McAfee®

Wireless Protection 2007

Guide de l'utilisateur

Table des matières

CHAPITRE 1

McAfee Wireless Protection

McAfee Wireless Protection Suite élimine les complications sur le réseau et les risques liés à la sécurité sans fil. Sa protection fiable empêche les pirates de s'attaquer à votre réseau Wi-Fi®, protège vos informations personnelles et vos transactions, et interdit à d'autres utilisateurs d'utiliser votre réseau pour accéder à Internet ; et tout cela, en un clic ! La rotation programmée des clés de sécurité longues de McAfee Wireless Network Security bloque les pirates même les plus déterminés. Wireless Protection inclut également McAfee EasyNetwork, qui permet de partager en toute simplicité fichiers et imprimantes sur votre réseau. De plus, McAfee Network Manager est également fourni pour surveiller les vulnérabilités des ordinateurs de votre réseau en matière de sécurité et pour permettre de résoudre facilement les problèmes potentiels de sécurité.

Wireless Protection comprend les programmes suivants :

- SecurityCenter
- Wireless Network Security
- Network Manager
- EasyNetwork

CHAPITRE 2

McAfee SecurityCenter

McAfee SecurityCenter est un environnement convivial que les utilisateurs de McAfee peuvent utiliser pour lancer, gérer et configurer leurs abonnements de sécurité.

Il est également une source d'informations sur les alertes de virus, les produits, l'assistance et l'abonnement. En un seul clic, SecurityCenter permet d'accéder aux outils et aux informations du site Web de McAfee.

Contenu de ce chapitre

Caractéristiques

McAfee SecurityCenter vous offre les nouvelles fonctions et avantages suivants :

Niveau de protection redéfini

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

Mises à jour et mises à niveau permanentes

Installez automatiquement les mises à jour quotidiennes. Lorsqu'une nouvelle version d'un logiciel McAfee est disponible, vous l'obtenez automatiquement sans frais pendant toute la durée de votre abonnement. Vous bénéficiez ainsi d'une protection à jour en permanence.

Alertes en temps réel

Les alertes de sécurité vous avertissent des nouvelles épidémies virales et des menaces de sécurité, tout en vous fournissant des possibilités de réponse pour supprimer, neutraliser ou mieux connaître la menace.

Une protection pratique

Plusieurs options de renouvellement permettent de maintenir à jour votre protection McAfee.

Outils de performances

Supprimez les fichiers inutilisés, défragmentez les fichiers utilisés et utilisez l'option de restauration du système pour maintenir le niveau de performances optimal de votre ordinateur.

Une Aide en ligne concrète

Bénéficiez du support des experts McAfee en matière de sécurité informatique, par chat sur Internet, par e-mail ou par téléphone.

Protection de la navigation

S'il est installé, le plug-in de navigateur McAfee SiteAdvisor vous aide à vous protéger contre les logiciels espions, spams, virus et e-mails frauduleux en établissant une classification des sites Web que vous consultez ou qui apparaissent dans les résultats des recherches que vous effectuez sur le Web. Vous pouvez afficher des évaluations de sécurité détaillées illustrant la manière dont un site a été testé en termes de pratiques d'e-mail, de téléchargement, d'affiliations en ligne et d'interventions non sollicitées telles que les fenêtres instantanées et les cookies tiers traceurs.

CHAPITRE 3

Utilisation de SecurityCenter

Vous pouvez lancer SecurityCenter depuis le bureau Windows ou la zone de notification Windows située à l'extrême droite de la barre des tâches (pour ce faire, utilisez l'icône McAfee SecurityCenter).

Une fois SecurityCenter ouvert, vous pouvez visualiser l'état de sécurité de votre ordinateur dans le volet Accueil et accéder rapidement à des tâches courantes, notamment aux opérations de mise à jour et d'analyse (si McAfee VirusScan est installé) :

En-tête

Aide

Affiche le fichier d'aide du programme.

Colonne de gauche

Mise à jour

Met à jour votre produit pour protéger votre ordinateur contre les dernières menaces.

Analyse

Permet d'effectuer une analyse manuelle de votre ordinateur (si McAfee VirusScan est installé).

Tâches courantes

Exécute des tâches courantes comme revenir au volet Accueil, afficher les événements récents, mettre à jour votre ordinateur et gérer votre réseau informatique (si l'ordinateur utilisé dispose des droits appropriés). Si McAfee Data Backup est installé, vous pouvez également sauvegarder vos données.

Composants installés

Permet de connaître les services de sécurité de votre ordinateur.

Volet principal

Etat de protection

Affiche le niveau général de protection informatique dans la section **Suis-je protégé**. Au-dessous de celle-ci, vous pouvez consulter l'état de chaque catégorie et type de protection.

SecurityCenter - Informations

Permet de connaître le moment de la dernière mise à jour de votre ordinateur, celui de l'expiration de votre abonnement et celui de la dernière analyse (si McAfee VirusScan est installé).

Contenu de ce chapitre

Signification des icônes SecurityCenter

Les icônes SecurityCenter s'affichent dans la zone de notification Windows située à l'extrême droite de la barre des tâches. Utilisez-les pour voir si votre ordinateur est totalement protégé, visualiser l'état d'une analyse en cours (si McAfee VirusScan est installé), rechercher des mises à jour, afficher les événements récents, mettre à jour votre ordinateur et obtenir de l'aide sur le site Web de McAfee.

Ouverture de SecurityCenter et utilisation des fonctionnalités supplémentaires

Lorsque SecurityCenter est en cours d'exécution, l'icône M de SecurityCenter s'affiche dans la zone de notification Windows située à l'extrême droite de la barre des tâches.

Pour ouvrir SecurityCenter ou utiliser des fonctionnalités supplémentaires :

- Cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, puis cliquez sur l'une des options suivantes :
  - Ouvrir SecurityCenter
  - Mises à jour
  - Liens rapides

    Le sous-menu contient des liens vers les sections suivantes Accueil, Afficher les événements récents, Gérer un réseau, Mettre à jour l'ordinateur et Sauvegarde des données (si ces fonctionnalités sont installées).
  - Vérifier l'abonnement

    (Cet élément apparaît lorsque l'abonnement à au moins un produit a expiré.)
  - Centre de mise à niveau
  - Service clientèle

Vérification de votre état de protection

Si votre ordinateur n'est pas totalement protégé, l'icône d'état de protection s'affiche dans la zone de notification Windows située à l'extrême droite de la barre des tâches. Cette icône peut être rouge ou jaune selon l'état de protection.

Pour vérifier votre état de protection :

- Cliquez sur l'icône d'état de protection pour ouvrir SecurityCenter et corriger les éventuels problèmes.

Vérification de l'état de vos mises à jour.

Si vous recherchez des mises à jour, l'icône Mises à jour s'affiche dans la zone de notification Windows située à l'extrême droite de la barre des tâches.

Pour vérifier l'état des mises à jour :

- Pointez sur l'icône Mises à jour pour afficher l'état de vos mises à jour sous forme d'info-bulle.

Explications sur l'état de protection

L'état de protection générale de votre ordinateur apparaît dans la section **Suis-je protégé** de SecurityCenter.

L'état de protection vous indique si votre ordinateur est totalement protégé contre les dernières menaces de sécurité ou s'il existe des problèmes nécessitant une attention particulière et comment les résoudre. Si un problème affecte plusieurs catégories de protection, sa résolution peut permettre à celles-ci de retrouver un état de protection totale.

Les critères pris en compte pour déterminer votre état de protection comprennent notamment les menaces de sécurité externes, les produits de sécurité installés sur votre ordinateur, les produits d'accès à Internet, ainsi que la configuration de ces produits de sécurité et d'accès à Internet.

Par défaut, si les fonctionnalités Protection antispam ou Blocage de contenu ne sont pas installées, ces problèmes de protection mineurs sont automatiquement ignorés et ne sont pas consignés dans l'état de protection générale de votre ordinateur. Toutefois, lorsqu'un problème de protection est suivi d'un lien **Ignorer**, vous pouvez choisir d'ignorer le problème en question si vous êtes sûr de ne pas vouloir le résoudre.

Suis-je protégé ?

Dans la section **Suis-je protégé** de SecurityCenter, consultez le niveau général de protection de votre ordinateur :

- **Oui** apparaît si votre ordinateur est totalement protégé (vert).
- **Non** apparaît si votre ordinateur est partiellement protégé (jaune) ou s'il n'est pas protégé du tout (rouge).

Pour résoudre la plupart des problèmes de protection automatiquement, cliquez sur **Corriger** en regard de l'état de protection. Toutefois, si certains problèmes persistent et nécessitent une réponse de votre part, cliquez sur le lien suivant le problème en question pour effectuer l'action suggérée.

Explications sur les catégories et les types de protection

Dans la section **Suis-je protégé** de SecurityCenter, vous pouvez consulter l'état des catégories et types de protection suivants :

- Ordinateur et fichiers
- Réseau et Internet
- E-mails et messages instantanés
- Contrôle parental

Les types de protection affichés dans SecurityCenter dépendent des produits installés. Par exemple, si McAfee Data Backup est installé, le type de protection de l'état du PC apparaît.

Les catégories qui ne présentent pas de problèmes de protection ont l'état vert. Si vous cliquez sur une catégorie verte, la liste des types de protection activés s'affiche sur la droite, suivie de la liste des problèmes ignorés. Si aucun problème n'a été relevé, une information sur les virus s'affiche à la place. Vous pouvez également cliquer sur **Configurer** pour modifier les options sélectionnées pour cette catégorie.

Si tous les types de protection d'une catégorie ont l'état vert, la catégorie est elle aussi définie sur l'état vert. De même, si toutes les catégories de protection ont l'état vert, l'état de protection générale de votre ordinateur est lui aussi défini sur l'état vert.

Si une catégorie de protection a l'état jaune ou rouge, vous pouvez régler les problèmes de protection en les résolvant ou en les ignorant afin d'obtenir l'état vert.

Explications sur la protection des ordinateurs et des fichiers

Cette catégorie de protection comprend les types de protection suivants.

- **Protection antivirus** : l'analyse en temps réel protège votre ordinateur contre les virus, vers, chevaux de Troie, scripts suspects, attaques hybrides et autres menaces. Le système analyse automatiquement les fichiers et essaie de les nettoyer (y compris les fichiers compressés au format .exe, le secteur d'amorçage, la mémoire et les fichiers critiques) lorsque vous ou votre ordinateur y accédez.
- **Protection contre les logiciels espions** : cette fonction détecte, bloque et éradique rapidement les logiciels espions, les logiciels publicitaires et autres programmes potentiellement indésirables qui accèdent à vos données personnelles et les transmettent sans votre autorisation.
- **SystemGuards** : cette fonction détecte les modifications intervenant sur votre ordinateur et vous alerte. Vous pouvez alors examiner les modifications et décider de les autoriser ou non.
- **Protection Windows** : cette protection indique l'état des mises à jour de Windows sur votre ordinateur. Si McAfee VirusScan est installé, la protection contre le débordement de la mémoire tampon est également disponible.

L'un des facteurs déterminants du niveau de protection de l'ordinateur et des fichiers est les menaces virales externes. Par exemple, si un virus se déclare, votre logiciel antivirus vous protège-t-il contre ce virus ? Parmi les autres facteurs figurent notamment la configuration de votre logiciel antivirus et la fréquence des mises à jour de celui-ci avec les derniers fichiers de signatures afin de protéger votre ordinateur contre les dernières menaces de sécurité.

Ouverture du volet de configuration de l'ordinateur et des fichiers

Si aucun problème n'a été relevé pour **l'ordinateur et les fichiers**, vous pouvez ouvrir le volet de configuration à partir du volet d'information.

Pour ouvrir le volet de configuration de l'ordinateur et des fichiers :

1. Dans le volet Accueil, cliquez sur l'option relative à l'**ordinateur** et **aux fichiers**.
2. Dans le volet de droite, cliquez sur **Configurer**.

Explications sur la protection Internet et réseau

Cette catégorie de protection comprend les types de protection suivants.

- **Protection par pare-feu** : cette fonction protège votre ordinateur contre les intrusions et contre le trafic réseau indésirable. Elle vous permet de gérer les connexions Internet entrantes et sortantes.
- **Protection sans fil** : la protection sans fil empêche toute intrusion et interception de données sur votre réseau domestique sans fil. Toutefois, si vous êtes connecté à un réseau sans fil externe, cette protection varie en fonction du niveau de sécurité de ce dernier.
- **Protection de la navigation sur le Web** : la fonction de protection de navigation Web masque les publicités, les fenêtres instantanées et les pixels invisibles sur votre ordinateur.
- **Protection antiphishing** : la protection antiphishing permet de bloquer les sites Web frauduleux qui vous invitent à donner des informations personnelles grâce à des liens hypertexte dans les e-mails et les messages instantanés, les fenêtres instantanées et d'autres sources.
- **Protection des informations personnelles** : la protection des informations personnelles permet de bloquer la diffusion d'informations sensibles ou confidentielles sur Internet.

Ouverture du volet de configuration Internet et réseau

Si aucun problème n'a été relevé pour **Internet et le réseau**, vous pouvez ouvrir le volet de configuration à partir du volet d'information.

Pour ouvrir le volet de configuration Internet et réseau :

1. Dans le volet Accueil, cliquez sur l'option relative à **Internet et au réseau**.
2. Dans le volet de droite, cliquez sur **Configurer**.

Explications sur la protection des e-mails et des messages instantanés

Cette catégorie de protection comprend les types de protection suivants.

- **Protection des e-mails** : la fonction de protection des e-mails analyse et essaie automatiquement de nettoyer les virus, les logiciels espions et autres menaces potentielles contenus dans vos messages et pièces jointes entrants et sortants.
- **Protection antispam** : la protection antispam vous aide à bloquer l'accès des messages indésirables à votre boîte de réception.
- **Protection de la messagerie instantanée** : la fonction de protection de la messagerie instantanée analyse et essaie automatiquement de nettoyer les virus, les logiciels espions et autres menaces potentielles contenus dans vos messages et pièces jointes entrants et sortants. Elle empêche également les clients de messagerie instantanée d'échanger du contenu indésirable ou des informations personnelles sur Internet.
- **Protection de la navigation** : s'il est installé, le plug-in de navigateur McAfee SiteAdvisor vous aide à vous protéger contre les logiciels espions, spams, virus et e-mails frauduleux en définissant une classification des sites Web que vous visitez ou qui apparaissent dans les résultats de recherches que vous effectuez sur le Web. Vous pouvez afficher des évaluations de sécurité détaillées illustrant la manière dont un site a été testé en termes de pratiques d'e-mail, de téléchargement, d'affiliations en ligne et d'interventions non sollicitées telles que les fenêtres instantanées et les cookies tiers traceurs.

Ouverture du volet de configuration des e-mails et des messages instantanés

Si aucun problème n'a été relevé pour les **e-mails et les messages instantanés**, vous pouvez ouvrir le volet de configuration à partir du volet d'information.

Pour ouvrir le volet de configuration des e-mails et messages instantanés :

1. Dans le volet Accueil, cliquez sur l'option des **e-mails et messages instantanés**.
2. Dans le volet de droite, cliquez sur **Configurer**.

Explications sur la protection par contrôle parental

Cette catégorie de protection comprend les types de protection suivants.

- **Protection par contrôle parental** : le blocage de contenu empêche les utilisateurs de visualiser du contenu Internet indésirable en bloquant l'accès aux sites Web potentiellement dangereux. L'activité et l'utilisation d'Internet que font les utilisateurs peuvent aussi être surveillées et limitées.

Ouverture du volet de configuration Contrôle parental

Si aucun problème n'a été relevé sous **Contrôle parental**, vous pouvez ouvrir le volet de configuration à partir du volet d'information.

Pour ouvrir le volet de configuration Contrôle parental :

1. Dans le volet Accueil, cliquez sur **Contrôle parental**.
2. Dans le volet de droite, cliquez sur **Configurer**.

Résolution des problèmes de protection

La plupart des problèmes de protection rencontrés par les utilisateurs peuvent être résolus automatiquement. Toutefois, si un ou plusieurs problèmes persistent, il est indispensable de les résoudre.

Résolution automatique des problèmes de protection

La plupart des problèmes de protection rencontrés par les utilisateurs peuvent être résolus automatiquement.

Pour résoudre automatiquement les problèmes de protection :

- Cliquez sur **Corriger** en regard de l'état de protection.

Résolution manuelle des problèmes de protection

Si certains problèmes ne peuvent pas être résolus automatiquement, cliquez sur le lien suivant le problème en question pour effectuer l'action suggérée.

Pour résoudre manuellement les problèmes de protection :

- Effectuez l'une des opérations suivantes.
  - Si l'analyse complète de votre ordinateur n'a pas été exécutée depuis au moins 30 jours, cliquez sur l'option **Analyser** située à gauche de l'état de protection principal pour effectuer une analyse manuelle (cette option est disponible si McAfee VirusScan est installé).
  - Si vos fichiers de signatures (DAT) sont dépassés, cliquez sur le lien **Mettre à jour** situé à gauche de l'état de protection principal pour mettre à jour votre protection.
  - Si un programme n'est pas installé, cliquez sur **Bénéficiez d'une protection complète** pour l'installer.
  - Si certains composants d'un programme sont manquants, réinstallez-le.
  - Si un programme doit être enregistré pour bénéficier d'une protection complète, cliquez sur **M'enregistrer maintenant**. Cet élément apparaît si l'abonnement à un ou plusieurs programmes a expiré.
  - Dans ce cas, cliquez sur **Vérifiez votre abonnement maintenant** pour vérifier l'état de votre compte. Cet élément apparaît si l'abonnement à un ou plusieurs programmes a expiré.

Affichage des informations sur SecurityCenter

En bas du volet Etat de protection, la section SecurityCenter - Informations vous permet d'accéder aux options de SecurityCenter et vous indique la dernière mise à jour, la dernière analyse (si McAfee VirusScan est installé) et des informations sur l'expiration de l'abonnement à vos produits McAfee.

Ouverture du volet de configuration SecurityCenter

Pour votre commodité, vous pouvez ouvrir le volet de configuration SecurityCenter pour modifier les options définies depuis le volet Accueil.

Pour ouvrir le volet de configuration SecurityCenter :

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

Affichage des informations sur les produits installés

Vous pouvez afficher la liste des produits installés avec le numéro de version de chaque produit et la date de la dernière mise à jour.

Pour consulter les informations de produits McAfee :

- Dans le volet Accueil, sous **SecurityCenter - Informations**, cliquez sur **Afficher les détails** pour ouvrir la fenêtre des informations sur le produit.

Utilisation du Menu avancé

A la première ouverture de SecurityCenter, le Menu de base apparaît dans la colonne de gauche. Si vous êtes un utilisateur expérimenté, vous pouvez cliquer sur **Menu avancé** pour afficher à la place un menu de commandes plus détaillé. Pour votre commodité, le dernier menu utilisé sera affiché à la prochaine ouverture de SecurityCenter.

La page Menu avancé comprend les éléments suivants :

- Particuliers
- Journaux et rapports (comprend la liste des événements les plus récents et des journaux par type relatifs aux 30, 60 et 90 derniers jours)
- Configurer
- Restaurer
- Outils

CHAPITRE 4

Configuration des options de SecurityCenter

SecurityCenter vous permet de consulter l'état de protection générale de votre ordinateur, de créer des comptes utilisateur McAfee, d'installer automatiquement les dernières mises à jour du produit, et d'être averti automatiquement par des alertes et des signaux sonores en cas d'attaques générales de virus, de menaces et de mises à jour de produits.

Dans le volet Configuration de SecurityCenter, vous pouvez modifier les options SecurityCenter définies pour les fonctions suivantes :

- Etat de protection
- Utilisateurs
- Mises à jour automatiques
- Alertes

Contenu de ce chapitre

Configuration de l'état de protection

L'état de protection générale de votre ordinateur apparaît dans la section **Suis-je protégé** de SecurityCenter.

L'état de protection vous indique si votre ordinateur est totalement protégé contre les dernières menaces de sécurité ou s'il existe des problèmes nécessitant une attention particulière et comment les résoudre.

Par défaut, si les fonctionnalités Protection antispam ou Blocage de contenu ne sont pas installées, ces problèmes de protection mineurs sont automatiquement ignorés et ne sont pas consignés dans l'état de protection générale de votre ordinateur. Toutefois, lorsqu'un problème de protection est suivi d'un lien **Ignorer**, vous pouvez choisir d'ignorer le problème en question si vous êtes sûr de ne pas vouloir le résoudre. Si vous décidez par la suite de régler un problème précédemment ignoré, vous pourrez l'inclure dans l'état de protection de l'ordinateur afin que celui-ci soit contrôlé.

Configuration des problèmes ignorés

Vous pouvez inclure ou exclure des problèmes de l'état de protection générale de votre ordinateur. Lorsqu'un problème de protection est suivi d'un lien **Ignorer**, vous pouvez choisir d'ignorer le problème en question si vous êtes sûr de ne pas vouloir le résoudre. Si vous décidez par la suite de régler un problème précédemment ignoré, vous pourrez l'inclure dans l'état de protection de l'ordinateur afin que celui-ci soit contrôlé.

Pour configurer les problèmes ignorés :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'option **Etat de protection** pour ouvrir le volet correspondant, puis sur **Options avancées**.
3. Effectuez l'une des opérations suivantes dans le volet Problèmes ignorés :
   - Pour ne plus ignorer certains problèmes dans l'état de protection, désactivez les cases à cocher correspondantes.
   - Pour exclure des problèmes de l'état de protection, activez les cases à cocher correspondantes.
4. Cliquez sur **OK**.

Configuration des options utilisateur

Si vous exécutez des programmes McAfee qui nécessitent des autorisations utilisateur, celles-ci correspondent par défaut aux comptes utilisateur Windows de cet ordinateur. Pour faciliter la gestion des utilisateurs de ces programmes, vous pouvez changer de compte utilisateur McAfee à tout moment.

Dans ce cas, les noms d'utilisateur et autorisations de votre programme de contrôle parental sont importés automatiquement. Toutefois, lors du premier changement de compte utilisateur, vous devez créer un compte administrateur. Vous pouvez ensuite commencer à créer et à configurer d'autres comptes utilisateur McAfee.

Passage aux comptes utilisateur McAfee

Par défaut, vous utilisez les comptes utilisateur de Windows. Toutefois, pour utiliser des comptes utilisateur McAfee, il n'est pas nécessaire de créer des comptes utilisateur supplémentaires sous Windows.

Pour basculer vers les comptes utilisateur McAfee :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'option **Utilisateurs** pour ouvrir le volet correspondant, puis sur **Options avancées**.
3. Pour utiliser les comptes utilisateur McAfee, cliquez sur **Basculer**.

Si vous basculez vers les comptes utilisateur McAfee pour la première fois, vous devez créer un compte administrateur (page 23).

Création d'un compte administrateur

Lors du premier changement de compte utilisateur McAfee, vous êtes invité à créer un compte administrateur.

Pour créer un compte administrateur :

1. Entrez un mot de passe dans la zone **Mot de passe**, puis entrez-le à nouveau dans la zone **Confirmer le mot de passe**.
2. Sélectionnez une question permettant de récupérer le mot de passe dans la liste, puis entrez la réponse à celle-ci dans la zone **Réponse**.
3. Cliquez sur **Appliquer**.

   Lorsque vous avez terminé, le type de compte utilisateur est mis à jour (le cas échéant) avec les noms d'utilisateur et

autorisations existants de votre programme de contrôle parental. Si vous configurez des comptes utilisateur pour la première fois, le volet Gérer les utilisateurs s'affiche.

Configuration des options utilisateur

Dans ce cas, les noms d'utilisateur et autorisations de votre programme de contrôle parental sont importés automatiquement. Toutefois, lors du premier changement de compte utilisateur, vous devez créer un compte administrateur. Vous pouvez ensuite commencer à créer et à configurer d'autres comptes utilisateur McAfee.

Pour configurer des options utilisateur :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'option **Utilisateurs** pour ouvrir le volet correspondant, puis sur **Options avancées**.
3. Sous **Comptes utilisateur**, cliquez sur **Ajouter**.
4. Entrez le nom d'utilisateur dans la zone **Nom d'utilisateur**.
5. Entrez un mot de passe dans la zone **Mot de passe**, puis entrez-le à nouveau dans la zone **Confirmer le mot de passe**.
6. Sélectionnez la case **Utilisateur au démarrage** si vous voulez que ce nouvel utilisateur se connecte automatiquement au démarrage de SecurityCenter.
7. Sous **Type de compte utilisateur**, sélectionnez un type de compte pour l'utilisateur voulu, puis cliquez sur **Créer**.

   Remarque : vous devez ensuite configurer les paramètres d'utilisateur limité sous Contrôle parental.

8. Pour changer le mot de passe d'un utilisateur, la connexion automatique ou le type de compte, sélectionnez un nom d'utilisateur dans la liste, puis cliquez sur **Modifier**.
9. Lorsque vous avez terminé, cliquez sur **Appliquer**.

Récupération du mot de passe administrateur

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

Pour récupérer le mot de passe administrateur :

1. Cliquez à l'aide du bouton droit de la souris sur l'icône M de SecurityCenter, puis cliquez sur **Changer d'utilisateur**.
2. Dans la liste **Nom d'utilisateur**, sélectionnez **Administrateur** et cliquez sur **Mot de passe oublié**.
3. Entrez la réponse à la question secrète que vous avez sélectionnée lors de la création de votre compte administrateur.
4. Cliquez sur **Valider**.

   Votre mot de passe d'administrateur s'affiche.

Modification du mot de passe administrateur

Si vous ne vous souvenez pas du mot de passe administrateur ou si vous pensez que sa confidentialité a pu être compromise, vous pouvez le modifier.

Pour modifier le mot de passe administrateur :

1. Cliquez à l'aide du bouton droit de la souris sur l'icône M de SecurityCenter, puis cliquez sur **Changer d'utilisateur**.
2. Dans la liste **Nom d'utilisateur**, sélectionnez **Administrateur** et cliquez sur **Changer le mot de passe**.
3. Entrez votre mot de passe dans la zone **Ancien mot de passe**.
4. Entrez un nouveau mot de passe dans la zone **Mot de passe**, puis entrez-le à nouveau dans la zone **Confirmer le mot de passe**.
5. Cliquez sur **OK**.

Configuration des options de mise jour

SecurityCenter est configuré pour vérifier automatiquement toutes les quatre heures les mises à jour de tous vos services McAfee lorsque vous êtes connecté à Internet et pour installer automatiquement les dernières mises à jour du produit. Toutefois, vous pouvez à tout moment rechercher manuellement les mises à jour grâce à l'icône SecurityCenter de la zone de notification située à l'extrême droite de la barre des tâches.

Recherche automatique de mises à jour

SecurityCenter recherche automatiquement les mises à jour toutes les quatre heures lorsque vous êtes connecté à Internet. Cependant, vous pouvez configurer SecurityCenter de manière à recevoir une notification avant le téléchargement ou l'installation automatique des mises à jour.

Pour rechercher des mises à jour automatiquement :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'état **Des mises à jour automatiques sont activées** pour ouvrir le volet correspondant, puis sur **Options avancées**.
3. Sélectionnez l'une des options suivantes dans le volet Options de mise à jour :
   - Installer les mises à jour automatiquement et m'avertir quand le produit est mis à jour (recommandé) (page 27)
   - Télécharger automatiquement les mises à jour et m'avertir de la possibilité de les installer (page 28)
   - M'avertir avant de télécharger une mise à jour (page 28)
4. Cliquez sur **OK**.

