McAfee®

VirusScan® Plus

AntiVirus, Firewall & AntiSpyware

Guide de l'utilisateur

Table des matières

Introduction 3

McAfee SecurityCenter 5
Fonctions de SecurityCenter 6
Utilisation de SecurityCenter 7
Résoudre ou ignorer des problèmes de protection 17
Utilisation des alertes 21
Affichage des événements 27
McAfee VirusScan 29
Fonctions de VirusScan 30
Analyse de votre ordinateur 31
Exploitation des résultats d'analyse 37
Types d'analyse 41
Utilisation d'une protection supplémentaire 43
Configuration de la protection antivirus 47
McAfee Personal Firewall 67
Fonctionnalités de Personal Firewall 68
Démarrage du pare-feu 71
Utilisation des alertes 73
Gestion des alertes de type Informations 77
Configuration de la protection par pare-feu 79
Gestion des programmes et des autorisations 89
Gestion des connexions informatiques 99
Gestion des services système 107
Consignation, surveillance et analyse 113
Obtention d'informations sur la sécurité Internet 123
McAfee QuickClean 125
Fonctions de QuickClean 126
Nettoyage de votre ordinateur 127
Défragmentation de votre ordinateur 131
Programmation d'une tâche 133
McAfee Shredder 139
Fonctions de Shredder 140
Broyage de fichiers, dossiers et disques 140
McAfee Network Manager 143
Fonctionnalités de Network Manager 144
Présentation des icônes de Network Manager 145
Configuration d'un réseau géré 147
Gestion à distance du réseau 153
Surveillance des réseaux 159
McAfee EasyNetwork 163
Fonctionnalités d'EasyNetwork 164
Configuration de EasyNetwork 165
Partage et envoi des fichiers 171
Partage d'imprimantes 177

Référence 179

Glossaire 180

A propos de McAfee 195

Licence 195
Copyright 196
Service clientèle et support technique 197
Utilisation de McAfee Virtual Technician 198

Index 208

CHAPITRE 1

Introduction

Armez votre ordinateur d'une solution de sécurité regroupant les technologies de protection (pare-feu, analyse virale, protection contre les logiciels espions) de McAfee. Utilisez VirusScan Plus pour protéger votre ordinateur contre les virus, traquer les activités suspectes dans le trafic Internet et empêcher les logiciels espions d'altérer l'intégrité de vos informations personnelles.

Contenu de ce chapitre

McAfee SecurityCenter 5
McAfee VirusScan 29
McAfee Personal Firewall 67
McAfee QuickClean 125
McAfee Shredder 139
McAfee Network Manager 143
McAfee EasyNetwork 163
Référence 179
A propos de McAfee 195
Service clientèle et support technique 197

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
Résoudre ou ignorer des problèmes de protection....17
Utilisation des alertes....21
Affichage des événements....27

Fonctions de SecurityCenter

Etat de protection simplifié

Permet de consulter facilement le niveau de protection de votre ordinateur, de rechercher les mises à jour disponibles et de résoudre les éventuels problèmes de protection.

Mises à jour et mises à niveau automatiques

Permet de télécharger et d'installer 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.

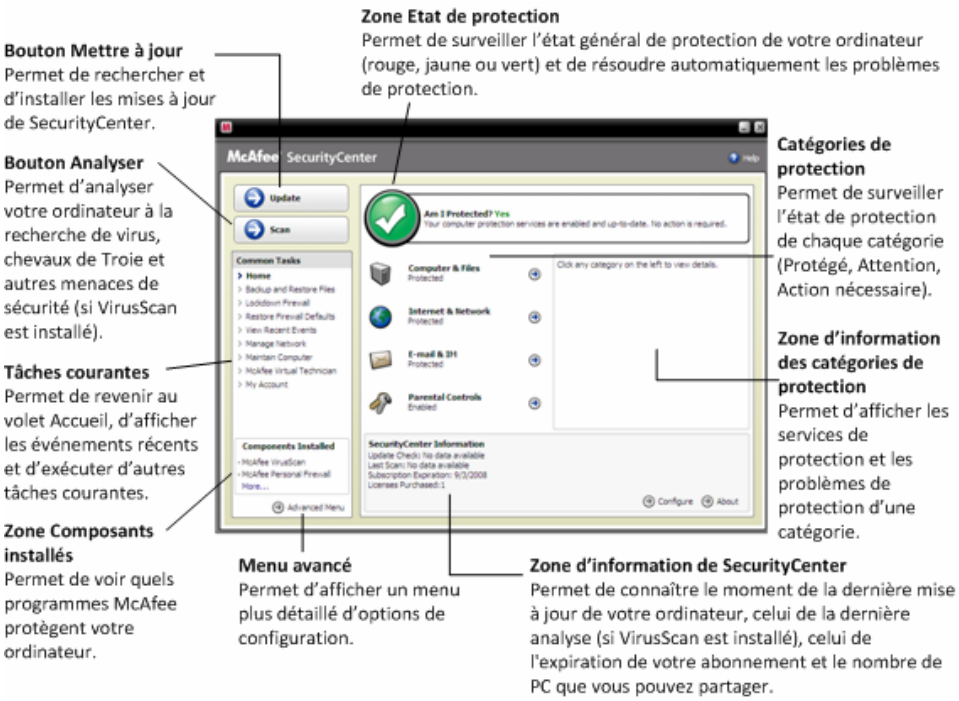
Alertes en temps réel

Les alertes de sécurité vous signalent la présence d'un virus et d'une menace de sécurité et permettent de supprimer la menace, de la neutraliser ou d'en savoir plus à son sujet.

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 vos abonnements 11
Mise à jour de SecurityCenter 13

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 : ordinateurs & 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 contre les logiciels espions ▪ SystemGuards ▪ Protection Windows ▪ Intégrité du PC
Internet & réseau	La catégorie Internet & réseau permet de configurer les services de protection suivants : ▪ Protection par pare-feu ▪ Protection antiphishing ▪ Protection des données personnelles
E-mail & messagerie instantanée	La catégorie E-mail & messagerie instantanée permet de configurer les services de protection suivants : ▪ Protection contre les virus électroniques ▪ Protection contre les virus IM ▪ Protection contre les logiciels espions de messagerie ▪ Protection contre les logiciels espions de messagerie instantanée ▪ 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 différents composants de sécurité que vous configurez pour protéger votre ordinateur et vos fichiers. 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 contre les logiciels espions, SystemGuards et analyse de script. 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 Parental controls, 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 vos abonnements

Chaque produit de protection McAfee acheté est accompagné d'un abonnement qui vous permet d'utiliser le produit sur un certain nombre d'ordinateurs pour une période donnée. La durée de l'abonnement varie en fonction de l'achat, mais démarre généralement lorsque vous activez le produit. L'activation est simple et gratuite. Vous avez juste besoin d'une connexion Internet—car l'activation vous permet de recevoir des mises à jour de produits automatiques régulières qui protègent votre ordinateur des menaces récentes.

L'activation survient généralement lorsque le produit est installé. Toutefois, si vous décidez d'attendre (si vous n'avez pas de connexion Internet par exemple), vous disposez d'un délai de 15 jours pour procéder à l'activation. Si vous n'activez pas le produit dans les 15 jours, vos produits ne recevront plus de mises à jour critiques et ne procèderont plus à des analyses. Vous recevrez également régulièrement des messages à l'écran avant que votre abonnement n'expire. De cette manière, vous pouvez bénéficier d'une protection continue en la renouvelant en avance ou en configurant un renouvellement automatique sur notre site Web.

Si un lien dans SecurityCenter vous invite à activer le produit, cela signifie que votre abonnement n'a pas été activé. Pour connaître la date d'expiration de votre abonnement, vous pouvez vérifier votre page Mon compte.

Accès à 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.

Activation de votre produit

L'activation survient généralement à l'installation de votre produit. Dans le cas contraire, un lien dans SecurityCenter vous invitera à procéder à l'activation. Vous recevrez régulièrement des notifications.

- Dans le volet Accueil de SecurityCenter, sous **SecurityCenter - Informations**, cliquez sur **Activez votre abonnement**.

Conseil : vous pouvez également activer le produit à partir des alertes qui s'affichent régulièrement.

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**.

Renouvelement de votre abonnement

Peu avant l'expiration de votre abonnement, un lien dans SecurityCenter vous invitera à le renouveler. Nous vous avertirons également régulièrement des expirations en attente associées à des alertes.

- Dans le volet Accueil de SecurityCenter, sous **SecurityCenter - Informations**, cliquez sur **Renouveler**.

Conseil : vous pouvez renouveler votre produit à partir du message de notification qui s'affiche régulièrement. Vous pouvez également accéder à la page Mon compte, dans laquelle vous pouvez effectuer un renouvellement ou configurer un renouvellement automatique.

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 activés, 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 votre produit McAfee à partir d'un CD-ROM, vous devez l'activer dans un délai de 15 jours sans quoi vos produits ne recevront pas les mises à jour critiques et n'effectueront pas d'analyses.

Contenu de ce chapitre

Rechercher des mises à jour....13
Configurer les mises à jour automatiques....14
Désactivation des 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 21).

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**.

Désactivation des 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 13).

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**.

3 Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.

Conseil : pour activer les mises à jour automatiques, cliquez sur le bouton **Activé** ou déselectionnez **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
Gestion des problèmes de protection.....19

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 activé et ne peut pas bénéficier d'une protection complète.	Activez le programme sur le site Web de McAfee.
Votre abonnement a expiré.	Vérifiez l'état de votre compte sur le site Web de McAfee. Pour plus d'informations, consultez Gestion de vos abonnements (page 11).

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 27).

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.

Gestion 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 Anti-Spam ou Parental Controls 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 22
Configuration des options d'alerte.....24

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**.

Masquage des 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**.

Masquage des messages de sécurité

Vous pouvez masquer les notifications de sécurité relatives à la protection de plusieurs ordinateurs de votre réseau domestique. Ces messages fournissent des informations sur votre abonnement, le nombre d'ordinateurs que vous pouvez protéger grâce à celui-ci et la procédure à suivre pour étendre votre abonnement à plusieurs ordinateurs.

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 **Afficher les informations relatives aux virus ou les autres messages de sécurité**.

Conseil : vous pouvez afficher ces messages de sécurité à tout moment en activant la case à cocher **Afficher les informations relatives aux virus ou les autres messages de sécurité**.

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 27
Afficher tous les événements 28

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 30
Analyse de votre ordinateur 31
Exploitation des résultats d'analyse 37
Types d'analyse 41
Utilisation d'une protection supplémentaire 43
Configuration de la protection antivirus 47

Fonctions de VirusScan

Protection antivirus complète	Protège votre ordinateur des derniers virus, chevaux de Troie, cookies de suivi, logiciels espions, logiciels publicitaires et autres programmes indésirables. La protection s'étend au-delà des fichiers et dossiers de votre bureau pour contrer les menaces provenant de différents points d'entrée, dont le courrier électronique, la messagerie instantanée et le Web. En outre, il est inutile d'avoir recours à des tâches d'administration fastidieuses pour en bénéficier.
Options d'analyse économes en ressources	Il est possible de personnaliser des options d'analyse manuelles et en temps réel, mais si vous ne faites pas, votre ordinateur reste protégé. Si l'analyse est lente, vous pouvez désactiver l'option afin de minimiser l'utilisation des ressources de l'ordinateur. Sachez toutefois que la protection antivirus sera prioritaire par rapport aux autres tâches.
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 n'ayez à intervenir. Il est rare que VirusScan ne soit pas en mesure de neutraliser lui-même la menace. Si cela se produit, il vous laisse décider de l'action à entreprendre : refaire l'analyse 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 en mode plein écran, VirusScan suspend un certain nombre de tâches, notamment les analyses manuelles.

