateur de tâches.

Comment ?

1. Dans McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Planificateur de tâches**, cliquez sur **Démarrer**.

2 Dans la liste **Sélectionner une opération à planifier**, cliquez sur **Défragmenteur de disque**.

3 Sélectionnez la tâche dans la liste **Sélectionner une tâche existante**.

4 Cliquez sur **Supprimer**, puis sur **Oui** pour confirmer la suppression.

5 Cliquez sur **Terminer**.

CHAPITRE 38

McAfee Shredder

McAfee Shredder supprime (broie) de manière définitive des éléments se trouvant sur le disque dur de votre ordinateur. Même lorsque vous supprimez manuellement des fichiers et des dossiers, puis que vous videz la Corbeille ou que vous supprimez votre dossier Fichiers Internet temporaires, vous pouvez encore récupérer ces informations à l'aide d'outils d'expertise informatique judiciaire. De même, un fichier supprimé peut être récupéré, car certains programmes effectuent des copies temporaires masquées des fichiers ouverts. Shredder protège votre confidentialité en supprimant en toute sécurité et de manière définitive ces fichiers indésirables. Il importe de ne pas oublier que des fichiers broyés ne peuvent plus être restaurés.

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctions de Shredder.....220
Broyage de fichiers, dossiers et disques 221

Fonctions de Shredder

Shredder supprime des éléments du disque dur de votre ordinateur de sorte que les informations y associées ne puissent plus être récupérées. Il protège votre confidentialité en supprimant en toute sécurité et de manière définitive des fichiers et dossiers, des éléments contenus dans la Corbeille et le dossier Fichiers Internet temporaires, ainsi que le contenu entier de disques tels que des CD réinscriptibles, des disques durs externes et des disquettes.

Broyage de fichiers, dossiers et disques

Shredder veille à ce que les informations contenues dans les fichiers supprimés placés dans votre Corbeille et dans votre dossier Fichiers Internet temporaires ne puissent plus être récupérées, même avec des outils spéciaux. Avec Shredder, vous pouvez spécifier combien de fois (jusqu'à 10) vous voulez qu'un élément soit broyé. Un nombre élevé de broyages augmente le niveau de sécurité de suppression des fichiers.

Broyer les fichiers et les dossiers

Vous pouvez broyer des fichiers et dossiers du disque dur de votre ordinateur, y compris des éléments de la Corbeille et du dossier Fichiers Internet temporaires.

1 Ouvrez **Shredder**.

   Comment ?

   1. Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Menu Avancé**.
   2. Dans le volet gauche, cliquez sur **Outils**.
   3. Cliquez sur **Shredder**.

2 Dans le volet Broyer les fichiers et les dossiers, sous **Je souhaite**, cliquez sur **Effacer des fichiers et des dossiers**.

3 Sous **Niveau de broyage**, cliquez sur l'un des niveaux de broyage suivants :

   - **Rapide** : broie une seule fois les éléments sélectionnés.
   - **Complet** : broie 7 fois les éléments sélectionnés.
   - **Personnalisé** : broie jusqu'à 10 fois les éléments sélectionnés.

4 Cliquez sur **Suivant**.

5 Effectuez l'une des opérations suivantes :

   - Dans la liste **Sélectionner le(s) fichier(s) à broyer**, cliquez sur **Contenu de la Corbeille** ou sur **Fichiers Internet temporaires**.
   - Cliquez sur **Parcourir**, naviguez jusqu'aux fichiers à broyer, puis cliquez sur **Ouvrir**.

6 Cliquez sur **Suivant**.

7 Cliquez sur **Démarrer**.

8 Lorsque Shredder a terminé, cliquez sur **Terminé**.

Remarque : N'utilisez aucun fichier tant que Shredder n'a pas terminé sa tâche.

Broyer un disque entier

Vous pouvez broyer en une fois le contenu entier d'un disque. Seuls des disques amovibles, comme des disques durs externes, des CD réinscriptibles et des disquettes peuvent être broyés.

1 Ouvrez **Shredder**.

Comment ?

1. Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Menu Avancé**.
2. Dans le volet gauche, cliquez sur **Outils**.
3. Cliquez sur **Shredder**.

2 Dans le volet Broyer des fichiers et des dossiers, sous **Je souhaite**, cliquez sur **Effacer un disque entier**.

3 Sous **Niveau de broyage**, cliquez sur l'un des niveaux de broyage suivants :

- **Rapide** : broie une seule fois le disque sélectionné.
- **Complet** : broie 7 fois le disque sélectionné.
- **Personnalisé** : broie jusqu'à 10 fois le disque sélectionné.

4 Cliquez sur **Suivant**.

5 Dans la liste **Sélectionnez le disque**, cliquez sur le disque à broyer.

6 Cliquez sur **Suivant**, puis sur **OK** pour confirmer.

7 Cliquez sur **Démarrer**.

8 Lorsque Shredder a terminé, cliquez sur **Terminé**.

Remarque : N'utilisez aucun fichier tant que Shredder n'a pas terminé sa tâche.

CHAPITRE 39

McAfee Network Manager

Network Manager présente sous forme graphique les ordinateurs et les autres composants de votre réseau. Vous pouvez utiliser Network Manager pour surveiller à distance l'état de protection de chaque ordinateur géré de votre réseau, mais aussi pour corriger à distance les points faibles de la sécurité de ces ordinateurs.

Avant d'utiliser Network Manager, nous vous conseillons de vous familiariser avec certaines de ses fonctionnalités. Pour plus de détails sur la configuration et l'utilisation de ces fonctionnalités, consultez l'aide de Network Manager.

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctionnalités de Network Manager 224
Présentation des icônes de Network Manager.....225
Configuration d'un réseau géré 227
Gestion à distance du réseau.....235

Fonctionnalités de Network Manager

Network Manager propose les fonctionnalités suivantes.

Carte graphique du réseau

La carte du réseau de Network Manager est une représentation graphique du niveau de protection des ordinateurs et des composants de votre réseau domestique. Lorsque vous modifiez votre réseau (lorsque vous ajoutez un ordinateur, par exemple), la carte du réseau identifie ces changements. Vous pouvez actualiser la carte du réseau, renommer le réseau, ou encore afficher ou masquer des composants de la carte du réseau. Vous pouvez également afficher les détails associés aux composants de la carte du réseau.

Gestion à distance

Utilisez la carte du réseau de Network Manager pour gérer le niveau de protection des ordinateurs qui constituent votre réseau domestique. Vous pouvez inviter un ordinateur à s'affilier au réseau géré, surveiller le niveau de protection des ordinateurs gérés et régler les problèmes connus de failles de sécurité du réseau à partir d'un ordinateur distant.

Présentation des icônes de Network Manager

Le tableau suivant décrit les icônes les plus utilisées sur la carte du réseau Network Manager.

Icône	Description
	Représente un ordinateur géré connecté au réseau
	Représente un ordinateur géré non connecté au réseau
	Représente un ordinateur non géré sur lequel SecurityCenter est installé
	Représente un ordinateur non géré non connecté au réseau
	Représente un ordinateur connecté au réseau sur lequel SecurityCenter n'est pas installé ou un matériel inconnu sur le réseau
	Représente un ordinateur non connecté au réseau sur lequel SecurityCenter n'est pas installé ou un matériel inconnu non connecté au réseau
	Signifie que l'élément correspondant est protégé et connecté
	Signifie que l'élément correspondant nécessite peut-être votre attention
	Signifie que l'élément correspondant nécessite votre attention immédiate
	Représente un routeur personnel sans fil
	Représente un routeur personnel standard
	Représente Internet en mode connexion
	Représente Internet en mode déconnexion

CHAPITRE 40

Configuration d'un réseau géré

Pour configurer un réseau géré, vous triez les éléments de la carte de votre réseau et vous ajoutez des membres (des ordinateurs) au réseau. Pour qu'un ordinateur puisse être géré à distance ou recevoir les autorisations nécessaires pour gérer d'autres ordinateurs à distance sur le réseau, il doit devenir membre autorisé du réseau. L'appartenance au réseau est accordée aux nouveaux ordinateurs par ceux qui sont déjà membres du réseau et qui possèdent des autorisations d'administration.

Vous pouvez voir les détails associés à un composant de la carte du réseau, même après avoir modifié votre réseau (par exemple, en ajoutant un ordinateur).

Contenu de ce chapitre

Utilisation de la carte du réseau.....228
Affiliation au réseau géré 230

Utilisation de la carte du réseau

Lorsque vous connectez un ordinateur au réseau, Network Manager analyse l'état du réseau afin de déterminer s'il y a des membres gérés ou non gérés, quels sont les attributs du routeur et quel est l'état d'Internet. Si aucun membre n'est trouvé, Network Manager suppose que l'ordinateur actuellement connecté est le premier du réseau et en fait automatiquement un membre géré avec des autorisations d'administration. Par défaut, le nom du réseau inclut le nom du groupe de travail ou du domaine du premier ordinateur qui se connecte au réseau équipé de SecurityCenter. Vous pouvez modifier le nom du réseau à tout moment.

Lorsque vous modifiez votre réseau (lorsque vous ajoutez un ordinateur, par exemple), vous pouvez personnaliser la carte du réseau. Ainsi, vous pouvez actualiser la carte du réseau, renommer le réseau et afficher/masquer des composants de la carte. Vous pouvez également afficher les détails associés aux composants de la carte du réseau.

Accéder à la carte du réseau

La carte du réseau propose une représentation graphique des ordinateurs et des autres composants de votre réseau.

- Dans le menu de base ou avancé, cliquez sur **Gérer un réseau**.

Remarque : vous devez commencer par autoriser les autres ordinateurs du réseau au premier accès à la carte.

Actualiser la carte du réseau

Vous pouvez actualiser la carte du réseau à tout moment, lorsqu'un nouvel ordinateur est affilié au réseau géré par exemple.

1. Dans le menu de base ou avancé, cliquez sur **Gérer un réseau**.
2. Cliquez sur **Actualiser la carte du réseau** sous **Je souhaite**.

Remarque : le lien **Actualiser la carte du réseau** n'est disponible que si aucun élément n'est sélectionné sur la carte du réseau. Pour désélectionner un élément, cliquez sur l'élément sélectionné ou sur une zone vide de la carte du réseau.

Attribution d'un nouveau nom au réseau

Par défaut, le nom du réseau inclut le nom du groupe de travail ou du domaine du premier ordinateur qui se connecte au réseau équipé de SecurityCenter. Si vous préférez utiliser un autre nom, vous pouvez le changer.

1. Dans le menu de base ou avancé, cliquez sur **Gérer un réseau**.
2. Cliquez sur **Renommer le réseau** sous **Je souhaite**.
3. Saisissez le nom du réseau dans la zone **Nom du réseau**.
4. Cliquez sur **OK**.

Remarque : Le lien **Attribution d'un nouveau nom au réseau** n'est disponible que si aucun élément n'est sélectionné sur la carte du réseau. Pour désélectionner un élément, cliquez sur l'élément sélectionné ou sur une zone vide de la carte du réseau.

Afficher ou masquer un élément de la carte du réseau

Par défaut, tous les ordinateurs et les autres composants de votre réseau apparaissent sur la carte du réseau. Si vous avez masqué des éléments, vous pouvez les réafficher à tout moment. Seuls les éléments non gérés peuvent être masqués. Les ordinateurs gérés ne peuvent pas être masqués.

Pour...	Dans le menu de base ou le menu avancé, cliquez sur **Gérer un réseau**, puis...
Masquer un élément de la carte du réseau	Cliquez sur un élément de la carte du réseau, puis sur **Masquer cet élément** sous **Je souhaite**. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.
Afficher des éléments masqués de la carte du réseau	Sous **Je souhaite**, cliquez sur **Afficher les éléments masqués**.

Afficher les détails d'un élément

Sélectionnez un composant de votre réseau dans la carte du réseau pour afficher des informations détaillées le concernant. Ces informations comprennent le nom du composant, l'état de sa protection et d'autres informations nécessaires pour gérer le composant.

1. Cliquez sur l'icône d'un élément sur la carte du réseau.
2. Sous **Détails**, affichez des informations sur l'objet.

Affiliation au réseau géré

Pour qu'un ordinateur puisse être géré à distance ou recevoir les autorisations nécessaires pour gérer d'autres ordinateurs à distance sur le réseau, il doit devenir membre autorisé du réseau. L'appartenance au réseau est accordée aux nouveaux ordinateurs par ceux qui sont déjà membres du réseau et qui possèdent des autorisations d'administration. Pour garantir que seuls les ordinateurs autorisés s'affilient au réseau, les utilisateurs des ordinateurs qui accordent les autorisations et ceux qui s'affilient au réseau doivent s'authentifier mutuellement.