Remarque : pour une protection maximale, il est préférable que SecurityCenter recherche et installe automatiquement les mises à jour. Toutefois, si vous souhaitez uniquement mettre à jour vos services de sécurité manuellement, vous pouvez désactiver la mise à jour automatique (page 29).

Téléchargement et installation automatiques de mises à jour

Si vous sélectionnez **Installer automatiquement les mises à jour de mes services et m'avertir de l'opération une fois terminée (recommandé)** dans les options de mise à jour, SecurityCenter télécharge et installe automatiquement les mises à jour.

Téléchargement automatique de mises à jour

Si vous sélectionnez **Télécharger les mises à jour automatiquement et m'avertir quand elles sont prêtes à être installées** dans la boîte de dialogue Options de mise à jour, SecurityCenter télécharge automatiquement les mises à jour et vous avertit dès qu'une mise à jour est prête à être installée. Vous pouvez choisir d'installer la mise à jour ou de la reporter (page 29).

Pour installer une mise à jour téléchargée automatiquement :

1. Cliquez sur **Mettre à jour mes produits maintenant**, puis sur **OK**.

   Si vous y êtes invité, vous devez vous connecter au site Web pour vérifier votre abonnement avant que le téléchargement ne puisse démarrer.

2. Une fois votre abonnement vérifié, cliquez sur **Mettre à jour** dans le volet Mises à jour afin de télécharger et d'installer la mise à jour. Si votre abonnement est arrivé à expiration, cliquez sur **Renouveler mon abonnement** dans le message d'alerte et suivez les indications.

Remarque : dans certains cas, vous serez invité à redémarrer votre ordinateur pour terminer la mise à jour. Enregistrez votre travail et fermez tous les programmes avant de redémarrer.

Notification avant téléchargement de mises à jour

Si vous sélectionnez **M'avertir avant de télécharger une mise à jour** dans la boîte de dialogue Options de mise à jour, SecurityCenter vous avertit avant de télécharger les mises à jour. Vous pouvez alors choisir de télécharger et d'installer la mise à jour de vos services de sécurité afin d'éliminer toute menace d'attaque.

Pour télécharger et installer une mise à jour :

1. Sélectionnez **Mettre à jour mes produits maintenant**, puis sur **OK**.

2. Connectez-vous au site Web si vous y êtes invité.

   La mise à jour est automatiquement téléchargée.

3. Cliquez sur **OK** une fois l'installation de la mise à jour terminée.

Remarque : dans certains cas, vous serez invité à redémarrer votre ordinateur pour terminer la mise à jour. Enregistrez votre travail et fermez tous les programmes avant de redémarrer.

Désactivation de la mise à jour automatique

Pour une protection maximale, il est préférable que SecurityCenter recherche et installe automatiquement les mises à jour. Toutefois, si vous souhaitez procéder uniquement à la mise à jour manuelle de vos services de sécurité, vous pouvez désactiver la mise à jour automatique.

Remarque : n'oubliez pas de rechercher manuellement les mises à jour (page 30) au moins une fois par semaine. Si vous ne recherchez pas de mises à jour, votre ordinateur n'est pas protégé par les dernières mises à jour de sécurité.

Pour désactiver la mise à jour automatique :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'état **Des mises à jour automatiques sont activées** pour ouvrir le volet correspondant.
3. Cliquez sur **Inactif**.
4. Cliquez sur **Oui** pour confirmer les modifications.

   L'état est mis à jour dans l'en-tête.

Si vous n'avez pas recherché manuellement les mises à jour au bout de sept jours, une alerte vous rappelle de le faire.

Report des mises à jour

Si vous êtes trop occupé pour mettre à jour vos services de sécurité lorsque l'alerte apparaît, vous pouvez choisir d'être rappelé ultérieurement ou ignorer l'alerte.

Pour reporter une mise à jour :

- Effectuez l'une des opérations suivantes.
  - Sélectionnez **Me le rappeler ultérieurement**, puis cliquez sur **OK**.
  - Sélectionnez **Fermer cette alerte**, puis cliquez sur **OK** pour fermer l'alerte sans rien faire d'autre.

Recherche manuelle de mises à jour

SecurityCenter est configuré pour rechercher automatiquement des mises à jour toutes les quatre heures lorsque vous êtes connecté à Internet et pour installer les dernières mises à jour du produit. Toutefois, vous pouvez à tout moment rechercher manuellement les mises à jour grâce à l'icône SecurityCenter de la zone de notification Windows située à l'extrême droite de la barre des tâches.

Remarque : pour une protection maximale, il est préférable que SecurityCenter recherche et installe automatiquement les mises à jour. Toutefois, si vous souhaitez uniquement mettre à jour vos services de sécurité manuellement, vous pouvez désactiver la mise à jour automatique (page 29).

Pour rechercher des mises à jour manuellement :

1. Assurez-vous que votre ordinateur est bien connecté à Internet.
2. Cliquez avec le bouton droit de la souris sur l'icône M de SecurityCenter dans la zone de notification Windows située à l'extrême droite de la barre des tâches, puis cliquez sur **Mises à jour**.

   Pendant que SecurityCenter recherche des mises à jour, vous pouvez continuer à travailler avec cette application.

   Pour plus de facilité, une icône animée s'affiche dans la zone de notification Windows située à l'extrême droite de la barre des tâches. Une fois que SecurityCenter a terminé, cette icône disparaît automatiquement.
3. Si vous y êtes invité, connectez-vous au site Web pour vérifier l'état de votre abonnement.

Remarque : dans certains cas, vous serez invité à redémarrer votre ordinateur pour terminer la mise à jour. Enregistrez votre travail et fermez tous les programmes avant de redémarrer.

Configuration des options d'alerte

SecurityCenter utilise des alertes et des sons pour vous avertir automatiquement des attaques générales de virus, des menaces et des mises à jour produit. Vous pouvez cependant configurer SecurityCenter pour afficher uniquement les alertes à traiter immédiatement.

Configuration des options d’alerte

SecurityCenter utilise des alertes et des sons pour vous avertir automatiquement des attaques générales de virus, des menaces et des mises à jour produit. Vous pouvez cependant configurer SecurityCenter pour afficher uniquement les alertes à traiter immédiatement.

Pour configurer les options d'alerte :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'option **Alertes** pour ouvrir le volet correspondant, puis sur **Options avancées**.
3. Sélectionnez l'une des options suivantes dans le volet Options d’alerte :
   - **M'avertir en cas d'attaque générale d'un virus ou de menace**
   - **Afficher les alertes d'information en mode jeu**
   - **Emettre un son en cas d’alerte**
   - **Afficher l'écran d'accueil de McAfee au démarrage de Windows**
4. Cliquez sur **OK**.

Remarque : pour désactiver les alertes d'information, cochez la case **Ne plus afficher cette alerte**. Vous pourrez les réactiver ultérieurement à partir du volet Alertes d'information.

Configuration des alertes d'information

Les alertes d'information ne nécessitent pas un traitement immédiat. Si vous désactivez les alertes de d'information depuis l'alerte, vous pourrez les réactiver ultérieurement à partir du volet Alertes d'information.

Pour configurer les alertes d'information :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'option **Alertes** pour ouvrir le volet correspondant, puis sur **Options avancées**.
3. Sous **Configuration de SecurityCenter**, cliquez sur **Alertes d'information**.
4. Décochez la case **Masquer les alertes de type Informations**, puis décochez dans la liste les cases correspondant aux alertes que vous souhaitez afficher.
5. Cliquez sur **OK**.

CHAPITRE 5

Exécution de tâches courantes

Vous pouvez exécuter des tâches courantes comme revenir au volet Accueil, afficher les événements récents, gérer votre réseau informatique (si l'ordinateur dispose des droits appropriés) et mettre à jour votre ordinateur. Si McAfee Data Backup est installé, vous pouvez également sauvegarder vos données.

Contenu de ce chapitre

Exécution de tâches courantes

Vous pouvez exécuter des tâches courantes comme revenir au volet Accueil, afficher les événements récents, mettre à jour votre ordinateur, gérer votre réseau informatique (si l'ordinateur dispose des droits appropriés) et sauvegarder vos données (si McAfee Data Backup est installé).

Pour exécuter des tâches courantes :

- Sous **Tâches courantes** dans le Menu de base, sélectionnez l'une des options suivantes :
  - Pour revenir au volet Accueil, cliquez sur **Accueil**.
  - Pour afficher les événements récents détectés par votre logiciel de sécurité, cliquez sur **Evénements récents**.
  - Pour supprimer des fichiers inutilisés, défragmenter vos données et rétablir les paramètres précédents de votre ordinateur, cliquez sur **Mettre à jour l'ordinateur**.
  - Pour gérer votre réseau informatique, cliquez sur **Gérer un réseau** à partir d'un ordinateur disposant des droits de gestion sur ce réseau.

    Network Manager surveille les vulnérabilités des ordinateurs de votre réseau en matière de sécurité pour vous permettre d'identifier facilement les problèmes de sécurité réseau.
  - Pour créer des copies de sauvegarde de vos fichiers, cliquez sur **Sauvegarde des données** si McAfee Data Backup est installé.

La fonction de sauvegarde automatique enregistre des copies de vos fichiers les plus précieux à tout moment, les chiffre et les stocke sur CD/DVD, clé USB ou disque externe réseau.

Conseil : pour votre commodité, vous pouvez effectuer des tâches courantes depuis deux autres emplacements (sous **Accueil** dans le Menu avancé et sous le menu **QuickLinks** accessible à partir de l'icône M de SecurityCenter située à l'extrême droite de la barre des tâches). Vous pouvez également consulter la liste des événements récents et des journaux complets par type sous **Journaux et rapports**, à partir du Menu avancé.

Affichage des événements récents

Les événements récents sont consignés lorsque des modifications sont apportées à votre ordinateur (par exemple, lorsqu'un type de protection est activé ou désactivé, qu'une menace potentielle est supprimée ou qu'une tentative de connexion Internet est bloquée). Vous pouvez afficher les 20 événements les plus récents et les informations sur ceux-ci.

Consultez le fichier d'aide du produit correspondant pour obtenir des informations détaillées sur ces événements.

Pour afficher les événements récents :

1. Cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, puis cliquez sur **Afficher les événements récents**.

   Tous les événements récents apparaissent dans la liste, accompagnés de la date et d'une description générale de celui-ci.

2. Sous **Evénements récents**, sélectionnez un événement pour afficher des informations complémentaires dans le volet Détails.

   La liste des actions disponibles apparaît sous **Je souhaite**.

3. Pour afficher une liste d'événements plus complète, cliquez sur **Afficher le journal**.

Mise à jour automatique de votre ordinateur

Pour libérer un espace précieux sur votre disque dur et optimiser les performances de votre ordinateur, vous pouvez planifier à intervalles réguliers l'exécution de tâches avec QuickClean ou le défragmenteur de disque. Le programme exécute notamment les tâches telles que la suppression, le broyage et la défragmentation des fichiers et dossiers.

Pour mettre à jour automatiquement les données de votre ordinateur :

1. Cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, puis cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Tâches planifiées**, cliquez sur **Démarrer**.
3. Dans la liste des opérations, sélectionnez **QuickClean** ou **défragmenteur de disque**.
4. Effectuez l'une des opérations suivantes.
   - Pour modifier une tâche existante, sélectionnez-la puis cliquez sur **Modifier**. Suivez les instructions à l'écran.
   - Pour créer une tâche, entrez un nom dans la zone **Nom de la tâche**, puis cliquez sur **Créer**. Suivez les instructions à l'écran.
   - Pour supprimer une tâche, sélectionnez-la et cliquez sur **Supprimer**.
5. Sous **Récapitulatif de la tâche**, consultez le moment de la dernière exécution, celui de la prochaine exécution et l'état de la tâche.

Mise à jour manuelle de votre ordinateur

Vous pouvez exécuter des tâches de maintenance manuelles pour supprimer des fichiers inutilisés, défragmenter vos données ou rétablir les paramètres précédents de votre ordinateur.

Pour mettre à jour manuellement les données de votre ordinateur :

- Effectuez l'une des opérations suivantes.
  - Pour utiliser QuickClean, cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, cliquez sur **Mettre à jour l'ordinateur**, puis sur **Démarrer**.
  - Pour utiliser le défragmenteur de disque, cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, cliquez sur **Mettre à jour l'ordinateur**, puis sur **Analyser**.
  - Pour restaurer le système, dans le Menu avancé, cliquez sur **Outils**, **Restauration du système**, puis sur **Démarrer**.

Suppression de fichiers et de dossiers inutilisés

QuickClean permet de libérer un espace précieux sur votre disque dur et d'optimiser les performances de votre ordinateur.

Pour supprimer des fichiers et des dossiers inutilisés :

1. Cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, puis cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **QuickClean**, cliquez sur **Démarrer**.
3. Suivez les instructions à l'écran.

Défragmentation de fichiers et dossiers

La fragmentation des fichiers se produit lors de la suppression et de la création des fichiers et des dossiers. Généralement sans gravité, cette fragmentation ralentit les accès au disque et diminue les performances générales de l'ordinateur.

Utilisez la défragmentation pour réécrire des parties d'un fichier sur des secteurs contigus d'un disque dur afin d'augmenter la vitesse d'accès aux données et la récupération de celles-ci.

Pour défragmenter des fichiers et des dossiers :

1. Cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, puis cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Défragmenteur de disque**, cliquez sur **Analyse**.
3. Suivez les instructions à l'écran.

Restauration des paramètres précédents de votre ordinateur

Les points de restauration sont des « instantanés » de votre ordinateur enregistrés périodiquement par Windows et en cas d'événement significatif (par exemple, l'installation d'un programme ou d'un pilote). Toutefois, vous pouvez également créer et nommer à tout moment vos propres points de restauration.

Utilisez les points de restauration pour annuler des modifications importantes apportées aux paramètres de votre ordinateur et rétablir les paramètres précédents.

Pour rétablir les paramètres précédents de votre ordinateur :

1. Dans le menu Avancé, cliquez sur **Outils**, puis sur **Restauration du système**.
2. Sous **Restauration du système**, cliquez sur **Démarrer**.
3. Suivez les instructions à l'écran.

Gestion de votre réseau

Si votre ordinateur dispose des droits de gestion sur le réseau, Network Manager surveille les vulnérabilités des ordinateurs de votre réseau en matière de sécurité pour vous permettre d'identifier facilement les problèmes de sécurité.

Si l'état de protection de votre ordinateur n'est pas surveillé sur ce réseau, cet ordinateur ne fait pas partie du réseau ou il est défini comme membre non géré de celui-ci. Consultez le fichier d'aide sur Network Manager pour plus d'informations.

Pour gérer votre réseau :

1. Cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, puis cliquez sur **Gérer un réseau**.
2. Cliquez sur l'icône représentant cet ordinateur sur la carte du réseau.
3. Sous **Je souhaite**, cliquez sur **Surveiller cet ordinateur**.

Plus d'informations sur les virus

Utilisez la bibliothèque d'informations sur les virus et Virus Map pour effectuer les opérations suivantes :

- Obtenez des informations sur les derniers virus, canulars par e-mail et autres menaces.
- Bénéficiez d'outils de suppressions de virus gratuits pour réparer votre ordinateur.
- Obtenez une vue aérienne en temps réel de la carte des ordinateurs infectés par les derniers virus dans le monde.

Pour plus d'informations sur les virus :

1. Dans le menu Avancé, cliquez sur **Outils**, puis sur **Informations sur les virus**.
2. Effectuez l'une des opérations suivantes :
   - Recherchez les virus à l'aide de la bibliothèque d'informations sur les virus de McAfee.
   - Recherchez les virus à l'aide de World Virus Map sur le site Web de McAfee.

CHAPITRE 6

McAfee QuickClean

Lorsque vous surfez sur Internet, votre ordinateur accumule rapidement des fichiers encombrants. Avec QuickClean, protégez votre confidentialité et débarrassez-vous de l'encombrement inutile engendré par Internet et les e-mails. QuickClean identifie et supprime les fichiers qui s'accumulent au cours de la navigation sur Internet, tels que les cookies, les e-mails, les téléchargements et les historiques, autant de fichiers de données qui contiennent des informations personnelles vous concernant. Il protège votre confidentialité en permettant la suppression sécurisée de ces informations sensibles.

QuickClean supprime également les programmes indésirables. Indiquez les fichiers à supprimer et éliminez l'encombrement tout en préservant les informations essentielles.

Contenu de ce chapitre

Présentation des fonctions de QuickClean

Cette section décrit les fonctions de QuickClean.

Fonctions

QuickClean offre un ensemble d'outils efficaces et faciles à utiliser qui suppriment en toute sécurité les éléments inutiles de votre ordinateur. Vous pouvez ainsi libérer un espace disque précieux et optimiser les performances de votre ordinateur.

CHAPITRE 7

Nettoyage de votre ordinateur

QuickClean vous permet de vraiment supprimer des fichiers et des dossiers.

Lorsque vous naviguez sur Internet, votre navigateur copie chaque page Internet et ses graphiques dans un dossier cache du disque dur. Il peut ainsi charger rapidement une page sur laquelle vous retournez. La mise en cache des fichiers est utile si vous consultez souvent les mêmes pages Internet et que leur contenu ne change que rarement. Mais, la plupart du temps, les fichiers mis en cache sont inutiles et peuvent donc être supprimés.

Les nettoyeurs suivants vous permettent de supprimer divers éléments.

- Nettoyeur de la Corbeille : nettoie la Corbeille de Windows.
- Nettoyeur de fichiers temporaires : supprime les fichiers stockés dans des dossiers temporaires.
- Nettoyeur de raccourcis : supprime les raccourcis inutilisables et les raccourcis non associés à un programme.
- Nettoyeur de fragments de fichiers perdus : supprime de l'ordinateur les fragments de fichier perdus.
- Nettoyeur de registre : supprime du registre Windows les informations correspondant à des programmes désormais inexistants.
- Nettoyeur du cache : supprime les fichiers mis en cache qui s'accumulent lorsque vous naviguez sur Internet. Ils sont généralement stockés sous forme de fichiers Internet temporaires.
- Nettoyeur de cookies : supprime les cookies. Ils sont généralement stockés sous forme de fichiers Internet temporaires.
  Les cookies sont de petits fichiers que votre navigateur Internet stocke sur l'ordinateur à la demande d'un serveur Web. Chaque fois que vous affichez une page à partir du serveur Web, le navigateur renvoie le cookie au serveur. Ces cookies peuvent jouer le rôle d'étiquette, ce qui permet au serveur Web de savoir quelles pages vous consultez et à quelle fréquence.
- Nettoyeur de l'historique du navigateur : supprime l'historique de votre navigateur.

- Nettoyeur d'e-mails Outlook Express et Outlook (éléments supprimés et envoyés) : supprime les e-mails des dossiers Outlook Envoyé et Supprimé.
- Nettoyeur récemment utilisé : supprime les éléments récemment utilisés stockés sur votre ordinateur, tels que les documents Microsoft Office.
- Nettoyeur de plug-ins et de contrôles ActiveX : supprime les plug-ins et les contrôles ActiveX.
  ActiveX est une technologie utilisée pour implémenter des contrôles dans un programme. Un contrôle ActiveX permet, par exemple, d'ajouter un bouton à l'interface d'un programme. La plupart de ces contrôles sont inoffensifs ; cependant, des personnes mal intentionnées utilisent la technologie ActiveX pour récupérer des informations sur votre ordinateur.
  Les plug-ins sont de petits programmes qui s'intègrent à des applications plus importantes pour offrir une fonctionnalité supplémentaire. Grâce aux plug-ins, le navigateur Web peut exécuter des fichiers incorporés à des documents HTML, dans des formats qu'il ne reconnaîtrait pas normalement (par exemple, fichiers vidéo, audio et d'animation).
- Nettoyeur de points de restauration du système : supprime les anciens points de restauration du système de votre ordinateur.

Contenu de ce chapitre

Utilisation de QuickClean

Cette section présente l'utilisation de QuickClean.

Nettoyage de votre ordinateur

Vous pouvez supprimer les fichiers et dossiers inutilisés, libérer de l'espace disque et améliorer le fonctionnement de votre ordinateur.

Pour nettoyer votre ordinateur :

1. dans le menu Avancé, cliquez sur **Outils**.
2. Cliquez sur **Gérer l'ordinateur**, puis sur **Démarrer** sous **McAfee QuickClean**.
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.** Pour le Nettoyeur récemment utilisé, vous pouvez cliquer sur **Propriétés** pour éliminer les programmes dont vous ne souhaitez pas nettoyer les listes.
   - Cliquez sur **Paramètres par défaut** pour rétablir les nettoyeurs par défaut, puis cliquez sur **Suivant.**
4. Lorsque l'analyse est terminée, cliquez sur **Suivant** pour confirmer la suppression des fichiers. Vous pouvez développer cette liste pour voir les fichiers qui seront nettoyés et leur emplacement.
5. Cliquez sur **Suivant**.
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** et spécifiez le nombre de passages. Les fichiers supprimés à l'aide de Shredder ne peuvent pas être récupérés.
7. Cliquez sur **Terminer**.
8. Sous **Résumé QuickClean**, consultez le nombre de fichiers de registre supprimés et le volume d'espace disque récupéré après le nettoyage du disque et la suppression des éléments générés par Internet.

CHAPITRE 8

McAfee Shredder

Vous pouvez récupérer les fichiers supprimés sur votre ordinateur, même après avoir vidé la Corbeille. Lorsque vous supprimez un fichier, Windows marque cet espace sur votre lecteur de disque comme inutilisé, mais le fichier est toujours là. Avec des outils d'expertise informatique judiciaire, il est possible de récupérer des déclarations d'impôt, des CV ou d'autres documents que vous avez supprimés. Shredder protège votre confidentialité en supprimant en toute sécurité et de manière définitive les fichiers indésirables.

Pour supprimer un fichier définitivement, vous devez écraser le fichier existant plusieurs fois avec de nouvelles données. Microsoft® Windows ne supprime pas les fichiers de manière définitive parce que cette opération serait très lente. Le fait de broyer un document n'empêche pas sa récupération, car certains programmes créent des copies cachées temporaires des documents ouverts. Si vous ne broyez que les documents visibles dans l'Explorateur Windows®, il se peut qu'il existe encore des copies temporaires de ces documents.

Remarque : les fichiers broyés ne sont pas sauvegardés. Il est impossible de restaurer des fichiers effacés par Shredder.

Contenu de ce chapitre

Présentation des fonctions de Shredder

Cette section décrit les fonctions de Shredder.

Fonctionnalités

Shredder vous permet d'effacer le contenu de la Corbeille, les fichiers Internet temporaires, l'historique des sites Web, les fichiers, les dossiers et les disques.

CHAPITRE 9

Effacement des fichiers indésirables avec Shredder

Shredder protège votre confidentialité en supprimant en toute sécurité et de manière définitive les fichiers indésirables tels que le contenu de la Corbeille, les fichiers Internet temporaires et l'historique des sites Web. Vous pouvez sélectionner les fichiers et les dossiers à broyer, ou naviguer jusqu'à leur emplacement.

Contenu de ce chapitre

Utilisation de Shredder

Cette section vous explique comment utiliser Shredder.

Broyage des fichiers, des dossiers et des disques.

Des fichiers peuvent résider sur votre ordinateur, même après que vous ayez vidé la Corbeille. Cependant, lorsque vous broyez des fichiers, vos données sont définitivement supprimées et les pirates informatiques ne peuvent plus y accéder.

Pour broyer des fichiers, des dossiers et des disques :

1. Dans le menu Avancé, cliquez sur **Outils**, puis sur **Shredder**.
2. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Effacer des fichiers et des dossiers** pour broyer des fichiers et des dossiers.
   - Cliquez sur **Effacer un disque entier** pour broyer des disques.
3. Sélectionnez l'un des niveaux de broyage suivants :
   - **Rapide** : broie 1 fois les éléments sélectionnés.
   - **Complet** : broie 7 fois les éléments sélectionnés.
   - **Personnalisé** : broie jusqu'à 10 fois les éléments sélectionnés. Un nombre élevé de broyages augmente le niveau de sécurité de suppression des fichiers.
4. Cliquez sur **Suivant**.
5. Effectuez l'une des opérations suivantes :
   - Si vous broyez des fichiers, cliquez sur **Contenu de la Corbeille**, **Fichiers Internet temporaires** ou **Historique des sites Web** dans la liste **Sélectionnez le(s) fichier(s) à broyer**. Si vous broyez un disque, sélectionnez le disque.
   - Cliquez sur **Parcourir**, naviguez jusqu'aux fichiers que vous voulez broyer, puis sélectionnez-les.
   - Saisissez le chemin d'accès aux fichiers que vous voulez broyer dans la liste **Sélectionnez le(s) fichier(s) à broyer**.
6. Cliquez sur **Suivant**.
7. Cliquez sur **Terminer** pour terminer l'opération.
8. Cliquez sur **Terminé**.

CHAPITRE 10

McAfee Network Manager

McAfee® Network Manager présente sous forme graphique les ordinateurs et les autres composants de votre réseau. Vous pouvez utiliser Network Manager pour surveiller à distance l'état de protection de chaque ordinateur géré de votre réseau, mais aussi pour corriger à distance les points faibles de la sécurité de ces ordinateurs gérés.

Avant de commencer à utiliser Network Manager, nous vous conseillons de vous familiariser avec ses fonctionnalités les plus utilisées. Pour plus de détails sur la configuration et l'utilisation de ces fonctionnalités, consultez l'aide de Network Manager.

Contenu de ce chapitre

Fonctionnalités

Network Manager propose les fonctionnalités suivantes :

Carte graphique du réseau

La carte du réseau de Network Manager est une représentation graphique du niveau de sécurité des ordinateurs et des composants de votre réseau domestique. Lorsque vous modifiez votre réseau (lorsque vous ajoutez un ordinateur, par exemple), la carte du réseau identifie ces changements. Vous pouvez actualiser la carte du réseau, renommer le réseau, ou encore afficher ou masquer des composants de la carte du réseau. Vous pouvez également afficher les détails associés aux composants de la carte du réseau.

Gestion à distance

Utilisez la carte du réseau de Network Manager pour gérer le niveau de sécurité des ordinateurs qui constituent votre réseau domestique. Vous pouvez inviter un ordinateur à s'affilier au réseau géré, surveiller le niveau de protection des ordinateurs gérés et régler les problèmes connus de failles de sécurité du réseau à partir d'un ordinateur distant.

Présentation des icônes de Network Manager

Le tableau suivant décrit les icônes les plus utilisées sur la carte du réseau Network Manager.

Icône	Description
	Représente un ordinateur géré connecté au réseau
	Représente un ordinateur géré non connecté au réseau
	Représente un ordinateur non géré sur lequel McAfee Security 2007 est installé
	Représente un ordinateur non géré non connecté au réseau
	Représente un ordinateur connecté au réseau sur lequel McAfee Security 2007 n'est pas installé ou un matériel inconnu sur le réseau
	Représente un ordinateur non connecté au réseau sur lequel McAfee Security 2007 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 votre attention
	Signifie que l'élément correspondant nécessite votre attention et qu'il est déconnecté
	Représente un routeur personnel sans fil
	Représente un routeur personnel standard
	Représente Internet en mode connexion
	Représente Internet en mode déconnexion

CHAPITRE 11

Configuration d'un réseau géré

Pour configurer un réseau géré, vous triez les éléments de la carte de votre réseau et vous ajoutez des membres (des ordinateurs) au réseau.