CHAPITRE 9

Analyse de votre ordinateur

Avant de lancer 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. A 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 plus d'informations sur le paramétrage des options d'analyse, consultez Configuration de la protection antivirus (page 47).

VirusScan offre une palette plus détaillée d'options d'analyse pour la protection antivirus, vous permettant ainsi d'exécuter périodiquement des analyses plus poussées. Vous pouvez exécuter une analyse complète, rapide, personnalisée ou programmée à partir de SecurityCenter. Vous pouvez également exécuter des analyses manuelles dans l'Explorateur Windows tout en travaillant. 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 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

Analyse de votre PC.....32
Affichage des résultats de l'analyse 35

Analyse de votre PC

VirusScan fournit une palette complète d'options d'analyse pour la protection antivirus, notamment l'analyse en temps réel (qui surveille en permanence votre PC pour déceler toute menace), l'analyse manuelle à partir de l'Explorateur Windows et l'analyse complète, rapide, personnalisée ou programmée à partir de SecurityCenter.

Pour...	Opération à exécuter...
Démarrer une analyse en temps réel et surveiller en permanence votre ordinateur pour déceler toute activité virale, en analysant les fichiers chaque fois que vous ou votre ordinateur y accédez	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 antivirus**, cliquez sur **Activé**. **Remarque :** l'analyse en temps réel est activée par défaut.
Démarrer QuickScan et rechercher rapidement les menaces présentes sur votre ordinateur	1. Cliquez sur **Analyser** dans le menu de base. 2. Dans le volet Options d'analyse, sous Analyse rapide, cliquez sur **Démarrer**.
Démarrer une analyse complète et rechercher les menaces présentes sur votre ordinateur	1. Cliquez sur **Analyser** dans le menu de base. 2. Dans le volet Options d'analyse, sous Analyse complète, cliquez sur **Démarrer**.

Pour...	Opération à exécuter...
Démarrer une analyse personnalisée basée sur vos propres paramètres	1. Cliquez sur **Analyser** dans le menu de base. 2. Dans le volet Options d'analyse, sous Me laisser choisir, cliquez sur **Démarrer**. 3. Personnalisez une analyse en désactivant ou activant : **Toutes les menaces dans tous les fichiers** **Virus inconnus** **Fichiers d'archive** **Logiciels espions et menaces potentielles** **Cookies de suivi** **Programmes furtifs** 4. Cliquez sur **Démarrer**.
Démarrer une analyse manuelle et rechercher des menaces dans les fichiers, dossiers ou lecteurs	1. Ouvrez l'Explorateur Windows. 2. Cliquez avec le bouton droit sur un fichier, dossier ou disque, puis cliquez sur **Analyser**.

Pour...	Opération à exécuter...
Démarrer une analyse programmée qui analyse régulièrement votre ordinateur pour y rechercher des menaces	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**.

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.

Remarque : pour en apprendre davantage sur les options d'analyse, consultez Types d'analyses (page 41).

Affichage des résultats de l'analyse

Lorsqu'une analyse 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	Afficher 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	1. Double-cliquez sur l'icône **Analyse terminée** dans la zone de notification de votre barre des tâches. 2. Cliquez sur **Détails** dans le volet Analyse complète, Analyse rapide, Analyse personnalisée ou Analyse manuelle.
Afficher des détails sur la dernière analyse	Double-cliquez sur l'icône **Analyse terminée** dans la zone de notification de votre barre des tâches et affichez les détails de la dernière analyse sous Votre analyse dans le volet Analyse complète, Analyse rapide, Analyse personnalisée ou Analyse manuelle.

CHAPITRE 10

Exploitation des résultats d'analyse

Si VirusScan détecte une menace lors d'une analyse, 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. VirusScan envoie toujours un fichier en quarantaine avant de tenter de le désinfecter. S'il n'est pas nettoyé, le fichier est mis 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

Gestion des virus et chevaux de Troie.....38
Gestion des programmes potentiellement indésirables.....38
Gérer des fichiers en quarantaine 39
Gérer des programmes et cookies en quarantaine.....40

Gestion des virus et chevaux de Troie

Si VirusScan détecte un virus ou un cheval de Troie sur votre ordinateur, il tente de nettoyer le fichier infecté. 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 39).

Gestion des programmes potentiellement indésirables

Si VirusScan détecte un programme potentiellement indésirable sur votre ordinateur, vous avez le choix de supprimer ou d'autoriser le programme. Si vous ne connaissez pas le programme, nous vous recommandons de le supprimer. 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.

Types d'analyse

VirusScan fournit une palette complète d'options d'analyse pour la protection antivirus, notamment l'analyse en temps réel (qui surveille en permanence votre PC pour déceler toute menace), l'analyse manuelle à partir de l'Explorateur Windows et la possibilité d'exécuter une analyse complète, rapide ou personnalisée à partir de SecurityCenter, ou de personnaliser le moment de l'analyse. L'analyse dans SecurityCenter offre l'avantage de permettre de changer les options d'analyse sur le moment.

Analyse en temps réel :

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. 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.

Vous pouvez configurer des options par défaut pour l'analyse en temps réel, notamment l'analyse des virus inconnus et la recherche de menaces dans les cookies de suivi et les lecteurs réseau. Vous pouvez également tirer avantage de la protection de débordement de mémoire tampon, qui est activée par défaut (sauf en cas d'utilisation du système d'exploitation Windows Vista 64 bits). Pour en savoir plus, consultez Configuration des options d'analyse en temps réel (page 48).

Analyse rapide

L'analyse rapide vous permet de rechercher les menaces dans les processus, les fichiers Windows critiques, ainsi que d'autres zones sensibles de votre ordinateur.

Analyse complète

L'analyse complète vous permet de rechercher sur votre ordinateur les virus, logiciels espions et autres menaces de sécurité présents sur votre PC.

Analyse personnalisée

L'analyse personnalisée vous permet de choisir vos propres paramètres de recherche de menaces sur votre PC. Outre l'analyse de recherche des virus inconnus, logiciels espions et programmes furtifs, les options d'analyse personnalisée incluent la recherche de menaces dans tous les fichiers, dans les fichiers d'archive et dans les cookies.

Vous pouvez configurer des options par défaut pour les analyses personnalisées, qui incluent la recherche de virus inconnus, de fichiers d'archive, de logiciels espions, de menaces potentielles, de cookies de suivi et de programmes furtifs. Vous pouvez également procéder à une analyse via une utilisation minimale des ressources de l'ordinateur. Pour en savoir plus, consultez Configuration des options d'analyse personnalisée (page 51).

Analyse manuelle

L'analyse manuelle vous permet de rechercher rapidement des menaces dans les fichiers, dossiers et lecteurs à partir de l'Explorateur Windows.

Programmer des analyses

Les analyses programmées procèdent 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. Pour en savoir plus, consultez Programmation d'une analyse (page 54).

Remarque : pour en savoir plus sur les options d'analyse les plus adaptées à vos besoins, consultez Analyse de votre PC (page 32)

CHAPITRE 11

Utilisation d'une 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 ou navigateur Web. 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.

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 44
Démarrer la protection contre les logiciels espions 44
Démarrer la protection des e-mails 45
Démarrer la protection de la messagerie instantanée 45

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 12

Configuration de la protection antivirus

Vous pouvez configurer différentes options pour les analyses programmées, personnalisées et en temps réel. 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.

Vous pouvez également décider du mode de gestion par VirusScan des modifications potentiellement non autorisées ou indésirables sur votre PC à l'aide des fonctions SystemGuards et Listes approuvées. 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. Vous pouvez utiliser les listes approuvées pour décider d'autoriser ou de supprimer les règles de détection des modifications de fichiers, des programmes ou des débordements de mémoire tampon. 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.

Contenu de ce chapitre

Configuration des options d'analyse en temps réel 48
Configuration des options d'analyse personnalisée 51
Programmation d'une analyse 54
Utilisation des options SystemGuards.....55
Utilisation des listes approuvées.....62

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.

Configuration des 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 disques 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	Sélectionnez **Rechercher les virus inconnus**.
Détecter les cookies	Sélectionnez **Rechercher et supprimer les cookies de suivi**.
Détecter les virus et autres menaces potentielles sur les disques connectés à votre réseau	Sélectionnez **Analyser les lecteurs réseau**.
Protéger votre ordinateur contre les débordements de mémoire tampon	Sélectionnez **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**.

Arrêt de la protection antivirus en temps réel

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.

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 antivirus**, cliquez sur **Désactivé**.

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

4 Cliquez sur **OK**.

Configuration des options d'analyse personnalisée

La protection antivirus personnalisée vous permet d'analyser des fichiers à la demande. Lorsque vous lancez une analyse personnalisée, 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 personnalisée, 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 et 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 et les lecteurs réseau chaque fois qu'il effectue une analyse personnalisée ; vous pouvez cependant modifier les emplacements par défaut pour les adapter à vos besoins. Par exemple, vous pouvez limiter l'analyse aux fichiers critiques du PC, aux éléments placés sur votre bureau ou à ceux de votre dossier Program Files. A moins de vouloir lancer vous-même chaque analyse personnalisée, 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 en mode plein écran, VirusScan suspend un certain nombre de tâches, notamment les mises à jour automatiques et les analyses personnalisées.

Configuration des options d'analyse personnalisée

Vous configurez les options d'analyse personnalisée pour personnaliser la cible des contrôles effectués par VirusScan lors d'une analyse personnalisée, 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. Vous pouvez également définir l'emplacement de l'analyse personnalisée pour spécifier où VirusScan doit rechercher des virus et autres éléments nuisibles lors d'une analyse personnalisée. 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 personnalisée.

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 personnalisée, puis cliquez sur **OK**.

Pour...	Opération à exécuter...
Détecter les virus inconnus et les nouvelles variantes de virus connus	Sélectionnez **Rechercher les virus inconnus**.
Détecter et supprimer les virus dans les fichiers .zip et autres fichiers d'archive	Sélectionnez **Analyser les fichiers d'archive**.
Détecter les logiciels espions, logiciels publicitaires et autres applications potentiellement indésirables.	Sélectionnez **Rechercher les logiciels espions et les menaces potentielles**.
Détecter les cookies	Sélectionnez **Rechercher et supprimer les cookies de suivi**.

Pour...	Opération à exécuter...
Détecter les rootkits et les programmes furtifs pouvant altérer et exploiter les fichiers système Windows existants	Sélectionnez **Rechercher les 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)	Sélectionnez **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**.

3 Cliquez sur **Emplacement par défaut à analyser**, puis activez ou désactivez les emplacements que vous souhaitez analyser ou ignorer, puis cliquez sur **OK** :

Pour...	Opération à exécuter...
Analyser tous les fichiers et dossiers de votre ordinateur	Activez **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**.

Programmation d'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.

Programmez des analyses qui recherchent sur votre ordinateur des virus et autres menaces à l'aide des options d'analyse par défaut. Par défaut, VirusScan effectue une analyse programmée une fois par semaine.

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 58).

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.

SystemGuard	Détection
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.

SystemGuard	Détection
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 63).

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.

Option	Description
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.

Option	Description
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 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

Fonctionnalités de Personal Firewall....68
Démarrage du pare-feu....71
Utilisation des alertes....73
Gestion des alertes de type Informations....77
Configuration de la protection par pare-feu....79
Gestion des programmes et des autorisations....89
Gestion des connexions informatiques....99
Gestion des services système....107
Consignation, surveillance et analyse....113
Obtention d'informations sur la sécurité Internet....123

Fonctionnalités de Personal Firewall

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	Vous pouvez recevoir 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.
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	Protégez votre ordinateur contre les tentatives d'intrusion ainsi que contre les programmes et le trafic réseau indésirables dès le démarrage de Windows®.
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 tout le trafic réseau 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 malveillantes, telles que les chevaux de Troie, d'envoyer 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, nous apportons 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 Automatique (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.....71
Désactivation de la protection par pare-feu 72

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 74

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.