Lorsqu'un ordinateur s'affilie au réseau, il est invité à indiquer l'état de sa protection McAfee aux autres ordinateurs du réseau. Si un ordinateur accepte d'afficher l'état de sa protection, il devient un membre géré du réseau. Si un ordinateur refuse d'afficher l'état de sa protection, il devient un membre non géré du réseau. Les membres non gérés du réseau sont généralement des invités qui souhaitent accéder à d'autres fonctionnalités du réseau (par exemple, envoyer des fichiers ou partager des imprimantes).

Remarque : après vous être affilié, si d'autres programmes réseau McAfee sont installés (EasyNetwork, par exemple), l'ordinateur est également reconnu comme étant un ordinateur géré pour ces programmes. Le niveau d'autorisation affecté à un ordinateur dans Network Manager s'applique à tous les programmes réseau McAfee. Pour obtenir des informations sur la signification des autorisations de type Invité, Complet ou Administration dans un autre programme réseau McAfee, reportez-vous à sa documentation.

Affiliation à un réseau géré

Lorsque vous êtes invité à vous affilier à un réseau géré, vous pouvez accepter ou refuser l'invitation. Vous pouvez également déterminer si vous voulez que cet ordinateur et les autres ordinateurs du réseau surveillent mutuellement leurs paramètres de sécurité (pour savoir par exemple si les services de protection antivirus d'un ordinateur sont à jour).

1. Dans la boîte de dialogue Réseau géré, assurez-vous que la case **Autoriser tous les ordinateurs de ce réseau à surveiller les paramètres de sécurité** est sélectionnée.
2. Cliquez sur l'option d'**affiliation**.
   Lorsque vous acceptez l'invitation, deux cartes à jouer s'affichent.
3. Vérifiez que ces cartes sont identiques à celles affichées sur l'ordinateur qui vous a invité à vous affilier au réseau géré.
4. Cliquez sur **OK**.

Remarque : si l'ordinateur qui vous a invité à vous affilier au réseau géré n'affiche pas les mêmes cartes que celles de la boîte de dialogue de confirmation de la sécurité, le réseau géré est victime d'une faille de sécurité. Le fait de vous affilier au réseau risque de compromettre la sécurité de votre ordinateur. Par conséquent, nous vous conseillons de cliquer sur **Annuler** dans la boîte de dialogue Réseau géré.

Inviter un ordinateur à s'affilier au réseau géré

Si un ordinateur est ajouté au réseau géré ou si un autre ordinateur non géré est déjà présent sur le réseau, vous pouvez inviter cet ordinateur à s'affilier au réseau géré. Seuls les ordinateurs avec des autorisations d'administration sur le réseau peuvent en inviter d'autres à s'y affilier. Lorsque vous envoyez l'invitation, vous spécifiez également le niveau d'autorisation que vous affectez à cet ordinateur.

1. Cliquez sur l'icône d'un ordinateur non géré sur la carte du réseau.
2. Cliquez sur **Surveiller cet ordinateur** sous **Je souhaite**.
3. Dans la boîte de dialogue d'invitation à l'affiliation au réseau géré, effectuez l'une des opérations suivantes :
   - Cliquez sur **Accorder un accès invité aux programmes du réseau géré** pour permettre à l'ordinateur d'accéder au réseau (vous pouvez utiliser cette option pour des utilisateurs temporaires chez vous).
   - Cliquez sur **Accorder un accès total aux programmes du réseau géré** pour permettre à l'ordinateur d'accéder au réseau.

- Cliquez sur **Accorder un accès administrateur aux programmes du réseau géré** pour permettre à l'ordinateur d'accéder au réseau avec des droits d'administration. L'ordinateur a par ailleurs la possibilité d'accorder un accès aux autres ordinateurs qui veulent s'affilier au réseau.

4 Cliquez sur **OK**.
Une invitation à s'affilier au réseau géré est envoyée à l'ordinateur. Lorsque l'ordinateur accepte l'invitation, deux cartes à jouer s'affichent.

5 Vérifiez que ces cartes sont identiques à celles affichées sur l'ordinateur que vous avez invité à s'affilier au réseau.

6 Cliquez sur **Autoriser l'accès**.

Remarque : si l'ordinateur qui vous a invité à vous affilier au réseau géré n'affiche pas les mêmes cartes que celles de la boîte de dialogue de confirmation de la sécurité, le réseau géré est victime d'une faille de sécurité. Le fait d'autoriser l'ordinateur à s'affilier au réseau risque de compromettre la sécurité des autres ordinateurs. Par conséquent, nous vous conseillons de cliquer sur **Refuser l'accès** dans la boîte de dialogue de confirmation de la sécurité.

Ne plus approuver les ordinateurs du réseau

Si vous avez approuvé d'autres ordinateurs par erreur, vous pouvez arrêter de les approuver.

- Cliquez sur **Arrêter de faire confiance aux ordinateurs du réseau** sous **Je souhaite**.

Remarque : Le lien **Arrêter de faire confiance aux ordinateurs du réseau** n'est disponible que si vous avez des droits d'administration et qu'il y a d'autres ordinateurs gérés sur le réseau.

CHAPITRE 41

Gestion à distance du réseau

Une fois que vous avez configuré votre réseau géré, vous pouvez gérer à distance les ordinateurs et les autres composants de votre réseau. Vous pouvez surveiller l'état et les niveaux de permission des ordinateurs et des autres composants, mais aussi corriger la plupart des problèmes de vulnérabilité, le tout à distance.

Contenu de ce chapitre

Surveillance de l'état et des autorisations 236
Réparation des failles de sécurité.....239

Surveillance de l'état et des autorisations

Un réseau géré comporte des membres gérés et des membres non gérés. Les membres gérés autorisent les autres ordinateurs du réseau à surveiller l'état de leur protection McAfee, contrairement aux membres non gérés. Les membres non gérés sont généralement des invités qui souhaitent accéder à d'autres fonctionnalités du réseau (par exemple, envoyer des fichiers et partager des imprimantes). Un ordinateur non géré peut être invité à devenir géré à tout moment par un autre ordinateur géré du réseau. De même, un ordinateur géré peut devenir non géré à tout moment.

Les ordinateurs gérés ont des autorisations de type Administration, Complet ou Invité. Les autorisations de type Administration permettent à l'ordinateur géré de gérer l'état de protection de tous les autres ordinateurs gérés du réseau, mais aussi d'accorder une appartenance aux autres ordinateurs du réseau. Les autorisations de type Complet et Invité ne permettent que l'accès au réseau. Vous pouvez modifier le niveau d'autorisation d'un ordinateur à tout moment.

Un réseau géré pouvant aussi comporter du matériel (des routeurs, par exemple), vous pouvez utiliser Network Manager pour les gérer. Vous pouvez aussi configurer et modifier les propriétés d'affichage d'un matériel sur la carte du réseau.

Surveillance de l'état de protection d'un ordinateur

Si l'état de protection d'un ordinateur n'est pas surveillé sur le réseau (l'ordinateur n'est pas un membre ou est un membre non géré), vous pouvez demander sa surveillance.

1. Cliquez sur l'icône d'un ordinateur non géré sur la carte du réseau.
2. Cliquez sur **Surveiller cet ordinateur** sous **Je souhaite**.

Arrêt de la surveillance de l'état de protection d'un ordinateur

Vous pouvez arrêter de surveiller l'état de protection d'un ordinateur géré de votre réseau ; cependant, l'ordinateur devient alors non géré et vous ne pouvez pas en contrôler l'état de protection à distance.

1. Cliquez sur l'icône d'un ordinateur géré sur la carte du réseau.
2. Cliquez sur **Arrêter de surveiller cet ordinateur** sous **Je souhaite**.
3. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.

Modification des autorisations d'un ordinateur géré

Vous pouvez modifier les autorisations d'un ordinateur géré à tout moment. Ainsi, vous pouvez changer les ordinateurs qui vont surveiller l'état de protection des autres ordinateurs du réseau.

1. Cliquez sur l'icône d'un ordinateur géré sur la carte du réseau.
2. Cliquez sur **Modifier les autorisations de cet ordinateur** sous **Je souhaite**.
3. Dans la boîte de dialogue de modification des autorisations, sélectionnez ou désélectionnez la case à cocher afin de déterminer si cet ordinateur et les autres ordinateurs du réseau géré peuvent surveiller mutuellement l'état de leur protection.
4. Cliquez sur **OK**.

Gestion d'un matériel

Pour gérer un matériel, accédez à sa page Web d'administration depuis Network Manager.

1. Cliquez sur l'icône d'un matériel sur la carte du réseau.
2. Cliquez sur **Gérer ce matériel** sous **Je souhaite**.
   Un navigateur Web s'ouvre pour afficher la page Web d'administration du matériel.
3. Dans votre navigateur Web, fournissez vos informations de connexion, puis configurez les paramètres de sécurité du matériel.

Remarque : si le matériel est un point d'accès ou un routeur sans fil protégé par Wireless Network Security, vous devez utiliser Wireless Network Security pour en configurer les paramètres de sécurité.

Modification des paramètres d'affichage d'un matériel

Lorsque vous modifiez les paramètres d'affichage d'un matériel, vous pouvez le renommer sur la carte du réseau et spécifier s'il s'agit d'un routeur sans fil.

1. Cliquez sur l'icône d'un matériel sur la carte du réseau.
2. Cliquez sur **Modifier les propriétés du matériel** sous **Je souhaite**.
3. Pour spécifier le nom d'affichage du matériel, saisissez un nom dans la zone **Nom**.
4. Pour spécifier le type de matériel, cliquez **Routeur standard** s'il ne s'agit pas d'un routeur sans fil ou **Routeur sans fil** dans le cas contraire.
5. Cliquez sur **OK**.

Réparation des failles de sécurité

Les ordinateurs gérés avec des autorisations de type Administration peuvent surveiller l'état de protection McAfee des autres ordinateurs gérés du réseau, mais aussi corriger à distance toute défaillance détectée en matière de sécurité. Ainsi, si l'état de protection McAfee d'un ordinateur géré indique que VirusScan est désactivé, un autre ordinateur géré avec des autorisations de type Administration peut activer VirusScan à distance.

Lorsque vous corrigez à distance des défaillances en matière de sécurité, Network Manager répare la plupart des problèmes rencontrés. Dans certains cas, une intervention manuelle directement sur l'ordinateur peut être nécessaire. Dans ce cas, Network Manager corrige tous les problèmes qui peuvent être réglés à distance, puis vous invite à corriger les problèmes restants. Connectez-vous alors à SecurityCenter sur l'ordinateur vulnérable et suivez les recommandations fournies. Dans certains cas, la solution suggérée consiste à installer la dernière version de SecurityCenter sur les ordinateurs distants du réseau.

Réparation automatique des failles de sécurité

Network Manager permet de corriger la plupart des problèmes de sécurité sur les ordinateurs gérés distants. Par exemple, si VirusScan est désactivé sur un ordinateur distant, vous pouvez le réactiver.

1. Cliquez sur l'icône d'un élément sur la carte du réseau.
2. Sous **Détails**, affichez l'état de protection de l'élément.
3. Cliquez sur **Réparer les failles de sécurité** sous **Je souhaite**.
4. Une fois les problèmes de sécurité réglés, cliquez sur **OK**.

Remarque : bien que Network Manager corrige automatiquement la plupart des failles de sécurité, il peut parfois être nécessaire d'ouvrir SecurityCenter sur l'ordinateur vulnérable et de suivre les recommandations fournies.

Installation de McAfee Security sur les ordinateurs distants

Si des ordinateurs de votre réseau n'utilisent pas la dernière version de SecurityCenter, leur état de protection ne peut pas être surveillé à distance. Pour surveiller ces ordinateurs à distance, vous devez installer la dernière version de SecurityCenter sur chacun d'entre eux.

1. Sur l'ordinateur où vous souhaitez installer le logiciel de sécurité, ouvrez SecurityCenter.
2. Sous **Tâches courantes**, cliquez sur **Mon compte**.
3. Connectez-vous avec l'adresse électronique et le mot de passe que vous avez utilisés pour enregistrer votre logiciel de sécurité la première fois que vous l'avez installé.
4. Sélectionnez le produit approprié, cliquez sur l'icône **Télécharger/Installer**, puis suivez les instructions à l'écran.

CHAPITRE 42

McAfee EasyNetwork

EasyNetwork permet de partager des fichiers en sécurité, de simplifier les transferts de fichiers et de partager des imprimantes entre les ordinateurs de votre réseau domestique. Cependant, EasyNetwork doit être installé sur les ordinateurs de votre réseau pour que ceux-ci puissent accéder aux fonctionnalités de ce programme.

Avant d'utiliser EasyNetwork, nous vous conseillons de vous familiariser avec certaines de ses fonctionnalités. Pour plus de détails sur la configuration et l'utilisation de ces fonctionnalités, consultez l'aide de EasyNetwork.

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctionnalités d'EasyNetwork 242
Configuration de EasyNetwork 243
Partage et envoi des fichiers 249
Partage d'imprimantes 255

Fonctionnalités d'EasyNetwork

EasyNetwork propose les fonctionnalités suivantes :

Partage de fichiers

EasyNetwork permet de partager facilement des fichiers avec d'autres ordinateurs du réseau. Lorsque vous partagez des fichiers, vous donnez aux autres ordinateurs un accès en lecture seule à ces fichiers. Seuls les ordinateurs possédant un accès complet ou administratif à votre réseau géré (membres) peuvent partager ou accéder à des fichiers partagés par d'autres membres.