Contenu de ce chapitre

Utilisation de la carte du réseau

Chaque fois que vous connectez un ordinateur au réseau, Network Manager analyse l'état du réseau afin de déterminer ses membres (gérés ou non), les attributs du routeur et l'état Internet. Si aucun membre n'est trouvé, Network Manager suppose que l'ordinateur actuellement connecté est le premier du réseau et en fait automatiquement un membre géré avec des autorisations d'administration. Par défaut, le nom du réseau inclut le nom du groupe de travail ou du domaine du premier ordinateur qui se connecte au réseau équipé de McAfee Security 2007. Vous pouvez modifier le nom du réseau à tout moment.

Lorsque vous modifiez votre réseau (lorsque vous ajoutez un ordinateur, par exemple), vous pouvez personnaliser la carte du réseau. Ainsi, vous pouvez actualiser la carte du réseau, renommer le réseau et afficher/masquer des composants de la carte. Vous pouvez également afficher les détails associés aux composants de la carte du réseau.

Accéder à la carte du réseau

Pour accéder à une carte de votre réseau, lancez Network Manager depuis la liste des tâches communes de SecurityCenter. La carte du réseau propose une représentation graphique des ordinateurs et des autres composants de votre réseau.

Pour accéder à la carte du réseau :

- Dans le menu de base ou le menu avancé, cliquez sur **Gérer un réseau**.
  La carte du réseau apparaît dans le panneau de droite.

Remarque : pour afficher la carte du réseau, vous devez commencer par autoriser les autres ordinateurs du réseau au premier accès à la carte.

Actualiser la carte du réseau

Vous pouvez actualiser la carte du réseau à tout moment, lorsqu'un nouvel ordinateur est affilié au réseau géré par exemple.

Pour actualiser la carte du réseau :

1. Dans le menu de base ou le menu avancé, cliquez sur **Gérer un réseau**.
   La carte du réseau apparaît dans le panneau de droite.
2. Cliquez sur **Actualiser la carte du réseau** sous **Je souhaite**.

Remarque : le lien **Actualiser la carte du réseau** n'est disponible que si aucun élément n'est sélectionné sur la carte du réseau. Pour désélectionner un élément, cliquez sur l'élément sélectionné ou sur une zone vide de la carte du réseau.

Attribution d'un nouveau nom au réseau

Par défaut, le nom du réseau inclut le nom du groupe de travail ou du domaine du premier ordinateur qui se connecte au réseau équipé de McAfee Security 2007. Si ce nom ne vous convient pas, vous pouvez le modifier.

Pour renommer le réseau :

1. Dans le menu de base ou le menu avancé, cliquez sur **Gérer un réseau**.
   La carte du réseau apparaît dans le panneau de droite.
2. Cliquez sur **Renommer le réseau** sous **Je souhaite**.
3. Saisissez le nom de votre ami dans le champ **Renommer le 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.

Afficher ou masquer des éléments de la carte du réseau

Par défaut, les ordinateurs et les autres composants de votre réseau apparaissent sur la carte du réseau. Si vous avez masqué des éléments, vous pouvez les réafficher à tout moment. Seuls les éléments non gérés peuvent être masqués. Les ordinateurs gérés ne peuvent pas être masqués.

Pour...	Dans le menu de base ou le menu avancé, cliquez sur **Gérer un réseau**, puis...
Masquer un élément de la carte du réseau	Cliquez sur un élément de la carte du réseau, puis sur **Masquer cet élément** sous **Je souhaite**. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.
Afficher des éléments masqués de la carte du réseau	Sous **Je souhaite**, cliquez sur **Afficher les éléments masqués**.

Afficher les détails d'un élément

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

Pour afficher les détails d'un 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 qu'il reçoive 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 (partage de fichiers ou d'impression, par exemple).

Remarque : après vous être affilié, si d'autres programmes réseau McAfee sont installés (McAfee Wireless Network Security ou EasyNetwork, par exemple), l'ordinateur est également reconnu comme étant un ordinateur géré pour ces programmes. Le niveau d'autorisation affecté à un ordinateur dans Network Manager s'applique à tous les programmes réseau McAfee. Pour obtenir des informations sur la signification des autorisations de type Invité, Complet ou Administration dans un autre programme réseau McAfee, reportez-vous à sa documentation.

Affiliation à un réseau géré

Lorsque vous êtes invité à vous affilier à un réseau géré, vous pouvez accepter ou refuser l'invitation. Vous pouvez également déterminer si vous voulez que cet ordinateur et les autres ordinateurs du réseau surveillent mutuellement leurs paramètres de sécurité (pour savoir par exemple si les services de protection antivirus d'un ordinateur sont à jour).

Pour s'affilier à un réseau géré :

1. Dans la boîte de dialogue d'invitation, cochez la case **Autoriser cet ordinateur et d'autres ordinateurs à surveiller les paramètres de sécurité les uns les autres** pour autoriser les autres ordinateurs du réseau géré à surveiller les paramètres de sécurité.
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 **Confirmer**.

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 **Refuser** dans la boîte de dialogue de confirmation de la sécurité.

Inviter un ordinateur à s'affilier au réseau géré

Si un ordinateur est ajouté au réseau géré ou si un autre ordinateur non géré est déjà présent sur le réseau, vous pouvez inviter cet ordinateur à s'affilier au réseau géré. Seuls les ordinateurs avec des autorisations d'administration sur le réseau peuvent en inviter d'autres à s'y affilier. Lorsque vous envoyez l'invitation, vous spécifiez également le niveau d'autorisation que vous affectez à cet ordinateur.

Pour inviter un ordinateur à s'affilier au réseau géré :

1. Cliquez sur l'icône d'un ordinateur non géré sur la carte du réseau.
2. Cliquez sur **Surveiller cet ordinateur** sous **Je souhaite**.
3. Dans la boîte de dialogue d'invitation à l'affiliation au réseau géré, cliquez sur l'une des options suivantes :
   - **Accorder l'accès à un invité**
     Permet à l'ordinateur d'accéder au réseau.

- **Accorder un accès complet à toutes les applications du réseau géré**
  Permet à l'ordinateur d'accéder au réseau, comme pour l'accès Invité.
- **Accorder un accès administratif à toutes les applications du réseau géré**
  Permet à l'ordinateur d'accéder au réseau avec des autorisations 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 **Inviter**.
Une invitation à s'affilier au réseau géré est envoyée à l'ordinateur. Lorsque l'ordinateur accepte l'invitation, deux cartes à jouer s'affichent.

5 Vérifiez que ces cartes sont identiques à celles affichées sur l'ordinateur que vous avez invité à s'affilier au réseau.

6 Cliquez sur **Autoriser l'accès**.

Remarque : si l'ordinateur que vous avez invité à s'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 accepté par erreur de faire confiance aux autres ordinateurs du réseau, vous pouvez arrêter de leur faire confiance.

Pour arrêter de faire confiance aux ordinateurs du réseau :

- 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 aucun autre ordinateur géré ne s'est affilié au réseau.

CHAPITRE 12

Gestion à distance du réseau

Une fois que vous avez configuré votre réseau géré, vous pouvez utiliser Network Manager pour gérer à distance les ordinateurs et les autres composants de votre réseau. Vous pouvez surveiller l'état et les niveaux de permission des ordinateurs et des autres composants, mais aussi corriger les problèmes de vulnérabilités, le tout à distance.

Contenu de ce chapitre

Surveillance de l'état et des autorisations

Un réseau géré comporte deux types de membres : des membres gérés et des membres non gérés. Les membres gérés autorisent les autres ordinateurs du réseau à surveiller l'état de leur protection McAfee, contrairement aux membres non gérés. Les membres non gérés sont généralement des invités qui souhaitent accéder à d'autres fonctionnalités du réseau (partage de fichiers ou d'impression, par exemple). Un ordinateur non géré peut être invité à devenir géré à tout moment par un autre ordinateur géré du réseau. De même, un ordinateur géré peut devenir non géré à tout moment.

Des autorisations de type Administration, Complet ou Invité sont associées aux ordinateurs gérés. Les autorisations de type Administration permettent à l'ordinateur géré de gérer l'état de protection de tous les autres ordinateurs gérés du réseau, mais aussi d'accorder une appartenance aux autres ordinateurs du réseau. Les autorisations de type Complet et Invité ne permettent que l'accès au réseau. Vous pouvez modifier le niveau d'autorisation d'un ordinateur à tout moment.

Un réseau géré comporte également du matériel gérable via Network Manager (des routeurs, par exemple). Vous pouvez aussi configurer et modifier les propriétés d'affichage d'un matériel sur la carte du réseau.

Surveillance de l'état de protection d'un ordinateur

Si l'état de protection d'un ordinateur n'est pas surveillé sur le réseau (parce que l'ordinateur n'est pas membre du réseau ou parce qu'il est membre non géré), vous pouvez demander sa surveillance.

Pour surveiller l'état de protection d'un ordinateur :

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

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

Vous pouvez arrêter de surveiller l'état de protection d'un ordinateur de votre réseau. L'ordinateur devient alors non géré.

Pour arrêter de surveiller l'état de protection d'un ordinateur :

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

Modification des autorisations d'un ordinateur géré

Vous pouvez modifier les autorisations d'un ordinateur géré à tout moment. Ainsi, vous pouvez choisir les ordinateurs qui vont surveiller l'état de protection (paramètres de sécurité) des autres ordinateurs du réseau.

Pour modifier les autorisations d'un ordinateur géré :

1. Cliquez sur l'icône d'un ordinateur géré sur la carte du réseau.
2. Cliquez sur **Modifier les autorisations de cet ordinateur** sous **Je souhaite**.
3. Dans la boîte de dialogue de modification des autorisations, sélectionnez ou désélectionnez la case à cocher afin de déterminer si cet ordinateur et les autres ordinateurs du réseau géré peuvent surveiller mutuellement l'état de leur protection.
4. Cliquez sur **OK**.

Gestion d'un matériel

Pour gérer un matériel, accédez à sa page Web d'administration depuis Network Manager.

Pour gérer un matériel :

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.

Pour modifier les paramètres d'affichage d'un matériel :

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 sur un des éléments suivants :

- **Routeur**
  Représente un routeur personnel standard.
- **Routeur sans fil**
  Représente un routeur personnel sans fil.

5 Cliquez sur **OK**.

Réparation des failles de sécurité

Les ordinateurs gérés avec des autorisations de type Administration peuvent surveiller l'état de protection McAfee des autres ordinateurs gérés du réseau, mais aussi corriger à distance toute défaillance détectée en matière de sécurité. Ainsi, si l'état de protection McAfee d'un ordinateur géré indique que VirusScan est désactivé, un autre ordinateur géré avec des autorisations de type Administration peut activer VirusScan à distance pour *corriger* ce problème.

Lorsque vous corrigez à distance des défaillances en matière de sécurité, Network Manager répare automatiquement 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, vous êtes invité à installer McAfee Security 2007 sur les ordinateurs du réseau.

Réparation automatique des failles de sécurité

Network Manager permet de corriger automatiquement la plupart des problèmes de sécurité sur les ordinateurs gérés distants. Par exemple, si VirusScan est désactivé sur un ordinateur distant, vous pouvez utiliser Network Manager pour le réactiver automatiquement.

Pour réparer les problèmes de sécurité :

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 de lancer 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'exécutent pas McAfee Security 2007, l'état de leur sécurité ne peut pas être surveillé à distance. Pour surveiller ces ordinateurs à distance, vous devez installer McAfee Security 2007 sur chacun d'entre eux.

Pour installer McAfee Security sur un ordinateur distant :

1. Dans un navigateur de l'ordinateur distant, rendez-vous sur http://download.mcafee.com/us/.
2. Suivez les instructions à l'écran pour installer McAfee Security 2007 sur l'ordinateur.

CHAPITRE 13

McAfee Wireless Network Security

Wireless Network Security fournit une protection automatique aux normes du secteur contre le vol de données ou l'accès non autorisé au réseau, et contre le "chargement parasite" large bande via une interface simple et intuitive par simple clic. Wireless Network Security chiffre vos données personnelles et confidentielles en les envoyant par Wi-Fi et empêche les pirates d'accéder à votre réseau sans fil.

Wireless Network Security empêche les pirates d'attaquer votre réseau sans fil en :

- bloquant des connexions non autorisées au réseau Wi-Fi
- empêchant la capture de données transmises par un réseau Wi-Fi
- détectant les tentatives de connexion à un réseau Wi-Fi

Wireless Network Security associe des fonctions faciles à utiliser, comme par exemple un verrouillage instantané du réseau et la possibilité d'ajouter rapidement des utilisateurs légitimes au réseau, à des fonctions de sécurité fiables, comme par exemple la génération automatique de clés chiffrées et la rotation programmée des clés.

Contenu de ce chapitre

Caractéristiques

Wireless Network Security offre les fonctionnalités suivantes.

Protection permanente

Wireless Network Security détecte automatiquement et protège les réseaux sans fil vulnérables auxquels vous vous connectez.

Interface intuitive

Protégez votre réseau sans avoir à prendre de décisions difficiles ou à apprendre des termes techniques complexes.

Chiffrement optimisé automatique

Ne laissez personne d'autre que vos amis et les membres de votre famille accéder à votre réseau et protégez vos données pendant leur transmission.

Solution logicielle uniquement

Wireless Network Security fonctionne avec votre routeur sans fil standard ou avec votre logiciel de point d'accès et de sécurité. Vous n'avez pas besoin d'acheter de matériel supplémentaire.

Rotation des clés automatique

Même les pirates les plus déterminés sont incapables de capturer vos informations du fait de la rotation des clés.

Ajout d'utilisateurs réseau

Vous pouvez facilement autoriser vos amis et votre famille à accéder à votre réseau. Vous pouvez ajouter des utilisateurs via une connexion sans fil ou en transférant les logiciels via une clé USB.

Outil de connexion intuitif

L'outil de connexion sans fil est intuitif et vous fournit des informations, notamment sur l'intensité du signal et le niveau de sécurité.

Consignation des événements et alertes

Des rapports faciles à comprendre et des alertes donnent aux utilisateurs avancés des informations supplémentaires sur votre réseau sans fil.

Mode Interruption

Arrêtez temporairement la rotation des clés de manière à ce que certaines applications puissent s'exécuter sans interruption.

Compatibilité avec d'autres équipements

Wireless Network Security se met automatiquement à jour avec les derniers modules de routeurs ou de points d'accès sans fil de grandes marques telles que : Linksys®, NETGEAR®, D-Link®, Belkin®, TRENDnet® et bien d'autres.

Démarrage de Wireless Network Security

Une fois installé, Wireless Network Security est automatiquement activé ; inutile de le démarrer manuellement. Vous pouvez cependant activer et désactiver manuellement la protection sans fil.

Une fois que vous avez installé Wireless Network Security, votre ordinateur tente d'établir une connexion au routeur sans fil. Une fois la connexion établie, l'ordinateur programme la clé de chiffrement dans le routeur sans fil. Si le mot de passe par défaut a été modifié, le système vous demande le mot de passe, de façon à ce que Wireless Network Security puisse configurer le routeur sans fil avec la clé de chiffrement partagée et un mode de sécurité complexe. Votre ordinateur est également configuré avec le même mode de chiffrement et de clé partagée, en établissant une connexion sans fil sécurisée.

Démarrage de Wireless Network Security

Wireless Network Security est activé par défaut, mais vous pouvez activer ou désactiver manuellement la protection sans fil.

L'activation de la protection sans fil empêche toute intrusion et interception de données sur votre réseau sans fil. Toutefois, si vous êtes connecté à un réseau sans fil externe, cette protection varie en fonction du niveau de sécurité de ce dernier.

Pour activer manuellement la protection sans fil :

1. Dans le volet McAfee SecurityCenter, effectuez l'une des opérations suivantes :
   - Cliquez sur **Internet & Réseau**, puis sur **Configurer**.
   - Cliquez sur **Menu avancé**, puis sur **Configurer** dans le volet **Accueil**, et pointez ensuite le curseur de la souris sur **Internet & Réseau**.
2. Dans le volet **Internet & Configuration réseau**, sous **Protection sans fil**, cliquez sur **Activé**.

Remarque : Wireless Network Security est automatiquement activé si vous avez installé un adaptateur sans fil compatible.

Arrêt de Wireless Network Security

Wireless Network Security est activé par défaut, mais vous pouvez activer ou désactiver manuellement la protection sans fil.

Le fait de désactiver la protection sans fil rend votre réseau vulnérable à l'intrusion et l'interception de données.

Pour désactiver la protection sans fil :

1. Dans le volet McAfee SecurityCenter, effectuez l'une des opérations suivantes :
   - Cliquez sur **Internet & Réseau**, puis sur **Configurer**.
   - Cliquez sur **Menu avancé**, puis sur **Configurer** dans le volet **Accueil**, et pointez ensuite le curseur de la souris sur **Internet & Réseau**.
2. Dans le volet **Internet & Configuration réseau**, sous **Protection sans fil**, cliquez sur **Désactivé**.

CHAPITRE 14

Protection des réseaux sans fil

Wireless Network Security protège votre réseau par la mise en oeuvre d'un chiffrement sans fil (par WEP, WPA ou WPA2, selon votre équipement). Il programme automatiquement des clients et des routeurs sans fil avec les informations d'authentification de clé de chiffrement valides, de façon à ce que le routeur sans fil autorise les ordinateurs à se connecter. Les réseaux sans fil protégés par le chiffrement empêchent les utilisateurs non autorisés d'accéder au réseau sans fil et protègent les données envoyées via un réseau sans fil. Wireless Network Security effectue cela en :

- créant et distribuant une clé de chiffrement longue, complexe, aléatoire et partagée
- effectuant une rotation de la clé de chiffrement de façon programmée
- configurant chaque périphérique sans fil avec des clés de chiffrement

Contenu de ce chapitre

configurant des réseaux sans fil protégés

Lorsque Wireless Network Security est installé, il vous demande automatiquement de protéger le réseau sans fil non sécurisé auquel vous êtes connecté ou de vous connecter à un réseau sans fil protégé auparavant.

Si vous n'êtes pas connecté à un réseau sans fil, Wireless Network Security recherche un réseau protégé par McAfee avec une intensité de signal élevée et invite l'utilisateur à se connecter au réseau. Si aucun réseau protégé n'est disponible, Wireless Network Security recherche des réseaux non sécurisés avec des signaux élevés et, lorsqu'il en trouve un, il vous invite à protéger ce réseau.

A moins qu'un réseau sans fil ait été protégé par McAfee Wireless Network Security, McAfee considère les réseaux sans fil comme étant "non protégés", même s'ils utilisent des mécanismes de sécurité sans fil comme WEP et WPA.

A moins qu'un réseau sans fil soit protégé par Wireless Network Security, McAfee considère le réseau comme étant non protégé, même s'il utilise un mécanisme de sécurité sans fil comme WEP et WPA.

A propos des types d'accès

Tout ordinateur sans fil équipé de Wireless Network Security peut créer un réseau sans fil protégé. Le premier ordinateur à protéger un routeur et à créer un réseau sans fil protégé se voit automatiquement accorder un accès administratif sur ce réseau. Les ordinateurs qui se connectent ultérieurement peuvent se voir accorder un accès administratif, total ou invité par un utilisateur existant qui dispose d'un accès administratif.

Les ordinateurs disposant d'accès de type administratif et total peuvent effectuer les tâches suivantes :

- protéger et supprimer un routeur ou point d'accès
- effectuer une rotation des clés de sécurité
- modifier les paramètres de sécurité du réseau
- réparer des réseaux
- accorder l'accès des ordinateurs au réseau
- révoquer l'accès au réseau sans fil protégé
- modifier le niveau d'administration d'un ordinateur

Les ordinateurs disposant d'un accès de type invité peuvent effectuer les tâches suivantes sur le réseau :

- se connecter à un réseau
- être affilié à un réseau
- modifier les paramètres spécifiques à l'ordinateur invité

Remarque : des ordinateurs peuvent avoir un accès administratif sur un réseau sans fil, mais un accès invité ou total sur un autre réseau. Un ordinateur qui dispose d'un accès invité ou total sur un réseau peut créer un nouveau réseau.

Rubriques connexes

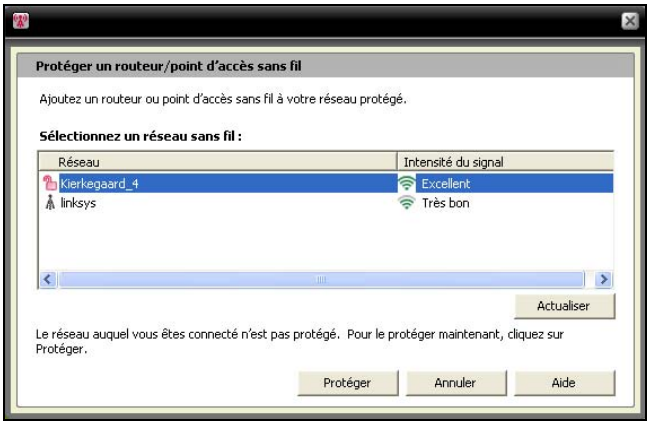
- Affiliation à un réseau sans fil protégé (page 78)
- Autorisation d'accès administratif à des ordinateurs (page 82)
- Révocation de l'accès au réseau (page 99)

Création des réseaux sans fil protégés

Pour créer un réseau sans fil protégé, vous devez d'abord ajouter le routeur sans fil ou le point d'accès du réseau sans fil.

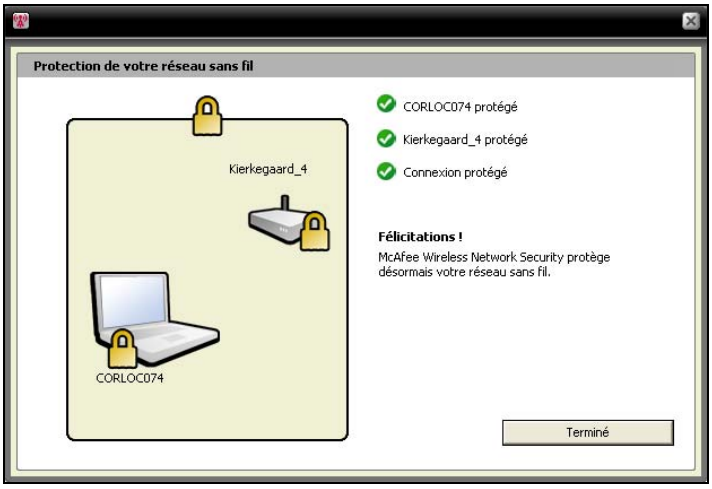
Pour ajouter un routeur ou un point d'accès sans fil :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les outils**.
3. Dans le volet Outils de protection, sous **Protéger un routeur/point d'accès sans fil**, cliquez sur **Protéger**.
4. Dans le volet Protéger un routeur/point d'accès sans fil, sélectionnez un réseau sans fil à protéger, puis cliquez sur **Protéger**.



Le volet Protection de votre réseau sans fil apparaît alors que Wireless Network Security tente de protéger votre ordinateur, routeur et connexion réseau.

La protection réussie de tous ces composants signifie que l'ensemble de votre réseau sans fil est protégé.



5 Cliquez sur **Terminé**.

Remarque : une fois que vous avez protégé un réseau, la boîte de dialogue Vos étapes suivantes vous rappelle d'installer Wireless Network Security sur chacun de vos ordinateurs sans fil pour leur permettre de se connecter au réseau.

Si vous avez configuré manuellement une clé pré-partagée auparavant pour votre routeur ou point d'accès et que vous n'étiez pas connecté lorsque vous avez tenté de protéger le routeur ou point d'accès, vous devez également saisir la clé dans la case Clé WEP, puis cliquer sur Se connecter. Si vous aviez modifié vos nom d'utilisateur et mot de passe administratifs de routeur sans fil auparavant, vous êtes invité à saisir ces informations avant de protéger un routeur ou point d'accès.

Rubriques connexes

- Protection d'autres périphériques sans fil (page 83)
- Ajout d'ordinateurs au réseau sans fil protégé (page 85)

Affiliation à des réseaux sans fil protégés

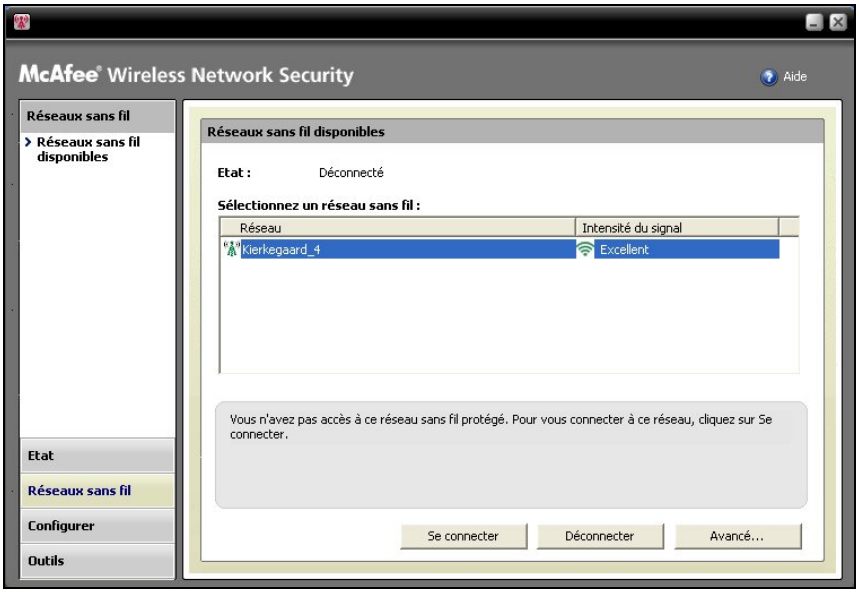
Un réseau protégé empêche les pirates d'intercepter les données qui sont transmises via le réseau et de se connecter à votre réseau. Pour qu'un ordinateur autorisé puisse accéder à un réseau sans fil protégé, il doit d'abord s'y affilier.

Lorsqu'un ordinateur demande à être affilié au réseau géré, un message est envoyé aux autres ordinateurs du réseau possédant des droits d'administration. C'est à l'administrateur de définir le type d'accès à accorder à l'ordinateur : invité, total ou administratif.

Pour pouvoir vous affilier à un réseau protégé, vous devez installer Wireless Network Security, puis vous connecter au réseau sans fil protégé. Un utilisateur du réseau existant possédant des droits d'administration sur le réseau sans fil protégé doit vous donner l'autorisation de vous affilier. Une fois que vous êtes affilié au réseau, il est inutile de vous affilier à nouveau pour vous reconnecter. L'administrateur de droits d'accès et l'affilié doivent avoir une connexion sans fil active. L'administrateur doit être un ordinateur possédant des droits d'administration et être connecté au réseau.