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 **Nouvelle connexion réseau** s'affiche lorsqu'un ordinateur équipé du pare-feu est connecté à un nouveau réseau. Vous pouvez spécifier le niveau de confiance à attribuer à ce nouveau réseau, et il apparaît alors dans votre liste des Réseaux. Si les recommandations intelligentes sont activées, les programmes connus sont automatiquement 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.

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 77
Masquer les alertes de type Informations 78

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 Automatique 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 80
Configuration des recommandations intelligentes pour les alertes 82
Optimisation de la sécurité du pare-feu 84
Verrouillage et restauration du pare-feu 87

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 Automatique, n'autorisant qu'un accès sortant.

Lorsque le niveau de sécurité Automatique 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. Bien que les alertes vertes soient désactivées, elles apparaissent lorsque des programmes connus sont détectés et l'accès 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 Standard), 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 trois niveaux de sécurité du pare-feu, du plus restrictif au plus laxiste :

Niveau	Description
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.
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.
Automatique	Octroie aux programmes des accès Internet soit entrants et sortants (complets) ou sortants uniquement. Le niveau de sécurité par défaut est Automatique, 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.

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

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 **Internet & Réseau**, 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 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 Automatique

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

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

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 appliquées (et que le niveau de sécurité Automatique est activé, avec accès sortant uniquement), le pare-feu autorise les programmes connus et bloque les programmes potentiellement dangereux automatiquement.

Lorsque les recommandations intelligentes ne sont pas appliquées, le pare-feu n'autorise ni ne bloque l'accès à Internet et ne fournit pas non plus de recommandation dans l'alerte.

Lorsque les recommandations intelligentes sont définies à Afficher, une alerte vous invite à autoriser ou bloquer l'accès, et le pare-feu fournit une recommandation dans l'alerte.

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 **Internet & Réseau**, 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 **Appliquer 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 **Internet & Réseau**, 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 **Ne pas appliquer les recommandations intelligentes**.
4. Cliquez sur **OK**.

Affichage des recommandations intelligentes

Vous pouvez afficher les recommandations intelligentes pour afficher uniquement une recommandation dans les alertes afin que vous décidiez d'autoriser ou de bloquer l'accès aux programmes non reconnus et potentiellement dangereux.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Internet &Réseau**, 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 les recommandations intelligentes**.
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 pendant 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. De même, ils peuvent envoyer les informations à votre ordinateur, avec le protocole UDP, sous forme d'unités de message (datagrammes). Le pare-feu défend votre ordinateur contre ces types d'intrusions en permettant de bloquer l'accès des programmes à Internet au démarrage de Windows et les requêtes ping grâce auxquelles d'autres utilisateurs peuvent détecter votre ordinateur dans un réseau, et d'empêcher les autres utilisateurs d'envoyer des informations de votre ordinateur sous la forme d'unités de message (datagrammes).

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.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Internet & Réseau**, 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 de Windows**.
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 des paramètres UDP

Vous pouvez autoriser les autres utilisateurs d'ordinateurs dans le réseau à envoyer des unités de message (datagrammes) vers votre ordinateur, à l'aide du protocole UDP. Cependant, vous pouvez uniquement faire ceci si vous avez fermé un port de service système pour bloquer ce protocole.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Internet & Réseau**, 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 **Activer le suivi UDP** pour autoriser les autres utilisateurs d'ordinateurs dans le réseau à envoyer des unités de message (datagrammes) vers votre ordinateur.
   - Désactivez la case à cocher **Activer le suivi UDP** pour empêcher les autres utilisateurs d'ordinateurs dans le réseau d'envoyer des unités de message (datagrammes) vers votre ordinateur.
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.**

Configuration des 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 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 toutes les connexions réseau entrantes et sortantes, notamment l'accès à des sites Web, des e-mails et des mises à jour de sécurité. Le verrouillage a le même résultat que la déconnexion des câbles réseau de votre ordinateur. Vous pouvez utiliser ce paramètre pour bloquer les ports ouverts dans le volet Services système et pour identifier et dépanner 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 tout réseau, y compris 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 **Activer le verrouillage du pare-feu**.

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 tout réseau, y compris Internet.

1 Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Verrouiller le pare-feu**.

2 Dans le volet Verrouillage activé, cliquez sur **Désactiver le verrouillage du pare-feu**.

3 Cliquez sur **Oui** pour confirmer.

Restauration des 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 Automatique 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.

4 Cliquez sur **OK**.

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 90
Autorisation de l'accès sortant uniquement des programmes ...92
Blocage de l'accès Internet des programmes.....94
Suppression des autorisations d'accès de certains programmes 95
En savoir plus sur les programmes.....96

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 115)

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 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 adresses 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 un ordinateur fiable 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 protégés par un pare-feu et un programme antivirus à jour. Le pare-feu ne consigne pas le trafic et ne génère aucune alerte pour les adresses IP autorisées figurant dans la liste des **Réseaux**.

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.

Le pare-feu 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.

Contenu de ce chapitre

A propos des connexions informatiques 100
Interdiction de connexions informatiques.....104

A propos des connexions informatiques

Les connexions informatiques sont les connexions créées entre d'autres d'ordinateurs sur n'importe quel réseau et le votre. Vous pouvez ajouter, modifier et supprimer les adresses IP dans la liste des **Réseaux**. Ces adresses IP sont associées à des réseaux auxquels vous voulez associer un niveau de confiance lors de la connexion à votre ordinateur : Autorisé, Standard ou Public.

Niveau	Description
Autorisé	Le pare-feu autorise le trafic provenant d'une adresse IP d'atteindre votre ordinateur via n'importe quel port. 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, le premier réseau privé que le pare-feu trouve est listé comme Fiable dans la liste des **Réseaux**. Un exemple de réseau fiable est un ou des ordinateurs dans votre réseau local ou domestique.
Standard	le pare-feu contrôle le trafic provenant d'une adresse IP (mais pas celui provenant d'autres ordinateurs dans ce réseau) lorsqu'elle se connecte à votre ordinateur, et l'autorise ou le bloque en fonction des règles de la liste **Services système**. Le pare-feu consigne le trafic et génère des alertes d'événement provenant d'adresses IP Standard. Un exemple de réseau standard est un ou des ordinateurs dans un réseau d'entreprise.
Public	Le pare-feu contrôle le trafic provenant d'un réseau public en fonction des règles de la liste **Services système**. Un exemple de réseau public est un réseau Internet dans un café, hôtel ou aéroport.

Lorsque vous autorisez une connexion, assurez-vous que l'ordinateur que vous autorisez n'est pas infecté. Si un ordinateur fiable 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 protégés par un pare-feu et un programme antivirus à jour.

Ajout d'une connexion à un ordinateur

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

1. Dans le volet McAfee SecurityCenter, cliquez sur **Internet & Réseau**, 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 **Réseaux**.
4. Dans le volet Réseaux, cliquez sur **Ajouter**.
5. Si la connexion de l'ordinateur est sur un réseau IPv6, activez la case à cocher **IPv6**.
6. Sous **Ajouter une règle**, vous pouvez soit :
   - Sélectionner **Une seule** adresse IP, puis entrer l'adresse IP dans le champ **Adresse IP**.
   - 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**. Si votre connexion informatique est sur un réseau IPv6, entrez l'adresse IP de départ et la longueur du préfixe dans les champs **De l'adresse IP** et **Longueur du préfixe**.
7. Sous **Type**, vous pouvez soit :
   - Sélectionnez **Fiable** pour spécifier que la connexion informatique est fiable (par exemple, un ordinateur dans un réseau domestique).
   - Sélectionnez **Standard** pour spécifier que cette connexion informatique (et pas les autres ordinateurs dans son réseau) est fiable (par exemple, un ordinateur dans un réseau d'entreprise).
   - Sélectionnez **Public** pour spécifier que la connexion informatique est publique (par exemple, un ordinateur dans un cybercafé, un hôtel ou un aéroport).
8. 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.
9. Eventuellement, sélectionnez **La règle expire dans**, puis entrez le nombre de jours où la règle doit être appliquée.
10. Eventuellement, entrez une description de cette règle.
11. Cliquez sur **OK**.

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

Ajout d'un ordinateur depuis le journal des événements entrants

Vous pouvez ajouter la connexion d'un ordinateur fiable ou standard 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 **Internet & Réseau**, puis sur **Evénements entrants**.
5. Sélectionnez une adresse IP source, et sous **Je souhaite**, effectuez l'une des actions suivantes :
   - Cliquez sur **Ajouter cette adresse IP à Fiable** pour ajouter un ordinateur comme Fiable dans votre liste **Réseaux**.
   - Cliquez sur **Ajouter cette adresse IP à Standard** pour ajouter une connexion à un ordinateur comme Standard dans votre liste **Réseaux**.
6. Cliquez sur **Oui** pour confirmer.

Modification d'une connexion à un ordinateur

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

1. Dans le volet McAfee SecurityCenter, cliquez sur **Internet & Réseau**, 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 **Réseaux**.
4. Dans le volet Réseaux, sélectionnez une adresse IP, puis cliquez sur **Modifier**.
5. Si la connexion de l'ordinateur est sur un réseau IPv6, activez la case à cocher **IPv6**.
6. Sous **Modifier une règle**, vous pouvez soit :
   - Sélectionner **Une seule** adresse IP, puis entrer l'adresse IP dans le champ **Adresse IP**.
   - 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**. Si votre connexion informatique est sur un réseau IPv6, entrez l'adresse IP de départ et la longueur du préfixe dans les champs **De l'adresse IP** et **Longueur du préfixe**.

7 Sous **Type**, vous pouvez soit :

- Sélectionnez **Fiable** pour spécifier que la connexion informatique est fiable (par exemple, un ordinateur dans un réseau domestique).
- Sélectionnez **Standard** pour spécifier que cette connexion informatique (et pas les autres ordinateurs dans son réseau) est fiable (par exemple, un ordinateur dans un réseau d'entreprise).
- Sélectionnez **Public** pour spécifier que la connexion informatique est publique (par exemple, un ordinateur dans un cybercafé, un hôtel ou un aéroport).

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

9 Eventuellement, entrez une description de cette règle.

10 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 à un ordinateur

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

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

4 Dans le volet Réseaux, sélectionnez une adresse IP, puis cliquez sur **Supprimer**.

5 Cliquez sur **Oui** pour confirmer.

Interdiction de connexions informatiques

Vous pouvez ajouter, modifier et supprimer les adresses IP interdites dans le volet 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.

Le pare-feu 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.

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 **Internet & Réseau**, 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 interdites**.
4. Dans le volet Adresses IP interdites, cliquez sur **Ajouter**.
5. Si la connexion de l'ordinateur est sur un réseau IPv6, activez la case à cocher **IPv6**.
6. Sous **Ajouter une règle**, vous pouvez soit :
   - Sélectionner **Une seule** adresse IP, puis entrer l'adresse IP dans le champ **Adresse IP**.
   - 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**. Si votre connexion informatique est sur un réseau IPv6, entrez l'adresse IP de départ et la longueur du préfixe dans les champs **De l'adresse IP** et **Longueur du préfixe**.
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. 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 **Internet & Réseau**, 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 interdites**.
4. Dans le volet Adresses IP interdites, cliquez sur **Modifier**.
5. Si la connexion de l'ordinateur est sur un réseau IPv6, activez la case à cocher **IPv6**.
6. Sous **Modifier une règle**, vous pouvez soit :
   - Sélectionner **Une seule** adresse IP, puis entrer l'adresse IP dans le champ **Adresse IP**.
   - 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**. Si votre connexion informatique est sur un réseau IPv6, entrez l'adresse IP de départ et la longueur du préfixe dans les champs **De l'adresse IP** et **Longueur du préfixe**.
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**.