Transfert de fichiers

Vous pouvez envoyer des fichiers à d'autres ordinateurs qui possèdent un accès complet ou administratif à votre réseau géré (membres). Lorsque vous recevez un fichier, il apparaît dans votre boîte de réception EasyNetwork. La boîte de réception est un emplacement de stockage temporaire pour tous les fichiers que vous envoyez à d'autres ordinateurs sur le réseau.

Partage d'imprimantes automatique

Lorsque vous vous affiliez au réseau géré, vous pouvez partager avec les autres membres toutes les imprimantes locales reliées à votre ordinateur, en utilisant le nom actuel de l'imprimante comme nom d'imprimante partagée. L'application détecte également les imprimantes partagées par d'autres ordinateurs sur votre réseau et permet de configurer et d'utiliser ces imprimantes.

CHAPITRE 43

Configuration de EasyNetwork

Pour pouvoir utiliser les fonctionnalités d'EasyNetwork, vous devez d'abord ouvrir le programme et vous affilier à un réseau géré. Après vous être affilié au réseau géré, vous pouvez partager, rechercher et envoyer des fichiers à d'autres ordinateurs du réseau. Vous pouvez aussi partager des imprimantes. Si vous décidez de quitter le réseau, vous pouvez le faire à tout moment.

Contenu de ce chapitre

Ouvrir EasyNetwork.....243
Affiliation à un réseau géré.....244
Comment quitter un réseau géré.....248

Ouvrir EasyNetwork

Par défaut, le système vous invite à ouvrir EasyNetwork après l'installation, mais vous pouvez également ouvrir l'application ultérieurement.

- Dans le menu **Démarrer**, pointez le curseur de la souris sur **Tous les programmes**, puis sur **McAfee** et cliquez sur **McAfee EasyNetwork**.

Conseil : si vous avez créé des icônes de l'application sur le bureau et dans la zone de lancement rapide lors de l'installation, vous pouvez également ouvrir EasyNetwork en double-cliquant sur son icône sur le bureau ou dans la zone de notification à l'extrême droite de la barre des tâches.

Affiliation à un réseau géré

Si aucun ordinateur du réseau auquel vous êtes connecté ne possède SecurityCenter, vous êtes fait membre du réseau et êtes invité à indiquer si le réseau est fiable. Dans la mesure où votre ordinateur est le premier à être affilié au réseau, son nom est intégré à celui du réseau. Toutefois, vous pouvez modifier le nom du réseau à tout moment.

Lorsqu'un ordinateur se connecte au réseau, il envoie une demande d'affiliation aux autres ordinateurs présents sur le réseau. La demande peut être accordée par tout ordinateur du réseau possédant des droits d'administration. Celui-ci peut également définir le niveau d'autorisation du nouvel ordinateur affilié au réseau : par exemple invité (transfert de fichiers uniquement) ou accès complet ou d'administration (transfert et partage de fichiers). Avec EasyNetwork, les ordinateurs possédant des droits d'administration peuvent autoriser l'accès d'autres ordinateurs et gérer leurs autorisations (c'est-à-dire favoriser ou empêcher l'accès des ordinateurs) ; les ordinateurs bénéficiant d'un accès complet ne peuvent pas effectuer ces tâches administratives.

Remarque : après vous être affilié, si d'autres programmes réseau McAfee sont installés (Network Manager, par exemple), l'ordinateur est également reconnu comme étant un ordinateur géré pour ces programmes. Le niveau d'autorisation affecté à un ordinateur dans EasyNetwork s'applique à tous les programmes réseau McAfee. Pour obtenir des informations sur la signification des autorisations de type Invité, Complet ou Administration dans un autre programme réseau McAfee, reportez-vous à sa documentation.

Affiliation au réseau

Lorsqu'un ordinateur se connecte à un réseau fiable pour la première fois après l'installation de EasyNetwork, un message s'affiche, vous proposant de vous affilier au réseau géré. Si vous acceptez, une demande est envoyée à tous les ordinateurs du réseau ayant des droits d'administration. Cette demande doit être accordée pour que l'ordinateur puisse partager des imprimantes ou des fichiers, ou encore envoyer et copier des fichiers sur le réseau. Le premier ordinateur du réseau reçoit automatiquement des autorisations de type Administration.

1. Dans la fenêtre Fichiers partagés, cliquez sur **S'affilier à ce réseau**.
   Lorsqu'un ordinateur du réseau qui possède des droits d'administration vous accorde l'accès, un message s'affiche, vous demandant si vous souhaitez autoriser cet ordinateur et les autres ordinateurs présents sur le réseau à gérer les paramètres de sécurité les uns des autres.
2. Si vous souhaitez accorder cette autorisation, cliquez sur **OK**. Dans le cas contraire, cliquez sur **Annuler**.
3. Vérifiez que l'ordinateur qui a autorisé l'accès affiche les cartes à jouer présentées dans la boîte de dialogue de confirmation de sécurité, puis cliquez sur **OK**.

Remarque : si l'ordinateur qui vous a invité à vous affilier au réseau géré n'affiche pas les mêmes cartes que celles de la boîte de dialogue de confirmation de la sécurité, le réseau géré est victime d'une faille de sécurité. Le fait de vous affilier au réseau risque de compromettre la sécurité de votre ordinateur. Par conséquent, nous vous conseillons de cliquer sur **Annuler** dans la boîte de dialogue de confirmation de sécurité.

Autorisation d'accès au réseau

Lorsqu'un ordinateur demande à être affilié au réseau géré, un message est envoyé aux autres ordinateurs du réseau possédant des droits d'administration. Le premier ordinateur qui répond devient l'administrateur des droits d'accès. L'administrateur de droits d'accès doit définir le type d'accès à accorder à l'ordinateur : invité, total ou administratif.

1. Dans l'alerte, cliquez sur le niveau d'accès approprié.
2. Dans la boîte de dialogue d'invitation à l'affiliation au réseau géré, effectuez l'une des opérations suivantes :
   - Cliquez sur **Accorder un accès invité aux programmes du réseau géré** pour permettre à l'ordinateur d'accéder au réseau (vous pouvez utiliser cette option pour des utilisateurs temporaires chez vous).
   - Cliquez sur **Accorder un accès total aux programmes du réseau géré** pour permettre à l'ordinateur d'accéder au réseau.

- Cliquez sur **Accorder un accès administrateur aux programmes du réseau géré** pour permettre à l'ordinateur d'accéder au réseau avec des droits d'administration. L'ordinateur a par ailleurs la possibilité d'accorder un accès aux autres ordinateurs qui veulent s'affilier au réseau.

3 Cliquez sur **OK**.

4 Vérifiez que l'ordinateur affiche les cartes à jouer présentées dans la boîte de dialogue de confirmation de sécurité, puis cliquez sur **Autoriser l'accès**.

Remarque : si ce n'est pas le cas, cela signifie que le réseau géré est victime d'une faille de sécurité. Le fait d'autoriser l'accès de cet ordinateur au réseau risque de compromettre la sécurité de votre ordinateur. Par conséquent, nous vous conseillons de cliquer sur **Refuser l'accès** dans la boîte de dialogue de confirmation de sécurité.

Attribution d'un nouveau nom au réseau

Par défaut, le nom du réseau inclut celui du premier ordinateur à s'être affilié. Toutefois, vous pouvez modifier ce nom à tout moment. Lorsque vous modifiez le nom du réseau, vous modifiez la description du réseau affichée dans EasyNetwork.

1. Dans le menu **Options**, cliquez sur **Configurer**.
2. Dans la boîte de dialogue Configurer, saisissez le nom du réseau dans la zone **Nom du réseau**.
3. Cliquez sur **OK**.

Comment quitter un réseau géré

Si vous vous affiliez à un réseau géré et si vous décidez par la suite que vous ne souhaitez pas en faire partie, vous pouvez le quitter. Après avoir quitté le réseau géré, vous pouvez toujours vous réaffilier, mais vous devrez à nouveau en recevoir l'autorisation. Pour plus d'informations sur l'affiliation, consultez Affiliation à un réseau géré (page 244).

Comment quitter un réseau géré

Vous pouvez quitter un réseau géré auquel vous êtes affilié.

1. Dans le menu **Outils**, cliquez sur **Quitter le réseau**.
2. Dans la boîte de dialogue Quitter le réseau, sélectionnez le nom du réseau que vous souhaitez quitter.
3. Cliquez sur **Quitter le réseau**.

CHAPITRE 44

Partage et envoi des fichiers

Grâce à EasyNetwork, il est facile de partager et d'envoyer des fichiers entre ordinateurs du réseau. Lorsque vous partagez des fichiers, vous donnez aux autres ordinateurs un accès en lecture seule à ces fichiers. Seuls les ordinateurs affiliés au réseau géré (c'est-à-dire ceux qui ont un accès complet ou administratif) peuvent partager des fichiers ou accéder à des fichiers partagés par d'autres ordinateurs affiliés.

Remarque : Si vous partagez un grand nombre de fichiers, cela peut affecter les ressources de votre ordinateur.

Contenu de ce chapitre

Partage de fichiers 250
Envoi de fichiers à d'autres ordinateurs 253

Partage de fichiers

Seuls les ordinateurs affiliés au réseau géré (c'est-à-dire ceux qui ont un accès complet ou administratif) peuvent partager des fichiers ou accéder à des fichiers partagés par d'autres ordinateurs affiliés. Lorsque vous partagez un dossier, vous partagez tous les fichiers contenus dans ce dossier et ses sous-dossiers. En revanche, les fichiers qui sont ajoutés au dossier par la suite ne sont pas automatiquement partagés. Si un fichier ou un dossier partagé est supprimé, il est supprimé de la fenêtre Fichiers partagés. Vous pouvez mettre fin au partage de fichiers à tout moment.

Pour accéder à un fichier partagé, ouvrez le fichier directement depuis EasyNetwork ou copiez-le vers votre ordinateur, puis ouvrez cette copie. Si votre liste de fichiers partagés est longue et que vous avez du mal à voir où se trouve le fichier, vous pouvez effectuer une recherche.

Remarque : Les fichiers partagés avec EasyNetwork ne sont pas accessibles par d'autres ordinateurs utilisant Windows Explorer car le partage de fichiers EasyNetwork exige des connexions sécurisées.

Partage d'un fichier

Lorsque vous partagez un fichier, il est mis à la disposition de tous les ordinateurs affiliés ayant un accès complet ou administratif au réseau géré.

1. Dans l'Explorateur Windows, recherchez le fichier que vous souhaitez partager.
2. Faites glisser le fichier depuis son emplacement dans l'Explorateur Windows vers la fenêtre Fichiers partagés de EasyNetwork.

Conseil : pour partager un fichier, vous pouvez également cliquer sur **Partager les fichiers** dans le menu **Outils**. Dans la boîte de dialogue Partager, recherchez le dossier contenant le fichier que vous souhaitez partager, sélectionnez-le, puis cliquez sur **Partager**.

Fin de partage d'un fichier

Si vous partagez un fichier sur le réseau géré, vous pouvez mettre fin au partage à tout moment. Lorsque vous cessez de partager un fichier, les autres ordinateurs affiliés au réseau géré ne peuvent pas y accéder.

1. Dans le menu **Outils**, cliquez sur **Arrêter de partager des fichiers**.
2. Dans la boîte de dialogue Arrêter de partager des fichiers, sélectionnez le fichier que vous ne souhaitez plus partager.
3. Cliquez sur **OK**.

Copie d'un fichier partagé

Vous pouvez copier un fichier partagé pour en disposer encore lorsqu'il ne sera plus partagé. Vous pouvez copier un fichier partagé depuis n'importe quel ordinateur du réseau géré.

- Faites glisser le fichier depuis la fenêtre Fichiers partagés dans EasyNetwork vers un emplacement de l'Explorateur Windows ou vers le bureau Windows.

Conseil : pour copier un fichier partagé, vous pouvez également sélectionner le fichier dans EasyNetwork puis cliquer sur **Copier dans** dans le menu **Outils**. Dans la boîte de dialogue Copier dans le dossier, recherchez le dossier où vous souhaitez copier le fichier, sélectionnez-le et cliquez sur **Enregistrer**.

Recherche d'un fichier partagé

Vous pouvez rechercher un fichier qui a été partagé par vous-même ou par un autre ordinateur affilié au réseau. Au fur et à mesure que vous entrez vos critères de recherche, EasyNetwork affiche les résultats correspondants dans la fenêtre Fichiers partagés.