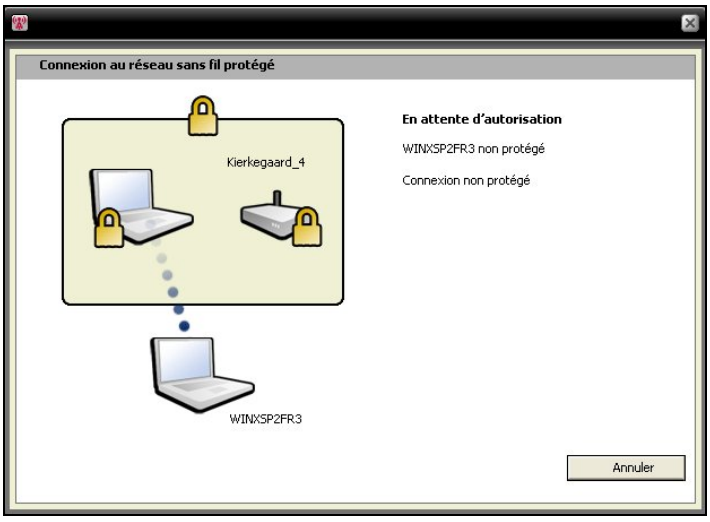
Pour être affilié à un réseau sans fil protégé :

1. Sur l'ordinateur non protégé, cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les réseaux sans fil**.
3. Dans le volet Réseaux sans fil disponibles, sélectionnez un réseau puis cliquez sur **Se connecter**.



4 Dans la boîte de dialogue Etre affilié à un réseau sans fil protégé, cliquez sur **Oui** pour être affilié au réseau.

Alors que Wireless Network Security tente de demander l'autorisation d'affiliation au réseau, le volet Affiliation à un réseau sans fil protégé s'affiche sur l'ordinateur qui tente de s'affilier au réseau.



5 Le volet Etre affilié au réseau s'affiche sur l'ordinateur administrateur à partir duquel un accès invité, total ou administratif peut être accordé.

Dans la boîte de dialogue Etre affilié au réseau, sélectionnez l'une des options suivantes :

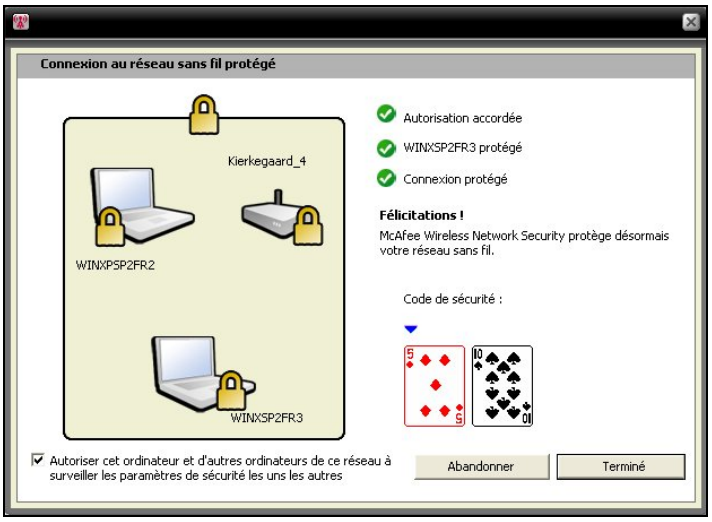
Autoriser l'accès à un invité	Permet à l'ordinateur d'envoyer des fichiers à d'autres ordinateurs sur le réseau sans fil, mais pas de partager des fichiers avec McAfee EasyNetwork.
Autoriser un accès complet à toutes les applications du réseau géré	Permet à l'ordinateur d'envoyer et de partager des fichiers avec McAfee EasyNetwork.
Autoriser un accès administratif à toutes les applications du réseau géré :	permet à l'ordinateur d'envoyer et de partager des fichiers avec McAfee EasyNetwork, d'autoriser l'accès à d'autres ordinateurs et de modifier les niveaux d'accès d'autres ordinateurs sur le réseau sans fil.

6 Cliquez sur **Autoriser l'accès**.

7 Confirmez que les cartes affichées sur le volet Autoriser l'accès au réseau correspondent à celles affichées sur l'ordinateur qui tente de se connecter au réseau sans fil. Si les cartes correspondent, cliquez sur **Autoriser l'accès**.

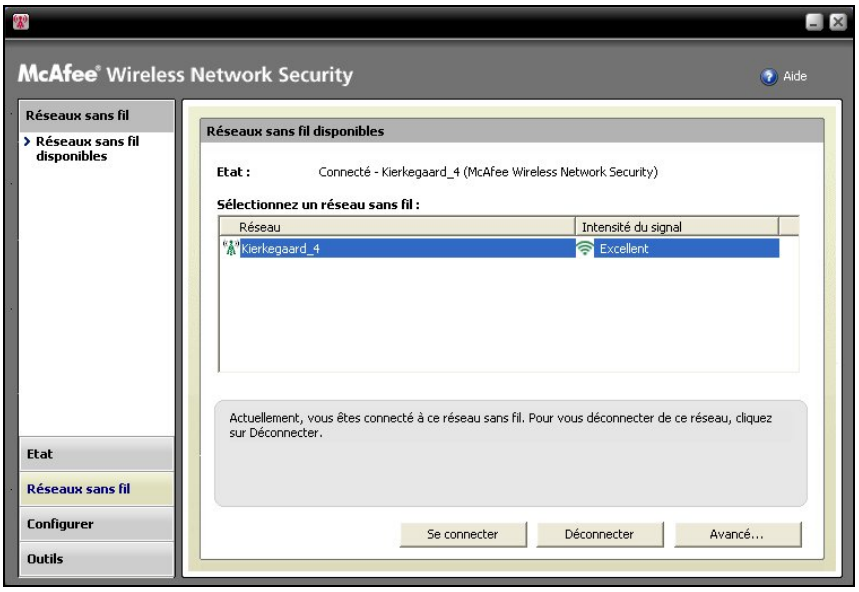
Si les ordinateurs affichent des cartes à jouer différentes, il est possible qu'il y ait une faille de sécurité. Autoriser l'accès au réseau à cet ordinateur risque d'en compromettre la sécurité. Pour interdire l'ordinateur d'accéder au réseau sans fil, cliquez sur **Refuser l'accès**.

8 Le volet Autoriser l'accès au réseau confirme que le nouvel ordinateur est protégé par Wireless Network Security. Pour surveiller les paramètres de sécurité d'autres ordinateurs et pour être surveillé par ceux-ci, sélectionnez l'option **Autoriser cet ordinateur et d'autres ordinateurs de ce réseau à surveiller les paramètres de sécurité les uns des autres.**



9 Cliquez sur **Terminé**.

10 Le volet Réseaux sans fil disponibles indique que vous êtes connecté au réseau sans fil protégé.



Rubriques connexes

- Ajout d'ordinateurs au réseau sans fil protégé (page 85)

Connexion à des réseaux sans fil protégés

Si vous êtes déjà affilié à un réseau sans fil protégé, mais que vous vous êtes déconnecté ensuite et que votre accès n'a pas été révoqué, vous pouvez vous reconnecter à tout moment sans avoir à vous réaffilier.

Pour se connecter à un réseau sans fil protégé :

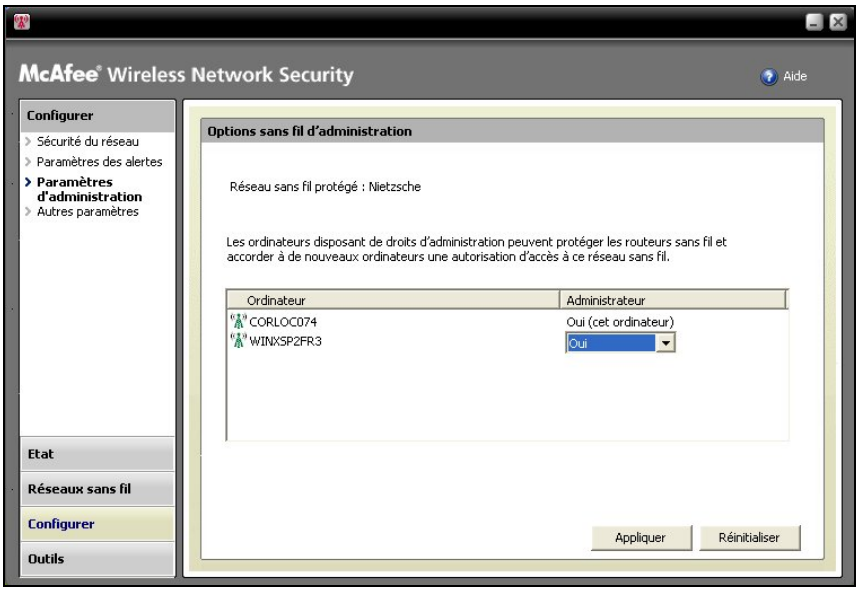
1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les réseaux sans fil**.
3. Dans le volet Réseaux sans fil disponibles, sélectionnez un réseau puis cliquez sur **Se connecter**.

Autorisation d'accès administratif à des ordinateurs

Les ordinateurs disposant de droits d'administration peuvent protéger les routeurs sans fil, modifier les modes de sécurité et accorder à de nouveaux ordinateurs une autorisation d'accès au réseau sans fil protégé.

Pour configurer un accès administratif :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher la configuration**.
3. Dans le volet Configurer, sélectionnez **Paramètres d'administration**.
4. Dans le volet Options d'administration sans fil, sélectionnez **Oui** ou **Non** pour autoriser ou interdire l'accès administratif.



5 Cliquez sur **Appliquer**.

Rubriques connexes

- A propos des types d'accès (page 75)
- Révocation de l'accès au réseau (page 99)

Protection d'autres périphériques sans fil

Wireless Network Security vous permet d'ajouter une ou plusieurs imprimantes, un ou plusieurs serveurs d'impression ou une ou plusieurs consoles de jeu sans fil au réseau.

Pour ajouter une imprimante, un serveur d'impression ou une console de jeu sans fil :

1 Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.

2 Sélectionnez **Afficher les outils**.

3 Dans le volet Outils de protection, sous **Protéger des périphériques autres qu'un point d'accès**, cliquez sur **Protéger**.

4 Dans le volet Protéger un périphérique sans fil, sélectionnez un périphérique sans fil, puis cliquez sur **Protéger**.

5 L'alerte Périphérique autre qu'un point d'accès protégé confirme que le périphérique a été ajouté au réseau.

Se connecter aux réseaux dont la Diffusion SSID est désactivée

Vous pouvez vous connecter à des réseaux sans fil dont la Diffusion SSID est désactivée. Lorsque la fonction Diffusion SSID des routeurs est désactivée, ceux-ci ne figurent pas dans le volet Réseaux sans fil disponibles.

McAfee vous recommande de ne pas protéger des routeurs sans fil dont la fonction Diffusion SSID est désactivée avec Wireless Network Security.

Pour vous connecter à un réseau sans fil dont la Diffusion SSID est désactivée :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les réseaux sans fil**.
3. Dans le volet Réseaux sans fil disponibles, cliquez sur **Avancé**.
4. Dans le volet Réseaux sans fil, cliquez sur **Ajouter**.
5. Dans le volet Ajouter un réseau sans fil, précisez les paramètres suivants, puis cliquez sur **OK** :

Paramètre	Description
Réseau	Le nom de votre réseau. Si vous modifiez un réseau, vous ne pouvez pas modifier le nom.
Paramètres de sécurité	La sécurité de votre réseau non protégé. Notez que si l'adaptateur sans fil ne prend pas en charge le mode que vous sélectionnez, vous ne pouvez pas vous connecter. Les modes de sécurité comprennent les modes suivants : désactivé, WEP ouverte, WEP partagée, WEP auto., WPA-PSK, WPA2-PSK.
Mode de chiffrement	Le chiffrement associé au mode de sécurité que vous avez sélectionné. Les modes de chiffrement comprennent : WEP, TKIP, AES et TKIP+AES.

Remarque : McAfee vous recommande de ne pas protéger des routeurs sans fil dont la fonction Diffusion SSID est désactivée avec Wireless Network Security. Si vous devez utiliser cette fonction, faites-le uniquement lorsque la fonction Diffusion SSID est désactivée.

Ajout d'ordinateurs au réseau sans fil protégé

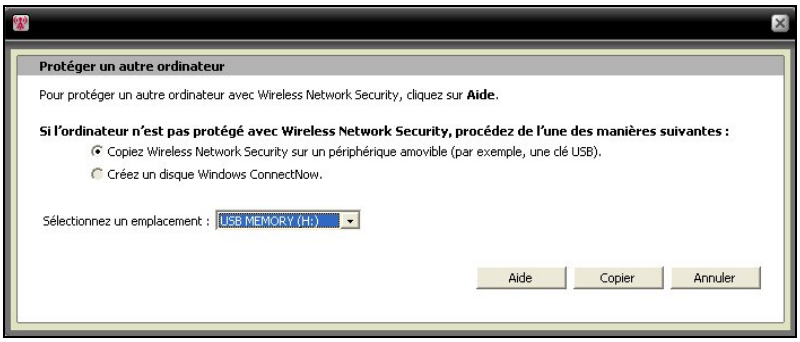
Vous pouvez ajouter des ordinateurs au réseau sans fil protégé grâce à un périphérique amovible, comme par exemple une clé USB Flash Drive, un CD enregistrable ou la technologie Windows Connect Now.

Ajout d'ordinateurs à l'aide d'un périphérique amovible

Wireless Network Security vous permet d'ajouter d'autres ordinateurs au réseau sans fil protégé qui n'exécutent pas Wireless Network Security, à l'aide d'une clé USB Flash Drive ou d'un CD enregistrable.

Pour ajouter un ordinateur :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les outils**.
3. Dans le volet Outils de protection, sous **Protéger un ordinateur**, cliquez sur **Protéger**.
4. Dans le volet Protéger un autre ordinateur, sélectionnez **Copier Wireless Network Security sur un périphérique amovible, comme une clé USB**.



5 Sélectionnez un emplacement du lecteur CD ou de la clé USB sur lequel copier Wireless Network Security.

6 Cliquez sur **Copier**.

7 Une fois que tous les fichiers sont copiés sur le CD ou la clé USB, insérez le périphérique amovible dans l'ordinateur que vous voulez protéger. Si le programme ne se lance pas automatiquement, parcourez le contenu du support amovible dans Windows Explorer, puis cliquez sur **Install.exe**.

8 Suivez les instructions affichées à l'écran.

Remarque : vous pouvez également ajouter un ordinateur au réseau sans fil protégé à l'aide de la technologie Windows Connect Now.

Rubriques connexes

- Ajout d'ordinateurs à l'aide de la technologie Windows Connect Now (page 87)

Ajout d'ordinateurs à l'aide de la technologie Windows Connect Now

Wireless Network Security vous permet d'ajouter à votre réseau d'autres ordinateurs qui n'exécutent pas Wireless Network Security, grâce à la technologie Windows Connect Now.

Pour ajouter un ordinateur à l'aide de la technologie Windows Connect Now :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les outils**.
3. Dans le volet Outils de protection, sous **Protéger un ordinateur**, cliquez sur **Protéger**.
4. Dans le volet Protéger un autre ordinateur, sélectionnez **Créer un disque Windows Connect Now**
5. Sélectionnez un emplacement où copier les informations Windows Connect Now.
6. Cliquez sur **Copier**.
7. Insérez le disque Windows Connect Now dans l'ordinateur que vous voulez protéger.
8. Si le disque ne démarre pas automatiquement, procédez à l'une des actions suivantes :
   - Installez la technologie Wireless Connect Now : Cliquez sur **Démarrer** dans la barre des tâches Windows, puis cliquez sur le Panneau de configuration. Si vous utilisez la vue Catégorie du Panneau de configuration, cliquez sur **Connexions réseau et Internet**, puis cliquez sur **Assistant de configuration de réseau sans fil**. Si vous utilisez la vue Classique du Panneau de configuration, cliquez sur **Assistant de configuration de réseau sans fil**. Suivez les instructions affichées à l'écran.
   - Ouvrez `setupSNK.exe` sur le disque Windows Connect, puis copiez et collez la clé dans votre client de sélection de réseau sans fil.

Remarque : interrompez la rotation de la clé si vous utilisez la technologie Windows Connect pour vous connecter au réseau sans fil, sinon votre connexion réseau échouera. La connexion échoue car la rotation des clés crée une nouvelle clé qui diffère de celle utilisée par la technologie Windows Connect Now.

Vous pouvez également ajouter des ordinateurs au réseau sans fil protégé grâce à un périphérique amovible, comme par exemple un CD enregistrable ou une clé USB Flash Drive.

Rubriques connexes

- Ajout d'ordinateurs à l'aide d'un périphérique amovible (page 85)

CHAPITRE 15

Administration de réseaux sans fil

Wireless Network Security fournit un ensemble complet d'outils d'administration conçus pour vous aider à gérer et à mettre à jour votre réseau sans fil.

Contenu de ce chapitre

Gestion de réseaux sans fil

Lorsque vous êtes connecté à un réseau sans fil protégé, les informations qui sont envoyées et reçues sont chiffrées. Les pirates ne peuvent pas déchiffrer les donnéees transmises via le réseau protégé et ne peuvent pas se connecter à votre réseau. Wireless Network Security fournit un certain nombre d'outils conçus pour vous aider à gérer votre réseau pour empêcher toute intrusion.

A propos des icônes Wireless Network Security

Wireless Network Security affiche des icônes qui représentent différents types de connexion réseau et différentes intensités de signal.

Icônes de connexion réseau

Le tableau suivant décrit les icônes couramment utilisées par Wireless Network Security dans les volets Etats du réseau sans fil et les volets Outils de protection et Réseaux sans fil disponibles.

Les icônes représentent différents états de sécurité et de connexion réseau.

Icône	Volets Etats	Volets Protection
	Votre ordinateur est connecté au réseau sans fil protégé sélectionné.	Le périphérique est protégé par Wireless Network Security.
	Votre ordinateur peut accéder au réseau sans fil protégé, mais n'est actuellement pas connecté.	Le périphérique utilise une sécurité WEP ou WPA.
	Votre ordinateur est un ancien membre du réseau sans fil protégé, mais l'accès a été révoqué lorsque l'ordinateur s'est déconnecté du réseau.	Wireless Network Security est désactivé sur le périphérique.

Icônes d'intensité du signal

Le tableau suivant décrit les icônes couramment utilisées par Wireless Network Security pour représenter différentes intensités de signal du réseau.

Icône	Description
	Intensité du signal excellente
	Intensité du signal très bonne
	Intensité du signal bonne
	Intensité du signal faible

Rubriques connexes

- Affichage de l'intensité du signal du réseau (page 121)
- Affichage des ordinateurs actuellement protégés (page 128)
- Affichage du mode de sécurité du réseau (page 120)

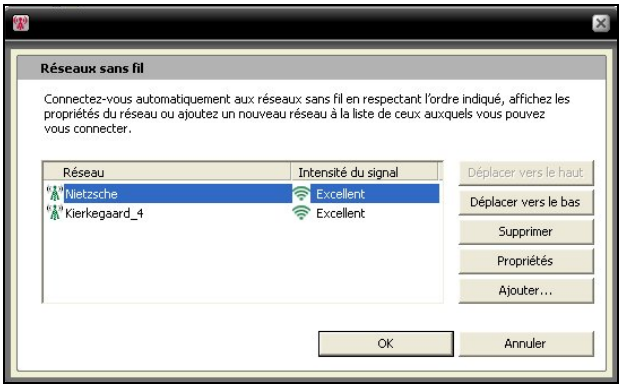
Etablissement de la liste des réseaux préférés

Wireless Network Security vous permet de préciser les réseaux sans fil préférés. Ceci vous permet de préciser l'ordre des réseaux auxquels votre ordinateur se connecte automatiquement. Wireless Network Security tente de se connecter au premier réseau qui apparaît sur la liste.

Cette fonction est utile lorsque, par exemple, vous voulez vous connecter automatiquement au réseau sans fil de votre ami lorsque vous vous trouvez dans sa région. Vous pouvez donner la préférence à un autre réseau de la liste.

Pour dresser la liste des réseaux préférés :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les réseaux sans fil**.
3. Dans le volet Réseaux sans fil disponibles, cliquez sur **Avancé**.
4. Sélectionnez le réseau dont vous voulez modifier l'ordre, puis cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas**.



5. Cliquez sur **OK**.

Rubriques connexes

- Suppression des réseaux sans fil préférés (page 93)

Suppression des réseaux sans fil préférés

Vous pouvez utiliser Wireless Network Security pour supprimer des réseaux préférés.

Ceci est utile lorsque, par exemple, vous souhaitez supprimer un réseau obsolète de la liste.

Pour supprimer des réseaux préférés :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les réseaux sans fil**.
3. Dans le volet Réseaux sans fil disponibles, cliquez sur **Avancé**.
4. Dans le volet Réseaux sans fil, sélectionnez un réseau puis cliquez sur **Supprimer**.
5. Cliquez sur **OK**.

Rubriques connexes

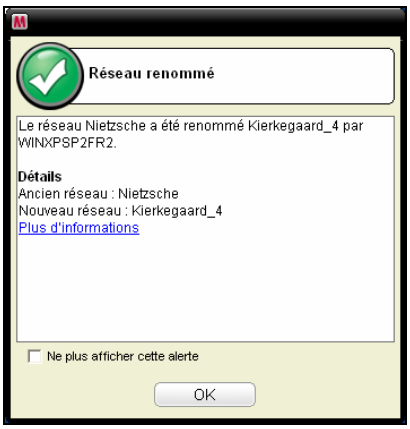
- Etablissement de la liste des réseaux préférés (page 92)

Modification du nom des réseaux sans fil protégés

Vous pouvez utiliser Wireless Network Security pour renommer votre réseau sans fil protégé existant.

Renommer le réseau peut être utile si son nom est similaire ou identique à celui utilisé par votre voisin ou si vous voulez créer un nom unique de façon à ce qu'il soit plus facile pour vous de faire la distinction.

Les ordinateurs connectés au réseau sans fil protégé peuvent être nécessaires pour se reconnecter manuellement et reçoivent une notification en cas de changement de nom.



Une fois que le réseau a été renommé, le nouveau nom apparaît sur le volet Routeur/point d'accès sans fil protégé.

Pour modifier le nom de votre réseau sans fil protégé :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher la configuration**.
3. Dans le volet Sécurité réseau, saisissez le nouveau nom dans la case **Nom du réseau sans fil protégé**.
4. Cliquez sur **Appliquer**.

   La boîte de dialogue Mise à jour des paramètres de sécurité réseau s'affiche lorsque Wireless Network Security change le nom de votre réseau sans fil protégé. Selon les paramètres de votre ordinateur et l'intensité du signal, le nom du réseau est modifié en moins d'une minute.

Remarque : pour des raisons de sécurité, McAfee vous recommande de renommer le SSID par défaut du routeur ou du point d'accès. Bien que Wireless Network Security prenne en charge les SSID par défaut comme "linksys", "belkin54g" ou "NETGEAR", le fait de renommer les SSID vous protège contre les menaces de point d'accès rouges.

Configuration des paramètres d'alerte

Wireless Network Security vous permet de configurer les paramètres d'alerte pour afficher des alertes lors de certains événements, comme par exemple lorsqu'un nouvel ordinateur se connecte à votre réseau.

Pour configurer le comportement d'une alerte :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher la configuration**.
3. Cliquez sur **Paramètres d'alerte**.
4. Sélectionnez ou décochez un ou plusieurs des événements suivants, puis cliquez sur **Appliquer** :

Paramètre d'alerte	Description
La clé de sécurité de votre réseau sans fil protégé fait l'objet d'une rotation.	Elle affiche l'alerte Rotation de la clé de sécurité après une rotation manuelle ou automatique de la clé de sécurité. La rotation de la clé protège votre réseau des pirates qui tentent d'intercepter vos données ou de se connecter à votre réseau.
Un autre ordinateur protégé se connecte ou se déconnecte du réseau.	Affiche l'alerte Ordinateur connecté ou Ordinateur déconnecté après la connexion ou la déconnexion d'un ordinateur du réseau sans fil protégé. Les données des ordinateurs connectés sont désormais protégées contre toute intrusion et interception de données.
Un autre ordinateur reçoit une autorisation d'accès à votre réseau sans fil protégé.	Affiche l'alerte Accès au réseau autorisé à l'ordinateur lorsqu'un ordinateur administrateur permet à un autre ordinateur de se connecter au réseau sans fil protégé. Le fait d'autoriser un ordinateur à accéder au réseau protégé le protège contre les pirates qui tentent d'intercepter vos données.
La rotation de la clé de votre réseau sans fil protégé vient d'être suspendue ou de reprendre.	Affiche l'alerte Rotation de la clé suspendue ou Rotation de la clé reprise après une suspension ou une reprise manuelle de la rotation de la clé. La rotation de la clé protège votre réseau des pirates qui tentent d'intercepter vos données ou de se connecter à votre réseau.
L'autorisation d'accès à tous les ordinateurs déconnectés est révoquée.	Affiche l'alerte Accès révoqué lorsque l'accès des ordinateurs non connectés au réseau est révoqué. Ces ordinateurs doivent se reconnecter au réseau.
Un routeur est ajouté ou supprimé dans votre réseau sans fil protégé.	Affiche l'alerte Routeur/point d'accès ajouté au réseau ou Routeur/point d'accès non protégé lorsque le routeur ou point d'accès sans fil est ajouté à ou supprimé du réseau sans fil protégé.
Les informations de connexion d'un routeur sans fil protégé changent.	Affiche l'alerte Informations de connexion du routeur/point d'accès modifiées lorsque l'administrateur Wireless Network Security modifie le nom d'utilisateur ou le mot de passe d'un routeur ou d'un point d'accès.
Le nom ou un paramètre de sécurité de votre réseau sans fil protégé change.	Affiche l'alerte Paramètres réseau modifiés ou Réseau renommé lorsque vous renommez le réseau sans fil protégé ou que vous modifiez son paramètre de sécurité.

Les paramètres de votre réseau sans fil protégé sont corrigés.	Affiche l'alerte Réseau réparé lorsque les paramètres de sécurité des routeurs ou points d'accès sans fil de votre réseau sont corrigés.

Remarque : pour sélectionner ou effacer tous les paramètres d'alerte, cliquez sur **Sélectionner tout** ou **Effacer tout**. Pour réinitialiser les paramètres d'alerte de Wireless Network Security, cliquez sur **Restaurer les paramètres par défaut**.

Rubriques connexes

- Rotation automatique des clés (page 108)
- Affiliation à un réseau sans fil protégé (page 78)
- Connexion à des réseaux sans fil protégés (page 82)
- Déconnexion de réseaux sans fil protégés (page 98)
- Suspension de la rotation automatique de la clé (page 111)
- Révocation de l'accès au réseau (page 99)
- Suppression de routeurs ou points d'accès sans fil (page 97)
- Modification des informations d'authentification des périphériques sans fil (page 105)
- Modification du nom des réseaux sans fil protégés (page 93)
- Correction des paramètres de sécurité réseau (page 106)

Affichage des notifications de connexion

Vous pouvez configurer Wireless Network Security de façon à recevoir une notification lorsque votre ordinateur se connecte à un réseau sans fil.

Pour afficher une notification lorsque vous vous connectez à un réseau sans fil :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher la configuration**.
3. Cliquez sur **Autres paramètres**.
4. Sélectionnez **Afficher un message de notification lors de la connexion à un réseau sans fil**.
5. Cliquez sur **Appliquer**.