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 **Internet & Réseau**, 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 interdites**.
4. Dans le volet Adresses IP interdites, sélectionnez une adresse IP, puis cliquez sur **Supprimer**.
5. 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. Utilisez ce journal, 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.

Ajoutez une adresse IP à votre liste **Adresses IP interdites** si vous voulez bloquer tout le trafic Internet entrant provenant de cette adresse IP, que vos ports de service système soient ouverts ou fermés.

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 **Internet & Réseau**, puis sur **Evénements entrants**.
5. Sélectionnez une adresse IP source et, sous **Je souhaite**, cliquez sur **Interdire cette adresse IP**.
6. 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 dans 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 **Internet & Réseau**, puis sur **Evénements de détection des intrusions**.
5. Sélectionnez une adresse IP source et, sous **Je souhaite**, cliquez sur **Interdire cette adresse IP**.
6. Cliquez sur **Oui** pour confirmer.

CHAPITRE 20

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, le pare-feu 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.....108

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. Ces ports de service système peuvent être ouverts ou fermés pour les ordinateurs énumérés comme Fiable, Standard ou Public dans votre liste **Réseaux**.

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

- Port courant 5357 du système d'exploitation
- 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.

Autorisation de l'accès à un port de service système existant

Vous pouvez ouvrir un port existant pour autoriser l'accès réseau distant à un service système 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 **Internet & Réseau**, 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 **Edition**.
6. Effectuez l'une des opérations suivantes :
   - Pour ouvrir le port vers n'importe quel ordinateur sur un réseau fiable, standard ou public (par exemple, un réseau domestique, un réseau d'entreprise ou un réseau Internet), sélectionnez **Fiable, Standard et Public**.
   - Pour ouvrir le port vers n'importe quel ordinateur sur un réseau standard (par exemple, un réseau d'entreprise), sélectionnez **Standard (y compris Fiable)**.
7. 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 système de votre ordinateur.

1. Dans le volet McAfee SecurityCenter, cliquez sur **Internet & Réseau**, 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**, désactivez la case à cocher en regard du port de service système à fermer.
5. Cliquez sur **OK**.

Configuration d'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 **Internet & Réseau**, 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 **Ajouter une règle Service système**, entrez les informations suivantes :
   - Nom du service système
   - Catégorie de service système
   - Ports TCP/IP locaux
   - Ports UDP locaux
6. Effectuez l'une des opérations suivantes :
   - Pour ouvrir le port vers n'importe quel ordinateur sur un réseau fiable, standard ou public (par exemple, un réseau domestique, un réseau d'entreprise ou un réseau Internet), sélectionnez **Fiable, Standard et Public**.
   - Pour ouvrir le port vers n'importe quel ordinateur sur un réseau standard (par exemple, un réseau d'entreprise), sélectionnez **Standard (y compris Fiable)**.
7. 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**.
8. Eventuellement, décrivez la nouvelle configuration.
9. Cliquez sur **OK**.

Remarque : Si votre ordinateur possède un programme 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 **Réseaux**. Pour plus d'informations, consultez Ajouter une connexion 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 **Internet & Réseau**, 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 la case à cocher en regard d'un service système, puis cliquez sur **Modifier**.
5. Dans le volet Services système, sous **Ajouter une règle Service système**, modifiez les informations suivantes :
   - Nom du service système
   - Ports TCP/IP locaux
   - Ports UDP locaux
6. Effectuez l'une des opérations suivantes :
   - Pour ouvrir le port vers n'importe quel ordinateur sur un réseau fiable, standard ou public (par exemple, un réseau domestique, un réseau d'entreprise ou un réseau Internet), sélectionnez **Fiable, Standard et Public**.
   - Pour ouvrir le port vers n'importe quel ordinateur sur un réseau standard (par exemple, un réseau d'entreprise), sélectionnez **Standard (y compris Fiable)**.
7. Si vous souhaitez envoyer les données d'activité de ce port à un autre ordinateur Windows en réseau partageant votre connexion Internet, sélectionnez **Transférer l'activité réseau de ce port aux ordinateurs du réseau qui utilisent le Partage de connexion Internet**.
8. Eventuellement, décrivez la configuration modifiée.
9. 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 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 114
Utilisation des statistiques 116
Suivi du trafic Internet 117
Surveillance du trafic Internet 120

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 IP**.
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**.

Suivi d'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 IP**.
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 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 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 124

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 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 126
Nettoyage de votre ordinateur 127
Défragmentation de votre ordinateur 131
Programmation d'une tâche 133

Fonctions de QuickClean

Nettoyage de fichiers	Permet de supprimer les fichiers inutiles de manière sûre et efficace à l'aide de divers nettoyeurs. La suppression de ces fichiers permet d'augmenter l'espace disponible sur le disque dur et d'améliorer les performances de votre ordinateur.

CHAPITRE 24

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.

Les nettoyeurs QuickClean permettent de supprimer des fichiers inutiles de votre ordinateur. Ils sont décrits dans le tableau suivant :

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 qui n'existent plus. 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.

Nom	Fonction
Nettoyeur du cache	supprime les fichiers mis en mémoire 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 accélérer et améliorer 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.
Nettoyeur de cookies	supprime les cookies. Ces fichiers prennent généralement la forme de fichiers temporaires. Un cookie est un petit fichier contenant des informations, telles que nom d'utilisateur, date et heure, stocké sur l'ordinateur d'une personne naviguant sur le Web. Les cookies sont normalement utilisés par les sites Web pour identifier des utilisateurs qui se sont déjà enregistrés ou qui ont déjà visité le site, mais ils peuvent aussi être une source d'informations pour les pirates.
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 d'éléments récemment utilisés	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 ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®

Nom	Fonction
Nettoyeur de contrôles ActiveX	supprime les contrôles ActiveX. ActiveX est un composant logiciel utilisé par des programmes ou des pages Web pour ajouter une fonctionnalité qui se fond au programme ou à la page pour en devenir une partie intégrante. Les plupart des contrôles ActiveX sont inoffensifs ; certains peuvent toutefois 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 de vous permettre de revenir à un état antérieur en cas de problème.

Contenu de ce chapitre

Nettoyage de votre ordinateur.....129

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.

CHAPITRE 25

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.

CHAPITRE 26

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 27

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 140
Broyage de fichiers, dossiers et disques.....140

Fonctions de Shredder

Destruction définitive de fichiers et dossiers

Permet de supprimer des éléments de votre disque dur en faisant en sorte que les informations qui y sont associées ne puissent plus être récupérées. La confidentialité est préservée grâce à la suppression définitive et sécurisée de fichiers et dossiers, d'éléments contenus dans la Corbeille et le dossier Fichiers Internet temporaires, ainsi que du contenu entier de disques, tels que CD réinscriptibles, disques durs externes et 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 28

McAfee Network Manager

Network Manager présente sous forme graphique les ordinateurs et les autres périphériques de votre réseau domestique. Vous pouvez utiliser Network Manager pour gérer 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. Si vous avez installé McAfee Total Protection, Network Manager peut également surveiller votre réseau afin d'y détecter des intrus (ordinateurs ou périphériques que vous ne reconnaissez ni n'approuvez) qui tentent de s'y connecter.

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 144
Présentation des icônes de Network Manager.....145
Configuration d'un réseau géré 147
Gestion à distance du réseau 153
Surveillance des réseaux.....159

Fonctionnalités de Network Manager

Carte graphique du réseau

Permet d'afficher une représentation graphique du niveau de protection des ordinateurs et périphériques 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 périphériques de la carte du réseau.

Gestion à distance

Permet de gérer l'état de protection des ordinateurs de votre réseau domestique. Vous pouvez inviter un ordinateur à s'affilier au réseau géré, surveiller le niveau de protection des ordinateurs gérés et résoudre les problèmes connus de failles de sécurité du réseau à partir d'un ordinateur distant.

Surveillance réseau

Cette fonction permet à Network Manager de contrôler vos réseaux et de vous informer lorsque des amis ou des intrus se connectent. Elle n'est toutefois disponible qu'avec McAfee Total Protection.

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 29

Configuration d'un réseau géré

Pour configurer un réseau géré, approuvez le réseau (si vous ne l'avez pas encore fait) et ajoutez des membres (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 des éléments 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 148
Affiliation au réseau géré.....150

Utilisation de la carte du réseau

Lorsque vous connectez un ordinateur au réseau, Network Manager analyse l'état du réseau afin de déterminer l'existence de membres gérés ou non gérés, les attributs du routeur et l'état de la connexion 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 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 éléments de la carte du réseau. Vous pouvez également afficher les détails associés aux éléments de la carte du réseau.

Accès à la carte du réseau

La carte du réseau propose une représentation graphique des ordinateurs et périphériques de votre réseau.

- Dans le menu de base ou avancé, cliquez sur **Gérer un réseau**.

Remarque : Si vous n'avez pas déjà autorisé le réseau (à l'aide de McAfee Personal Firewall), vous y êtes invité au premier accès à la carte du réseau.

Actualisation de 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 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 **Renommer le 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.

Affichage ou masquage d'un élément de la carte du réseau

Par défaut, tous les ordinateurs et les périphériques 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**. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.
Afficher des éléments masqués de la carte du réseau	Sous **Je souhaite**, cliquez sur **Afficher les éléments masqués**.

Affichage des détails d'un élément

Sélectionnez un élément de votre réseau dans la carte du réseau pour afficher des informations détaillées le concernant. Ces informations comprennent le nom de l'élément, l'état de sa protection et d'autres informations nécessaires pour gérer l'élément.

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 les autres ordinateurs du réseau gèrent les paramètres de sécurité de cet ordinateur.

1. Dans la boîte de dialogue Réseau géré, assurez-vous que la case **Autoriser tous les ordinateurs de ce réseau à gérer 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.

Invitation d'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 **Gérer 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 géré.

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 30

Gestion à distance du réseau

Une fois que vous avez configuré votre réseau géré, vous pouvez gérer à distance les ordinateurs et les périphériques de votre réseau. Vous pouvez gérer l'état et les niveaux de permission des ordinateurs et des périphériques, mais aussi corriger la plupart des problèmes de vulnérabilité, le tout à distance.

Contenu de ce chapitre

Gestion des états et autorisations.....154
Réparation des failles de sécurité.....156

Gestion des états et autorisations

Un réseau géré comporte des membres gérés et des membres non gérés. Les membres gérés autorisent les autres ordinateurs du réseau à gérer 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 disposant d'autorisations d'administration. De même, un ordinateur géré disposant d'autorisations d'administration peut rendre un autre ordinateur géré 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 surveiller 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.

Gestion de l'état de protection d'un ordinateur

Si l'état de protection d'un ordinateur n'est pas géré sur le réseau (l'ordinateur n'est pas un membre ou est un membre non géré), vous pouvez demander sa gestion.

1. Cliquez sur l'icône d'un ordinateur non géré sur la carte du réseau.
2. Cliquez sur **Gérer cet ordinateur** sous **Je souhaite**.

Arrêt de la surveillance de l'état de protection d'un ordinateur

Vous pouvez arrêter de gérer l'état de protection d'un ordinateur géré de votre réseau ; cependant, l'ordinateur devient alors non géré et vous ne pouvez pas en gérer l'état de protection à distance.

1. Cliquez sur l'icône d'un ordinateur géré sur la carte du réseau.
2. Cliquez sur **Arrêter la gestion de cet ordinateur** sous **Je souhaite**.
3. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.

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 gérer 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 gérer 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 la carte du réseau.

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 gérer 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 géré à distance. Pour gérer ces ordinateurs à distance, vous devez installer la dernière version de SecurityCenter sur chacun d'entre eux.