1. Dans la fenêtre Fichiers partagés, cliquez sur **Rechercher**.
2. Cliquez sur l'option appropriée (page 252) dans la liste **Contient**.
3. Saisissez une partie ou la totalité du nom de fichier ou de chemin dans la liste **Nom de fichier ou de chemin**.
4. Cliquez sur le type de fichier (page 252) approprié dans la liste **Type**.
5. Dans les listes **De** et **A**, cliquez sur les dates correspondant à la plage de dates au cours de laquelle le fichier a été créé.

Critères de recherche

La tableaux qui suivent décrivent les critères de recherche que vous pouvez spécifier lors de la recherche de fichiers partagés.

Nom de fichier ou de chemin

Contient	Description
Contient tous les mots	La recherche porte sur les noms de fichiers ou de chemins qui contiennent tous les mots que vous spécifiez dans la liste **Nom de fichier ou de chemin**, quel que soit l'ordre des mots.
Contient certains mots	La recherche porte sur les noms de fichiers ou de chemins qui contiennent au moins l'un des mots spécifiés dans la liste **Nom de fichier ou de chemin**.
Contient l'expression exacte	La recherche porte sur les noms de fichiers ou de chemins qui contiennent l'expression exacte spécifiée dans la liste **Nom de fichier ou de chemin**.

Type de fichier

Type	Description
Tous	La recherche porte sur tous les types de fichiers partagés.
Document	La recherche porte sur tous les documents partagés.
Image	La recherche porte sur tous les fichiers d'image partagés.
Vidéo	La recherche porte sur tous les fichiers vidéo partagés.
Audio	La recherche porte sur tous les fichiers audio partagés.
Compressé	La recherche porte sur tous les fichiers compressés (par exemple, fichiers .zip).

Envoi de fichiers à d'autres ordinateurs

Vous pouvez envoyer des fichiers à d'autres ordinateurs qui sont affiliés au réseau géré. Avant d'envoyer un fichier, EasyNetwork confirme que l'ordinateur qui reçoit le fichier dispose d'un espace disque suffisant.

Lorsque vous recevez un fichier, il apparaît dans votre boîte de réception EasyNetwork. La boîte de réception est un emplacement de stockage temporaire pour tous les fichiers que vous envoyez à d'autres ordinateurs sur le réseau. Si votre application EasyNetwork est ouverte lorsque vous recevez un fichier, celui-ci apparaît instantanément dans votre boîte de réception ; sinon, un message s'affiche dans la zone de notification située à l'extrême droite de la barre des tâches. Si vous ne souhaitez pas recevoir de messages de notification (par exemple, ils interrompent votre activité en cours), vous pouvez désactiver cette fonction. Si un fichier portant le même nom existe déjà dans la boîte de réception, le nouveau fichier est renommé avec un suffixe numérique. Les fichiers restent dans votre boîte de réception jusqu'à ce que vous les acceptiez (jusqu'à ce que vous les copiiez sur votre ordinateur).

Envoi d'un fichier à un autre ordinateur

Vous pouvez envoyer un fichier à un autre ordinateur présent sur le réseau géré sans pour autant le partager. Pour que l'utilisateur de l'ordinateur cible puisse voir le fichier, celui-ci doit être enregistré en local. Pour plus d'informations, reportez-vous à Acceptation d'un fichier provenant d'un autre ordinateur (page 254).

1. Dans l'Explorateur Windows, recherchez le fichier que vous souhaitez envoyer.
2. Faites glisser le fichier depuis son emplacement dans l'Explorateur Windows vers l'icône d'ordinateur actif de EasyNetwork.

Conseil : pour envoyer plusieurs fichiers à un ordinateur, appuyez sur Ctrl tout en sélectionnant les fichiers. Pour envoyer des fichiers, vous pouvez également cliquer sur **Envoyer** dans le menu **Outils**, sélectionner les fichiers, puis cliquer sur **Envoyer**.

Acceptation d'un fichier provenant d'un autre ordinateur

Si un autre ordinateur du réseau géré vous envoie un fichier, vous devez l'accepter (en l'enregistrant sur votre ordinateur). Si EasyNetwork n'est pas ouvert lorsque votre ordinateur reçoit un fichier, vous recevez un message de notification dans la zone à l'extrême droite de la barre des tâches. Cliquez sur ce message pour ouvrir EasyNetwork et accéder au fichier.

- Cliquez sur **Reçu**, puis faites glisser le fichier de votre boîte de réception EasyNetwork vers un des dossiers de l'Explorateur Windows.

Conseil : pour recevoir un fichier d'un autre ordinateur, vous pouvez également sélectionner le fichier dans EasyNetwork puis cliquer sur **Accepter** dans le menu **Outils**. Dans la boîte de dialogue Accepter dans le dossier, recherchez le dossier où vous souhaitez enregistrer les fichiers, sélectionnez-le et cliquez sur **Enregistrer**.

Réception d'une notification lors de l'envoi d'un fichier

Vous pouvez recevoir un message de notification lorsqu'un autre ordinateur du réseau géré vous envoie un fichier. Si EasyNetwork n'est pas ouvert, le message de notification apparaît dans la zone de notification à l'extrême droite de la barre des tâches.

1. Dans le menu **Options**, cliquez sur **Configurer**.
2. Dans la boîte de dialogue Configurer, activez la case **M'avertir lorsqu'un autre ordinateur m'envoie des fichiers.**.
3. Cliquez sur **OK**.

CHAPITRE 45

Partage d'imprimantes

Lorsque vous vous affiliez au réseau géré, EasyNetwork partage les imprimantes locales reliées à votre ordinateur et utilise le nom actuel de l'imprimante comme nom d'imprimante partagée. EasyNetwork détecte également les imprimantes partagées par d'autres ordinateurs sur votre réseau et permet de les configurer et de les utiliser.

Si vous avez configuré un pilote d'imprimante de manière à imprimer via un serveur d'impression du réseau (un serveur d'impression USB sans fil, par exemple), EasyNetwork considère qu'il s'agit d'une imprimante locale et la partage sur le réseau. Vous pouvez également mettre fin au partage d'une imprimante à tout moment.

Contenu de ce chapitre

Utilisation d'imprimantes partagées.....256

Utilisation d'imprimantes partagées

EasyNetwork détecte les imprimantes qui sont partagées par les ordinateurs du réseau. Si l'application détecte une imprimante distante qui n'est pas connectée à votre ordinateur, le lien **Imprimantes réseau disponibles** apparaît dans la fenêtre Fichiers partagés lorsque vous ouvrez EasyNetwork pour la première fois. Vous pouvez alors installer des imprimantes disponibles ou désinstaller des imprimantes qui sont déjà connectées à votre ordinateur. Vous pouvez aussi actualiser la liste des imprimantes pour vous assurer que les informations affichées sont à jour.

Si vous n'êtes pas affilié au réseau géré mais si vous y êtes connecté, vous pouvez accéder aux imprimantes partagées depuis le panneau de commande Windows de l'imprimante.

Fin de partage d'une imprimante

Lorsque vous arrêtez de partager une imprimante, les ordinateurs affiliés ne peuvent plus l'utiliser.

1. Dans le menu **Outils**, cliquez sur **Imprimantes**.
2. Dans la boîte de dialogue Gérer les imprimantes réseau, cliquez sur le nom de l'imprimante que vous ne souhaitez plus partager.
3. Cliquez sur **Ne pas partager**.

Installation d'une imprimante réseau disponible

Si vous êtes affilié au réseau géré, vous pouvez accéder aux imprimantes partagées ; cependant, vous devez installer le pilote d'imprimante approprié. Si le propriétaire de l'imprimante arrête de la partager, vous ne pouvez plus l'utiliser.

1. Dans le menu **Outils**, cliquez sur **Imprimantes**.
2. Dans la boîte de dialogue Imprimantes réseau disponibles, cliquez sur le nom d'une imprimante.
3. Cliquez sur **Installer**.

Référence

Le glossaire répertorie et définit les termes de sécurité les plus utilisés dans les produits McAfee.

Glossaire

8

802.11

Ensemble de standards IEEE pour la transmission de données sur un réseau sans fil. 802.11 est communément connu sous le nom de Wi-Fi.

802.11a

Extension de 802.11 qui transmet des données à un débit pouvant atteindre 54 Mbits/s dans la bande des 5 GHz. Même si le débit de transmission est plus rapide que celui du 802.11b, la distance couverte est inférieure.

802.11b

Extension de 802.11 qui transmet des données à un débit pouvant atteindre 11 Mbits/s dans la bande des 2,4 GHz. Même si le débit de transmission est plus lent que celui du 802.11a, la distance couverte est supérieure.

802.1x

Standard IEEE pour l'authentification sur les réseaux câblés et sans fil. 802.1x est couramment utilisé avec les réseaux sans fil 802.11.

A

adaptateur sans fil

Appareil qui ajoute une capacité de communication sans fil à un ordinateur ou un PDA. L'adaptateur est connecté via un port USB, un connecteur pour carte PC (CardBus), un connecteur de carte mémoire ou, à l'intérieur, sur le bus PCI.

Adresse IP

Identifiant d'un ordinateur ou d'un périphérique au sein d'un réseau TCP/IP. Les réseaux qui utilisent le protocole TCP/IP acheminent les messages en fonction de l'adresse IP de leur destination. Une adresse IP est au format numérique. Elle est codée sur 32 bits, sous la forme de quatre nombres séparés par des points. Chaque nombre peut être compris entre zéro et 255 (par exemple : 192.168.1.100).

Adresse MAC

(adresse Media Access Control) Numéro de série unique attribué à un appareil physique accédant au réseau.

Analyse à la demande

Analyse lancée à la demande (c'est-à-dire lorsque vous lancez l'opération). A la différence de l'analyse en temps réel, les analyses à la demande ne se lancent pas automatiquement.

analyse en temps réel

Permet d'analyser les fichiers et les dossiers, à la recherche de virus et d'autres activités, lorsque vous ou votre ordinateur y accédez.

archivage complet

Archiver un jeu complet de données en fonction des types des fichiers et des emplacements que vous avez déjà configurés. Voir aussi archivage rapide.

archivage rapide

Archivage des seuls fichiers modifiés depuis le dernier archivage complet ou rapide. Voir aussi archivage complet.

archiver

Créer une copie de fichiers importants sur CD, DVD, lecteur USB, disque dur externe ou disque réseau.

attaque en force

Méthode de décodage de données chiffrées, comme des mots de passe, basée sur un effort exhaustif (force brute) plutôt que sur une stratégie intellectuelle. La force brute est jugée comme une méthode d'attaque infaillible, mais longue. Aussi appelée craquage en force.

attaque par dictionnaire

Type d'attaque en force qui utilise des mots courants pour tenter de découvrir un mot de passe.

attaque par immixtion

Méthode visant à intercepter et éventuellement modifier des messages entre deux parties sans que celles-ci sachent que leur communication a été infiltrée.

authentification

Processus d'identification d'une personne, généralement par un nom unique et un mot de passe.

B

bande passante

Quantité de données pouvant être transmise sur une période donnée.

base de registre

Base de données où Windows stocke ses informations de configuration. Il contient des profils pour chaque utilisateur de l'ordinateur ainsi que des informations sur le matériel du système, les programmes installés et les paramètres des propriétés. Windows se réfère continuellement à ces informations en cours de travail.

bibliothèque

Zone de stockage en ligne pour des fichiers que vous avez sauvegardés et publiés. La bibliothèque Data Backup est un site Web sur Internet, accessible à toute personne disposant d'un accès Internet.

C

cache

Zone de stockage temporaire sur votre ordinateur. Par exemple, pour accélérer et augmenter l'efficacité de la navigation sur le Web, votre navigateur peut extraire une page Web de sa mémoire cache (plutôt que d'un serveur distant) la prochaine fois que vous l'affichez.

carte adaptateur sans fil USB

Carte adaptateur sans fil qui se connecte à un logement USB dans l'ordinateur.

carte du réseau

Représentation graphique des ordinateurs et des autres composants de votre réseau domestique.

cartes adaptateur sans fil PCI

(Peripheral Component Interconnect) Carte adaptateur sans fil qui se branche sur un connecteur d'extension PCI à l'intérieur de l'ordinateur.

certifié Wi-Fi

Testé et approuvé par la Wi-Fi Alliance. Les produits certifiés Wi-Fi sont réputés interopérables même s'ils proviennent de fabricants différents. Un utilisateur disposant d'un produit certifié Wi-Fi peut utiliser n'importe quelle marque de point d'accès avec toute autre marque de matériel client également certifié.

Cheval de Troie

Programmes qui semblent légitimes mais qui peuvent endommager de précieux fichiers, perturber les performances et permettre des accès non autorisés à votre ordinateur.

chiffrement

Processus de transformation de données, de texte en code, qui les obscurcit pour les rendre illisibles par les personnes ne sachant pas les déchiffrer. On dit aussi texte crypté.