Rubriques connexes

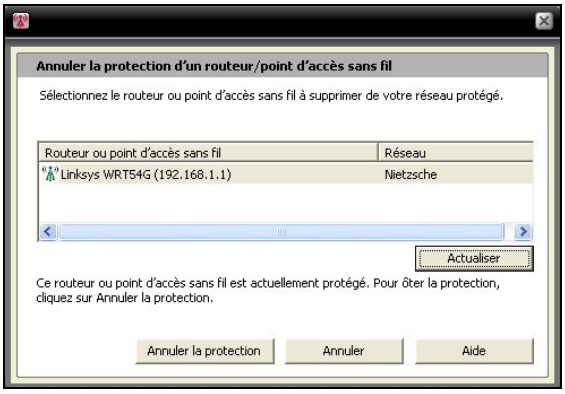
- Connexion à des réseaux sans fil protégés (page 82)

Suppression des routeurs ou points d'accès sans fil

Wireless Network Security vous permet de supprimer un ou plusieurs routeurs ou points d'accès de votre réseau protégé.

Pour supprimer un routeur ou un point d'accès sans fil :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les outils**.
3. Dans le volet Outils de protection, sous **Annuler la protection d'un périphérique**, cliquez sur **Annuler la protection**.
4. Dans le volet Annuler la protection d'un routeur/point d'accès sans fil, sélectionnez un routeur ou un point d'accès sans fil à supprimer du réseau protégé, puis cliquez sur **Annuler la protection**.



5. Cliquez sur **OK** dans la boîte de dialogue Routeur/point d'accès sans fil non protégé pour confirmer la suppression du réseau du routeur ou point d'accès sans fil.

Rubriques connexes

- Création de réseaux sans fil protégés (page 76)

Déconnexion de réseaux sans fil protégés

Wireless Network Security vous permet de déconnecter votre ordinateur du réseau.

Cette tâche est utile lorsque, par exemple, votre ordinateur s'est connecté à un réseau à l'aide d'un nom identique à celui de votre réseau. Vous pouvez vous déconnecter du réseau, puis vous reconnecter au vôtre.

Cette fonction est également utile lorsque vous vous connectez accidentellement au mauvais réseau en raison de l'intensité du signal d'un autre point d'accès ou suite à une interférence radio.

Pour se déconnecter d'un réseau sans fil protégé :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les réseaux sans fil**.
3. Dans le volet Réseaux sans fil disponibles, sélectionnez le réseau puis cliquez sur **Se déconnecter**.

Rubriques connexes

- Révocation de l'accès au réseau (page 99)
- Déconnexion des réseaux sans fil protégés (page 100)

Révocation de l'accès au réseau

Wireless Network Security vous permet de révoquer l'accès aux ordinateurs qui ne sont pas connectés au réseau. Un nouveau programme de rotation de clé de sécurité est établi : les ordinateurs non connectés perdront l'accès au réseau sans fil protégé, mais peuvent l'obtenir à nouveau en se reconnectant au réseau. L'accès des ordinateurs connectés est préservé.

Par exemple, vous pouvez révoquer l'accès d'un ordinateur visiteur avec Wireless Network Security une fois qu'il est déconnecté. De plus, un adulte peut révoquer l'accès d'un ordinateur utilisé par un enfant sous forme de contrôle parental de l'accès Internet. L'accès d'un ordinateur qui a été accidentellement autorisé peut également être révoqué.

Pour révoquer l'accès de tous les ordinateurs déconnectés du réseau protégé :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les outils**.
3. Dans le volet Outils, cliquez sur Outils de maintenance.
4. Dans le volet Outils de maintenance, sous **Révoquer l'accès**, cliquez sur **Révoquer**.
5. Dans le volet Révoquer l'accès, cliquez sur **Révoquer**.
6. Cliquez sur **OK** dans la boîte de dialogue Wireless Network Security.

Rubriques connexes

- Déconnexion de réseaux sans fil protégés (page 98)
- Déconnexion des réseaux sans fil protégés (page 100)

Déconnexion des réseaux sans fil protégés

Vous pouvez utiliser Wireless Network Security pour annuler vos droits d'accès à un réseau protégé.

Pour quitter un réseau :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher la configuration**.
3. Dans le volet Configurer, sélectionnez **Autres paramètres**.
4. Dans le volet Autres paramètres, sous Accès à un réseau protégé, sélectionnez le réseau que vous voulez quitter, puis cliquez sur **Quitter le réseau**.
5. Dans le volet Se déconnecter du réseau, cliquez sur **Oui** pour quitter le réseau.

Remarque : lorsque vous quittez un réseau, un autre utilisateur peut vous autoriser l'accès au réseau protégé avant de s'y connecter.

Rubriques connexes

- Déconnexion de réseaux sans fil protégés (page 98)
- Révocation de l'accès au réseau (page 99)

CHAPITRE 16

Gestion de la sécurité du réseau sans fil

Wireless Network Security fournit un ensemble complet d'outils conçus pour vous aider à gérer les fonctions de sécurité de votre réseau sans fil.

Contenu de ce chapitre

Configuration des paramètres de sécurité

Une fois que vous êtes connecté à un réseau sans fil protégé, Wireless Network Security protège automatiquement votre réseau ; cependant, vous pouvez configurer d'autres paramètres de sécurité à tout moment.

Configuration des modes de sécurité

Vous pouvez préciser le mode de sécurité de votre réseau sans fil protégé. Les modes de sécurité définissent le chiffrement entre votre ordinateur et le routeur ou point d'accès.

Lorsque vous protégez votre réseau, la sécurité WEP est automatiquement configurée. Cependant, McAfee vous recommande de modifier le mode de sécurité et de passer à la sécurité WPA2 ou WPA-PSK AES. Wireless Network Security utilise la sécurité WEP d'abord parce que ce mode est pris en charge par tous les routeurs et les adaptateurs de réseau sans fil. La plupart des nouveaux routeurs et adaptateurs de réseau sans fil, cependant, fonctionnent au mode WPA, qui est plus sécurisé.

Pour modifier le mode de sécurité d'un réseau sans fil protégé :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher la configuration**.
3. Dans le volet Sécurité réseau, sélectionnez le type de sécurité que vous voulez mettre en oeuvre dans la case **Mode de sécurité**, puis cliquez sur **Appliquer**.

Le tableau suivant décrit les modes de sécurité disponibles :

Intensité	Mode	Description
La plus faible	WEP	La sécurité WEP (Wired Equivalent Privacy) fait partie de la norme de mise en réseau sans fil IEEE 802.11 pour sécuriser les réseaux sans fil IEEE 802.11. La sécurité WEP fournit un niveau de sécurité qui peut empêcher l'espionnage simple, mais n'est généralement pas aussi sûre que le chiffrement WPA-PSK. Bien que Wireless Network Security fournisse une clé complexe (difficile à deviner et longue), McAfee vous recommande d'utiliser un mode de sécurité WPA.
Moyenne	WPA-PSK TKIP	La sécurité WPA (Wi-Fi Protected Access) est une version anticipée de la norme de sécurité 802.11i. La sécurité TKIP est conçue pour le WPA afin d'améliorer le WEP. La sécurité TKIP permet l'intégrité des messages, un mécanisme de redéfinition de clé et un mélange de clé par paquet
Complexe	WPA-PSK AES	Ce mode de sécurité combine les modes WPA et AES. La sécurité AES (Advanced Encryption Standard) est un chiffrement par blocs adopté comme norme de chiffrement par le gouvernement des Etats-Unis.
Plus complexe	WPA2-PSK AES	Ce mode de sécurité combine les modes WPA2 et AES. WPA2 est le stade suivant de la ratification de la norme de sécurité 802.11i. La sécurité WPA2 utilise le protocole Counter Mode CBC MAC (CCMP), une solution plus sécurisée et évolutive par rapport à TKIP. Il s'agit du mode de sécurité le plus complexe pour les clients.
La plus complexe	WPA2-PSK TKIP+AES	Ce mode de sécurité combine les modes WPA2, AES et WPA-PSK TKIP. Il permet une plus grande flexibilité de façon à ce que les adaptateurs sans fil anciens et nouveaux puissent se connecter.

Remarque : une fois que le mode de sécurité est modifié, vous devrez peut-être vous reconnecter manuellement.

Rubriques connexes

- Correction des paramètres de sécurité réseau (page 106)
- Affichage du mode de sécurité du réseau (page 120)

Configuration des paramètres de sécurité réseau

Vous pouvez modifier les propriétés réseau des réseaux protégés par Wireless Network Security. Ceci est utile lorsque, par exemple, vous voulez mettre à niveau la sécurité et passer de la sécurité WEP à WPA.

McAfee vous recommande de modifier les paramètres de sécurité réseau si une alerte vous suggère de le faire.

Pour configurer les propriétés d'un réseau non protégé :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les réseaux sans fil**.
3. Dans le volet Réseaux sans fil disponibles, cliquez sur **Avancé**.
4. Dans le volet Réseaux sans fil, cliquez sur **Propriétés**.
5. Dans le volet Propriétés du réseau sans fil, vous modifiez les paramètres suivants, puis cliquez sur **OK** :

Paramètre	Description
Réseau	Le nom de votre réseau. Si vous modifiez un réseau, vous ne pouvez pas en modifier le nom.
Paramètres de sécurité	La sécurité de votre réseau non protégé. Notez que si l'adaptateur sans fil ne prend pas en charge le mode que vous sélectionnez, vous ne pouvez pas vous connecter. Les modes de sécurité comprennent les modes suivants : désactivé, WEP ouverte, WEP partagée, WEP auto., WPA-PSK, WPA2-PSK.
Mode de chiffrement	Le chiffrement associé au mode de sécurité que vous avez sélectionné. Les modes de chiffrement comprennent les modes suivants : WEP, TKIP, AES et TKIP+AES.

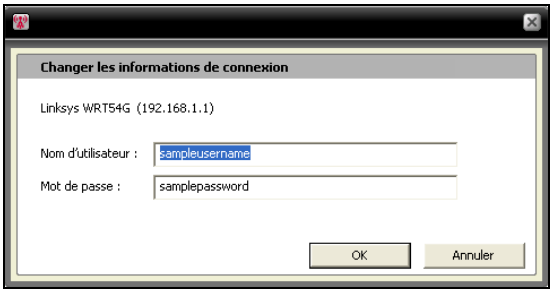
Modification des informations d'authentification des périphériques sans fil

Vous pouvez modifier le nom d'utilisateur ou le mot de passe d'un périphérique sur votre routeur ou point d'accès sans fil protégé. La liste des périphériques s'affiche sous **Périphériques du réseau sans fil protégé**.

McAfee vous recommande de modifier vos informations d'authentification car la majorité des périphériques sans fil fabriqués par un seul fabricant ont les mêmes informations d'authentification de connexion. Le fait de modifier les informations d'authentification de connexion empêche les autres d'accéder à votre routeur ou point d'accès sans fil, et de modifier ses paramètres.

Pour modifier le nom d'utilisateur ou le mot de passe d'un périphérique du réseau sans fil protégé :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher la configuration**.
3. Dans le volet Sécurité réseau, sous **Périphériques du réseau sans fil protégé**, sélectionnez un routeur ou point d'accès sans fil, puis cliquez sur **Modifier le nom d'utilisateur ou le mot de passe**.



4. Cliquez sur **OK** dans la boîte de dialogue Sécurité du réseau sans fil après avoir saisi vos informations de connexion.

   Les nouveaux nom d'utilisateur et mot de passe s'affichent sous **Périphériques du réseau sans fil protégé**.

Remarque : certains routeurs ne prennent pas en charge les noms d'utilisateur et, par conséquent, aucun nom d'utilisateur ne s'affichera sous **Périphériques du réseau sans fil protégé**.

Correction des paramètres de sécurité réseau

Si vous rencontrez des problèmes de paramètres ou de configuration de la sécurité, vous pouvez utiliser Wireless Network Security pour corriger les paramètres de votre routeur ou point d'accès.

Pour corriger vos paramètres de sécurité :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les outils**.
3. Dans le volet Outils, cliquez sur **Outils de maintenance**.
4. Sous **Corriger les paramètres de sécurité réseau**, cliquez sur **Corriger**.
5. Dans le volet Corriger les paramètres de sécurité réseau, cliquez sur **Corriger**.

   Une alerte Wireless Network Security indique si le réseau a ou n'a pas été réparé.

Remarque : si la tentative de réparation de votre réseau échoue, connectez-vous au réseau à l'aide d'un câble, puis réessayez. Si le mot de passe du routeur ou du point d'accès a changé, vous devez resaisir votre mot de passe pour vous connecter.

Administration des clés réseau

Wireless Network Security génère des clés de chiffrement longues, complexes et aléatoires grâce à un générateur de clés aléatoires. Avec la sécurité WEP, la clé est traduite en une valeur hexadécimale à 26 chiffres (pour 104 bits d'entropie, ou de complexité, la complexité maximale prise en charge par le WEP 128 bits), alors qu'avec la sécurité WPA, la clé est une chaîne ASCII de 63 caractères. Chaque caractère a 64 valeurs possibles (6 bits), d'une valeur de 384 bits d'entropie, ce qui dépasse la complexité de la clé WAP de 256 bits.

Lorsque vous gérez des clés réseau, vous pouvez afficher les clés en clair ou sous forme d'astérisques pour les points d'accès non protégés, éliminer des clés enregistrées pour les points d'accès non protégés, activer ou désactiver la rotation de la clé, modifier la fréquence de rotation de la clé, effectuer une rotation manuelle de la clé et suspendre la rotation de la clé.

Lorsque les clés effectuent une rotation automatique, les outils des pirates ne peuvent pas capturer vos informations car la clé change continuellement.

Cependant, si vous connectez des périphériques sans fil que Wireless Network Security ne prend pas en charge (par exemple, connecter un ordinateur portable sans fil à votre réseau), vous devez inscrire la clé, arrêter la rotation de la clé, puis la saisir sur le périphérique.

Affichage des clés actuelles

Wireless Network Security donne un accès rapide aux informations de sécurité sans fil, y compris la clé actuelle d'un réseau sans fil protégé.

Pour afficher la clé actuelle :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.
3. Dans le volet Etat du réseau sans fil, sous le volet Réseau sans fil protégé, cliquez sur **Clé actuelle**.

   La clé configurée pour votre réseau s'affiche dans la boîte de dialogue Configuration de la clé.

Rubriques connexes

- Affichage du nombre de rotations de clés (page 124)

Rotation automatique des clés

La rotation automatique de la clé est activée par défaut. Cependant, si vous suspendez la rotation de la clé, un ordinateur disposant d'un accès administratif peut la réactiver ultérieurement.

Vous pouvez configurer Wireless Network Security de façon à ce que la rotation de la clé de sécurité du réseau sans fil protégé soit automatique.

Wireless Network Security génère automatiquement une série infinie de clés complexes, synchronisée dans tout le réseau. La connexion sans fil peut être brièvement interrompue lorsque le routeur sans fil est réinitialisé avec la nouvelle configuration de la clé de sécurité, mais ceci n'est en général pas détecté par les utilisateurs du réseau.

Si aucun ordinateur n'est connecté au réseau, la rotation de la clé se produit après la première connexion.

Pour activer la rotation automatique de la clé :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher la configuration**.
3. Dans le volet Sécurité du réseau, cochez la case **Activer la rotation automatique de la clé.**

   Vous pouvez également reprendre la rotation de la clé à partir du volet Etat du réseau sans fil.
4. Cliquez sur **Appliquer**.

Remarque : la rotation de la clé s'effectue automatiquement toutes les trois heures par défaut, mais vous pouvez modifier la fréquence de la rotation de la clé de façon à satisfaire vos exigences de sécurité.

Rubriques connexes

- Modification de la fréquence de rotation de la clé (page 109)
- Reprise de la rotation de la clé (page 109)
- Affichage du nombre de rotations de la clé (page 124)

Reprise de la rotation de la clé

Bien que la rotation automatique des clés soit activée par défaut, un ordinateur disposant d'un accès administratif peut reprendre la rotation après l'avoir suspendue.

Pour reprendre la rotation des clés :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.
3. Dans le volet Etat du réseau sans fil, cliquez sur **Reprendre la rotation des clés**.

   Les alertes Rotation des clés démarrée et Rotation de la clé de sécurité effectuée confirment que la rotation des clés est démarrée et réussie.

Rubriques connexes

- Rotation automatique des clés (page 108)
- Suspension de la rotation automatique des clés (page 111)
- Affichage du nombre de rotations des clés (page 124)

Modification de la fréquence de rotation de la clé

Si Wireless Network Security est configuré de façon à effectuer une rotation automatique de la clé de sécurité du réseau sans fil protégé, vous pouvez modifier l'intervalle auquel la rotation des clés a lieu, entre toutes les quinze minutes et tous les quinze jours.

McAfee recommande que la rotation de la clé de sécurité soit effectuée tous les jours.

Pour modifier la fréquence de la rotation automatique des clés :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher la configuration**.
3. Dans le volet Sécurité du réseau, confirmez que la rotation automatique des clés est activée, puis faites glisser le curseur **Fréquence** sur l'un des paramètres suivants :
   - **toutes les 15 minutes**
   - **toutes les 30 minutes**
   - **toutes les heures**
   - **toutes les 3 heures**
   - **toutes les 12 heures**

- **tous les jours**
- **toutes les semaines**
- **tous les 15 jour**s

4 Cliquez sur **Appliquer**.

Remarque : assurez-vous que la rotation automatique des clés est activée avant de régler la fréquence de rotation des clés.

Rubriques connexes

- Activation de la rotation automatique des clés (page 108)
- Affichage du nombre de rotations des clés (page 124)

Suspension de la rotation automatique des clés

La rotation des clés peut être suspendue par tout ordinateur connecté au réseau sans fil. Vous voudrez peut-être suspendre la rotation des clés pour effectuer l'une des tâches suivantes :

- Permettre à un invité qui n'a pas installé Wireless Network Security d'accéder au réseau
- Permettre à un système autre que Windows, comme par exemple Macintosh, Linux ou TiVo d'obtenir un accès. Une fois que vous arrêtez la rotation des clés, notez la clé, puis saisissez-la sur le nouveau périphérique.
- Permettre une connexion sans fil qui est ininterrompue par des rotations de clés pour certains programmes, comme par exemple les jeux en ligne.
- Vous devez reprendre la rotation automatique des clés dès que possible pour que votre réseau soit complètement protégé des pirates.

Pour afficher la clé actuelle :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.
3. Dans le volet Etat du réseau sans fil, sous le volet Réseau sans fil protégé, cliquez sur **Clé actuelle**. Notez la clé qui s'affiche dans la boîte de dialogue Configuration de la clé. D'autres ordinateurs ne disposant pas de Wireless Network Security peuvent utiliser cette clé pour se connecter au réseau sans fil protégé.
4. Dans la boîte de dialogue Configuration de la clé, cliquez sur **Suspendre la rotation des clés**.
5. Dans la boîte de dialogue Rotation des clés suspendue, cliquez sur **OK** pour continuer à travailler.

Avertissement : si la rotation des clés n'est pas suspendue, des périphériques sans fil non pris en charge qui sont manuellement connectés au réseau se déconnectent lors de la rotation des clés.

Vous pouvez créer un disque Windows Connect Now, puis utiliser le fichier texte pour copier et coller la clé sur l'autre ordinateur et périphérique.

Rubriques connexes

- Activation de la rotation automatique des clés (page 108)
- Ajout d'ordinateurs à l'aide de la technologie Windows Connect Now (page 87)
- Reprise de la rotation des clés (page 109)

- Rotation automatique des clés (page 108)
- Affichage du nombre de rotations des clés (page 124)

Rotation manuelle des clés réseau

Wireless Network Security vous permet d'effectuer une rotation manuelle d'une clé réseau, même lorsque la rotation automatique des clés est activée.

Pour effectuer une rotation manuelle de la clé réseau :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher les outils**.
3. Dans le volet Outils, cliquez sur **Outils de maintenance**.
4. Sur la page Outils de maintenance, sous **Rotation manuelle de la clé de sécurité**, cliquez sur **Rotation**.

   L'alerte Rotation des clés démarrée s'affiche et confirme que la rotation des clés a commencé. Une fois que la rotation de la clé de sécurité est effectuée, l'alerte Rotation de la clé de sécurité effectuée s'affiche pour confirmer que la rotation des clés est réussie.

Remarque : pour faciliter la gestion de vos clés de sécurité, vous pouvez activer automatiquement la rotation des clés dans le volet Sécurité réseau.

Si aucun ordinateur n'est connecté à votre réseau sans fil, la rotation des clés se produit automatiquement après la première connexion.

Rubriques connexes

- Activation de la rotation automatique des clés (page 108)
- Modification de la fréquence de rotation de la clé (page 109)
- Affichage du nombre de rotations des clés (page 124)

Affichage des clés sous forme d'astérisques

Les clés sont, par défaut, affichées sous forme d'astérisques, mais vous pouvez configurer Wireless Network Security de façon à afficher les clés en clair sur les réseaux non protégés par Wireless Network Security.

Les réseaux protégés par Wireless Network Security affichent la clé en clair.

Pour afficher les clés sous forme d'astérisques :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher la configuration**.
3. Cliquez sur **Autres paramètres**.
4. Décochez la case **Afficher les clés en clair**.
5. Cliquez sur **Appliquer**.

Rubriques connexes

- Affichage des clés en clair (page 114)

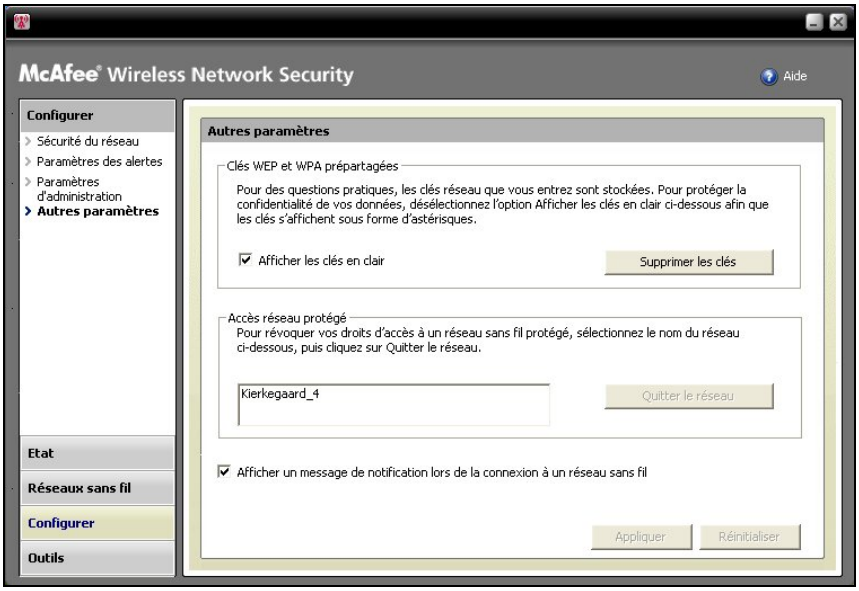
Affichage des clés en clair

Les clés sont, par défaut, affichées sous forme d'astérisques, mais vous pouvez configurer Wireless Network Security de façon à afficher les clés en clair sur les réseaux non protégés par Wireless Network Security.

Les réseaux protégés par Wireless Network Security affichent la clé en clair.

Pour afficher les clés en clair :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher la configuration**.
3. Cliquez sur **Autres paramètres**.



4. Sélectionnez la case **Afficher les clés en clair**.
5. Cliquez sur **Appliquer**.

Rubriques connexes

- Affichage des clés sous forme d'astérisques (page 113)

Suppression des clés réseau

Wireless Network Security enregistre automatiquement vos clés pré-partagées WEP et WPA, que vous pouvez supprimer à tout moment.

Pour supprimer toutes vos clés réseau :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher la configuration**.
3. Dans le volet **Configurer**, cliquez sur **Autres paramètres**.
4. Dans le volet **Autres paramètres**, sous **Clés pré-partagées WEP et WPA**, cliquez sur **Supprimer les clés**.
5. Dans la boîte de dialogue Effacer les clés, cliquez sur **Oui** si vous êtes sûr de vouloir supprimer toutes les clés pré-partagées WEP et WPA enregistrées.

Avertissement : la suppression des clés les élimine de façon définitive de votre ordinateur. Une fois que vous avez supprimé les clés de votre réseau, vous devez entrer la bonne clé pour vous connecter à un réseau WEP et WPA.

CHAPITRE 17

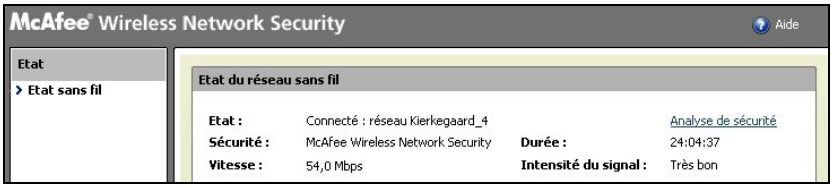
Surveillance de réseaux sans fil

Wireless Network Security vous permet de surveiller l'état de votre réseau sans fil et des ordinateurs protégés.

Contenu de ce chapitre

Surveillance de connexions réseau sans fil

Vous pouvez afficher l'état de votre connexion réseau, le mode de sécurité, la vitesse, la durée, l'intensité du signal et un rapport de sécurité dans le volet Etat du réseau sans fil.



Le tableau suivant décrit les indicateurs d'état des connexions au réseau sans fil.

Etat	Description	Informations
Etat	Indique si votre ordinateur est connecté à un réseau et à quel réseau il est connecté	Affichage de l'état de la connexion (page 119)
Sécurité	Affiche le mode de sécurité du réseau auquel vous êtes connecté. Wireless Network Security s'affiche si vous êtes protégé par Wireless Network Security.	Affichage du mode de sécurité du réseau (page 120)
Vitesse	Affiche la vitesse de la connexion de votre ordinateur au réseau.	Affichage de la vitesse de connexion au réseau (page 120)
Durée	Affiche la durée de connexion de votre ordinateur au réseau.	Affichage de votre temps de connexion au réseau (page 121)
Intensité du signal	Affiche l'intensité relative du signal du réseau.	Affichage de l'intensité du signal du réseau (page 122)
Analyse de sécurité	Cliquer sur **Analyse de sécurité** affiche des informations de sécurité, comme par exemple la vulnérabilité de la sécurité, les problèmes de performances et l'état de votre réseau sans fil.	Affichage du rapport de sécurité en ligne (page 122)

Rubriques connexes

- A propos des icônes Wireless Network Security (page 90)

Affichage de l'état de la connexion

Vous pouvez utiliser le volet Wireless Network Status pour vérifier l'état de votre connexion au réseau, afin de confirmer si vous êtes connecté ou déconnecté du réseau.

Pour afficher l'état de la connexion sans fil :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.