1. Assurez-vous de suivre les instructions suivantes sur l'ordinateur que vous voulez gérer à distance.
2. Préparez les informations de connexion McAfee, à savoir l'adresse de messagerie et le mot de passe utilisés lors de l'activation initiale du logiciel McAfee.
3. Dans un navigateur, accédez au site Web de McAfee, connectez-vous, puis cliquez sur **Mon compte**.
4. Recherchez le produit à installer, cliquez sur le bouton **Télécharger** correspondant, puis suivez les instructions à l'écran.

Conseil : vous pouvez également apprendre comment installer le logiciel de sécurité McAfee sur des ordinateurs distants en ouvrant la carte de votre réseau, et en cliquant sur **Protéger mes PC** sous **Je souhaite**.

CHAPITRE 31

Surveillance des réseaux

Si vous avez installé McAfee Total Protection, Network Manager surveille également vos réseaux à la recherche d'intrus. Lorsqu'un ordinateur ou périphérique inconnu se connecte à votre réseau, vous en serez averti afin de décider si cet ordinateur ou périphérique est un ami ou un intrus. Un ami est un ordinateur ou périphérique que vous reconnaissez et autorisez, contrairement à un intrus. Si vous avez marqué un ordinateur ou périphérique comme ami, vous pouvez choisir d'être notifié chaque fois qu'un ami se connecte au réseau. Si vous avez marqué un ordinateur ou périphérique comme intrus, nous vous alerterons automatiquement à chacune de ses connexions.

Lors de la première connexion à un réseau après l'installation ou la mise à niveau vers cette version de Total Protection, nous marquerons automatiquement chaque ordinateur ou périphérique comme ami et ne vous notifierons pas lorsqu'ils se connecteront au réseau. Après trois jours, nous commencerons à vous avertir de chaque ordinateur ou périphérique inconnu se connectant au réseau afin que vous puissiez les marquer.

Remarque : la surveillance réseau est une fonctionnalité de Network Manager disponible uniquement avec McAfee Total Protection. Pour plus d'informations sur Total Protection, consultez notre site Web.

Contenu de ce chapitre

Arrêter la surveillance des réseaux 160
Réactivation des notifications de surveillance du réseau 160
Marquage comme intrus 161
Marquage comme ami 162
Arrêt de la détection des nouveaux amis 162

Arrêter la surveillance des réseaux

Si vous désactivez la surveillance du réseau, nous ne serons plus en mesure de vous avertir si des intrus se connectent à votre réseau domestique ou à tout autre réseau auquel vous vous connectez.

1 Ouvrez le volet de configuration Internet & réseau.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Internet & réseau**.
3. Dans la section d'informations relatives à Internet et au réseau, cliquez sur **Configurer**.

2 Sous **Surveillance réseau**, cliquez sur **Désactivé**.

Réactivation des notifications de surveillance du réseau

Bien que vous puissiez désactiver les notifications de surveillance du réseau, ceci n'est pas recommandé. Si vous décidez de le faire, nous ne pourrons peut-être plus vous avertir lorsque des ordinateurs inconnus ou des intrus se connectent à votre réseau. Si vous désactivez par mégarde ces notifications (par exemple, si vous activez la case à cocher **Ne plus afficher cette alerte** dans une alerte), vous pouvez les réactiver à tout moment.

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, assurez-vous que les cases à cocher suivantes sont désactivées :

- **Ne pas montrer les alertes lorsque des PC ou des périphériques se connectent au réseau**
- **Ne pas montrer les alertes lorsque des intrus se connectent au réseau**
- **Ne pas montrer les alertes pour les amis pour lesquels je souhaite être averti**
- **Ne pas montrer les alertes lorsque des PC ou périphériques inconnus sont détectés**
- **Ne pas montrer d'alerte lorsque la détection des nouveaux amis par McAfee est terminée**

4 Cliquez sur **OK**.

Marquage comme intrus

Ne marquez un ordinateur ou périphérique de votre réseau comme intrus que si vous ne le reconnaissez pas ou ne l'autorisez pas. Nous vous avertirons automatiquement à chacune de ses connexions au réseau.

1 Dans le menu de base ou avancé, cliquez sur **Gérer un réseau**.

2 Sur la carte du réseau, cliquez sur un élément.

3 Sous **Je souhaite**, cliquez sur **Marquer comme ami ou intrus**.

4 Dans la boîte de dialogue, cliquez sur **Un intrus**.

Marquage comme ami

Ne marquez un ordinateur ou périphérique de votre réseau comme ami que si vous le reconnaissez et l'autorisez. Lorsque vous marquez un ordinateur ou périphérique comme ami, vous pouvez également choisir d'être notifié chaque fois qu'il se connecte au réseau.

1. Dans le menu de base ou avancé, cliquez sur **Gérer un réseau**.
2. Sur la carte du réseau, cliquez sur un élément.
3. Sous **Je souhaite**, cliquez sur **Marquer comme ami ou intrus**.
4. Dans la boîte de dialogue, cliquez sur **Un ami**.
5. Pour être notifié à chaque connexion de cet ami au réseau, activez la case à cocher **M'avertir lorsque cet ordinateur ou périphérique se connecte au réseau**.

Arrêt de la détection des nouveaux amis

Pendant les trois premiers jours après la connexion à un réseau avec cette version de Total Protection, nous marquerons automatiquement chaque ordinateur ou périphérique comme ami pour lequel vous ne souhaitez pas recevoir de notification. Vous pouvez interrompre ce marquage automatique à tout moment au cours de ces trois jours, et le redémarrer ultérieurement.

1. Dans le menu de base ou avancé, cliquez sur **Gérer un réseau**.
2. Sous **Je souhaite**, cliquez sur **Arrêter la détection des nouveaux amis**.

CHAPITRE 32

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 164
Configuration de EasyNetwork.....165
Partage et envoi des fichiers.....171
Partage d'imprimantes 177

Fonctionnalités d'EasyNetwork

Partage de fichiers	Permet de partager facilement des fichiers avec d'autres ordinateurs de votre 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	Permet d'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 l'emplacement de stockage temporaire de tous les fichiers que vous envoyez à d'autres ordinateurs sur le réseau.
Partage automatique d'imprimantes	En vous affiliant à un réseau géré, vous pouvez partager avec les autres membres toutes les imprimantes locales reliées à votre ordinateur, en utilisant le nom de l'imprimante active comme nom d'imprimante partagée. EasyNetwork détecte les imprimantes partagées par les autres ordinateurs du réseau et vous permet de les configurer et de les utiliser.

CHAPITRE 33

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

Ouverture d'EasyNetwork 165
Affiliation à un réseau géré 166
Comment quitter un réseau géré 169

Ouverture d'EasyNetwork

Vous pouvez ouvrir EasyNetwork à partir du menu Démarrer de Windows ou en cliquant sur l'icône du bureau correspondante.

- Dans le menu **Démarrer**, pointez le curseur de la souris sur **Tous les programmes**, puis sur **McAfee** et cliquez sur **McAfee EasyNetwork**.

Conseil : vous pouvez également ouvrir EasyNetwork en double-cliquant sur l'icône McAfee EasyNetwork sur votre bureau.

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 166).

Sortie d'un réseau géré

Vous pouvez quitter un réseau géré auquel vous êtes affilié.

1. Déconnectez votre ordinateur du réseau.
2. Dans EasyNetwork, dans le menu **Outils**, cliquez sur **Quitter le réseau**.
3. Dans la boîte de dialogue Quitter le réseau, sélectionnez le nom du réseau que vous souhaitez quitter.
4. Cliquez sur **Quitter le réseau**.

CHAPITRE 34

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 172
Envoi de fichiers à d'autres ordinateurs 175

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 174) 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 174) 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 176).

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 35

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 178

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 pour la description des produits McAfee.

Glossaire

8

802.11

Ensemble de normes 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 permet la transmission de données à un débit pouvant atteindre 54 Mbits/s sur la bande de fréquence des 5 GHz. Le débit de transmission est plus rapide que celui de 802.11b, mais la distance couverte est inférieure.

802.11b

Extension de 802.11 qui permet la transmission de données à un débit pouvant atteindre 11 Mbits/s sur la bande de fréquence des 2,4 GHz. Le débit de transmission est plus lent que celui de 802.11a, mais la distance couverte est supérieure.

802.1x

Norme d'authentification utilisée sur les réseaux câblés et sans fil. La norme 802.1x est couramment utilisée sur les réseaux sans fil 802.11. Voir également authentification (page 181).

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

adresse de protocole Internet utilisée pour identifier un ordinateur ou un périphérique sur un réseau TCP/IP. Une adresse IP se présente sous la forme d'une séquence numérique codée de 32 bits, composée de quatre nombres séparés par des points. Chaque nombre peut être compris entre zéro et 255 (par exemple : 192.168.1.100).

adresse MAC

Media Access Control. Numéro de série unique attribué à un périphérique physique (NIC, carte d'interface réseau) accédant au réseau.

analyse à la demande

Examen planifié de fichiers, applications ou périphériques réseau sélectionnés afin de détecter d'éventuelles menaces, vulnérabilités ou autre code indésirable. Il peut s'effectuer dans l'immédiat, à un moment ultérieur défini ou à des intervalles réguliers programmés. Comparer avec l'analyse lors de l'accès. Voir également vulnérabilité.

analyse en temps réel

Action d'analyser des fichiers et dossiers, au moment où vous ou votre ordinateur y accédez, afin de détecter d'éventuels virus ou autres activités malveillantes.

archiver

Copier des fichiers importants sur un CD, un DVD, un périphérique USB, un disque dur externe ou un disque réseau. Comparer avec sauvegarder (page 189).

attaque en force

Méthode de piratage visant à déchiffrer des mots de passe ou des clés de chiffrement en essayant toutes les combinaisons de caractères possibles.

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 à modifier des messages échangés par deux parties sans que celles-ci ne sachent que leur communication a été infiltrée.

attaque par saturation

Type d'attaque dirigée contre un ordinateur, un serveur ou un réseau qui ralentit ou interrompt le trafic sur un réseau. Elle survient lorsque le réseau est tellement submergé de demandes que le trafic normal se trouve ralenti ou complètement bloqué. L'attaque par saturation vise à inonder une cible de fausses demandes de connexion, de sorte qu'elle ignore les vraies demandes.

authentification

Processus de vérification de l'identité de l'expéditeur d'une communication électronique.

B

bande passante

Quantité de données (débit) pouvant être transmise au cours d'une période définie.

base de registre

Base de données utilisée par Windows pour stocker les informations de configuration de chaque utilisateur, des composants matériels du système, des programmes installés et des paramètres de propriétés. La base de données se décompose en clés, pour lesquelles des valeurs sont définies. Des programmes indésirables peuvent modifier la valeur des clés de registre ou créer de nouvelles valeurs pour exécuter un code malveillant.

C

cache

Zone de stockage temporaire située sur l'ordinateur et destinée aux données auxquelles on accède souvent ou auxquelles on a récemment accédé. Pour accélérer et améliorer la navigation sur le Web, votre navigateur peut par exemple 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 PCI

Peripheral Component Interconnect. Carte adaptateur sans fil qui se branche sur un connecteur d'extension PCI à l'intérieur de l'ordinateur.

carte adaptateur sans fil USB

Carte adaptateur sans fil qui se connecte à un logement USB de l'ordinateur.

carte du réseau

Représentation graphique des ordinateurs et des autres composants de votre réseau domestique.