Clé

Voir clé USB.

clé

Série de lettres et de chiffres utilisée par deux périphériques pour authentifier une communication. Les deux doivent disposer de la clé. Voir aussi WEP, WPA, WPA2, WPA-PSK et WPA2- PSK.

clé USB

Petit lecteur mémoire qui se branche sur un port USB de l'ordinateur. Un lecteur USB agit comme un petit lecteur de disque et facilite le transfert de fichiers entre deux ordinateurs.

client

Application qui s'exécute sur un ordinateur personnel ou une station de travail et qui s'appuie sur un serveur pour certaines de ses opérations. Un client de messagerie, par exemple, est une application qui permet d'envoyer et de recevoir du courrier électronique.

client de messagerie

Programme que vous exécutez sur votre ordinateur pour envoyer et recevoir des e-mails (par exemple, Microsoft Outlook).

code d'authentification des messages (MAC)

Code de sécurité utilisé pour chiffrer des messages transmis entre des ordinateurs. Le message est accepté si l'ordinateur reconnaît la validité du code déchiffré.

compression

Processus permettant de compresser des fichiers dans un format qui réduit l'espace nécessaire pour les stocker ou les transmettre.

compte de messagerie standard

Voir POP3.

Contrôle ActiveX

Composant logiciel utilisé par des programmes ou des pages Web pour ajouter une fonctionnalité qui apparaît comme une partie normale du programme ou de la page Web. Les plupart des contrôles ActiveX sont inoffensifs ; toutefois, certains peuvent subtiliser des informations sur votre ordinateur.

Contrôle parental

Réglages qui déterminent ce que vos enfants peuvent voir et faire sur le Web. Pour configurer le contrôle parental, vous pouvez activer ou désactiver le filtrage d'images, choisir un groupe de classification du contenu et définir des heures limites de navigation sur le Web.

cookie

Petit fichier contenant des informations, dont généralement un nom d'utilisateur et les date et heure actuelles, stocké sur l'ordinateur d'une personne naviguant sur le Web. Les cookies sont essentiellement utilisés par des sites Web pour identifier des utilisateurs qui se sont déjà enregistrés ou ont déjà visité le site ; toutefois, ils peuvent aussi être une source d'informations pour les hackers.

Corbeille

Imitation d'une corbeille à papiers, utilisée pour stocker les fichiers et dossiers supprimés dans Windows.

D

DAT

(Fichiers de signature de données) Fichiers contenant les définitions employées pour détecter des virus, des chevaux de Troie, des logiciels espions, des logiciels publicitaires et d'autres programmes potentiellement indésirables sur votre ordinateur ou votre lecteur USB.

débordement de la mémoire tampon

Condition qui se produit lorsque des programmes ou processus suspects tentent de stocker davantage de données dans une mémoire tampon (zone de stockage temporaire) de votre ordinateur que celle-ci peut en contenir. Les débordements de mémoire tampon endommagent ou écrasent les données contenues dans les tampons adjacents.

déni de service

Type d'attaque qui ralentit ou paralyse le trafic sur un réseau. Une attaque par déni de service se produit lorsqu'un réseau est inondé de requêtes supplémentaires au point que le trafic ordinaire est ralenti ou complètement bloqué. Il n'entraîne généralement aucun vol d'informations ni aucune autre vulnérabilité.

disque dur externe

Disque dur conservé en dehors de l'ordinateur.

DNS

(Système de noms de domaines) Système qui convertit les noms d'hôtes ou noms de domaines en adresses IP. Sur le Web, DNS est utilisé pour convertir une adresse Web facilement lisible (par exemple, www.monhote.com) en une adresse IP (par exemple, 111.2.3.44) pour permettre d'aller chercher la page Web. Sans DNS, vous devriez taper vous-même l'adresse IP dans votre navigateur Web.

domaine

Sous-réseau local ou descripteur de sites sur Internet.

Sur un réseau local (LAN), un domaine est un sous-réseau composé d'ordinateurs clients et serveurs contrôlés par une seule base de données de sécurité. Dans ce contexte, les domaines peuvent améliorer les performances. Sur Internet, un domaine est une partie de toute adresse Web (par exemple, dans www.abc.com, abc est le domaine).

E

e-mail

(courrier électronique) Messages envoyés et reçus électroniquement, à travers un réseau d'ordinateurs. Voir aussi Webmail.

emplacement de surveillance accrue

Dossier de votre ordinateur dont les changements sont surveillés par Data Backup. Si vous définissez un emplacement de surveillance accrue, Data Backup sauvegarde les types de fichiers de surveillance dans ce dossier ou ses sous-dossiers.

emplacements de surveillance de premier niveau

Dossier de votre ordinateur dont les changements sont surveillés par Data Backup. Si vous définissez un emplacement surveillé de premier niveau, Data Backup sauvegarde les types de fichiers de surveillance dans ce dossier, mais n'inclut pas ses sous-dossiers.

emplacements surveillés

Dossiers surveillés par Data Backup sur votre ordinateur.

ESS

(Extended Service Set) Ensemble de deux réseaux ou plus formant un même sous-réseau.

É

événement

Action entreprise par l'utilisateur, un périphérique ou l'ordinateur lui-même, qui déclenche une réponse. McAfee consigne les événements dans son journal des événements.

F

fenêtres instantanées

Petites fenêtres qui apparaissent au-dessus d'autres fenêtres plus grandes, sur l'écran de l'ordinateur. Les fenêtres instantanées servent souvent à afficher des publicités dans les navigateurs Web.

fichier temporaire

Fichier utile le temps d'une session, que le système d'exploitation ou un autre programme crée en mémoire ou sur disque, avant de le supprimer.

filtrage d'images

Option de contrôle parental qui empêche l'affichage d'images Web potentiellement inappropriées.

fragments de fichier

Restes d'un fichier éparpillés sur un disque. La fragmentation se produit à mesure que des fichiers sont ajoutés ou supprimés, et peut ralentir votre ordinateur.

G

groupe d'évaluation de contenu

Dans le contrôle parental, groupe d'âge auquel appartient un utilisateur. Le contenu est mis à disposition ou bloqué en fonction du groupe auquel appartient l'utilisateur. Les groupes d'évaluation du contenu incluent : les jeunes enfants, les enfants, les pré-adolescents, les adolescents et les adultes.

I

Internet

Ensemble d'un grand nombre de réseaux interconnectés qui utilisent le protocole TCP/IP pour localiser et transférer des données. Initialement, il s'agissait d'une liaison entre des ordinateurs d'universités (à la fin des années 1960 et au début des années 1970) financée par le Ministère de la Défense des États-Unis et appelée ARPANET. Aujourd'hui, Internet est un réseau mondial qui regroupe près de 100 000 réseaux indépendants.

intranet

Réseau d'ordinateurs privé, généralement au sein d'une organisation, qui n'est accessible qu'aux utilisateurs autorisés.

itinérance

Déplacement d'une zone de couverture d'un point d'accès à une autre, sans interruption du service, ni perte de connexion.

L

LAN

(Local Area Network - Réseau local) Réseau d'ordinateurs qui s'étend sur une zone relativement petite (par exemple, un seul bâtiment). Les ordinateurs connectés via un LAN peuvent communiquer entre eux et partager des ressources telles que des imprimantes et des fichiers.

Launchpad

Composant de l'interface U3 qui agit comme point de départ pour lancer et gérer les programmes USB U3.

lecteur réseau

Disque ou lecteur de bande relié à un serveur sur un réseau partagé par plusieurs utilisateurs. Les lecteurs réseau sont quelquefois appelés lecteurs distants.

liste approuvée

Contient des éléments que vous avez autorisés et ne sont donc plus détectés. Si vous autorisez par erreur un élément (par exemple, un programme potentiellement indésirable ou une modification du registre) ou si vous souhaitez à nouveau qu'il soit détecté, vous devez le supprimer de cette liste.

liste d'autorisation

Liste de sites Web auxquels les utilisateurs sont autorisés à accéder car ils ne sont pas considérés comme frauduleux.

liste de blocage

Dans la protection anti-hameçonnage, liste de sites Web considérés comme frauduleux.

M

MAPI

(Messaging Application Programming Interface) Spécification d'interface de Microsoft permettant à différentes applications de messagerie et de groupes de travail (messagerie électronique, messagerie vocale, télécopie...) de fonctionner sur un seul client, comme le client Exchange.

mot clé

Mot pouvant être affecté à un fichier sauvegardé pour établir une relation ou une connexion avec d'autres fichiers auxquels le même mot clé a été affecté. Les mots clés facilitent la recherche des fichiers publiés sur Internet.

mot de passe

Code (généralement composé de lettres et de chiffres) qui permet d'accéder à votre ordinateur, à un programme ou à un site Web.

MSN

(Microsoft Network) Groupe de services basés sur le Web offerts par Microsoft Corporation ; ce groupe comprend un moteur de recherche, une messagerie Web, une messagerie instantanée et un portail.

N

navigateur

Programme utilisé pour afficher des pages Web sur Internet. Les navigateurs Web les plus populaires sont Microsoft Internet Explorer et Mozilla Firefox.

NIC

(Network Interface Card - Carte d'interface réseau) Carte qui se branche sur un ordinateur portable ou un autre périphérique pour le relier au réseau local.

nœud

Ordinateur unique relié à un réseau.

numéroteur

Logiciel qui aide à établir une connexion Internet. Utilisé de manière malveillante, il peut rediriger vos connexions Internet vers quelqu'un d'autre que votre fournisseur d'accès (FAI) par défaut, sans vous informer du coût supplémentaire que cela implique.

P

pare-feu

Système (matériel et/ou logiciel) conçu pour empêcher les accès non autorisés à un réseau privé ou à partir de ce dernier. Ils sont fréquemment utilisés pour empêcher les utilisateurs non autorisés d'accéder à des réseaux privés connectés à Internet, en particulier des intranets. Tous les messages qui pénètrent ou quittent l'intranet passent par le pare-feu, qui étudie chaque message et bloque ceux qui ne répondent pas aux critères de sécurité spécifiés.

partager

Permettre aux destinataires d'e-mails d'accéder à certains fichiers sauvegardés pendant une certaine période. Lorsque vous partagez un fichier, vous en envoyez la copie sauvegardée aux destinataires que vous choisissez. Ces derniers reçoivent un courrier électronique de Data Backup leur signalant que des fichiers ont été partagés avec eux. Le courrier comporte également un lien vers ces fichiers partagés.

passerelle intégrée

Dispositif qui associe les fonctions d'un point d'accès, d'un routeur et d'un pare-feu. Certains peuvent aussi comporter des améliorations de sécurité et des fonctions de pont.

Password Vault

Zone de stockage sécurisée des mots de passe personnels. Ainsi, vous êtes assuré que personne ne peut accéder à vos mots de passe (pas même un administrateur).

phishing

Tromperie sur Internet visant à obtenir des informations précieuses (comme un numéro de carte de crédit ou de sécurité sociale, un nom d'utilisateur et des mots de passe) de personnes naïves en vue d'un usage frauduleux.

Pixels invisibles

Petits fichiers graphiques pouvant s'insérer dans vos pages HTML et permettant à une source non autorisée de placer des cookies sur votre ordinateur. Ces cookies peuvent ensuite transmettre des informations à la source non autorisée. Les pixels invisibles sont aussi appelés balises Web, GIF transparents ou GIF invisibles.

plug-in

Petit logiciel qui collabore avec un programme de plus grande taille pour fournir des fonctionnalités supplémentaires. Par exemple, des plug-ins permettent à un navigateur Web d'exécuter des fichiers incorporés dans des documents HTML, dans des formats qu'il ne reconnaîtrait pas normalement (par exemple, fichiers vidéo, audio et d'animation).

Point d'accès

Périphérique réseau (couramment appelé routeur sans fil) qui se connecte à un concentrateur ou commutateur Ethernet pour étendre la portée physique du service pour un utilisateur sans fil. Lorsque des utilisateurs sans fil se déplacent avec leur appareil mobile, la transmission passe d'un point d'accès à un autre pour maintenir la connectivité.

point d'accès non fiable

Point d'accès non autorisé. Des points d'accès non fiables peuvent être installés sur un réseau d'entreprise sûr pour permettre à des tiers non autorisés d'accéder au réseau. Ils peuvent aussi être créés pour permettre à un agresseur de mener une attaque par immixtion.

point d'accès sans fil

Zone géographique couverte par un point d'accès Wi-Fi (802.11). Un utilisateur qui y pénètre avec un portable sans fil peut se connecter à Internet, à condition que le point d'accès diffuse sa présence et n'exige pas d'authentification. Les points d'accès sans fil (hotspots) se situent souvent dans des zones très fréquentées (p. ex. aéroports).

point de restauration système

Instantané (image) du contenu de la mémoire d'un ordinateur ou d'une base de données. Windows crée des points de restauration périodiquement ainsi qu'au moment d'événements système significatifs (p. ex. lors de l'installation d'un programme ou d'un pilote). Vous pouvez également créer et nommer à tout moment vos propres points de restauration.

POP3

(Post Office Protocol 3) Interface entre un client de messagerie et le serveur de messagerie. La plupart des utilisateurs domestiques ont un compte POP3, qui est leur compte de messagerie standard.

port

Lieu par où des informations entrent et/ou sortent d'un ordinateur. Par exemple, un modem analogique conventionnel est connecté à un port série.