   Les ordinateurs connectés au réseau sans fil protégé et l'heure et la date auxquelles chacun s'est connecté sont affichées dans le volet Etat du réseau sans fil, sous **Ordinateurs.**

Rubriques connexes

- Surveillance des connexions réseau sans fil (page 118)
- Affichage du mode de sécurité du réseau (page 120)
- Affichage de la vitesse de connexion au réseau (page 120)
- Affichage de votre temps de connexion au réseau (page 121)
- Affichage de l'intensité du signal du réseau (page 122)
- Affichage du rapport de sécurité en ligne (page 122)

Affichage du mode de sécurité du réseau

Vous pouvez utiliser le volet Etat du réseau sans fil pour vérifier le mode de sécurité de la connexion réseau.

Pour afficher le mode de sécurité du réseau :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.

   Le mode de sécurité est affiché dans le volet Etat du réseau sans fil dans la case **Sécurité**.

   Wireless Network Security s'affiche si le réseau sans fil est protégé par Wireless Network Security.

Rubriques connexes

- Surveillance des connexions réseau sans fil (page 118)
- Affichage de l'état de la connexion (page 119)
- Affichage de la vitesse de connexion au réseau (page 120)
- Affichage de votre temps de connexion au réseau (page 121)
- Affichage de l'intensité du signal du réseau (page 122)
- Affichage du rapport de sécurité en ligne (page 122)

Affichage de la vitesse de connexion au réseau

Vous pouvez utiliser le volet Etat du réseau sans fil pour vérifier la vitesse de la connexion de votre ordinateur au réseau.

Pour afficher la vitesse de connexion au réseau :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.

   La vitesse de connexion est affichée dans le volet Etat du réseau sans fil dans la case **Vitesse**.

Rubriques connexes

- Surveillance des connexions réseau sans fil (page 118)
- Affichage de l'état de la connexion (page 119)
- Affichage du mode de sécurité du réseau (page 120)
- Affichage de votre temps de connexion au réseau (page 121)
- Affichage de l'intensité du signal du réseau (page 122)
- Affichage du rapport de sécurité en ligne (page 122)

Affichage de votre temps de connexion au réseau

Vous pouvez utiliser le volet Etat du réseau sans fil pour vérifier depuis quand vous êtes connecté au réseau.

Pour afficher votre temps de connexion au réseau :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.

   La durée de connexion de votre ordinateur au réseau sans fil est indiquée dans la case **Durée** .

Rubriques connexes

- Surveillance des connexions réseau sans fil (page 118)
- Affichage de l'état de la connexion (page 119)
- Affichage du mode de sécurité du réseau (page 120)
- Affichage de la vitesse de connexion au réseau (page 120)
- Affichage de l'intensité du signal du réseau (page 122)
- Affichage du rapport de sécurité en ligne (page 122)

Affichage de l'intensité du signal du réseau

Vous pouvez utiliser le volet Etat du réseau sans fil pour vérifier l'intensité du signal du réseau.

Pour afficher l'intensité du signal :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.

   La qualité de votre signal s'affiche dans la case **Intensité du signal**.

Rubriques connexes

- Surveillance des connexions réseau sans fil (page 118)
- Affichage de l'état de la connexion (page 119)
- Affichage du mode de sécurité du réseau (page 120)
- Affichage de la vitesse de connexion au réseau (page 120)
- Affichage de votre temps de connexion au réseau (page 121)
- Affichage du rapport de sécurité en ligne (page 122)

Affichage du rapport de sécurité en ligne

Vous pouvez utiliser le volet Etat du réseau sans fil pour afficher un rapport sur votre connexion sans fil, pour savoir si elle est sécurisée ou non.

La page Web Wi-Fiscan de McAfee affiche des informations sur la vulnérabilité de la sécurité sans fil, les problèmes de performances, des informations sur votre connexion sans fil, sur une solution de sécurité recommandée, et indique si votre connexion est sécurisée.

Avant d'afficher le rapport de sécurité, assurez-vous d'être connecté à Internet.

Pour afficher un rapport de sécurité en ligne sur votre réseau :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.
3. Dans le volet Etat du réseau sans fil, cliquez sur **Analyse de sécurité**.

   Une fois que votre navigateur est ouvert, vous devez télécharger et installer un composant ActiveX. Selon la configuration de votre navigateur, celui-ci peut bloquer le contrôle. Laissez votre navigateur télécharger le composant, puis exécutez-le avant de commencer l'analyse. Selon la vitesse de votre connexion à Internet, l'analyse peut prendre un certain temps.

Remarque : consultez la documentation de votre navigateur pour obtenir des informations sur le téléchargement de composants ActiveX.

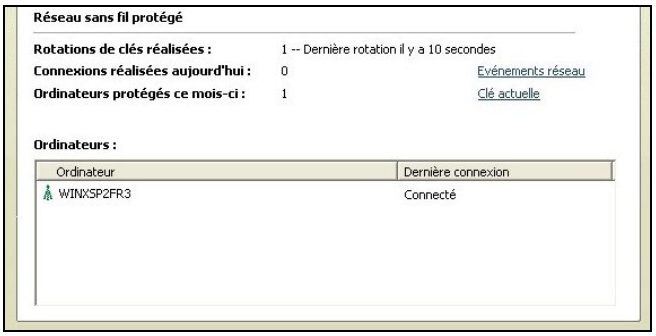
Le Wi-Fiscan de McAfee prend en charge Internet Explorer 5.5 et les versions ultérieures.

Rubriques connexes

- Surveillance des connexions réseau sans fil (page 118)
- Affichage de l'état de la connexion (page 119)
- Affichage du mode de sécurité du réseau (page 120)
- Affichage de la vitesse de connexion au réseau (page 120)
- Affichage de votre temps de connexion au réseau (page 121)
- Affichage de l'intensité du signal du réseau (page 122)

Surveillance de réseaux sans fil protégés

Wireless Network Security vous permet d'afficher le nombre de connexions, les rotations de clés et les ordinateurs protégés dans le volet Etat du réseau sans fil. Vous pouvez également afficher les événements liés au réseau, la clé actuelle et les ordinateurs actuellement protégés.



Le tableau suivant décrit les indicateurs d'état des connexions au réseau sans fil protégé.

Etat	Description	Informations
Rotations de clés réalisées aujourd'hui	Affiche le nombre de rotations de clés par jour sur le réseau sans fil protégé.	Affichage du nombre de rotations des clés (page 125)
Connexions réalisées aujourd'hui	Affiche le nombre de connexions par jour au réseau protégé.	Affichage du nombre de connexions par jour (page 126)
Ordinateurs protégés ce mois-ci	Affiche le nombre d'ordinateurs protégés pendant le mois en cours.	Affichage du nombre d'ordinateurs protégés par mois (page 126)
Evénements liés au réseau	Le fait de cliquer sur **Evénements liés au réseau** affiche les événements liés au réseau, à la connexion et à la rotation des clés.	Affichage des événements liés au réseau sans fil protégé (page 126)

Ordinateurs	Affiche le nombre d'ordinateurs connectés au réseau sans fil protégé et le moment auquel chaque ordinateur s'est connecté.	Affichage des ordinateurs actuellement protégés (page 128)

Affichage du nombre de rotations des clés

Wireless Network Security vous permet d'afficher le nombre de rotations de clés réalisées par jour sur votre réseau protégé, ainsi que l'heure de la dernière rotation.

Pour afficher le nombre de rotations de clés par jour :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.

   Le nombre total de connexions et la rotation de clés la plus récente s'affichent dans le volet Etat du réseau sans fil, sous **Réseau sans fil protégé**, dans le champ **Rotations de clés réalisées aujourd'hui**.

Rubriques connexes

- Surveillance des réseaux sans fil protégés (page 123)
- Affichage du nombre de connexions par jour (page 126)
- Affichage du nombre d'ordinateurs protégés par mois (page 126)
- Affichage des événements liés au réseau sans fil protégé (page 126)
- Affichage des ordinateurs actuellement protégés (page 128)
- Administration des clés réseau (page 107)
- Rotation automatique des clés (page 108)
- Rotation manuelle des clés réseau (page 112)

Affichage du nombre de connexions par jour

Wireless Network Security vous permet d'afficher le nombre de connexions par jour au réseau protégé.

Pour afficher les connexions de votre réseau sans fil protégé :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.

   Le nombre total de connexions s'affiche dans le volet Etat du réseau sans fil, sous **Réseau sans fil protégé**, dans le champ **Connexions réalisées aujourd'hui**.

Rubriques connexes

- Surveillance des réseaux sans fil protégés (page 123)
- Affichage du nombre d'ordinateurs protégés par mois (page 126)
- Affichage des événements liés au réseau sans fil protégé (page 126)
- Affichage des ordinateurs actuellement protégés (page 128)

Affichage du nombre d'ordinateurs protégés par mois

Wireless Network Security vous permet d'afficher le nombre d'ordinateurs protégés pendant le mois en cours.

Pour afficher le nombre d'ordinateurs protégés pendant le mois en cours :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.
3. Le nombre d'ordinateurs protégés pendant le mois en cours s'affiche dans le volet Etat du réseau sans fil, sous **Réseau sans fil protégé**, dans la case **Ordinateurs sécurisés ce mois-ci**.

Rubriques connexes

- Surveillance des réseaux sans fil protégés (page 123)
- Affichage du nombre de rotations des clés (page 125)
- Affichage du nombre de connexions par jour (page 126)
- Affichage des événements liés au réseau sans fil protégé (page 126)
- Affichage des ordinateurs actuellement protégés (page 128)

Affichage des événements liés au réseau sans fil protégé

Wireless Network Security enregistre les événements sur le réseau sans fil, comme par exemple lors de la rotation des clés de sécurité, lorsque d'autres ordinateurs se connectent au réseau protégé par McAfee et lorsque d'autres ordinateurs sont affiliés au réseau protégé par McAfee.

Wireless Network Security vous permet d'afficher un rapport qui décrit les événements qui se sont produits sur votre réseau. Vous pouvez préciser les types d'événements à afficher et trier les informations relatives aux événements par date, événement ou ordinateur.

Pour afficher des événements liés au réseau :

1 Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.

2 Effectuez l'une des opérations suivantes :

Pour...	Opération à exécuter...
Afficher les événements liés au réseau à partir du volet Etat du réseau sans fil	1. Sélectionnez **Afficher l'état**. 2. Dans le volet Etat du réseau sans fil, sous **Réseau sans fil protégé**, cliquez sur **Evénements liés au réseau**.
Afficher les événements liés au réseau à partir du volet Etat du réseau sans fil	1. Cliquez sur **Afficher les outils**. 2. Dans le volet Outils, cliquez sur **Outils de maintenance**. 3. Dans le volet Outils de maintenance, sous **Afficher le journal des événements**, cliquez sur **Afficher**.

3 Sélectionnez un ou plusieurs des événements suivants à afficher :

- **Evénements liés au réseau** : affiche des informations sur l'activité du réseau, comme par exemple la protection d'un routeur ou d'un point d'accès sans fil.
- **Evénements liés à la connexion** : affiche des informations sur les connexions réseau, comme par exemple la date et l'heure auxquelles un ordinateur s'est connecté au réseau.
- **Evénements liés à la rotation des clés** : affiche des informations sur la date et l'heure des rotations des clés de sécurité.

4 Cliquez sur **Fermer**.

Rubriques connexes

- Surveillance des réseaux sans fil protégés (page 123)
- Affichage du nombre de rotations des clés (page 125)
- Affichage du nombre de connexions par jour (page 125)
- Affichage du nombre de connexions par jour (page 126)
- Affichage des ordinateurs actuellement protégés (page 128)

Affichage des ordinateurs actuellement protégés

Vous pouvez afficher le nombre d'ordinateurs connectés au réseau sans fil protégé et la dernière connexion de chaque ordinateur.

Pour afficher les ordinateurs connectés au réseau protégé :

1. Cliquez avec le bouton droit de la souris sur l'icône Wireless Network Security de la zone de notification Windows.
2. Sélectionnez **Afficher l'état**.
3. Les ordinateurs connectés au réseau sans fil protégé et l'heure et la date de la dernière connexion de chacun d'entre eux s'affichent dans le volet Etat du réseau sans fil, sous **Ordinateurs.**

Rubriques connexes

- Surveillance des réseaux sans fil protégés (page 123)
- Affichage du nombre de rotations des clés (page 125)
- Affichage du nombre de connexions par jour (page 125)
- Affichage du nombre d'ordinateurs protégés par mois (page 126)
- Affichage des événements liés au réseau sans fil protégé (page 126)

CHAPITRE 18

Dépannage

Vous pouvez résoudre des problèmes lorsque vous utilisez Wireless Security et un équipement tiers, y compris :

- des difficultés d'installation
- une incapacité à protéger ou à configurer votre réseau
- une incapacité à connecter des ordinateurs à votre réseau
- une incapacité à vous connecter à un réseau ou à Internet
- autres problèmes

Contenu de ce chapitre

Installation de Wireless Network Security

Vous pouvez résoudre les problèmes d'installation suivants.

- Sur quels ordinateurs installer ce logiciel
- Adaptateur sans fil non détecté
- Plusieurs adaptateurs sans fil
- Incapacité à télécharger sur des ordinateurs sans fil car le réseau est déjà sécurisé

Sur quels ordinateurs installer ce logiciel

Installez Wireless Network Security sur tous les ordinateurs sans fil de votre réseau (contrairement à d'autres programmes McAfee, vous pouvez installer ce logiciel sur plusieurs ordinateurs). Acceptez l'accord de licence de votre logiciel acheté. Dans certains cas, vous devrez peut-être acheter d'autres licences.

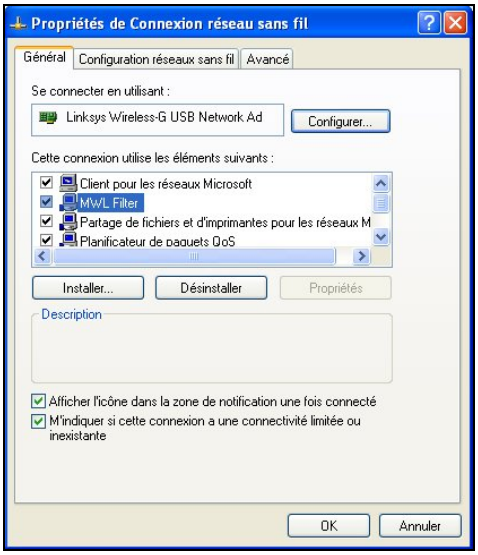
Vous pouvez (mais vous n'êtes pas obligé) l'installer sur des ordinateurs qui ne disposent pas d'adaptateur sans fil, mais le logiciel n'est pas actif sur ces ordinateurs car ils n'ont pas besoin de protection sans fil.

Wireless Network Security est actuellement pris en charge sous Windows XP ou Windows 2000.

Adaptateur sans fil compatible non détecté

Si votre adaptateur sans fil n'est pas détecté lorsqu'il est installé et activé, redémarrez votre ordinateur. Si l'adaptateur n'est toujours pas détecté après le redémarrage de votre ordinateur, procédez aux étapes suivantes.

1. Lancez la boîte de dialogue Propriétés de connexion au réseau sans fil de Windows.
2. Dans le menu Démarrer en affichage classique de Windows, cliquez sur **Démarrer**, pointez le curseur de la souris sur **Paramètres**, puis sélectionnez **Connexions réseau**.
3. Cliquez sur l'icône **Connexion au réseau sans fil**.
4. Dans la boîte de dialogue Etat de la connexion au réseau sans fil, cliquez sur **Propriétés**.
5. Dans le volet Propriétés de la connexion au réseau sans fil, décochez la case **Filtre MWL** puis resélectionnez-le.



6. Cliquez sur **OK**.

   Si cela ne résout pas le problème, testez le WiFi Scan. Si le wi-fi scan fonctionne, votre adaptateur est pris en charge. Dans le cas contraire, mettez à jour le pilote de votre adaptateur (utilisez Windows Update ou consultez le site Web du fabricant) ou achetez un nouveau périphérique.

Rubriques connexes

- Affichage du rapport de sécurité en ligne (page 122)

Plusieurs adaptateurs sans fil

Si un message d'erreur indique que vous avez installé plusieurs adaptateurs sans fil, vous devez en désactiver ou en débrancher un. Wireless Home Network Security fonctionne uniquement avec un adaptateur sans fil.

Echec du téléchargement sur un réseau sécurisé

Si vous avez un CD d'installation, installez Wireless Network Security à partir du CD sur tous vos ordinateurs sans fil.

Si vous avez installé le logiciel sur un ordinateur sans fil et que vous avez protégé votre réseau avant d'installer ce logiciel sur tous les autres ordinateurs sans fil, vous disposez des options suivantes.

- Annulez la protection de votre réseau, puis téléchargez le logiciel et installez-le sur tous les ordinateurs sans fil. Protégez votre réseau à nouveau.
- Affichez la clé réseau. Ensuite, saisissez la clé sur votre ordinateur sans fil pour vous connecter au réseau. Téléchargez et installez le logiciel, puis affiliez-vous au réseau à partir de l'ordinateur sans fil.
- Téléchargez le fichier exécutable sur l'ordinateur qui est déjà connecté au réseau et enregistrez-le sur une clé USB Flash Drive ou gravez-le sur un CD de façon à ce que vous puissiez l'installer sur les autres ordinateurs.
- Exécutez la technologie Windows Connect Now.

Rubriques connexes

- Suppression des routeurs ou points d'accès sans fil (page 97)
- Affichage des clés actuelles (page 107)
- Ajout d'ordinateurs à l'aide d'un périphérique amovible (page 85)
- Ajout d'ordinateurs à l'aide de la technologie Windows Connect Now (page 87)

Protection ou configuration de votre réseau

Vous pouvez résoudre les problèmes suivants lors de la protection ou de la configuration de votre réseau.

- Routeur ou point d'accès non pris en charge
- Mettre à jour le routeur ou le micrologiciel de point d'accès
- Dupliquer l'erreur administrateur
- Le réseau semble ne pas être sécurisé
- Incapacité à réparer

Routeur ou point d'accès non pris en charge

Si un message d'erreur indique que votre routeur ou point d'accès sans fil peut ne pas être pris en charge, Windows Network Security n'a pas pu configurer votre périphérique car il ne l'a pas reconnu ou trouvé.

Vérifiez que vous avez la dernière version de Wireless Network Security en demandant une mise à jour (McAfee ajoute constamment un support pour les nouveaux routeurs et points d'accès). Si votre routeur ou point d'accès figure sur la liste des routeurs pris en charge et que vous recevez toujours ce message d'erreur, il s'agit d'erreurs de communication entre votre ordinateur et le routeur ou point d'accès.

Rubriques connexes

- Routeurs sans fil pris en charge
  http://www.mcafee.com/router

Mettre à jour le routeur ou le micrologiciel de point d'accès

Si un message d'erreur indique que la révision du micrologiciel de votre routeur ou point d'accès sans fil n'est pas prise en charge, votre périphérique est pris en charge, mais la révision du micrologiciel du périphérique ne l'est pas. Vérifiez que vous avez la dernière version de Wireless Network Security en demandant une mise à jour (McAfee ajoute constamment un support pour les nouvelles révisions de micrologiciel).

Si vous avez la dernière version de Wireless Network Security, consultez le site Web du fabricant ou l'organisme de support de votre routeur ou point d'accès et installez une version de micrologiciel qui figure dans la liste des routeurs pris en charge.

Rubriques connexes

- Routeurs sans fil pris en charge
  http://www.mcafee.com/router

Dupliquer l'erreur administrateur

Après avoir configuré votre routeur ou point d'accès, vous devez vous déconnecter de l'interface d'administration. Dans certains cas, si vous ne vous déconnectez pas, le routeur ou point d'accès agit comme si un autre ordinateur le configurait encore et un message d'erreur s'affiche.

Si vous ne pouvez pas vous déconnecter, débranchez la source d'alimentation du routeur ou point d'accès, puis rebranchez-la.

Echec de la rotation des clés

La rotation des clés a échoué car :

- Les informations de connexion à votre routeur ou point d'accès ont été modifiées.
- La version de micrologiciel de votre routeur ou point d'accès a été modifiée et est passée à une version non prise en charge.
- Votre routeur ou point d'accès n'est pas disponible. Vérifiez que le routeur ou point d'accès est sous tension et qu'il est connecté à votre réseau.
- Dupliquer l'erreur administrateur.
- Pour certains routeurs sans fil, si un autre ordinateur est connecté manuellement à l'interface Web du routeur sans fil, le client McAfee peut ne pas être en mesure d'accéder à l'interface de gestion pour effectuer la rotation des clés de chiffrement.

Rubriques connexes

- Modification des informations d'authentification des périphériques sans fil (page 105)
- Rotation automatique des clés (page 108)

Incapacité à réparer le routeur ou point d'accès

Si la réparation échoue, essayez ce qui suit. Notez que chaque procédure est indépendante.

- Connectez-vous à votre réseau à l'aide d'un câble, puis réessayez de réparer.
- Débranchez la source d'alimentation du routeur ou point d'accès, rebranchez-la, puis essayez de vous connecter.
- Rétablissez les paramètres par défaut du routeur ou du point d'accès sans fil et réparez-le. Cette opération réinitialise les valeurs initiales des paramètres du périphérique sans fil. Réinitialisez ensuite vos paramètres de connexion Internet.
- A l'aide des options avancées, quittez le réseau de tous les ordinateurs et rétablissez les paramètres par défaut du routeur ou point d'accès sans fil, puis protégez-le. Cette opération réinitialise les valeurs initiales des paramètres du périphérique sans fil. Réinitialisez ensuite vos paramètres de connexion Internet.

Rubriques connexes

- Correction des paramètres de sécurité réseau (page 106)

Le réseau semble ne pas être protégé

Si votre réseau s'affiche comme étant non sécurisé, il n'est pas protégé. Vous devez protéger le réseau pour le sécuriser. Notez que Wireless Network Security fonctionne uniquement avec des routeurs ou points d'accès compatibles.

Rubriques connexes

- Création de réseaux sans fil protégés (page 76)
- Routeurs sans fil pris en charge
  http://www.mcafee.com/router

Connexion d'ordinateurs à votre réseau

Vous pouvez résoudre les problèmes suivants lors de la connexion d'ordinateurs à votre réseau.

- En attente d'autorisation
- Autorisation d'accès à un ordinateur inconnu

En attente d'autorisation

Si vous essayez de vous affilier à un réseau protégé et que votre ordinateur reste en mode d'attente d'autorisation, vérifiez les points suivants.

- Un ordinateur sans fil qui a déjà accès au réseau est sous tension et connecté au réseau.
- Quelqu'un est présent pour autoriser l'accès sur cet ordinateur lorsqu'il apparaît.
- Les ordinateurs se trouvent dans le rayon de portée sans fil les uns par rapport aux autres.

Si **Autoriser l'accès** n'apparaît pas sur l'ordinateur qui a déjà accès au réseau, essayez d'autoriser l'accès à partir d'un autre ordinateur.

Si aucun autre ordinateur n'est disponible, annulez la protection du réseau à partir de l'ordinateur qui a déjà accès, et protégez le réseau à partir de l'ordinateur qui n'avait pas accès. Ensuite, affiliez-vous au réseau à partir de l'ordinateur qui protégeait le réseau initialement.

Vous pouvez également utiliser la fonction Protéger un autre ordinateur.

Rubriques connexes

- Affiliation à un réseau sans fil protégé (page 78)
- Déconnexion des réseaux sans fil protégés (page 100)
- Suppression des routeurs ou points d'accès sans fil (page 97)
- Ajout d'ordinateurs au réseau sans fil protégé (page 85)

Autorisation d'accès à un ordinateur inconnu

Lorsque vous recevez une demande d'autorisation d'accès d'un ordinateur inconnu, refusez-la jusqu'à ce que vous puissiez vérifier sa légitimité. Il se peut que quelqu'un soit en train d'essayer d'accéder de façon illégitime à votre réseau.

Connexion à Internet et à un réseau

Vous pouvez résoudre les problèmes suivants lors de la connexion à un réseau ou à Internet.

- Mauvaise connexion à Internet
- La connexion s'interrompt brièvement
- Les périphériques (pas votre ordinateur) perdent la connexion
- Invite à saisir la clé WEP, WPA ou WPA2
- Impossible de se connecter
- Mettez à jour votre adaptateur sans fil
- Niveau de signal faible
- Windows ne peut pas configurer votre connexion sans fil
- Windows n'affiche aucune connexion

Impossible de se connecter à Internet

Si vous ne pouvez pas vous connecter, essayez d'accéder au réseau à l'aide d'un câble, puis connectez-vous à Internet. Si vous ne pouvez toujours pas vous connecter, vérifiez ce qui suit :

- Votre modem est sous tension
- Vos paramètres PPPoE sont corrects
- Votre ligne DSL ou câblée est active

Des problèmes de connectivité comme la vitesse et l'intensité du signal peuvent également être causés par une interférence sans fil. Essayez les méthodes suivantes pour corriger le problème :

- Modifier le canal de votre téléphone sans fil
- Eliminer les sources possibles d'interférence
- Modifier l'emplacement de votre routeur, point d'accès ou ordinateur sans fil
- Modifier le canal du routeur ou du point d'accès. Les canaux 1, 4, 7 et 11 sont recommandés pour l'Amérique du Nord et du Sud. Les canaux 1, 4, 7 et 13 sont recommandés pour les autres pays. De nombreux routeurs sont réglés sur le canal 6 par défaut
- Vérifiez que votre routeur et votre adaptateur sans fil (en particulier un adaptateur USB sans fil) ne se trouvent pas contre un mur
- Vérifiez que votre adaptateur sans fil USB ne se trouve pas près d'un point d'accès/routeur sans fil.
- Positionnez le routeur à l'écart des murs et du métal

Connexion interrompue

Lorsque votre connexion est brièvement interrompue (par exemple, lors d'un jeu en ligne), la rotation des clés peut en être la cause. Pour empêcher cela, vous pouvez suspendre la rotation des clés.

McAfee vous recommande de reprendre la rotation automatique des clés dès que possible pour que votre réseau soit complètement protégé des pirates.

Rubriques connexes

- Rotation automatique des clés (page 108)
- Reprise de la rotation des clés (page 109)
- Suspension de la rotation automatique des clés (page 111)
- Rotation manuelle des clés réseau (page 112)

Les périphériques perdent la connectivité

Si certains périphériques perdent leur connexion lorsque vous utilisez Wireless Network Security, essayez de résoudre le problème par les méthodes suivantes :

- Suspendre la rotation des clés
- Mettre à jour le pilote de l'adaptateur sans fil
- Désactiver le gestionnaire client de l'adaptateur

Rubriques connexes

- Suspension de la rotation automatique des clés (page 111)

Invitation à saisir la clé WEP, WPA ou WPA2

Si vous devez saisir une clé WEP, WPA ou WPA2 pour vous connecter à votre réseau sans fil protégé, c'est probablement parce que vous n'avez pas installé le logiciel sur votre ordinateur.

Pour fonctionner correctement, Wireless Network Security doit être installé sur chaque ordinateur sans fil de votre réseau.

Rubriques connexes

- Démarrage de Wireless Network Security (page 70)
- Ajout d'ordinateurs au réseau sans fil protégé (page 85)

Incapacité à se connecter au réseau sans fil

Si vous ne pouvez pas vous connecter, essayez ce qui suit : Notez que chaque procédure est indépendante.