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 une autre marque de matériel client certifié.

cheval de Troie

Programme qui ne se réplique pas mais provoque des dommages et compromet la sécurité de votre ordinateur. En général, le cheval de Troie est envoyé par e-mail par un individu, il ne se transmet pas seul. Vous pouvez aussi télécharger le cheval de Troie sans le savoir à partir d'un site Web ou via un réseau de poste à poste.

chiffrement

Méthode de codage des informations visant à empêcher des personnes non autorisées d'y accéder. Pour coder des données, le processus utilise une "clé" et des algorithmes mathématiques. Des informations chiffrées ne peuvent pas être déchiffrées sans la clé adéquate. Les virus utilisent parfois le chiffrement pour tenter de déjouer les systèmes de détection.

clé

Voir clé USB (page 182).

clé

Série de lettres et de chiffres utilisée par deux périphériques pour authentifier une communication. La clé doit être connue des deux périphériques. Voir également WEP (page 192), WPA (page 192), WPA2 (page 193), WPA2-PSK (page 193), WPA-PSK (page 193).

clé USB

Petit lecteur mémoire qui se branche sur un port USB de l'ordinateur. Une clé 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 effectuer un certain nombre d'opérations. Par exemple, un client de messagerie est une application qui vous permet d'envoyer et de recevoir des e-mails.

client de messagerie

Programme exécuté sur l'ordinateur pour envoyer et recevoir des e-mails (par exemple, Microsoft Outlook).

code d'authentification des messages

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 en un format qui réduit l'espace nécessaire à leur stockage ou à leur transmission.

compte de messagerie standard

Voir POP3 (page 188).

contrôle ActiveX

Composant logiciel utilisé par des programmes ou des pages Web pour ajouter une fonctionnalité qui devient une partie intégrante du programme ou de la page Web. Les plupart des contrôles ActiveX sont inoffensifs ; certains peuvent toutefois subtiliser des informations sur votre ordinateur.

cookie

Petit fichier texte utilisé par de nombreux sites Web pour stocker des informations sur les pages visitées. Les cookies sont enregistrés sur l'ordinateur lors de la navigation sur Internet. Ils peuvent contenir des informations de connexion ou d'enregistrement, des informations concernant les paniers ou les préférences de l'utilisateur. Les cookies sont normalement utilisés par les sites Web pour identifier des utilisateurs qui se sont déjà enregistrés ou qui ont déjà visité le site, mais ils peuvent aussi être une source d'informations pour les pirates.

Corbeille

Imitation d'une corbeille à papiers, utilisée pour stocker les fichiers et dossiers supprimés dans Windows.

D

DAT

Fichiers de définition de détection, également appelés fichiers de signature. Ils contiennent des définitions qui permettent d'identifier, de détecter et de neutraliser les virus, chevaux de Troie, logiciels espions, logiciels publicitaires et autres programmes indésirables.

débordement de la mémoire tampon

Etat dans lequel se trouve un système d'exploitation ou une application lorsque des programmes ou processus suspects essaient de stocker davantage de données que la mémoire tampon (zone de stockage temporaire) ne peut en contenir. Un débordement de la mémoire tampon peut altérer la mémoire ou écraser les données de mémoires tampons adjacentes.

disque dur externe

Disque dur conservé en dehors de l'ordinateur.

DNS

Domain Name System (système de noms de domaine). Système de base de données qui traduit une adresse IP, telle que 11.2.3.44 en nom de domaine, tel que www.mcafee.com.

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. Sur Internet, chaque adresse de site Web comporte un domaine. Par exemple, dans www.mcafee.com, le domaine est mcafee.

E

e-mail

Courrier électronique. Messages envoyés et reçus par voie électronique sur un réseau informatique. Voir également webmail (page 192).

emplacements surveillés

Dossiers contrôlés par Backup and Restore sur l'ordinateur.

ESS

Extended Service Set (jeu de service étendu). Plusieurs réseaux formant un seul sous-réseau.

É

événement

Dans un programme ou un système informatique, incident ou occurrence qui peut être détecté par un logiciel de sécurité, selon des critères prédéfinis. Un événement entraîne généralement une action, telle que l'envoi d'une notification ou l'ajout d'une entrée à un journal d'événement.

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 créé en mémoire ou sur disque par le système d'exploitation ou un autre programme ; il est utilisé le temps d'une session puis supprimé.

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 pour l'affichage sélectif des contenus

Groupe d'âge utilisé dans le cadre du contrôle parental. Le contenu est mis à disposition ou bloqué en fonction du groupe auquel appartient l'utilisateur. Les groupes pour l'affichage sélectif des contenus incluent : Jeune enfant, Enfant, Pré-adolescent, Adolescent et Adulte.

I

intranet

Réseau d'ordinateurs privé, généralement au sein d'une entreprise, 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 informatique qui s'étend sur une zone relativement restreinte (par exemple un seul bâtiment). Les ordinateurs connectés via un LAN peuvent communiquer entre eux et partager des ressources telles qu'imprimantes et 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

Liste d'éléments autorisés à être exclus de la détection. Si un élément figure par erreur dans cette liste (par exemple, un programme potentiellement indésirable ou une modification du registre) ou si vous souhaitez le soumettre à nouveau à la détection, il convient de le supprimer de la liste.

liste d'autorisation

Liste de sites Web ou d'adresses e-mail considérés comme fiables. Les sites Web inscrits sur une liste d'autorisation sont ceux auxquels les utilisateurs sont autorisés à accéder. Les adresses e-mail d'une liste d'autorisation correspondent à des sources fiables dont vous souhaitez recevoir des messages. Comparer avec liste de blocage (page 185).

liste de blocage

Liste d'adresses e-mail dont vous ne souhaitez pas recevoir de messages parce que vous les considérez comme des spams (dans Anti-Spam). Liste de sites Web considérés comme frauduleux (dans le cadre de l'antiphishing). Comparer avec liste d'autorisation (page 185).

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, etc.) de fonctionner sur un seul client, par exemple le client Exchange.

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

Réseau Microsoft. Ensemble de services Web offerts par Microsoft Corporation, comprenant moteur de recherche, messagerie électronique, messagerie instantanée et portail.

N

navigateur

Programme utilisé pour afficher des pages Web sur Internet. Parmi les navigateurs Web les plus populaires on trouve 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.

numéroteurs

Logiciel qui redirige les connexions Internet vers une partie autre que le FAI (fournisseur d'accès Internet) par défaut de l'utilisateur afin d'engendrer des frais de connexion supplémentaires au profit d'un fournisseur de contenu, un fournisseur ou un autre tiers.

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 de e-mails d'accéder aux fichiers de sauvegarde sélectionnés pendant une durée limitée. Partagez un fichier consiste à en envoyer une copie sauvegardée aux destinataires de votre choix. Les destinataires reçoivent un e-mail de Backup and Restore indiquant que des fichiers ont été partagés avec eux. Le message 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 (coffre-fort de mots de passe)

Zone de stockage sécurisée des mots de passe personnels. Elle assure que personne ne peut accéder à vos mots de passe (pas même un administrateur).

phishing

Méthode permettant d'obtenir illicitement des informations personnelles, telles que mots de passe, numéro de sécurité sociale, références de cartes de crédit. La technique consiste à envoyer des e-mails hameçons en se faisant passer pour une banque, une société ou une autre source fiable. Les destinataires sont le plus souvent conviés à cliquer sur un lien inclus dans le message sous prétexte de vérifier ou de mettre à jour leurs coordonnées personnelles ou les références de leur carte de crédit.

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", "pixels espions" "GIF transparents" ou "GIF invisibles".

plugin, plug-in

Petit programme permettant d'améliorer un logiciel plus grand ou d'y ajouter des fonctions. Des plug-ins permettent par exemple à un navigateur Web d'exécuter des fichiers incorporés dans des documents HTML, dont il ne reconnaîtrait pas le format normalement, tels que fichiers vidéo ou audio et fichiers 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 sécurisé 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 signale sa présence et n'exige pas d'authentification. Les points d'accès sans fil (hotspots) se situent souvent dans des zones très fréquentées telles que les 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 de manière régulière et au moment d'événements système significatifs, comme l'installation d'un programme ou d'un pilote. Vous pouvez en outre créer et nommer à tout moment vos propres points de restauration.

POP3

Post Office Protocol 3. Interface entre le programme d'un client de messagerie et le serveur de messagerie. La plupart des particuliers possèdent un compte de messagerie POP3, également appelé compte de messagerie standard.

port

Emplacement matériel pour transmettre des données à l'intérieur et à l'extérieur d'un périphérique informatique. Les ordinateurs individuels possèdent divers types de ports, notamment les ports internes pour la connexion de lecteurs de disques, moniteurs et claviers et les ports externes pour la connexion de modems, imprimantes, souris et autres périphériques.

PPPoE

Acronyme de Point-to-Point Protocol Over Ethernet. Méthode utilisant le protocole commuté PPP (Point-to-Point Protocol) avec Ethernet comme moyen de transport.

programme potentiellement indésirable

Programme qui peut être indésirable, même s'il n'est pas exclu que l'utilisateur l'ait volontairement téléchargé. Il peut mettre en danger la sécurité ou les paramètres de confidentialité de l'ordinateur sur lequel il est installé. Les programmes indésirables peuvent comprendre, sans s'y limiter, les logiciels espions, les logiciels publicitaires et les numéroteurs et peuvent être téléchargés avec un programme que l'utilisateur a choisi.

protocole

Ensemble de règles permettant aux ordinateurs ou périphériques d'échanger des données. Dans une architecture réseau en couches (modèle OSI), chaque couche a ses propres protocoles pour spécifier comment la communication s'effectue à ce niveau. Votre ordinateur ou périphérique doit prendre en charge le protocole adéquat pour pouvoir communiquer avec les autres ordinateurs. Voir également Open Systems Interconnection (OSI).

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 (page 190).

publier

Action de rendre un fichier sauvegardé accessible à tous sur Internet. Les fichiers publiés sont accessibles en faisant une recherche dans la bibliothèque Backup and Restore.

Q

quarantaine

Isolation forcée d'un fichier ou dossier soupçonné de contenir un virus, un spam, un contenu suspect ou des programmes non désirables. Ainsi mis à l'écart, le fichier ou dossier ne peut être ni ouvert ni exécuté.

R

raccourci

Fichier contenant uniquement l'emplacement d'un autre fichier sur votre ordinateur.

RADIUS

Remote Access Dial-In User Service. Protocole permettant d'authentifier un utilisateur, généralement dans le cadre d'un accès à distance. Initialement conçu pour des serveurs d'accès distant à commutation, on l'utilise maintenant dans divers environnements d'authentification, notamment l'authentification 802.1x du secret partagé d'un utilisateur de réseau local sans fil. Voir également secret partagé.

réseau

Ensemble de systèmes IP (tels que routeurs, commutateurs, serveurs et pare-feu) qui sont regroupés en une unité logique. Par exemple, un "réseau financier" peut comprendre tous les serveurs, routeurs et systèmes qui servent le département des finances. Voir également réseau domestique (page 189).

réseau domestique

Plusieurs ordinateurs connectés dans une maison afin de permettre le partage de fichiers et de l'accès à Internet. Voir également LAN (page 185).

rootkit

Ensemble d'outils (programmes) qui octroie le statut d'administrateur à un utilisateur afin de lui permettre d'accéder à un ordinateur ou un réseau d'ordinateurs. Les rootkits comprennent notamment les logiciels espions et d'autres programmes potentiellement indésirables qui peuvent mettre en danger la sécurité et la confidentialité de vos données ou informations personnelles.

routeur

Périphérique réseau qui transmet des paquets de données d'un réseau à un autre. Les routeurs lisent chaque paquet entrant et décident de la manière de l'envoyer, en fonction des adresses source et destination et des conditions du trafic. Un routeur est parfois appelé Point d'accès.

S

sauvegarder

Copier des fichiers importants, généralement sur un serveur sécurisé en ligne. Comparer avec archiver (page 181).

script

Liste de commandes qui peuvent être exécutées automatiquement (sans intervention de l'utilisateur). A la différence des programmes, les scripts sont généralement stockés en texte clair et compilés à chaque exécution. Les macros et fichiers à accès séquentiel (batch) sont aussi appelés scripts.

secret partagé

Chaîne ou clé (généralement un mot de passe) qui a été partagée entre deux interlocuteurs avant d'entamer une communication. Elle est utilisée pour protéger les parties sensibles des messages RADIUS. Voir également RADIUS (page 189).