PPPoE

(Point-to-Point Protocol Over Ethernet) Méthode utilisant le protocole PPP (Point-to-Point Protocol) avec Ethernet comme moyen de transport.

programme potentiellement indésirable (PUP)

Programme qui recueille et transmet des informations personnelles sans votre autorisation (par exemple logiciel espion ou publicitaire).

protocole

Format (matériel ou logiciel) de transmission de données entre deux périphériques. Votre ordinateur ou périphérique doit prendre en charge le protocole approprié pour pouvoir communiquer avec d'autres ordinateurs.

proxy

Ordinateur (ou logiciel s'exécutant sur cet ordinateur) qui agit comme une barrière entre un réseau et Internet en présentant une adresse réseau unique aux sites externes. En représentant tous les ordinateurs internes, le proxy protège les identités réseau tout en fournissant un accès à Internet. Voir également serveur proxy.

publier

Mettre à disposition du public, sur Internet, un fichier sauvegardé. Vous pouvez accéder à des fichiers publiés en feuilletant la bibliothèque Data Backup.

Q

quarantaine

Isolement. Par exemple, dans VirusScan, les fichiers suspects sont détectés et mis en quarantaine afin qu'ils ne puissent pas nuire à votre ordinateur ni à vos fichiers.

R

raccourci

Fichier contenant uniquement l'emplacement d'un autre fichier sur votre ordinateur.

RADIUS

(Remote Access Dial-In User Service) Protocole qui permet l'authentification des utilisateurs, généralement dans le contexte d'un accès à distance. Initialement défini pour être utilisé avec des serveurs d'accès distant à commutation, le protocole RADIUS sert maintenant dans divers environnements d'authentification, notamment l'authentification 802.1x d'un secret partagé de l'utilisateur d'un WLAN.

référentiel de sauvegarde en ligne

Emplacement sur le serveur en ligne pour stocker les fichiers après leur sauvegarde.

réseau

Ensemble de points d'accès et de leurs utilisateurs associés, qui équivaut à un ESS (jeu de service étendu).

réseau domestique

Plusieurs ordinateurs connectés dans une maison pour permettre le partage de fichiers et de l'accès à Internet. Voir aussi Réseau local.

réseau géré

Un réseau domestique comporte deux types de membres : des membres gérés et des membres non gérés. Les membres gérés autorisent les autres ordinateurs du réseau à surveiller l'état de leur protection, contrairement aux membres non gérés.

restauration

Récupération d'une copie d'un fichier à partir du référentiel de sauvegarde en ligne ou d'une archive.

rootkit

Ensemble d'outils (programmes) qui octroient à un utilisateur le niveau administrateur pour accéder à un ordinateur ou un réseau d'ordinateurs. Les rootkits peuvent comprendre des logiciels espions et d'autres programmes potentiellement indésirables qui peuvent engendrer des risques pour la sécurité et la confidentialité des données de votre ordinateur ou de vos informations personnelles.

routeur

Périphérique réseau qui transmet des paquets de données d'un réseau à un autre. Sur la base de tables de routage internes, les routeurs lisent les paquets entrants et décident comment les transférer d'après la combinaison d'adresses source et destination ainsi que les conditions de trafic actuelles (par exemple, charge, coût de la ligne et mauvaises lignes). Un routeur est parfois appelé Point d'accès (AP).

S

sauvegarder

Copier des fichiers importants sur un serveur sécurisé en ligne.

script

Liste de commandes qui peuvent être exécutées automatiquement (sans intervention de l'utilisateur). À la différence des programmes, les scripts sont généralement stockés en texte clair et compilés à chaque exécution. Les macros et fichiers batch sont aussi appelés scripts.

secret partagé

Chaîne ou clé (généralement un mot de passe) qui a été partagé entre deux interlocuteurs avant d'entamer une communication. Un secret partagé est utilisé pour protéger des parties sensibles de messages RADIUS.

serveur

Ordinateur ou programme qui accepte les connexions d'autres ordinateurs ou programmes et renvoie des réponses appropriées. Par exemple, votre programme de messagerie se connecte à un serveur de messagerie chaque fois que vous envoyez ou recevez des e-mails.

serveur DNS

Ordinateur qui renvoie l'adresse IP associée à un nom d'hôte ou de domaine. Voir aussi DNS.

serveur proxy

Composant du pare-feu qui gère le trafic Internet vers et depuis un réseau local (LAN). L'utilisation d'un serveur proxy améliore les performances par deux aspects : d'une part, il fournit des données fréquemment demandées, telles qu'une page Web, et d'autre part, il filtre les demandes et ignore celles que le propriétaire considère comme inappropriées (par exemple, les demandes d'accès non autorisées à des fichiers propriétaires).

SMTP

(Simple Mail Transfer Protocol) Protocole TCP/IP permettant de transmettre des messages d'un ordinateur à un autre sur un réseau. Ce protocole sert à router les courriers électroniques sur Internet.

SSID

(Service Set Identifier) Jeton (clé secrète) qui identifie un réseau Wi-Fi (802.11). Le SSID est défini par l'administrateur du réseau et doit être fourni par les utilisateurs qui souhaitent s'y joindre.

SSL

(Secure Sockets Layer) Protocole développé par Netscape pour transmettre des documents privés sur Internet. SSL utilise une clé publique pour chiffrer des données transférées sur une connexion SSL. Les URL qui exigent une connexion SSL commencent par https au lieu de http.

synchroniser

Résoudre les incohérences entre des fichiers sauvegardés et ceux stockés sur votre ordinateur local. La synchronisation des fichiers a lieu lorsque la version du fichier dans le référentiel de sauvegarde en ligne est plus récente que la version du fichier sur d'autres ordinateurs.

SystemGuard

Alertes McAfee qui détectent les modifications non autorisées apportées à votre ordinateur et vous en avertissent.

T

texte brut

Texte non chiffré. Voir aussi chiffrement.

texte chiffré

Texte codé par chiffrement. Le texte chiffré est illisible tant qu'il n'a pas été converti en texte brut (déchiffré).

TKIP

(Temporal Key Integrity Protocol) Protocole qui surmonte les faiblesses inhérentes à la sécurité WEP, notamment pour la réutilisation des clés de chiffrement. TKIP modifie les clés temporaires tous les 10 000 paquets, pour offrir une méthode de distribution dynamique qui améliore considérablement la sécurité du réseau. Le processus TKIP (sécurité) démarre par une clé temporaire à 128 bits partagée entre les clients et les points d'accès. Il associe la clé temporaire à l'adresse MAC du client, puis ajoute un vecteur d'initialisation de 16 octets relativement large pour produire la clé qui chiffre les données. Cette procédure permet de s'assurer que chaque station utilise des flux de clé différents pour chiffrer les données. TKIP utilise le RC4 pour procéder au chiffrement.

types de fichiers de surveillance

Types de fichiers (par exemple, .doc, .xls, etc.) que Data Backup sauvegarde ou archive dans les emplacements surveillés.

U

U3

(Plus simple, plus intelligent et mobile.) Plate-forme permettant d'exécuter Windows 2000 ou Windows XP directement depuis un lecteur USB. L'initiative U3 a été lancée en 2004 par M-Systems et SanDisk. Elle permet aux utilisateurs d'exécuter des programmes U3 sur un ordinateur Windows, sans installer ni stocker de données ou de paramètres sur l'ordinateur.

URL

(Uniform Resource Locator) Format standard des adresses Internet.

USB

(Bus série universel) Interface informatique série standardisée permettant de connecter des périphériques tels que des claviers, des joysticks et des imprimantes à votre ordinateur.

usurpation d'adresse IP

Action de falsifier les adresses IP dans un paquet IP. Ceci est utilisé dans de nombreux types d'attaques, notamment la prise de contrôle des sessions, et sert souvent à falsifier les en-têtes des courriers électroniques de spam pour empêcher leur traçage.

V

ver

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. Les vers reproduisent et consomment les ressources du système, ce qui ralentit les performances ou interrompt les tâches.

Virus

Programmes qui se propagent et peuvent endommager vos fichiers et données. En général, leur expéditeur semble digne de foi ou leur contenu apparaît comme fiable.

VPN

(Virtual Private Network) Réseau privé configuré au sein d'un réseau public afin de profiter des fonctions de gestion du réseau public. Les VPN sont utilisés par les entreprises pour créer des réseaux WAN (wide area networks) s'étendant sur de grandes régions géographiques, afin de fournir des connexions de site à site avec leurs filiales ou pour permettre à des utilisateurs mobiles de se connecter au LAN de l'entreprise par numérotation.

W

wardriver

Personne qui cherche des réseaux Wi-Fi (802.11) en se déplaçant dans les villes équipé d'un ordinateur Wi-Fi et d'un matériel ou logiciel spécial.

Webmail

Messages envoyés et reçus électroniquement via Internet. Voir aussi e-mail.

WEP

(Wired Equivalent Privacy) Protocole de chiffrement et d'authentification défini dans le cadre de la norme Wi-Fi (802.11). Les premières versions sont basées sur des chiffrements RC4 et présentent des faiblesses considérables. WEP tente d'apporter un minimum de sécurité en chiffrant les données sur des ondes radio pour qu'elles soient protégées lors de leur transfert d'un point d'extrémité à un autre. On a toutefois découvert que WEP n'est pas aussi sûr qu'on le pensait.

Wi-Fi

(Wireless Fidelity) Terme utilisé par la Wi-Fi Alliance pour faire référence à tout type de réseau 802.11.

Wi-Fi Alliance

Organisation composée des grands fournisseurs de matériels et logiciels sans fil. La Wi-Fi Alliance cherche à certifier l'interopérabilité de tous les produits basés sur 802.11 et à promouvoir le terme Wi-Fi comme nom de marque global sur tous les marchés pour tout produit LAN sans fil basé sur 802.11. L'organisation agit comme un consortium, un laboratoire de test et un centre d'informations pour les fournisseurs qui veulent promouvoir la croissance du marché.

WLAN

(Wireless Local Area Network) Réseau local (LAN) utilisant une connexion sans fil. Un réseau local sans fil utilise des ondes radio hautes fréquences à la place des fils pour permettre aux ordinateurs de communiquer entre eux.

WPA

(Wi-Fi Protected Access) Norme de spécification qui augmente fortement le niveau de protection des données et le contrôle d'accès des systèmes de réseau local sans fil actuels et futurs. Conçu pour fonctionner sur le matériel existant sous la forme d'une mise à niveau du logiciel, le WPA est issu de la norme IEEE 802.11i avec laquelle il est compatible. Lorsqu'il est correctement installé, il offre aux utilisateurs d'un réseau local sans fil un niveau de certitude élevé sur le fait que leurs données sont protégées et que seuls les utilisateurs autorisés à utiliser le réseau y auront accès.

WPA-PSK

Mode WPA spécial, conçu pour les utilisateurs à domicile qui n'ont pas besoin de la sécurité nécessaire aux entreprises et n'ont pas accès à des serveurs d'authentification. Avec ce mode, l'utilisateur à domicile entre manuellement le mot de passe de départ pour activer l'accès Wi-Fi protégé en mode clé pré-partagée et doit régulièrement modifier le mot de passe sur chaque ordinateur sans fil et point d'accès. Voir aussi WPA2-PSK et TKIP.

WPA2

Mise à jour de la norme de sécurité WPA, basée sur la norme 802.11i IEEE.

WPA2-PSK

Mode spécial de WPA, similaire à WPA-PSK, basé sur la norme WPA2. Cette norme établit, parmi ses fonctions générales, que les périphériques acceptent souvent plusieurs modes de chiffrement (comme AES, TKIP) simultanément, tandis que les plus anciens n'acceptent généralement qu'un mode de chiffrement à la fois (tous les clients doivent utiliser le même mode de chiffrement).

A propos de McAfee

McAfee, Inc., leader mondial en gestion des risques de sécurité et prévention des intrusions et dont le siège social est basé à Santa Clara, Californie, propose des solutions et services proactifs et éprouvés de sécurisation des systèmes et réseaux dans le monde entier. Avec son expérience de la sécurité et son engagement à l'innovation sans égal, McAfee donne aux particuliers, aux entreprises, au secteur public et aux prestataires de service la capacité de bloquer les attaques, de prévenir les perturbations et d'assurer et d'améliorer régulièrement leur sécurité.