- Si vous ne vous connectez pas à un réseau protégé, vérifiez que vous avez la bonne clé et saisissez-la à nouveau.
- Débranchez l'adaptateur sans fil et rebranchez-le, ou désactivez-le puis réactivez-le.
- Mettez le routeur ou point d'accès hors tension, puis sous tension à nouveau, et essayez de vous connecter.
- Vérifiez que votre routeur ou point d'accès sans fil est connecté, puis corrigez les paramètres de sécurité.
- Redémarrez votre ordinateur.
- Mettez à jour votre adaptateur sans fil ou achetez-en un neuf. Par exemple, il se peut que votre réseau utilise la sécurité WPA-PSK TKIP, et votre adaptateur sans fil peut ne pas prendre en charge ce mode de sécurité réseau (les réseaux affichent la sécurité WEP, même s'ils sont réglés sur WPA).
- Si vous ne pouvez pas vous connecter après avoir mis à niveau votre routeur ou point d'accès sans fil, il se peut que votre mise à niveau ait été effectuée vers une version non prise en charge. Vérifiez que le routeur ou point d'accès est pris en charge. S'il n'est pas pris en charge, utilisez une version antérieure prise en charge, ou patientez jusqu'à ce qu'une mise à jour de Wireless Security soit disponible.

Rubriques connexes

- Correction des paramètres de sécurité réseau (page 106)
- Mise à jour de votre adaptateur sans fil (page 139)

Mise à jour de votre adaptateur sans fil

Vous devrez peut-être mettre à jour votre adaptateur sans fil de façon à pouvoir utiliser Wireless Network Security.

Pour mettre à jour votre adaptateur :

1. sur le bureau, cliquez sur **Démarrer**, pointez sur **Paramètres**, puis sélectionnez **Panneau de configuration**.
2. Double-cliquez sur l'icône **Système**. La boîte de dialogue **Propriétés du système** s'affiche.
3. Sélectionnez l'onglet **Matériel**, puis cliquez sur **Gestionnaire de périphériques**.
4. Dans la liste du Gestionnaire de périphériques, double-cliquez sur votre adaptateur.
5. Sélectionnez l'onglet **Pilote** et notez la référence de votre pilote.
6. Allez sur le site Web du fabricant de l'adaptateur pour rechercher une mise à jour. Les pilotes se trouvent en général

à la section Support ou Téléchargements. Si vous utilisez une carte miniPCI, recherchez le fabricant de l'ordinateur et non pas celui de la carte.

7 Si une mise à jour du pilote est disponible, suivez les instructions sur le site Web pour la télécharger.

8 Retournez à l'onglet **Pilote** et cliquez sur **Mettre le pilote à jour**. Un assistant Windows apparaît.

9 Pour installer le pilote, suivez les instructions sur le site Web.

Niveau de signal faible

Si votre connexion est coupée ou est lente, le niveau de votre signal n'est peut-être pas assez fort. Pour améliorer votre signal, vérifiez les points suivants :

- Assurez-vous que vos périphériques sans fil ne sont pas bloqués par des objets métalliques comme des fours, des appareils à propagation ou des appareils volumineux. Les signaux sans fil ne traversent pas bien ces objets.
- Si votre signal traverse des murs, assurez-vous de l'absence d'angle faible. Plus le signal met de temps à traverser un mur, plus il s'affaiblit.
- Si votre point d'accès ou routeur sans fil dispose de plusieurs antennes, essayez de déplacer les deux antennes perpendiculairement l'une par rapport à l'autre (l'une à la verticale et l'autre à l'horizontale, à un angle de 90 degrés).
- Certains fabricants ont des antennes à gain élevé. Les antennes directionnelles offrent une portée plus longue, alors que les antennes omni-directionnelles offrent une plus grande souplesse d'utilisation. Consultez les instructions d'installation de votre fabricant pour installer l'antenne.

Si ces étapes échouent, ajoutez un point d'accès à votre réseau plus proche de l'ordinateur auquel vous essayez de vous connecter. Si vous le configurez avec le même nom de réseau (SSID) et un canal différent, votre adaptateur trouve automatiquement le signal le plus intense et se connecte via le point d'accès approprié.

Rubriques connexes

- Icônes d'intensité du signal (page 91)
- Affichage de l'intensité du signal du réseau (page 121)

Windows ne prend pas en charge la connexion sans fil

Si un message d'erreur Windows indique qu'il ne peut pas configurer votre connexion sans fil, vous pouvez l'ignorer. Utilisez Wireless Network Security pour vous connecter et configurer des réseaux sans fil.

Dans la boîte de dialogue Propriétés de la connexion au réseau sans fil, sous l'onglet Réseaux sans fil, assurez-vous que la case **Utiliser Windows pour configurer mon paramètre de réseau sans fil** est décochée.

Wireless Network Security permet :

- aux adaptateurs installés sur des ordinateurs fonctionnant sous Windows 2000 de se connecter à des réseaux WPA, même si le gestionnaire client de cartes n'est pas pris en charge.
- aux adaptateurs sur les ordinateurs fonctionnant sous Windows XP de se connecter à des réseaux WPA2 sans avoir à trouver et à installer le correctif Win XP SP2
- aux adaptateurs sous Windows XP SP1 de se connecter à des réseaux WPA et WPA2 sans avoir à trouver et à installer un correctif, qui n'est pas pris en charge par Windows XP SP1.

Windows n'affiche aucune connexion

Si vous êtes connecté, mais si l'icône Windows Network affiche un X (aucune connexion), ignorez ceci. Vous avez une bonne connexion.

Autres problèmes

Vous pouvez résoudre les problèmes suivants.

- Le nom du réseau est différent lors de l'utilisation d'autres programmes
- Problème lors de la configuration des routeurs ou points d'accès sans fil
- Remplacer les ordinateurs
- Sélectionner un autre mode de sécurité
- Le logiciel ne fonctionne pas après la mise à niveau des systèmes d'exploitation

Le nom du réseau est différent lors de l'utilisation d'autres programmes

Si le nom du réseau est différent lorsqu'il s'affiche dans d'autres programmes (par exemple, _SafeAaf fait partie du nom), ceci est normal.

Wireless Network Security attribue un code aux réseaux lorsqu'ils sont protégés.

Configuration des routeurs ou points d'accès sans fil

Si un message d'erreur s'affiche lors de la configuration de votre routeur ou point d'accès ou lors de l'ajout de plusieurs routeurs sur le réseau, vérifiez que tous les routeurs et points d'accès ont une adresse IP distincte.

Si le nom du routeur ou point d'accès sans fil apparaît dans la boîte de dialogue Protéger le routeur ou point d'accès sans fil, mais que vous obtenez un message d'erreur lorsque vous le configurez : vérifiez que votre routeur ou point d'accès est pris en charge.

Si votre routeur ou point d'accès est configuré, mais ne semble pas être sur le bon réseau (par exemple, vous ne voyez pas d'autres ordinateurs reliés au réseau local), vérifiez que vous avez configuré le routeur ou point d'accès approprié, et non pas celui de votre voisin. Débranchez la source d'alimentation du routeur ou point d'accès et assurez-vous que la connexion est coupée. Si le mauvais routeur ou point d'accès a été configuré, annulez sa protection, puis protégez le bon routeur ou point d'accès.

Si vous ne pouvez pas configurer ni ajouter votre routeur ou point d'accès, mais qu'il est pris en charge, certaines modifications que vous avez apportées peuvent l'empêcher d'être correctement configuré.

- Suivez les instructions du fabricant pour configurer votre routeur ou point d'accès sans fil sur DHCP, ou pour configurer la bonne adresse IP. Dans certains cas, le fabricant fournit un outil de configuration.
- Rétablissez les paramètres par défaut de votre routeur ou point d'accès et essayez de réparer votre réseau à nouveau. Vous avez peut-être modifié le port d'administration sur le routeur ou point d'accès, ou désactivé l'administration sans fil. Assurez-vous que vous utilisez la configuration par défaut, et que la configuration sans fil est activée. Une autre possibilité est que l'administration http soit désactivée. Dans ce cas, vérifiez que l'administration http est activée. Vérifiez que vous utilisez le port 80 pour l'administration.
- Si votre routeur ou point d'accès sans fil ne figure pas dans la liste des routeurs ou points d'accès sans fil à protéger ou auxquels se connecter, activez la Diffusion SSID et vérifiez que vous pouvez voir votre routeur ou point d'accès dans la liste des réseaux sans fil disponibles de Wireless Network Security.
- Si vous êtes déconnecté, ou si vous ne pouvez pas établir de connexion, un filtre MAC peut être activé. Désactivez le filtre MAC.
- Si vous ne pouvez pas effectuer d'opérations sur le réseau (par exemple, partager des fichiers ou imprimer sur des imprimantes partagées) entre deux ordinateurs avec une connexion sans fil au réseau, vérifiez que vous n'avez pas activé l'isolation du point d'accès. L'isolation des points

d'accès empêche les ordinateurs sans fil de se connecter l'un à l'autre via le réseau.

- Si vous utilisez un programme de pare-feu autre que McAfee Personal Firewall, assurez-vous que le sous-réseau est sécurisé.

Rubriques connexes

- Routeurs sans fil pris en charge
  http://www.mcafee.com/router

Remplacement des ordinateurs

Si l'ordinateur qui a protégé le réseau a été remplacé et qu'aucun ordinateur n'a accès (vous ne pouvez pas accéder au réseau), rétablissez les paramètres par défaut du routeur ou du point d'accès sans fil et protégez votre réseau à nouveau.

Sélectionnez un autre mode de sécurité

Si un message d'erreur indique que vous avez sélectionné un mode de sécurité non pris en charge par l'adaptateur sans fil, vous devez sélectionner un autre mode de sécurité.

- Tous les adaptateurs prennent en charge la sécurité WEP.
- La plupart des adaptateurs qui prennent en charge la sécurité WPA mettent en oeuvre les modes de sécurité WPA-PSK TKIP et WPA-PSK AES.
- Les adaptateurs qui prennent en charge la sécurité WPA2 mettent en oeuvre les modes de sécurité WPA et WPA2-PSK TKIP, WPA2-PSK AES et WPA2-PSK TKIP/AES.

Rubriques connexes

- Configuration des paramètres de sécurité (page 102)
- Affichage du mode de sécurité du réseau (page 120)

Echec du logiciel après une mise à niveau des systèmes d'exploitation

En cas d'échec de Wireless Network Security après une mise à niveau des systèmes d'exploitation, supprimez puis réinstallez le programme.

CHAPITRE 19

McAfee EasyNetwork

McAfee® EasyNetwork sécurise le partage des fichiers, simplifie les transferts de fichiers et automatise le partage d'imprimantes entre les ordinateurs de votre réseau domestique.

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

Contenu de ce chapitre

Caractéristiques

EasyNetwork propose les fonctionnalités suivantes :

Partage de fichiers

Grâce à EasyNetwork, il est facile de partager des fichiers depuis votre ordinateur vers d'autres ordinateurs du réseau. Lorsque vous partagez des fichiers, vous donnez aux autres ordinateurs un accès en lecture seule à ces fichiers. Seuls les ordinateurs 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.

Transfert de fichiers

Vous pouvez envoyer des fichiers à d'autres ordinateurs qui sont affiliés au réseau géré. Lorsque vous recevez un fichier, il apparaît dans votre boîte de réception EasyNetwork. La boîte de réception est un emplacement de stockage temporaire pour tous les fichiers que vous envoyez à d'autres ordinateurs sur le réseau.

Partage d'imprimantes automatique

Lorsque vous vous affiliez au réseau géré, EasyNetwork partage automatiquement toutes les imprimantes locales reliées à votre ordinateur, et utilise le nom actuel de l'imprimante comme nom d'imprimante partagée. L'application détecte également les imprimantes partagées par d'autres ordinateurs sur votre réseau et permet de configurer et d'utiliser ces imprimantes.

CHAPITRE 20

Configuration de EasyNetwork

Pour pouvoir utiliser les fonctionnalités de EasyNetwork, vous devez d'abord lancer le programme et vous affilier au réseau géré. Vous pourrez ensuite quitter le réseau à tout moment.

Contenu de ce chapitre

Lancement de l'application EasyNetwork

Par défaut, le système vous invite à lancer EasyNetwork immédiatement après l'installation, mais vous pouvez également lancer l'application ultérieurement.

Lancement de l'application EasyNetwork

Par défaut, le système vous invite à lancer EasyNetwork immédiatement après l'installation, mais vous pouvez également lancer l'application ultérieurement.

Pour lancer EasyNetwork :

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

Conseil : si vous avez demandé que des icônes de l'application soient créées pour le bureau et la zone de lancement rapide lors de l'installation, vous pouvez également double-cliquer sur l'icône McAfee EasyNetwork du bureau ou cliquer sur l'icône McAfee EasyNetwork de la zone de notification située à droite de la barre des tâches pour lancer EasyNetwork.

Affiliation à un réseau géré

Lorsque vous installez SecurityCenter, un agent réseau est installé sur votre ordinateur et s'exécute en arrière-plan. Dans le cas de EasyNetwork, l'agent réseau est chargé de détecter une connexion réseau valide, de détecter des imprimantes locales à partager et de surveiller l'état du réseau.

Si aucun autre ordinateur exécutant cet agent réseau n'est détecté sur le réseau auquel vous êtes actuellement connecté, vous êtes automatiquement affilié à ce 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, une demande d'affiliation est envoyée à tous les 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 : invité (possibilité de transférer des fichiers uniquement) ou accès complet ou d'administration (possibilité de transférer des fichiers et de les partager), par exemple. 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. Un contrôle de sécurité est effectué avant d'autoriser l'accès à l'ordinateur.

Remarque : après vous être connecté, si d'autres programmes réseau McAfee sont installés (McAfee Wireless Network Security ou 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 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 d'invite 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. Si l'ordinateur est le premier à s'affilier au réseau, des autorisations de type Administration lui sont automatiquement attribuées.

Pour s'affilier au réseau :

1. Dans la fenêtre Fichiers partagés, cliquez sur **Oui, je souhaite me connecter à ce réseau maintenant**. 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 **Oui**. Dans le cas contraire, cliquez sur **Non**.
3. Vérifiez que l'ordinateur qui a autorisé l'accès affiche les cartes à jouer suivantes dans la boîte de dialogue de confirmation de sécurité, puis cliquez sur **Confirmer**.

Remarque : si ce n'est pas le cas, cela signifie que 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 **Refuser** dans la boîte de dialogue de confirmation de la 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 à répondre au message devient l'administrateur de droits d'accès. L'administrateur de droits d'accès doit définir le type d'accès à accorder à l'ordinateur : invité, complet ou administratif.

Pour accorder l'accès au réseau :

1. Lors de l'alerte, cochez l'une des cases suivantes :
   - **Autoriser l'accès à un invité** : en tant qu'invité, l'utilisateur est autorisé à envoyer des fichiers à d'autres ordinateurs, mais pas à partager des fichiers.

- **Accorder un accès complet à toutes les applications du réseau géré** : ce niveau d'autorisation permet à l'utilisateur d'envoyer et de partager des fichiers.
- **Accorder un accès administratif à toutes les applications du réseau géré** : ce niveau d'autorisation permet à l'utilisateur d'envoyer et de partager des fichiers, d'accorder l'accès à d'autres ordinateurs et de modifier les niveaux d'autorisation des autres ordinateurs.

2 Cliquez sur **Autoriser l'accès**.

3 Vérifiez que l'ordinateur affiche les cartes à jouer suivantes dans la boîte de dialogue de confirmation de sécurité, puis cliquez sur **Confirmer**.

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** 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.

Pour renommer le réseau :

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 plus en faire partie, vous pouvez quitter le réseau. Une fois que vous avez annulé votre affiliation, vous pouvez revenir en arrière à tout moment. En revanche, vous devrez à nouveau demander une autorisation d'affiliation et effectuer le contrôle de sécurité. Pour plus d'informations, reportez-vous à Affiliation à un réseau géré (page 149).

Comment quitter un réseau géré

Vous pouvez quitter un réseau géré auquel vous êtes affilié.

Pour quitter un réseau géré :

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

CHAPITRE 21

Partage et envoi des fichiers

Grâce à EasyNetwork, il est facile de partager et d'envoyer des fichiers depuis votre ordinateur vers d'autres ordinateurs du réseau. Lorsque vous partagez des fichiers, vous donnez aux autres ordinateurs un accès en lecture seule à ces fichiers. Seuls les ordinateurs 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.

Contenu de ce chapitre

Partage de fichiers

Grâce à EasyNetwork, il est facile de partager des fichiers depuis votre ordinateur vers d'autres ordinateurs du réseau. Lorsque vous partagez des fichiers, vous donnez aux autres ordinateurs un accès en lecture seule à ces fichiers. Seuls les ordinateurs 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 automatiquement supprimé de la fenêtre Fichiers partagés. Vous pouvez mettre fin au partage de fichiers à tout moment.

Vous avez deux moyens d'accéder à un fichier partagé : en ouvrant le fichier directement à partir de EasyNetwork ou en copiant le fichier sur votre ordinateur et en l'ouvrant. Si la liste de vos fichiers partagés est trop longue, vous pouvez effectuer une recherche du/des fichier(s) partagé(s) au(x)quel(s) vous souhaitez accéder.

Remarque : les autres ordinateurs ne peuvent pas utiliser l'Explorateur Windows pour accéder aux fichiers partagés à l'aide de EasyNetwork. Le partage des fichiers EasyNetwork s'effectue via des connexions sécurisées.

Partage d'un fichier

Lorsque vous partagez un fichier, il est automatiquement mis à la disposition de tous les autres ordinateurs affiliés ayant un accès complet ou administratif au réseau géré.

Pour partager un fichier :

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 plus y accéder.

Pour mettre fin au partage d'un fichier :

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 **Ne pas partager**.

Copie d'un fichier partagé

Vous pouvez copier des fichiers partagés depuis n'importe quel ordinateur du réseau géré sur votre ordinateur. De cette façon, si l'ordinateur cesse de partager le fichier, vous en avez une copie à disposition.

Pour copier un fichier :

- 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 automatiquement les résultats correspondants dans la fenêtre Fichiers partagés.

Pour rechercher un fichier partagé :

1. Dans la fenêtre Fichiers partagés, cliquez sur **Rechercher**.
2. Cliquez sur l'une des options suivantes dans la liste **Contient** :
   - **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**.

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 l'un des types de fichiers suivants dans la liste **Type** :

- **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 image partagés.
- **Vidéo** : la recherche porte sur tous les fichiers vidéo partagés.
- **Audio** : la recherche porte sur tous les fichiers audio partagés.

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.

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 droite de la barre des tâches Windows. Si vous ne souhaitez pas recevoir de messages de notification, vous pouvez les désactiver. 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 (c'est-à-dire jusqu'à ce que vous les copiiez sur votre ordinateur).

Envoi d'un fichier à un autre ordinateur

Vous pouvez envoyer un fichier directement 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 160).

Pour envoyer un fichier à un autre ordinateur :

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 dans un dossier de votre ordinateur). Si l'application EasyNetwork n'est pas ouverte ou au premier plan lorsque votre ordinateur reçoit un fichier, vous recevez un message de notification dans la zone située à droite de la barre des tâches. Cliquez sur ce message pour ouvrir EasyNetwork et accéder au fichier.

Pour recevoir un fichier d'un autre ordinateur :

- 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 une notification lorsqu'un autre ordinateur du réseau géré vous envoie un fichier. Si EasyNetwork n'est pas ouvert ou au premier plan sur votre bureau, un message de notification apparaît dans la zone située à droite de la barre des tâches Windows.

Pour recevoir une notification lors de l'envoi d'un fichier :

1. Dans le menu **Options**, cliquez sur **Configurer**.
2. Dans la boîte de dialogue Configurer, cochez la case **M'avertir lorsqu'un autre ordinateur m'envoie des fichiers**.
3. Cliquez sur **OK**.

CHAPITRE 22

Partage d'imprimantes

Lorsque vous vous affiliez à un réseau géré, EasyNetwork partage automatiquement toutes les imprimantes locales reliées à votre ordinateur. L'application détecte également les imprimantes partagées par d'autres ordinateurs sur votre réseau et permet de configurer et d'utiliser ces imprimantes.

Contenu de ce chapitre

Utilisation d'imprimantes partagées

Lorsque vous vous affiliez au réseau géré, EasyNetwork partage automatiquement toutes les imprimantes locales reliées à votre ordinateur, et utilise le nom actuel de l'imprimante comme nom d'imprimante partagée. L'application détecte également les imprimantes partagées par d'autres ordinateurs sur votre réseau et permet de configurer et d'utiliser ces imprimantes. 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 automatiquement sur le réseau. Vous pouvez également mettre fin au partage d'une imprimante à tout moment.

EasyNetwork détecte également les imprimantes partagées par tous les autres ordinateurs du réseau. Si l'application détecte une imprimante distante qui n'est pas encore 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 ainsi installer des imprimantes disponibles ou désinstaller des imprimantes qui sont déjà connectées à votre ordinateur. Cela permet également d'actualiser la liste des imprimantes détectées sur le réseau.

Si vous n'êtes pas encore affilié au réseau géré mais si vous y êtes connecté, vous pouvez accéder aux imprimantes partagées depuis le panneau de commande Windows standard de l'imprimante.

Fin de partage d'une imprimante

Vous pouvez mettre fin au partage d'une imprimante à tout moment. Les ordinateurs affiliés sur lesquels l'imprimante est installée ne pourront plus imprimer dessus.

Pour mettre fin au partage d'une imprimante :

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

En tant que membre du réseau géré, vous pouvez accéder aux imprimantes partagées sur le réseau. Pour cela, vous devez installer le pilote utilisé par l'imprimante. Si le propriétaire de l'imprimante cesse de la partager une fois que vous avez installé le pilote, vous ne pouvez plus imprimer sur cette imprimante.

Pour installer une imprimante réseau disponible :

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**.

CHAPITRE 23

Référence

Le glossaire répertorie et définit les termes de sécurité les plus utilisés dans les produits McAfee.

"A propos de McAfee" fournit des informations juridiques relatives à McAfee Corporation.

Glossaire

8

802.11

Ensemble de normes IEEE utilisées dans le cadre de la technologie des réseaux locaux sans fil. 802.11 qualifie une interface par liaison radio entre un client sans fil et une station de base ou entre deux clients sans fil. Les diverses spécifications de 802.11 comprennent 802.11a, une norme pour les réseaux allant jusqu'à 54 Mbits/s dans la bande des 5 GHz, 802.11b, une norme pour les réseaux allant jusqu'à 11 Mbits/s dans la bande des 2,4 GHz, 802.11g, une norme pour les réseaux allant jusqu'à 54 Mbits/s dans la bande des 2,4 GHz et 802.11i, une série de normes de sécurité pour tous les réseaux Ethernet sans fil.

802.11a

Extension de 802.11 qui s'applique aux réseaux locaux sans fil et envoie des données à un débit pouvant atteindre 54 Mbits/s dans la bande des 5 GHz. Même si le débit de transmission est plus rapide que celui du 802.11b, la distance couverte est inférieure.

802.11b

Extension du 802.11 qui s'applique aux réseaux locaux sans fil et assure une transmission à 11 Mbits/s dans la bande des 2,4 GHz. 802.11b est actuellement considéré comme la norme pour la communication sans fil.

802.11g

Extension du 802.11 qui s'applique aux réseaux locaux sans fil et assure une transmission pouvant atteindre 54 Mbits/s dans la bande des 2,4 GHz.

802.1x

Non compatible avec Wireless Home Network Security. Norme IEEE destinée à l'authentification sur les réseaux avec et sans fil, plus souvent utilisée avec les réseaux 802.11 sans fil. Cette norme assure une authentification performante et mutuelle entre un client et un serveur d'authentification. En outre, 802.1x peut fournir des clés WEP dynamiques par utilisateur et par session, en supprimant la charge administrative et les risques de sécurité liés aux clés WEP statiques.

A

adaptateur sans fil

Elément contenant le circuit qui permet à un ordinateur ou à un autre périphérique de communiquer avec un routeur sans fil (de se connecter à un réseau sans fil). Les adaptateurs sans fil peuvent être intégrés dans le circuit principal d'un matériel ou constituer un élément séparé à insérer dans un périphérique par le biais du port approprié.

adresse IP

Le numéro de protocole Internet (IP), ou adresse IP, est un numéro unique comportant quatre parties séparées par des points (par exemple, 63.227.89.66). Chaque ordinateur relié à Internet, depuis le serveur le plus important jusqu'au portable connecté via un téléphone cellulaire, possède un numéro IP unique. Tous les ordinateurs ne possèdent pas de nom de domaine, mais tous ont une adresse IP.

Voici quelques types d'adresses IP inhabituels :

- Adresses IP non routables Elles sont également appelées "Espace d'adressage IP privé". Ces adresses IP ne peuvent pas être utilisées sur Internet. Les blocs d'adresses IP privées sont 10.x.x.x, 172.16.x.x - 172.31.x.x et 192.168.x.x.
- Adresses IP de bouclage : ces adresses sont utilisées pour des tests. Le trafic envoyé vers ce bloc d'adresses IP retourne directement au périphérique ayant généré le paquet. Il ne quitte donc jamais le périphérique et sert essentiellement à des tests matériels et logiciels. Le bloc d'adresses IP en boucle est 127.x.x.x.

Adresse IP nulle : il s'agit d'une adresse non valide. Elle apparaît lorsque l'adresse IP du trafic était vierge. De toute évidence, cela est anormal et signifie souvent que l'expéditeur masque délibérément l'origine du trafic. L'expéditeur n'aura de réponse à son trafic que si le paquet est reçu par une application en mesure de comprendre son contenu, incluant notamment des instructions spécifiques à cette application. Toute adresse commençant par 0 (0.x.x.x) est une adresse nulle. Par exemple, 0.0.0.0 est une adresse IP nulle.

adresse MAC (Media Access Control)

Adresse de bas niveau affectée au périphérique physique qui accède au réseau.

analyse des images

Empêche l'affichage des images potentiellement inappropriées. Les images sont bloquées pour tous les utilisateurs, à l'exception du groupe d'âge adulte.

analyse en temps réel

Analyse des fichiers à la recherche de virus ou d'autres activités lorsque vous ou votre ordinateur y accédez.

archivage complet

Archiver un jeu complet de données en fonction des types des fichiers de surveillance et des emplacements que vous avez déjà configurés.

archivage rapide

Archivage des seuls fichiers de surveillance modifiés depuis le dernier archivage complet ou rapide.

archive

Copie locale de vos fichiers de surveillance sur CD, DVD, lecteur USB, disque dur externe ou disque réseau.

archive

Copie locale de vos fichiers de surveillance sur CD, DVD, lecteur USB, disque dur externe ou disque réseau.

attaque en force

Aussi appelé craquage en force ; méthode par tâtonnement utilisée par les applications pour décoder des données chiffrées, comme des mots de passe, en employant une méthode exhaustive (en utilisant la force) plutôt qu'avec des stratégies intellectuelles. Tout comme un criminel pourrait entrer dans un coffre-fort en testant de nombreuses combinaisons possibles, une application de craquage en force passe par toutes les combinaisons possibles de caractères autorisés, les unes à la suite des autres. Ces méthodes en force sont jugées infaillibles mais longues.

attaque par dictionnaire

Ces attaques testent une série de mots dans une liste pour obtenir le mot de passe d'une personne. Les attaquants ne tentent pas manuellement toutes les combinaisons : ils disposent d'outils qui essaient d'identifier automatiquement le mot de passe.

attaque par immixtion

Ici, l'attaquant intercepte les messages dans un échange de clé publique, puis les retransmet, en substituant sa propre clé publique par celle demandée, de sorte que les deux parties aient toujours l'impression de communiquer directement entre elles. L'attaquant utilise un programme qui semble être le serveur pour le client et le client pour le serveur. L'attaque peut être simplement utilisée pour obtenir l'accès aux messages ou permettre à l'attaquant de les modifier avant de les retransmettre. Le terme anglais (man-in-the-middle, l'homme au milieu) est issu du jeu de ballon dans lequel des personnes tentent de s'envoyer la balle tandis qu'une autre, située entre deux, tente de l'intercepter.

authentification

Processus d'identification d'une personne, généralement basé sur un nom d'utilisateur et un mot de passe. L'authentification permet de s'assurer que la personne est bien celle qu'elle prétend être mais n'apporte aucune information sur ses droits d'accès.