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 proxy

Composant du pare-feu qui gère le trafic Internet vers et depuis un réseau local (LAN). L'utilisation d'un serveur proxy permet d'améliorer les performances en fournissant des données fréquemment demandées, par exemple une page Web, et de filtrer les demandes en ignorant 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 permet d'acheminer les e-mails sur Internet.

SSID

Service Set Identifier. Jeton (clé secrète) qui identifie un réseau Wi-Fi (802.11). Le SSID est défini par l'administrateur réseau et doit être fourni par les utilisateurs qui souhaitent se connecter au réseau.

SSL

Secure Sockets Layer. Protocole développé par Netscape pour transmettre des documents privés sur Internet. SSL utilise une clé publique pour chiffrer les 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 les fichiers sauvegardés et ceux stockés sur votre ordinateur local. Une synchronisation est nécessaire lorsque la version d'un fichier du référentiel de sauvegarde en ligne est plus récente que la version du fichier stockée sur d'autres ordinateurs.

SystemGuard

Alertes McAfee qui détectent les modifications non autorisées apportées à votre ordinateur et vous en avertissent.

T

texte chiffré

Texte codé par chiffrement. Le texte chiffré est illisible tant qu'il n'a pas été converti en texte en clair (c'est-à-dire déchiffré). Voir également chiffrement (page 182).

texte en clair

Texte non chiffré. Voir également chiffrement (page 182).

TKIP

Temporal Key Integrity Protocol. Partie de la norme de chiffrement 802.11i s'appliquant aux réseaux locaux sans fil. TKIP est la nouvelle génération des mécanismes de sécurité WEP utilisés pour sécuriser les réseaux locaux sans fil 802.11. Avec un système de mélange des clés pour chaque paquet, une vérification de l'intégrité du message et un mécanisme de redéfinition de la clé, TKIP corrige les faiblesses de WEP.

types de fichiers de surveillance

Types de fichiers (par exemple, .doc, .xls) archivés ou sauvegardés par Backup and Restore au sein d'emplacements surveillés.

U

U3

Pour trois qualités : plus simple, plus intelligent et mobile. Plate-forme permettant d'exécuter Windows 2000 ou XP directement depuis un périphérique 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

Localisateur de ressources universel. Format standard des adresses Internet.

USB

Universal Serial Bus. Connecteur standard présent sur la plupart des ordinateurs actuels. Il permet de connecter plusieurs périphériques, tels que claviers, souris, webcams, scanneurs et imprimantes.

usurpation d'adresse IP

Action de falsifier les adresses IP dans un paquet IP. Ce procédé est utilisé dans de nombreux types d'attaques, notamment la prise de contrôle de sessions et il sert souvent à falsifier les en-têtes des spams dans le but d'empêcher leur traçage.

V

ver

Virus qui se propage en se dupliquant sur d'autres lecteurs, systèmes ou réseaux. Un ver à diffusion massive nécessite l'intervention d'un utilisateur pour se propager, par exemple par l'ouverture d'une pièce jointe ou l'exécution d'un fichier téléchargé. A l'heure actuelle, la plupart des virus provenant des e-mails sont des vers. Certains vers peuvent aussi se propager seuls, sans l'intervention d'un utilisateur. On connaît par exemple Blaster et Sasser qui font partie de cette catégorie.

virus

Programme informatique qui peut se copier lui-même et infecter un ordinateur à l'insu de l'utilisateur.

VPN

Virtual Private Network. Réseau de communication privé configuré à travers un réseau hôte tel qu'Internet. Les données transmises via une connexion VPN sont chiffrées et possèdent des fonctions de sécurité très élaborées.

W

wardriver

Personne qui, munie d'un ordinateur Wi-Fi et d'un matériel ou logiciel spécial, parcourt une ville en voiture, à la recherche de réseaux Wi-Fi (802.11).

webmail

Courrier basé sur Internet. Service de messagerie électronique auquel on accède principalement via un navigateur, plutôt que par un client de messagerie installé sur l'ordinateur, tel que Microsoft Outlook. Voir également e-mail (page 184).

WEP

Wired Equivalent Privacy. Protocole de chiffrement et d'authentification défini avec la norme Wi-Fi (802.11). Les premières versions sont basées sur des chiffrements RC4 et présentent des faiblesses considérables. WEP tente de sécuriser les données en les chiffrant sur des ondes radio pour qu'elles soient protégées lors de leur transfert d'un point d'extrémité à un autre. WEP ne s'avère toutefois pas aussi sûr qu'on pouvait le penser.

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 garantir 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 constitue un consortium, un laboratoire de test et un centre d'informations pour les fournisseurs qui souhaitent développer le secteur.

WLAN

Wireless Local Area Network (réseau local sans fil). Réseau local doté d'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 logicielle, le WPA est issu de la norme 802.11i avec laquelle il est compatible. Correctement installé, il offre aux utilisateurs d'un réseau local sans fil la quasi certitude 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 du niveau de sécurité des entreprises et qui 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 également WPA2-PSK (page 193), TKIP (page 191).

WPA2

Mise à jour de la norme de sécurité WPA, basée sur la norme 802.11i.

WPA2-PSK

Mode WPA spécial, similaire à WPA-PSK, basé sur la norme WPA2. Cette norme permet souvent aux périphériques d'accepter plusieurs modes de chiffrement (comme AES, TKIP) simultanément, tandis que les périphériques 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.

Licence

Copyright

CHAPITRE 36

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 198

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.

Lancement de 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.

Les tableaux suivants répertorient les sites Assistance et téléchargements McAfee des divers pays ou régions, où vous trouverez les Guides de l'utilisateur.

Assistance et téléchargements

Pays/région :	Assistance McAfee	Téléchargements McAfee
Allemagne	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
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.mcafeehelp.com	ca.mcafee.com/root/downloads.asp?langid=48

Chine (chinois simplifié)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Corée	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Danemark	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Espagne	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Etats-Unis	www.mcafeehelp.com	us.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
Grèce	www.mcafeehelp.com	el.mcafee.com/root/downloads.asp
Hongrie	www.mcafeehelp.com	hu.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
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
République tchèque	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Royaume-Uni	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Russie	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
Slovaquie	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
Suède	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Taiwan	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Turquie	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp

Guides de l'utilisateur de McAfee Total Protection

Pays/région :	Guides de l'utilisateur McAfee
Allemagne	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
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 (chinois simplifié)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Corée	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Danemark	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Espagne	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Etats-Unis	download.mcafee.com/products/manuals/en-us/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
Grèce	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
Hongrie	download.mcafee.com/products/manuals/hu/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
Mexique	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norvège	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Pays-Bas	download.mcafee.com/products/manuals/nl/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

République tchèque	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Royaume-Uni	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Russie	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
Slovaquie	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
Suède	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Turquie	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf

Guides de l'utilisateur McAfee Internet Security

Pays/région :	Guides de l'utilisateur McAfee
Allemagne	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
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 (chinois simplifié)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Corée	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Danemark	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Espagne	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Etats-Unis	download.mcafee.com/products/manuals/en-us/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

Grèce	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf
Hongrie	download.mcafee.com/products/manuals/hu/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
Mexique	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norvège	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Pays-Bas	download.mcafee.com/products/manuals/nl/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
République tchèque	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Royaume-Uni	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Russie	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Slovaquie	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
Suède	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Turquie	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf

Guides de l'utilisateur de McAfee VirusScan Plus

Pays/région :	Guides de l'utilisateur McAfee
Allemagne	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
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 (chinois simplifié)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Corée	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Danemark	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Espagne	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Etats-Unis	download.mcafee.com/products/manuals/en-us/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
Grèce	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf
Hongrie	download.mcafee.com/products/manuals/hu/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
Mexique	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norvège	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Pays-Bas	download.mcafee.com/products/manuals/nl/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
République tchèque	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Royaume-Uni	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Russie	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf
Slovaquie	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
Suède	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf

Taiwan	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Turquie	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf

Guides de l'utilisateur de McAfee VirusScan

Pays/région :	Guides de l'utilisateur McAfee
Allemagne	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
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 (chinois simplifié)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Corée	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Danemark	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Espagne	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Etats-Unis	download.mcafee.com/products/manuals/en-us/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
Grèce	download.mcafee.com/products/manuals/el/VS_userguide.2008.pdf
Hongrie	download.mcafee.com/products/manuals/hu/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
Mexique	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norvège	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf

Pays-Bas	download.mcafee.com/products/manuals/nl/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
République tchèque	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Royaume-Uni	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Russie	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
Slovaquie	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
Suède	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Turquie	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf

Le tableau suivant répertorie les Centres de menaces et les sites d'informations sur les virus de McAfee dans les divers pays ou régions.

Pays/région :	Siège social du service de sécurité	Informations sur les virus
Allemagne	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
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 (chinois simplifié)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Corée	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Danemark	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo

Espagne	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Etats-Unis	www.mcafee.com/us/threat_center	us.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
Grèce	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo
Hongrie	www.mcafee.com/us/threat_center	hu.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
Mexique	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norvège	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Pays-Bas	www.mcafee.com/us/threat_center	nl.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
République tchèque	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Royaume-Uni	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Russie	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Slovaquie	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
Suède	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Taiwan	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Turquie	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo

Le tableau suivant présente une liste des sites HackerWatch des divers pays ou régions.

Pays/région :	HackerWatch
Allemagne	www.hackerwatch.org/?lang=de
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 (chinois simplifié)	www.hackerwatch.org/?lang=zh-cn
Corée	www.hackerwatch.org/?lang=ko
Danemark	www.hackerwatch.org/?lang=da
Espagne	www.hackerwatch.org/?lang=es
Etats-Unis	www.hackerwatch.org
Finlande	www.hackerwatch.org/?lang=fi
France	www.hackerwatch.org/?lang=fr
Grèce	www.hackerwatch.org/?lang=el
Hongrie	www.hackerwatch.org/?lang=hu
Italie	www.hackerwatch.org/?lang=it
Japon	www.hackerwatch.org/?lang=jp
Mexique	www.hackerwatch.org/?lang=es-mx
Norvège	www.hackerwatch.org/?lang=no
Pays-Bas	www.hackerwatch.org/?lang=nl
Pologne	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
République tchèque	www.hackerwatch.org/?lang=cs
Royaume-Uni	www.hackerwatch.org
Russie	www.hackerwatch.org/?lang=ru
Slovaquie	www.hackerwatch.org/?lang=sk
Suède	www.hackerwatch.org/?lang=sv
Taiwan	www.hackerwatch.org/?lang=zh-tw
Turquie	www.hackerwatch.org/?lang=tr