Copyright

Licence

A L'ATTENTION DE TOUS LES UTILISATEURS : LISEZ ATTENTIVEMENT L'ACCORD JURIDIQUE CORRESPONDANT A LA LICENCE QUE VOUS AVEZ ACHETEE. IL DEFINIT LES CONDITIONS GENERALES D'UTILISATION DU LOGICIEL SOUS LICENCE. SI VOUS IGNOREZ LE TYPE DE LICENCE QUE VOUS AVEZ ACQUIS, REPORTEZ-VOUS AUX DOCUMENTS COMMERCIAUX ET AUTRES DOCUMENTS D'OCTROI DE LICENCE, OU AU BON DE COMMANDE, QUI ACCOMPAGNENT VOTRE PROGICIEL OU QUI VOUS ONT ÉTÉ TRANSMIS SÉPARÉMENT DANS LE CADRE DE VOTRE ACHAT (SOUS LA FORME D'UN LIVRET, D'UN FICHIER INCLUS DANS LE CD DU PRODUIT OU D'UN FICHIER DISPONIBLE SUR LE SITE WEB A PARTIR DUQUEL VOUS AVEZ TÉLÉCHARGÉ LE PROGICIEL). SI VOUS N’ÊTES PAS D’ACCORD AVEC CERTAINS TERMES DE CET ACCORD, N’INSTALLEZ PAS LE LOGICIEL. LE CAS ECHEANT, VOUS POUVEZ RENVOYER LE PRODUIT A MCAFEE, INC. OU A L’ENDROIT OU VOUS L’AVEZ ACHETE AFIN D’EN OBTENIR LE REMBOURSEMENT INTEGRAL.

CHAPITRE 46

Service clientèle et support technique

SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Les problèmes de protection critiques exigent une action immédiate et compromettent votre état de protection (qui passe au rouge). Les problèmes de protection non critiques n'exigent pas d'action immédiate et peuvent ou non compromettre votre état de protection (selon le type de problème). Pour obtenir un état de protection vert, vous devez corriger tous les problèmes critiques et résoudre ou ignorer tous les problèmes non critiques. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician. Pour plus d'informations sur McAfee Virtual Technician, consultez l'aide de McAfee Virtual Technician.

Si vous avez acheté votre logiciel de sécurité chez un partenaire ou un fournisseur autre que McAfee, ouvrez un navigateur Web et accédez à www.mcafeeaide.com. Sous Partner Links, sélectionnez votre partenaire ou fournisseur pour accéder à McAfee Virtual Technician.

Remarque : Pour installer et exécuter McAfee Virtual Technician, vous devez vous connecter à votre ordinateur en tant qu'administrateur Windows. Si vous ne le faites pas, MVT sera peut-être dans l'impossibilité de résoudre vos problèmes. Pour plus d'informations sur la connexion en tant qu'administrateur Windows, consultez l'aide de Windows. Dans Windows Vista™, une invite s'affiche lorsque vous lancez MVT. Cliquez alors sur **Accepter**. Virtual Technician ne fonctionne pas avec Mozilla® Firefox.

Contenu de ce chapitre

Utilisation de McAfee Virtual Technician 278
Assistance et téléchargements 279

Utilisation de McAfee Virtual Technician

À la manière d'un technicien d'assistance personnel, Virtual Technician collecte des informations sur vos programmes SecurityCenter pour résoudre les problèmes de protection de votre ordinateur. Lorsque vous exécutez Virtual Technician, il s'assure que vos programmes SecurityCenter fonctionnent correctement. S'il découvre des problèmes, il propose de les corriger pour vous ou dispense des informations détaillées à leur sujet. Lorsqu'il a terminé, Virtual Technician affiche les résultats de son analyse et vous permet de demander une aide technique supplémentaire de McAfee, le cas échéant.

Pour maintenir la sécurité et l'intégrité de votre ordinateur et de vos fichiers, Virtual Technician ne collecte pas d'informations personnelles identifiables.

Remarque : Pour plus d'informations sur Virtual Technician, cliquez sur l'icône **Aide** dans Virtual Technician.

Lancez Virtual Technician

Virtual Technician collecte des informations sur vos programmes SecurityCenter pour vous aider à résoudre vos problèmes de protection. Afin de préserver votre confidentialité, ces informations ne comprennent pas de données personnelles identifiables.

1. Sous **Tâches courantes**, cliquez sur **McAfee Virtual Technician**.
2. Suivez les instructions à l'écran pour télécharger et exécuter Virtual Technician.

Assistance et téléchargements

Consultez les tableaux suivants pour trouver les sites Assistance et téléchargements McAfee de votre pays, y compris les Guides de l'utilisateur.

Assistance et téléchargements

Pays	Assistance McAfee	Téléchargements McAfee
Australie	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brésil	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canada (anglais)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Canada (français)	www.mcafeeaide.com	ca.mcafee.com/root/downloads.asp
Chine (chn)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Chine (tw)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
République tchèque	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Danemark	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finlande	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
France	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Allemagne	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Grande-Bretagne	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Italie	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japon	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Corée	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Mexique	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Norvège	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Pologne	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp

Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Espagne	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Suède	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Turquie	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Etats-Unis	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

Guides de l'utilisateur de McAfee Total Protection

Pays	Guides de l'utilisateur McAfee
Australie	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brésil	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canada (anglais)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Canada (français)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Chine (chn)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Chine (tw)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
République tchèque	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Danemark	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finlande	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
France	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Allemagne	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Grande-Bretagne	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Pays-Bas	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Italie	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japon	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf

Corée	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Mexique	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norvège	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Pologne	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Espagne	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Suède	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Turquie	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Etats-Unis	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

Guides de l'utilisateur McAfee Internet Security

Pays	Guides de l'utilisateur McAfee
Australie	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brésil	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Canada (anglais)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Canada (français)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Chine (chn)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Chine (tw)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
République tchèque	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Danemark	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finlande	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
France	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Allemagne	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf

Grande-Bretagne	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Pays-Bas	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Italie	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japon	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Corée	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Mexique	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norvège	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Pologne	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Espagne	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Suède	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Turquie	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Etats-Unis	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

Guides de l'utilisateur de McAfee VirusScan Plus

Pays	Guides de l'utilisateur McAfee
Australie	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brésil	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canada (anglais)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Canada (français)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Chine (chn)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Chine (tw)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
République tchèque	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf

Danemark	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finlande	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
France	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Allemagne	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Grande-Bretagne	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Pays-Bas	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Italie	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japon	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Corée	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Mexique	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norvège	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Pologne	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Espagne	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Suède	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Turquie	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Etats-Unis	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

Guides de l'utilisateur de McAfee VirusScan

Pays	Guides de l'utilisateur McAfee
Australie	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brésil	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Canada (anglais)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf

Canada (français)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Chine (chn)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Chine (tw)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
République tchèque	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Danemark	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finlande	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
France	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Allemagne	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Grande-Bretagne	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Pays-Bas	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Italie	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japon	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Corée	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Mexique	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norvège	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Pologne	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Espagne	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Suède	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Turquie	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Etats-Unis	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Consultez le tableau suivant pour connaître les sites d'informations Centre de menaces et Informations sur les virus McAfee dans votre pays.

Pays	Siège social du service de sécurité	Informations sur les virus
Australie	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brésil	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canada (anglais)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canada (français)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Chine (chn)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Chine (tw)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
République tchèque	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Danemark	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finlande	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
France	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Allemagne	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Grande-Bretagne	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Pays-Bas	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Italie	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japon	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Corée	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Mexique	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norvège	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Pologne	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo

Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Espagne	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Suède	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Turquie	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Etats-Unis	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Consultez le tableau suivant puor connaître les sites HackerWatch dans votre pays.

Pays	HackerWatch
Australie	www.hackerwatch.org
Brésil	www.hackerwatch.org/?lang=pt-br
Canada (anglais)	www.hackerwatch.org
Canada (français)	www.hackerwatch.org/?lang=fr-ca
Chine (chn)	www.hackerwatch.org/?lang=zh-cn
Chine (tw)	www.hackerwatch.org/?lang=zh-tw
République tchèque	www.hackerwatch.org/?lang=cs
Danemark	www.hackerwatch.org/?lang=da
Finlande	www.hackerwatch.org/?lang=fi
France	www.hackerwatch.org/?lang=fr
Allemagne	www.hackerwatch.org/?lang=de
Grande-Bretagne	www.hackerwatch.org
Pays-Bas	www.hackerwatch.org/?lang=nl
Italie	www.hackerwatch.org/?lang=it
Japon	www.hackerwatch.org/?lang=jp
Corée	www.hackerwatch.org/?lang=ko
Mexique	www.hackerwatch.org/?lang=es-mx
Norvège	www.hackerwatch.org/?lang=no
Pologne	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Espagne	www.hackerwatch.org/?lang=es

Suède	www.hackerwatch.org/?lang=sv
Turquie	www.hackerwatch.org/?lang=tr
Etats-Unis	www.hackerwatch.org

Index

8

802.11 259
802.11a....259
802.11b 259
802.1x....259

A

A propos de McAfee....275
A propos des alertes....72
À propos des types de listes approuvées54
À propos des types de SystemGuards ...48, 49
A propos du graphique d'analyse du trafic 124
Accéder à la carte du réseau 228
Acceptation d'un fichier provenant d'un autre ordinateur 253, 254
Activation de la protection par pare-feu69
Activation des recommandations intelligentes 83
Activation du niveau de sécurité Elevé ..80
Activation du niveau de sécurité Faible.81
Activation du niveau de sécurité Furtif..80
Activation du niveau de sécurité Ouvert82
Activation du niveau de sécurité Standard 81
Activation du niveau de sécurité Verrouillage 79
Activer la protection SystemGuards....47
Actualiser la carte du réseau 228
adaptateur sans fil 259
Adresse IP....259
Adresse MAC....259
Affichage des événements....18, 29
Affichage des événements de détection des intrusions 119
Affichage des recommandations intelligentes uniquement 84
Affichage et masquage d'alertes d'information 24
Afficher des alertes durant une session de jeu....75
Afficher les détails d'un élément 229
Afficher les événements entrants 119
Afficher les événements récents 29, 118
Afficher les événements sortants....93, 119
Afficher les résultats de l'analyse 59
Afficher les statistiques générales des événements de sécurité 120
Afficher ou masquer des alertes d'information 24
Afficher ou masquer des alertes d'information pendant un jeu 25
Afficher ou masquer des problèmes ignorés 20
Afficher ou masquer un élément de la carte du réseau 229
Afficher tous les événements....30
Afficher un événement associé à un Webmail filtré....160
Afficher un résumé de votre activité d'archivage 206
Affiliation à un réseau géré ... 231, 244, 248
Affiliation au réseau 245
Affiliation au réseau géré 230
Ajout d'une connexion fiable à un ordinateur....110
Ajout d'une connexion interdite à un ordinateur....113
Ajouter manuellement un ami 143
Ajouter un ami à partir de la barre d'outils d'Anti-Spam 143
Ajouter un carnet d'adresses 140
Ajouter un compte Webmail 134
Ajouter un domaine 144
Ajouter un filtre personnel 152
Ajouter un mot de passe 186
Ajouter un ordinateur autorisé depuis le journal des événements entrants 111
Ajouter un site Web à la liste d'autorisation....161
Ajouter un utilisateur McAfee 170
Analyse à la demande 259
Analyse de votre ordinateur 33, 57
analyse en temps réel....260
Analyser le trafic entrant et sortant....125
Analyser votre ordinateur....58
Appliquer les filtres de jeux de caractères 150
archivage complet....260
Archivage de fichiers....193
archivage rapide....260
archiver 260

Arrêt de la surveillance de l'état de protection d'un ordinateur.....236
Arrêter la protection antivirus en temps réel.....34
Assistance et téléchargements.....279
attaque en force.....260
attaque par dictionnaire.....260
attaque par immixtion.....260
Attribution d'un nouveau nom au réseau.....229, 247
authentification.....260
Autorisation d'accès au réseau.....245
Autorisation de l'accès Internet des programmes.....92
Autorisation de l'accès sortant uniquement des programmes.....95
Autoriser l'accès à un port de service système existant.....105
Autoriser l'accès sortant uniquement d'un programme.....95
Autoriser l'accès total d'un nouveau programme.....93
Autoriser l'accès total d'un programme 92
Autoriser un accès sortant uniquement depuis le journal des événements récents.....95
Autoriser un accès sortant uniquement depuis le journal des événements sortants.....96
Autoriser un accès total depuis le journal des événements récents.....93
Autoriser un accès total depuis le journal des événements sortants.....94
Autoriser un site Web.....179

B

bande passante.....260
Basculer vers des utilisateurs Windows.....170
base de registre.....260
bibliothèque.....260
Blocage de l'accès à un port de service système.....105
Blocage de l'accès d'un nouveau programme.....97
Blocage de l'accès d'un programme.....97
Blocage de l'accès Internet des programmes.....97
Blocage de sites Web en fonction de mots clés.....182
Blocage d'un site Web.....178
Bloquer l'accès depuis le journal des événements récents.....98
Broyage de fichiers, dossiers et disques.....221
Broyer les fichiers et les dossiers.....221
Broyer un disque entier.....222

C

cache.....261
Caractéristiques.....192
carte adaptateur sans fil USB.....261
carte du réseau.....261
cartes adaptateur sans fil PCI.....261
certifié Wi-Fi.....261
Cheval de Troie.....261
chiffrement.....261
clé.....261
Clé.....261
clé USB.....261
client.....261
client de messagerie.....262
code d'authentification des messages (MAC).....262
Comment quitter un réseau géré.....248
compression.....262
compte de messagerie standard.....262
Configuration automatique d'amis.....140
Configuration de EasyNetwork.....243
Configuration de la détection de spam147
Configuration de la détection des intrusions.....86
Configuration de la protection antiphishing.....161
Configuration de la protection antivirus.....39, 57
Configuration de la protection par pare-feu.....77
Configuration de Password Vault.....186
Configuration des amis.....139
Configuration des comptes Webmail.....133
Configuration des heures limites de navigation Web.....177
Configuration des options d'alerte.....26
Configuration des options d'analyse en temps réel.....40
Configuration des options d'analyse manuelle.....42
Configuration des options SystemGuards.....48
Configuration des paramètres de requête ping.....86
Configuration des paramètres du journal d'événements.....118
Configuration des ports de service système.....104

Configuration des recommandations intelligentes pour les alertes.....83
Configuration des utilisateurs 168
Configuration du contrôle parental 167
Configuration du groupe de classification du contenu.....174, 175
Configuration du groupe de classification du contenu pour un utilisateur.....175
Configuration d'un réseau géré.....227
Configuration manuelle d'amis.....143
Configurer l'emplacement de l'analyse manuelle 44
Configurer les mises à jour automatiques 14
Configurer les options d'analyse en temps réel.....40
Configurer les options d'analyse manuelle 43
Configurer les paramètres relatifs à l'état de la protection par pare-feu.....87
Configurer un nouveau port de service système 105
Consignation, surveillance et analyse..117
Consulter l'activité générale des ports Internet 120
Contrôle ActiveX.....262
Contrôle parental 262
cookie 262
Copie d'un fichier partagé 251
Copier ou supprimer un message Webmail filtré.....160
Copyright 275
Corbeille.....262
Critères de recherche 251, 252

D

DAT.....262
débordement de la mémoire tampon..263
Définir des heures limites de navigation Web 177
Définition des options de filtrage.....148
Définition des types de fichiers archivés 196
Défragmentation de votre ordinateur..212
Défragmenter votre ordinateur 212
Démarrage de la protection antivirus en temps réel 33
Démarrage de la protection supplémentaire 35
Démarrage du pare-feu.....69
Démarrer la protection antivirus en temps réel 33
Démarrer la protection contre les logiciels espions.....36
Démarrer la protection de la messagerie instantanée.....37
Démarrer la protection des e-mails 37
déni de service 263
Désactivation de la protection antiphishing 163
Désactivation de la protection antispam 147
Désactivation de la protection par pare-feu 70
Désactivation des recommandations intelligentes 84
Désactivation du chiffrement et la compression des archives 198
Désactiver la barre d'outils Anti-Spam 157
Désactiver le filtrage par mots clés 181
Désactiver les mises à jour automatiques 15
Désactiver un filtre spécial 149
Déverrouillage instantané du pare-feu..88
disque dur externe 263
DNS 263
domaine 263

E

e-mail 263
Emettre un son en cas d'alerte 26
emplacement de surveillance accrue ..263
emplacements de surveillance de premier niveau 263
emplacements surveillés 263
En savoir plus sur les programmes 100
Envoi de fichiers à d'autres ordinateurs 253
Envoi d'un fichier à un autre ordinateur 253
ESS.....264
événement 264
Exclusion d'un emplacement des archives 196
Explications sur les catégories de protection 7, 9, 29
Explications sur les informations de compte Webmail..... 134, 135, 136
Explications sur les services de protection 10
Explications sur l'état de protection 7, 8, 9
Exploitation des résultats d'analyse.....61

F

fenêtres instantanées.....264
Fiabilité des connexions informatiques 110
fichier temporaire 264

Filtrage de sites Web.....175, 178
Filtrage de sites Web par mots clés 178, 181
Filtrage des e-mails 155
Filtrage des images Web potentiellement inappropriées 174
filtrage d'images 264
Filtrer les images Web potentiellement inappropriées 174
Fin de partage d'un fichier.....251
Fin de partage d'une imprimante 256
Fonctionnalités d'Anti-Spam 131
Fonctionnalités de Network Manager .224
Fonctionnalités de Privacy Service.....166
Fonctionnalités d'EasyNetwork 242
Fonctions de Personal Firewall 66
Fonctions de QuickClean.....208
Fonctions de SecurityCenter 6
Fonctions de Shredder.....220
Fonctions de VirusScan.....32
fragments de fichier.....264

G

Gérer des fichiers en quarantaine 62, 63
Gérer des programmes et cookies en quarantaine 63
Gérer les programmes potentiellement indésirables 62
Gérer les virus et chevaux de Troie.....62
Gérer votre compte McAfee.....11
Gestion à distance du réseau.....235
Gestion de votre compte McAfee 11
Gestion des alertes de type Informations 75
Gestion des archives.....206
Gestion des connexions informatiques 109
Gestion des listes approuvées.....53
Gestion des niveaux de sécurité du pare-feu.....78
Gestion des programmes et des autorisations.....91
Gestion des services système.....103
Gestion des utilisateurs McAfee ...169, 170
Gestion des utilisateurs Windows 169
Gestion d'un matériel.....237
groupe d'évaluation de contenu 264

I

Ignorer des problèmes de protection.....20
Ignorer un problème de protection 20
Inclusion d'un emplacement dans les archives 195
Installation de McAfee Security sur les ordinateurs distants.....240
Installation d'une imprimante réseau disponible.....256
Interdiction de connexions informatiques 113
Interdiction d'un ordinateur depuis le journal des événements de détection des intrusions.....116
Interdiction d'un ordinateur depuis le journal des événements entrants 115
Internet 264
Interruption d'un archivage automatique 200
intranet 264
Inviter un ordinateur à s'affilier au réseau géré.....231
itinérance.....265

J

Journalisation des événements 118

L

LAN.....265
Lancement d'archivages complets et rapides 199
Lancement du didacticiel HackerWatch 128
Lancement manuel de l'archivage.....200
Lancer l'analyse de scripts.....36
Lancez Virtual Technician.....278
Launchpad.....265
lecteur réseau 265
Licence 276
liste approuvée 265
liste d'autorisation 265
liste de blocage 265

M

MAPI.....265
Marquer un message à partir de la barre d'outils Anti-Spam.....155
Masquer l'écran d'accueil au démarrage 26
Masquer les alertes d'attaque virale 27
Masquer les alertes de type Informations 76
McAfee Anti-Spam 129
McAfee Data Backup.....191
McAfee EasyNetwork 241
McAfee Internet Security 3
McAfee Network Manager.....223
McAfee Personal Firewall 65
McAfee Privacy Service 165

McAfee QuickClean 207
McAfee SecurityCenter 5
McAfee Shredder 219
McAfee VirusScan 31
Mettre à jour un site Web filtré 179
Mise à jour de SecurityCenter 13
Modification de l'emplacement d'archivage 197
Modification des autorisations d'un ordinateur géré 237
Modification des paramètres d'affichage d'un matériel 238
Modification d'un port de service système 106
Modification d'une connexion fiable à un ordinateur 111
Modification d'une connexion interdite à un ordinateur 114
Modifier des sites dans la liste d'autorisation 162
Modifier la façon dont un message est traité et marqué 152, 156
Modifier le mot de passe de l'administrateur McAfee 172
Modifier le mot de passe Password Vault 188
Modifier le niveau de filtrage 149
Modifier les données d'un compte utilisateur McAfee 171
Modifier un ami 144
Modifier un carnet d'adresses 141
Modifier un compte Webmail 134
Modifier un domaine 145
Modifier un filtre personnel 153
Modifier un mot de passe 186
Modifier une tâche Défragmenteur de disque 216
Modifier une tâche QuickClean 214
mot clé 265
mot de passe 265
MSN 266

N

navigateur 266
Ne plus approuver les ordinateurs du réseau 233
Nettoyage de votre ordinateur 209, 211
NIC 266
nœud 266
numéroteur 266

O

Obtenir des informations concernant l'enregistrement d'un ordinateur 121
Obtenir des informations sur un programme depuis le journal des événements sortants 101
Obtention d'informations concernant le réseau d'un ordinateur 122
Obtention d'informations sur la sécurité Internet 127
Obtention d'informations sur un programme 100
Optimisation de la sécurité du pare-feu 85
Ouvrir EasyNetwork 243
Ouvrir un fichier archivé 203

P

pare-feu 266
Partage de fichiers 250
Partage d'imprimantes 255
Partage d'un fichier 250
Partage et envoi des fichiers 249
partager 266
passerelle intégrée 266
Password Vault 266
phishing 267
Pixels invisibles 267
Planification d'archivages automatiques 199
plug-in 267
Point d'accès 267
point d'accès non fiable 267
point d'accès sans fil 267
point de restauration système 267
POP3 267
port 267
PPPoE 268
Présentation des icônes de Network Manager 225
Programmation d'une tâche 213
programme potentiellement indésirable (PUP) 268
Programmer une analyse 45
Programmer une tâche Défragmenteur de disque 216
Programmer une tâche QuickClean 213
Protection de votre ordinateur au démarrage 85
Protection des informations personnelles 184
Protection des mots de passe 185
Protection d'informations sur le Web 183
Protéger les informations personnelles 184
protocole 268
proxy 268
publier 268

Q

quarantaine....268

R

raccourci....268
RADIUS....268
Réception d'une notification lors de l'envoi d'un fichier....254
Recherche d'un fichier archivé....203
Recherche d'un fichier partagé....251
Rechercher des mises à jour....14, 15
Récupérer le mot de passe de l'administrateur McAfee....173
Référence....258
référentiel de sauvegarde en ligne....268
Réglage des options d'archivage....194
Réinitialiser le mot de passe Password Vault....188
Réparation automatique des failles de sécurité....239
Réparation des failles de sécurité....239
réseau....268
réseau domestique....269
réseau géré....269
Résolution automatique des problèmes de protection....18
Résolution des problèmes de protection 8, 18
Résolution manuelle des problèmes de protection....19
Résoudre ou ignorer des problèmes de protection....8, 17
restauration....269
Restauration de fichiers archivés....204
Restauration des fichiers manquants à partir d'une archive locale....204
Restauration d'une ancienne version d'un fichier à partir des archives locales....205
Restaurer les paramètres du pare-feu....89
rootkit....269
routeur....269

S

sauvegarder....269
script....269
secret partagé....269
serveur....269
serveur DNS....270
serveur proxy....270
Service clientèle et support technique....277
Signaler les spams à McAfee....159
SMTP....270
Spécification d'un filtre personnel....153, 154
SSID....270
SSL....270
Suivi du trafic Internet....121
Suivi d'un ordinateur depuis le journal des événements entrants....122
Suivi d'une adresse IP surveillée....123
Suivre géographiquement un ordinateur en réseau....121
Suivre un ordinateur depuis le journal des événements de détection des intrusions....122
Suppression des autorisations d'accès de certains programmes....99
Suppression des autorisations d'un programme....99
Suppression d'un port de service système....107
Suppression d'une connexion fiable à un ordinateur....112
Suppression d'une connexion interdite à un ordinateur....114
Supprimer les fichiers de la liste des fichiers manquants....205
Supprimer un ami....145
Supprimer un carnet d'adresses....141
Supprimer un compte Webmail....135
Supprimer un filtre personnel....153
Supprimer un mot de passe....187
Supprimer un site Web de la liste d'autorisation....162
Supprimer un site Web filtré....180
Supprimer un utilisateur McAfee....171
Supprimer une tâche Défragmenteur de disque....217
Supprimer une tâche QuickClean....215
Surveillance de la bande passante utilisée par les programmes....125
Surveillance de l'activité des programmes....125
Surveillance de l'état de protection d'un ordinateur....236
Surveillance de l'état et des autorisations....236
Surveillance du trafic Internet....124
synchroniser....270
SystemGuard....270

T

texte brut....270
texte chiffré....270
TKIP....271
Traitement du e-mails filtrés....159

Tri des fichiers archivés.....202
types de fichiers de surveillance.....271

U

U3 271
URL.....271
USB.....271
usurpation d'adresse IP 271
Utilisation de filtres personnels 152
Utilisation de la carte du réseau.....228
Utilisation de l'explorateur d'archives locales 202
Utilisation de McAfee Virtual Technician 278
Utilisation de SecurityCenter 7
Utilisation des alertes..... 14, 23, 71
Utilisation des fichiers archivés.....201
Utilisation des listes approuvées.....53
Utilisation des options SystemGuards...46
Utilisation des statistiques.....120
Utilisation d'imprimantes partagées ...256

V

ver 271
Vérifier votre abonnement.....11
Verrouillage et restauration du pare-feu88
Verrouillage instantané du pare-feu 88
Virus.....271
VPN.....272

W

wardriver 272
Webmail 272
WEP 272
Wi-Fi 272
Wi-Fi Alliance.....272
WLAN 272
WPA 272
WPA2 273
WPA2-PSK 273
WPA-PSK 273