Index

8

802.11 180
802.11a 180
802.11b 180
802.1x 180

A

A propos de McAfee 195
A propos des alertes 74
A propos des connexions informatiques 100
À propos des types de listes approuvées 63
À propos des types de SystemGuards ... 57, 58
A propos du graphique d'analyse du trafic 120
Acceptation d'un fichier provenant d'un autre ordinateur 175, 176
Accès à la carte du réseau 148
Accès à votre compte McAfee 11
Activation de la protection par pare-feu 71
Activation de votre produit 11
Activation des recommandations intelligentes 83
Activation du niveau de sécurité Automatique 82
Activation du niveau de sécurité Furtif . 81
Activation du niveau de sécurité Standard 81
Activer la protection SystemGuards 56
Actualisation de la carte du réseau 148
adaptateur sans fil 180
adresse IP 180
adresse MAC 180
Affichage des détails d'un élément 149
Affichage des événements 18, 27
Affichage des événements de détection des intrusions 115
Affichage des recommandations intelligentes 84
Affichage des résultats de l'analyse 35
Affichage et masquage d'alertes d'information 22
Affichage ou masquage d'un élément de la carte du réseau 149
Afficher des alertes durant une session de jeu 77
Afficher les événements entrants 115
Afficher les événements récents 27, 114
Afficher les événements sortants ... 91, 115
Afficher les statistiques générales des événements de sécurité 116
Afficher ou masquer des alertes d'information 22
Afficher ou masquer des alertes d'information pendant un jeu 23
Afficher ou masquer des problèmes ignorés 20
Afficher tous les événements 28
Affiliation à un réseau géré 151, 166, 169
Affiliation au réseau 167
Affiliation au réseau géré 150
Ajout d'un ordinateur depuis le journal des événements entrants 102
Ajout d'une connexion à un ordinateur 101
Ajout d'une connexion interdite à un ordinateur 104
analyse à la demande 180
Analyse de votre ordinateur 31
Analyse de votre PC 32, 42
analyse en temps réel 181
Analyser le trafic entrant et sortant 121
archiver 181, 189
Arrêt de la détection des nouveaux amis 162
Arrêt de la protection antivirus en temps réel 50
Arrêt de la surveillance de l'état de protection d'un ordinateur 154
Arrêter la surveillance des réseaux 160
attaque en force 181
attaque par dictionnaire 181
attaque par immixtion 181
attaque par saturation 181
Attribution d'un nouveau nom au réseau 149, 169
authentification 180, 181
Autorisation d'accès au réseau 168
Autorisation de l'accès à un port de service système existant 109

Autorisation de l'accès Internet des programmes 90
Autorisation de l'accès sortant uniquement des programmes 92
Autoriser l'accès sortant uniquement d'un programme 92
Autoriser l'accès total d'un nouveau programme 91
Autoriser l'accès total d'un programme 90
Autoriser un accès sortant uniquement depuis le journal des événements récents 93
Autoriser un accès sortant uniquement depuis le journal des événements sortants 93
Autoriser un accès total depuis le journal des événements récents 91
Autoriser un accès total depuis le journal des événements sortants 92

B

bande passante 181
base de registre 181
Blocage de l'accès à un port de service système 109
Blocage de l'accès d'un nouveau programme 94
Blocage de l'accès d'un programme..... 94
Blocage de l'accès Internet des programmes 94
Bloquer l'accès depuis le journal des événements récents 95
Broyage de fichiers, dossiers et disques 140
Broyer les fichiers et les dossiers..... 140
Broyer un disque entier 141

C

cache 181
carte adaptateur sans fil PCI 182
carte adaptateur sans fil USB 182
carte du réseau..... 182
certifié Wi-Fi 182
cheval de Troie..... 182
chiffrement..... 182, 191
clé 182
clé USB..... 182
client 182
client de messagerie 183
code d'authentification des messages 183
Comment quitter un réseau géré..... 169
compression 183
compte de messagerie standard 183
Configuration de EasyNetwork..... 165
Configuration de la détection des intrusions 86
Configuration de la protection antivirus 31, 47
Configuration de la protection par pare-feu..... 79
Configuration des options d'alerte..... 24
Configuration des options d'analyse en temps réel 41, 48
Configuration des options d'analyse personnalisée 42, 51, 52
Configuration des options SystemGuards 57
Configuration des paramètres de requête ping..... 85
Configuration des paramètres du journal d'événements 114
Configuration des paramètres relatifs à l'état de la protection par pare-feu. ... 87
Configuration des paramètres UDP 86
Configuration des ports de service système 108
Configuration des recommandations intelligentes pour les alertes 82
Configuration d'un nouveau port de service système..... 110
Configuration d'un réseau géré 147
Configurer les mises à jour automatiques 14
Consignation, surveillance et analyse . 113
Consulter l'activité générale des ports Internet 116
contrôle ActiveX..... 183
cookie..... 183
Copie d'un fichier partagé 173
Copyright..... 196
Corbeille 183
Critères de recherche 173, 174

D

DAT 183
débordement de la mémoire tampon . 183
Défragmentation de votre ordinateur . 131
Défragmenter votre ordinateur..... 131
Démarrage du pare-feu 71
Démarrer la protection contre les logiciels espions 44
Démarrer la protection de la messagerie instantanée..... 45
Démarrer la protection des e-mails..... 45
Désactivation de la protection par pare-feu..... 72
Désactivation des mises à jour automatiques 15

Désactivation des recommandations intelligentes 83
Déverrouillage instantané du pare-feu . 88
disque dur externe..... 183
DNS..... 184
domaine 184

E

e-mail..... 184, 192
Emettre un son en cas d'alerte..... 24
emplacements surveillés 184
En savoir plus sur les programmes..... 96
Envoi de fichiers à d'autres ordinateurs 175
Envoi d'un fichier à un autre ordinateur 175
ESS 184
événement..... 184
Explications sur les catégories de protection 7, 9, 27
Explications sur les services de protection 10
Explications sur l'état de protection.7, 8, 9
Exploitation des résultats d'analyse 37

F

fenêtres instantanées..... 184
fichier temporaire..... 184
Fin de partage d'un fichier 173
Fin de partage d'une imprimante..... 178
Fonctionnalités de Network Manager. 144
Fonctionnalités de Personal Firewall 68
Fonctionnalités d'EasyNetwork..... 164
Fonctions de QuickClean 126
Fonctions de SecurityCenter..... 6
Fonctions de Shredder..... 140
Fonctions de VirusScan 30
fragments de fichier 184

G

Gérer des fichiers en quarantaine.....38, 39
Gérer des programmes et cookies en quarantaine 40
Gestion à distance du réseau 153
Gestion de l'état de protection d'un ordinateur..... 154
Gestion de vos abonnements.....11, 18
Gestion des alertes de type Informations 77
Gestion des connexions informatiques 99
Gestion des états et autorisations..... 154
Gestion des listes approuvées. 62
Gestion des niveaux de sécurité du pare-feu..... 80
Gestion des problèmes de protection ... 19
Gestion des programmes et des autorisations..... 89
Gestion des programmes potentiellement indésirables 38
Gestion des services système 107
Gestion des virus et chevaux de Troie ... 38
Gestion d'un matériel 155
groupe pour l'affichage sélectif des contenus 185

I

Ignorer un problème de protection..... 19
Installation de McAfee Security sur les ordinateurs distants..... 157
Installation d'une imprimante réseau disponible 178
Interdiction de connexions informatiques 104
Interdiction d'un ordinateur depuis le journal des événements de détection des intrusions 106
Interdiction d'un ordinateur depuis le journal des événements entrants 106
intranet..... 185
Introduction..... 3
Invitation d'un ordinateur à s'affilier au réseau géré..... 151
itinérance 185

J

Journalisation des événements..... 114

L

LAN 185, 189
Lancement de Virtual Technician 198
Lancement du didacticiel HackerWatch 124
Lancer l'analyse de scripts..... 44
launchpad 185
lecteur réseau..... 185
Licence..... 195
liste approuvée 185
liste d'autorisation 185
liste de blocage 185

M

MAPI 186
Marquage comme ami..... 162
Marquage comme intrus 161
Masquage des alertes d'attaque virale .. 25
Masquage des messages de sécurité 25
Masquer l'écran d'accueil au démarrage 24

Masquer les alertes de type Informations 78
McAfee EasyNetwork 163
McAfee Network Manager 143
McAfee Personal Firewall 67
McAfee QuickClean 125
McAfee SecurityCenter 5
McAfee Shredder 139
McAfee VirusScan 29
Mise à jour de SecurityCenter 13
Modification des autorisations d'un ordinateur géré 155
Modification des paramètres d'affichage d'un matériel 155
Modification d'un port de service système 111
Modification d'une connexion à un ordinateur 102
Modification d'une connexion interdite à un ordinateur 105
Modifier une tâche Défragmenteur de disque 136
Modifier une tâche QuickClean 134
mot de passe 186
MSN 186

N

navigateur 186
Ne plus approuver les ordinateurs du réseau 152
Nettoyage de votre ordinateur 127, 129
NIC 186
nœud 186
numéroteurs 186

O

Obtenir des informations concernant l'enregistrement d'un ordinateur 117
Obtenir des informations sur un programme depuis le journal des événements sortants 97
Obtention d'informations concernant le réseau d'un ordinateur 118
Obtention d'informations sur la sécurité Internet 123
Obtention d'informations sur un programme 96
Optimisation de la sécurité du pare-feu 84
Ouverture d'EasyNetwork 165

P

pare-feu 186
Partage de fichiers 172
Partage d'imprimantes 177
Partage d'un fichier 172
Partage et envoi des fichiers 171
partager 186
passerelle intégrée 187
password vault (coffre-fort de mots de passe) 187
phishing 187
pixels invisibles 187
plugin, plug-in 187
point d'accès 187
point d'accès non fiable 187
point d'accès sans fil 187
point de restauration système 188
POP3 ..... 183, 188
port 188
PPPoE 188
Présentation des icônes de Network Manager 145
Programmation d'une analyse 42, 54
Programmation d'une tâche 133
programme potentiellement indésirable 188
Programmer une tâche Défragmenteur de disque 136
Programmer une tâche QuickClean 133
Protection de votre ordinateur au démarrage 85
protocole 188
proxy 188
publier 188

Q

quarantaine 189

R

raccourci 189
RADIUS 189, 190
Réactivation des notifications de surveillance du réseau 160
Réception d'une notification lors de l'envoi d'un fichier 176
Recherche d'un fichier partagé 173
Rechercher des mises à jour 13, 15
Référence 179
Renouvelement de votre abonnement . 12
Réparation automatique des failles de sécurité 156
Réparation des failles de sécurité 156
réseau 189
réseau domestique 189
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 des paramètres du pare-feu 88
rootkit 189
routeur 189

S

sauvegarder 181, 189
script 190
secret partagé 190
serveur 190
serveur proxy 188, 190
Service clientèle et support technique 197
SMTP 190
Sortie d'un réseau géré 169
SSID 190
SSL 190
Suivi du trafic Internet 117
Suivi d'un ordinateur depuis le journal des événements de détection des intrusions 119
Suivi d'un ordinateur depuis le journal des événements entrants 118
Suivi d'une adresse IP surveillée 119
Suivre géographiquement un ordinateur en réseau 117
Suppression des autorisations d'accès de certains programmes 95
Suppression des autorisations d'un programme 95
Suppression d'un port de service système 112
Suppression d'une connexion à un ordinateur 103
Suppression d'une connexion interdite à un ordinateur 105
Supprimer une tâche Défragmenteur de disque 137
Supprimer une tâche QuickClean 135
Surveillance de la bande passante utilisée par les programmes 121
Surveillance de l'activité des programmes 122
Surveillance des réseaux 159
Surveillance du trafic Internet 120
synchroniser 190
SystemGuard 190

T

texte chiffré 191
texte en clair 191
TKIP 191, 193
Types d'analyse 34, 41
types de fichiers de surveillance 191

U

U3 191
URL 191
USB 191
usurpation d'adresse IP 191
Utilisation de la carte du réseau 148
Utilisation de McAfee Virtual Technician 198
Utilisation de SecurityCenter 7
Utilisation des alertes 14, 21, 73
Utilisation des listes approuvées 62
Utilisation des options SystemGuards .. 55
Utilisation des statistiques 116
Utilisation d'imprimantes partagées .. 178
Utilisation d'une protection supplémentaire 43

V

ver 191
Vérifier votre abonnement 12
Verrouillage et restauration du pare-feu87
Verrouillage instantané du pare-feu 87
virus 192
VPN 192

W

wardriver 192
webmail 184, 192
WEP 182, 192
Wi-Fi 192
Wi-Fi Alliance 192
WLAN 192
WPA 182, 193
WPA2 ..... 182, 193
WPA2-PSK 182, 193
WPA-PSK 182, 193