B

bande passante

Quantité de données pouvant être transmise sur une période donnée. Pour les périphériques numériques, la bande passante est généralement exprimée en bits par seconde (bits/s) ou en octets par seconde. Pour les périphériques analogiques, la bande passante est exprimée en cycles par seconde ou en Hertz (Hz).

bibliothèque

Zone de stockage en ligne des fichiers publiés par les utilisateurs de Data Backup. La bibliothèque est un site Web sur Internet, accessible à toute personne disposant d'un accès Internet.

C

carte du réseau

Dans Network Manager, il s'agit d'une représentation graphique des ordinateurs et des autres composants de votre réseau domestique.

cartes adaptateur sans fil PCI

Carte permettant de connecter un ordinateur de bureau à un réseau. La carte se branche dans un connecteur d'extension PCI de l'ordinateur.

cartes adaptateur sans fil USB

Cartes qui fournissent une interface série Plug and Play évolutive. Cette interface assure une connexion sans fil standard, à faible coût, pour des périphériques tels que des claviers, des souris, des manettes de jeu, des imprimantes, des scanners, des périphériques de stockage et des Webcams.

certifié Wi-Fi

Tous les produits testés et approuvés comme des produits certifiés Wi-Fi (une marque déposée) par la Wi-Fi Alliance sont certifiés compatibles les uns avec les autres, même s'ils proviennent de différents fabricants. Un utilisateur disposant d'un produit certifié Wi-Fi peut utiliser n'importe quelle marque de point d'accès avec toute autre marque de matériel client également certifié. Toutefois, d'ordinaire, tout produit Wi-Fi utilisant la même fréquence radio (par exemple 2,4 GHz pour 802.11b ou 11g, 5 GHz pour 802.11a) fonctionne avec n'importe quel autre, même s'il n'est pas certifié Wi-Fi.

cheval de Troie

Programmes qui prétendent être des applications inoffensives. Les chevaux de Troie ne sont pas des virus, car ils ne se répliquent pas, mais ils sont tout aussi ravageurs.

chiffrement

Processus de transformation de données, de texte en code, qui les obscurcit pour les rendre illisibles par les personnes ne sachant pas les déchiffrer.

clé

Série de lettres ou de chiffres utilisée par deux périphériques pour authentifier une communication. Les deux doivent disposer de la clé. Voir aussi WEP, WPA, WPA2, WPA-PSK et WPA2- PSK.

client

Application qui s'exécute sur un ordinateur personnel ou une station de travail et qui s'appuie sur un serveur pour certaines de ses opérations. Un client de messagerie, par exemple, est une application qui permet d'envoyer et de recevoir des courriers électroniques.

client de messagerie

Compte de messagerie électronique. Par exemple, Microsoft Outlook ou Eudora.

compression

Processus permettant de compresser des données (fichiers) dans un format qui réduit l'espace nécessaire pour les stocker ou les transmettre.

compte de messagerie standard

La plupart des particuliers utilisent ce type de compte. Voir aussi compte POP3.

compte MAPI

Acronyme de Messaging Application Programming Interface. Spécification d'interface de Microsoft permettant à différentes applications de messagerie et de groupes de travail (messagerie électronique, messagerie vocale, télécopie...) de fonctionner sur un seul client, comme le client Exchange. Par conséquent, les entreprises exploitent généralement le système MAPI si elles utilisent Microsoft™ Exchange Server. Toutefois, de nombreuses personnes continuent à utiliser Microsoft Outlook pour gérer leurs e-mails personnels.

compte MSN

Acronyme de Microsoft Network. Service en ligne et portail Internet. Il s'agit d'un compte basé sur le Web.

compte POP3

Acronyme de Post Office Protocol 3. La plupart des particuliers utilisent ce type de compte. Il s'agit de la version actuelle de la norme Post Office Protocol, généralement utilisée sur les réseaux TCP/IP. Aussi appelée compte de messagerie standard.

contrôle parental

Paramètres permettant de configurer la classification du contenu. Celle-ci restreint l'affichage des sites Web et du contenu, ainsi que les limites horaires. En d'autres termes, elle gère la période et la durée de connexion à Internet. Selon la tranche d'âge et les mots-clés associés, Parental Controls permet globalement de restreindre, d'accorder ou de bloquer l'accès à certains sites Web.

cookie

Sur le Web, bloc de données qu'un serveur Web stocke sur un système client. Lorsqu'un utilisateur revient sur le même site Web, le navigateur renvoie une copie du cookie au serveur. Les cookies servent à identifier des utilisateurs, demander au serveur d'envoyer une version personnalisée de la page Web demandée, soumettre des informations de compte à l'utilisateur et réaliser d'autres tâches administratives.

Ils permettent au site Web de se souvenir de vous et de connaître le nombre de visiteurs, les dates de consultation et les pages consultées. Les cookies peuvent également aider une entreprise à personnaliser son site Web pour vous. De nombreux sites Web vous demandent d'entrer un nom d'utilisateur et un mot de passe avant de vous donner accès à certaines pages et envoient un cookie à votre ordinateur pour que vous n'ayez pas à vous connecter à chaque fois. Cependant, les cookies peuvent être utilisés à des fins malveillantes. Les agences de publicité en ligne utilisent souvent des cookies pour identifier les sites que vous consultez le plus souvent, puis placent des publicités sur vos sites Web favoris. N'acceptez que les cookies des sites auxquels vous faites confiance.

Bien que les cookies constituent une source d'informations pour des entreprises honnêtes, ils peuvent également constituer une source d'informations pour les pirates informatiques. De nombreux sites disposant de boutiques virtuelles enregistrent les numéros de carte de crédit et d'autres informations personnelles dans des cookies pour simplifier les achats de leurs clients. Malheureusement, des bogues de sécurité peuvent survenir et permettre à des pirates informatiques d'accéder aux informations des cookies stockés sur les ordinateurs des clients.

D

débordement de la mémoire tampon

Les débordements de tampon se produisent lorsque des programmes ou des processus suspects tentent de stocker dans un tampon (zone de stockage temporaire des données) une quantité de données plus importante que votre ordinateur ne peut en contenir, ce qui endommage ou écrase les données valides des tampons adjacents.

déni de service

Sur Internet, incident au cours duquel un utilisateur ou une entreprise est privé des services d'une ressource dont il s'attendait à disposer. Généralement, la perte de service réside dans l'indisponibilité d'un service réseau en particulier, comme la messagerie électronique, ou la perte temporaire de toutes les connexions et de tous les services du réseau. Dans le pire des cas, par exemple, un site Web auquel accèdent des millions de personnes peut, à l'occasion, être obligé de cesser ses opérations de manière temporaire. Une attaque de déni de service peut également détruire la programmation et les fichiers d'un système informatique. Même si elle est généralement intentionnelle et malveillante, une attaque de déni de service peut quelquefois survenir accidentellement. Une attaque de déni de service est un type de violation de la sécurité d'un système informatique qui n'entraîne généralement pas le vol d'informations ni une baisse de la sécurité. Ces attaques peuvent toutefois coûter beaucoup d'argent et de temps à la victime, qui peut être un particulier ou une société.

disque dur externe

Disque dur conservé en dehors du boîtier de l'ordinateur.

DNS

Acronyme de Domain Name System. Système hiérarchique par lequel les hôtes sur Internet possèdent des adresses de nom de domaine (comme bluestem.prairienet.org) et des adresses IP (comme 192.17.3.4). L'adresse du nom de domaine sert aux utilisateurs humains et elle est automatiquement traduite en adresse IP numérique, qui sert au logiciel de routage des paquets. Les noms DNS sont composés d'un domaine de niveau supérieur (.com, .org, .net...), d'un domaine de niveau secondaire (nom du site d'une entreprise, d'un organisme ou d'une personne) et, parfois, d'un ou de plusieurs sous-domaines (serveurs placés dans un domaine de niveau secondaire). Voir aussi serveur DNS et adresse IP.

domaine

Adresse d'une connexion réseau qui identifie le propriétaire de cette adresse dans un format hiérarchique : serveur.organisation.type. Par exemple, www.whitehouse.gov identifie le serveur Web de la Maison blanche, qui fait partie du gouvernement des Etats-Unis.

E

e-mail

Courrier, messages électroniques envoyés via Internet ou sur le réseau local ou étendu d'une entreprise. Les virus et chevaux de Troie sont de plus en plus transmis par les pièces jointes aux courriers électroniques sous la forme de fichiers EXE (exécutables) ou VBS (scripts Visual Basic).

emplacement de surveillance accrue

Dossier (et ses sous-dossiers) de votre ordinateur dont les changements sont surveillés par Data Backup. Si vous définissez un emplacement de surveillance accrue, Data Backup sauvegarde les types de fichiers de surveillance dans ce dossier ou ses sous-dossiers.

emplacements de surveillance de premier niveau

Dossier de votre ordinateur dont les changements sont surveillés par Data Backup. Si vous définissez un emplacement surveillé de premier niveau, Data Backup sauvegarde les types de fichiers de surveillance dans ce dossier, mais n'inclut pas ses sous-dossiers.

emplacements surveillés

Dossiers surveillés par Data Backup sur votre ordinateur.

en-tête

Informations ajoutées à la partie du message au cours de son cycle de vie. L'en-tête indique au logiciel Internet comment livrer votre message et où envoyer les réponses ; il lui fournit un numéro d'identification unique, ainsi que d'autres informations administratives. Exemples de champs d'en-tête : A, De, Cc, Date, Objet, ID du message et Reçu.

ESS (jeu de service étendu)

Ensemble de deux réseaux ou plus formant un même sous-réseau.

É

événements

événements provenant de 0.0.0.0

Si vous rencontrez des événements provenant de l'adresse IP 0.0.0.0, il existe deux causes probables : la première (la plus courante) est que, pour une raison indéterminée, votre ordinateur a reçu un paquet dans un format non valide. Internet n'est pas toujours fiable à 100 % et les paquets de ce type peuvent survenir. Comme Firewall détecte les paquets avant que ceux-ci ne soient validés par TCP/IP, il risque de les signaler comme événement.

L'autre situation se présente lorsque la source IP est usurpée ou fausse. Les paquets usurpés peuvent signifier que quelqu'un est à la recherche d'un cheval de Troie et teste votre ordinateur. Il est important de se souvenir que Firewall bloque la tentative.

événements provenant de 127.0.0.1

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

Quel que soit l'ordinateur que vous utilisez, 127.0.0.1 fera toujours référence à votre ordinateur local. Cette adresse est également appelée "localhost" (hôte local), car le nom d'ordinateur localhost sera toujours traduit par l'adresse IP 127.0.0.1. Cela signifie-t-il que votre ordinateur tente de s'auto-pirater ? Un cheval de Troie ou un logiciel espion cherche-t-il à prendre le contrôle de votre ordinateur ? C'est peu probable. De nombreux programmes légitimes utilisent l'adresse de bouclage à des fins de communication entre leurs composants. Par exemple, de nombreux serveurs de messagerie ou serveurs Web personnels sont configurables via une interface Web, généralement accessible depuis une adresse de type http://localhost/.

Cependant, Firewall autorise le trafic émanant de ces programmes ; par conséquent, si vous détectez des événements provenant de l'adresse IP 127.0.0.1, celle-ci est sans doute usurpée ou fausse. Les paquets usurpés indiquent généralement un utilisateur à la recherche d'un cheval de Troie. Il est important de se souvenir que Firewall bloque la tentative. A l'évidence, il sera inutile de signaler les événements provenant de l'adresse 127.0.0.01.

Ceci dit, certains programmes, notamment Netscape version 6.2 ou ultérieure, requièrent l'ajout de 127.0.0.1 à la liste **Adresses IP autorisées**. Ces composants du programme communiquent entre eux de telle manière que Firewall ne peut pas déterminer si le trafic est local ou non.

Par exemple, avec Netscape 6.2, vous devez autoriser l'adresse 127.0.0.1 pour pouvoir utiliser votre liste d'amis. Si vous détectez du trafic provenant de127.0.0.1 et que toutes les applications sur votre ordinateur fonctionnent normalement, vous pouvez bloquer ce trafic en toute sécurité. Toutefois, si un programme (tel que Netscape) rencontre des difficultés, ajoutez 127.0.0.1 à la liste des **adresses IP autorisées** de Firewall, puis regardez si cela résout le problème.

Si cela résout le problème, vous devrez faire un choix : si vous autorisez 127.0.0.1, votre programme fonctionnera, mais vous serez davantage exposé aux attaques par usurpation ; si vous n'autorisez pas cette adresse, votre programme ne fonctionnera pas, mais vous demeurerez protégé contre ce type de trafic malveillant.

événements provenant d'ordinateurs de votre réseau local

Pour la plupart des paramètres de réseaux locaux d'entreprise, vous pouvez autoriser tous les ordinateurs de votre réseau local.

événements provenant d'adresses IP privées

Les adresses IP au format 192.168.xxx.xxx, 10.xxx.xxx.xxx et 172.16.0.0 - 172.31.255.255 sont appelées adresses IP non routables ou privées. Ces adresses IP ne quittent jamais votre réseau et vous pouvez leur faire confiance la plupart du temps.

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

Si vous n'êtes pas connecté à un réseau privé et si vous détectez des événements provenant de ces plages d'adresses IP, il se pourrait que l'adresse IP source soit usurpée ou falsifiée. Les paquets usurpés indiquent généralement qu'un utilisateur recherche un cheval de Troie. Il est important de se souvenir que Firewall bloque la tentative.

Les adresses IP privées étant différentes des adresses IP sur Internet, il est inutile de signaler ces événements.

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. McAfee bloque les fenêtres instantanées chargées automatiquement lors de l'ouverture d'une page Web dans le navigateur et non celles qui apparaissent lorsque vous cliquez sur un lien.

groupes d'évaluation de contenu

Groupes d'âge auxquels appartient un utilisateur. Le contenu est évalué (à savoir qu'il est mis à disposition ou bloqué) en fonction du groupe auquel appartient l'utilisateur. Les groupes d'évaluation du contenu incluent : les jeunes enfants, les enfants, les pré-adolescents, les adolescents et les adultes.

Internet

Ensemble d'un grand nombre de réseaux interconnectés qui utilisent le protocole TCP/IP pour localiser et transférer des données. Initialement, il s'agissait d'une liaison entre des ordinateurs d'universités (à la fin des années 1960 et au début des années 1970) financée par le Ministère de la Défense des Etats-Unis et appelée ARPANET. Aujourd'hui, Internet est un réseau mondial qui regroupe près de 100 000 réseaux indépendants.

intranet

Réseau privé, généralement interne à une entreprise, de fonctionnement similaire à celui d'Internet. Désormais, les entreprises et les universités autorisent couramment des employés ou des étudiants travaillant en dehors des locaux à se connecter à leur intranet depuis un ordinateur autonome. Les Firewalls, ainsi que les procédures et les mots de passe de connexion, sont conçus pour en sécuriser l'accès.

itinérance

Capacité à se déplacer d'une zone de couverture d'un point d'accès à une autre, sans interruption du service, ni perte de connexion.

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 d'autorisation

Liste de sites Web auquel l'accès est autorisé car ils ne sont pas considérés comme frauduleux.

liste de blocage

Liste de sites Web considérés malveillants. Un site Web peut être placé sur une liste de blocage du fait d'une opération frauduleuse ou parce qu'il exploite une vulnérabilité du navigateur pour envoyer des programmes potentiellement indésirables à l'utilisateur.

MAC (Media Access Control ou Message Authenticator Code)

Pour le premier, voir adresse MAC. Le deuxième est un code servant à identifier un message donné (par exemple, un message RADIUS). Le code représente généralement un hachage cryptographique efficace du contenu du message, comprenant une valeur unique pour se prémunir contre les répétitions.

mot de passe

Code (généralement alphanumérique) qui permet d'accéder à votre ordinateur, à un programme ou à un site Web spécifique.

mot-clé

Mot pouvant être affecté à un fichier sauvegardé pour établir une relation ou une connexion avec d'autres fichiers auxquels le même mot-clé a été affecté. Les mots-clé facilitent la recherche des fichiers publiés sur Internet.

navigateur

Programme client qui utilise le protocole HTTP (Hypertext Transfer Protocol) pour adresser des requêtes aux serveurs Web sur Internet. Il affiche le contenu Internet sous forme graphique, afin de le rendre compréhensible par l'utilisateur.

NIC (Network Interface Card)

Carte qui se branche sur un ordinateur portable ou un autre périphérique pour le relier au réseau local.

noeud

Ordinateur unique relié à un réseau.

pare-feu

Système conçu pour empêcher les accès non autorisés à un réseau privé ou à partir de ce dernier. Les pare-feux peuvent être mis en oeuvre dans des configurations matérielles ou logicielles, ou une combinaison des deux. 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 entrant ou sortant de l'intranet passent par le pare-feu. Celui-ci étudie chaque message et bloque ceux qui ne répondent pas aux critères de sécurité spécifiés. Un pare-feu est considéré comme une première ligne de défense pour protéger les informations privées. Les données peuvent être chiffrées pour plus de sécurité.

partage

Opération permettant aux destinataires des courriers électroniques d'accéder à certains fichiers sauvegardés pendant une certaine période. Lorsque vous partagez un fichier, vous en envoyez la copie sauvegardée aux destinataires que vous choisissez. Ces derniers reçoivent un courrier électronique de Data Backup leur signalant que des fichiers ont été partagés avec eux. Le courrier comporte également un lien vers ces fichiers partagés.

passerelle intégrée

Dispositif qui associe les fonctions d'un point d'accès, d'un routeur et d'un pare-feu. Certains peuvent aussi comporter des améliorations de sécurité et des fonctions de pont.

Password Vault

Zone de stockage sécurisée des mots de passe personnels. Ainsi, vous êtes assuré que personne ne peut accéder à vos mots de passe (pas même un administrateur système ou McAfee).

phishing

(Prononcer "fishing"). Arnaque visant à voler des informations précieuses, comme les numéros de carte de crédit et de sécurité sociale, les ID utilisateur et les mots de passe. Un courrier électronique, paraissant officiel, est envoyé aux victimes potentielles en leur faisant croire qu'il provient de leur FAI, de leur banque ou de leur magasin. Les courriers peuvent être envoyés à des personnes apparaissant sur certaines listes ou sur n'importe laquelle et supposent qu'une certaine partie des destinataires auront réellement un compte dans cet organisme.

pixels invisibles

Petits fichiers graphiques pouvant s'insérer dans vos pages HTML et permettant à une source non autorisée de placer des cookies sur votre ordinateur. Ces cookies peuvent ensuite transmettre des informations à la source non autorisée. Les pixels invisibles sont aussi appelés balises Web, GIF transparents ou GIF invisibles.

point d'accès

Périphérique réseau permettant aux clients 802.11 de se connecter à un réseau local. Les points d'accès prolongent la gamme de service physique pour un utilisateur sans fil. Quelquefois appelé routeur sans fil.

point d'accès non fiable

Point d'accès dont une société n'autorise pas le fonctionnement. Bien souvent, les points d'accès non fiables ne se conforment pas aux stratégies de sécurité d'un réseau local sans fil. Ils autorisent une interface ouverte et non sécurisée à accéder au réseau de l'entreprise depuis l'extérieur de la structure physiquement contrôlée.

Dans un réseau local sans fil correctement sécurisé, les points d'accès non fiables sont plus dévastateurs que les utilisateurs malveillants. En effet, si des mécanismes efficaces d'authentification sont installés, les utilisateurs non autorisés qui tentent d'accéder à un réseau local sans fil ne parviendront pas à atteindre les ressources précieuses de l'entreprise. Des problèmes majeurs apparaissent toutefois lorsqu'un employé ou un pirate se connecte à un point d'accès non fiable. Le point d'accès autorise quasiment tous les périphériques équipés du 802.11 du réseau de l'entreprise à entrer. Ceci les rapproche dangereusement des ressources essentielles.

point d'accès sans fil

Emplacement géographique spécifique dans lequel un point d'accès assure des services de réseau large bande sans fil public aux visiteurs itinérants, grâce à un réseau sans fil. Les points d'accès sans fil sont souvent situés dans des lieux très fréquentés comme les aéroports, les gares ferroviaires, les bibliothèques, les marinas, les centres de conférence et les hôtels. Ils présentent généralement une plage de fonctionnement assez courte.

port

Endroit par lequel les informations entrent dans un ordinateur ou en sortent. Par exemple, un modem analogique traditionnel se connecte à un port série. Les numéros de port des communications TCP/IP sont des valeurs virtuelles qui permettent de séparer les données qui transitent dans des flux spécifiques à chaque application. Les ports sont attribués à des protocoles standard tels que SMTP ou HTTP pour permettre aux programmes de savoir sur quel port établir des connexions. Le port de destination des paquets TCP indique l'application ou le serveur recherchés.

PPPoE

Acronyme de Point-to-Point Protocol Over Ethernet. Utilisé par de nombreux fournisseurs de services DSL, le PPPoE accepte les couches de protocole et l'authentification généralement utilisées en PPP et permet l'établissement d'une connexion en point à point dans l'architecture généralement multipoint d'Ethernet.

programme potentiellement indésirable

Programmes comprenant les logiciels espions et publicitaires et les autres programmes qui accèdent à vos données personnelles et les transmettent sans votre autorisation.

protocole

Format accepté pour transmettre des données entre deux périphériques. Du point de vue de l'utilisateur, la seule chose à savoir sur les protocoles réside dans le fait que leur ordinateur ou leur périphérique doit accepter le protocole adéquat pour communiquer avec d'autres ordinateurs. Le protocole peut être mis en place dans le matériel ou dans le logiciel.

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. Le proxy joue le rôle d'intermédiaire pour l'ensemble des ordinateurs internes afin de protéger les identités réseau tout en fournissant un accès à Internet. Voir aussi serveur proxy.

publier

Mettre à disposition du public, sur Internet, un fichier sauvegardé.

quarantaine

Mise à l'écart des fichiers suspects détectés. L'utilisateur peut alors entreprendre l'action appropriée.

RADIUS (Remote Access Dial-In User Service)

Protocole assurant l'authentification des utilisateurs, généralement dans le contexte d'un accès distant. Initialement défini pour être utilisé avec des serveurs d'accès distant à commutation, le protocole sert maintenant dans divers environnements d'authentification, notamment l'authentification 802.1x d'un secret partagé de l'utilisateur d'un WLAN.

référentiel de sauvegarde en ligne

Emplacement sur le serveur en ligne pour stocker les fichiers de surveillance après leur sauvegarde.

réseau

Connexion de plusieurs ordinateurs.

réseau géré

Un réseau domestique comporte deux types de membres : des membres gérés et des membres non gérés. Les membres gérés autorisent les autres ordinateurs du réseau à surveiller l'état de leur protection McAfee, contrairement aux membres non gérés.

réseau local (LAN)

Réseau d'ordinateurs qui s'étend sur une zone relativement petite. La plupart des réseaux locaux sont limités à un seul bâtiment ou groupe de bâtiments. Un réseau local peut toutefois être relié à d'autres, quelle que soit la distance, par le téléphone et les ondes radio. Un système de réseaux locaux reliés de cette manière est appelé réseau étendu (WAN). La plupart des réseaux locaux relient des stations de travail et des ordinateurs, généralement par des concentrateurs ou des commutateurs simples. Chaque noeud (ordinateur) d'un réseau local possède sa propre unité centrale grâce à laquelle il exécute des programmes, mais il peut aussi accéder aux données et aux périphériques (comme les imprimantes) n'importe où sur le réseau. Ainsi, de nombreux utilisateurs peuvent partager des périphériques onéreux, comme des imprimantes laser, ou des données. Les utilisateurs peuvent aussi utiliser le réseau local pour communiquer entre eux, par exemple pour envoyer des messages électroniques ou discuter en direct.

réseau local sans fil (WLAN)

Voir aussi réseau local. Réseau local utilisant un support sans fil pour sa connexion. Un réseau local sans fil utilise des ondes radio hautes fréquences à la place des fils pour communiquer d'un noeud à un autre.

restauration

Récupération d'une copie d'un fichier à partir du référentiel de sauvegarde en ligne ou d'une archive.

routeur

Périphérique réseau qui transmet les paquets d'un réseau à un autre. Selon les tables de routage internes, les routeurs lisent chaque paquet entrant et décident ou non de le transmettre. L'interface à laquelle sont envoyés les paquets sortants du routeur peut être déterminée par une combinaison des adresses source et cible, ainsi que par les conditions actuelles du trafic, comme la charge, les coûts de la ligne et les lignes endommagées. Quelquefois appelé point d'accès.

sauvegarde

Copie des fichiers de surveillance sur un serveur sécurisé en ligne.

script

Elément capable de créer, copier ou supprimer des fichiers. Il peut également ouvrir votre registre Windows.

secret partagé

Voir aussi RADIUS. Protection des parties sensibles des messages RADIUS. Ce secret partagé est un mot de passe partagé entre l'authentificateur et le serveur d'authentification, de manière sécurisée.

serveur

Ordinateur ou logiciel qui fournit des services spécifiques aux logiciels exécutés sur d'autres ordinateurs. Le "serveur de messagerie" de votre FAI est un logiciel qui gère tous les messages entrants et sortants pour l'ensemble de ses utilisateurs. Un serveur sur un réseau local est un système matériel qui constitue le noeud principal du réseau. Il peut également exécuter des logiciels fournissant des services ou des données spécifiques à l'ensemble des ordinateurs clients qui y sont reliés, ou leur offrir d'autres fonctionnalités.

serveur DNS

Version abrégée de serveur de Domain Name System. Ordinateur capable de répondre à des requêtes de DNS. Le serveur DNS conserve une base de données d'ordinateurs hôtes et de leurs adresses IP correspondantes. Si on lui présente le nom apex.com, par exemple, le serveur DNS renvoie l'adresse IP de la société Apex imaginaire. Aussi appelé : serveur de nommage. Voir aussi DNS et adresse IP.

serveur proxy

Composant de Firewall qui gère le trafic Internet vers et depuis un réseau local (LAN). L'utilisation d'un serveur proxy améliore les performances par deux aspects : d'une part, il fournit des données fréquemment demandées, telles qu'une page Web et, d'autre part, il filtre les demandes et ignore celles que le propriétaire considère comme inappropriées (par exemple, les demandes d'accès non autorisées à des fichiers propriétaires).

serveur SMTP

Acronyme de Simple Mail Transfer Protocol. Protocole TCP/IP permettant de transmettre des messages d'un ordinateur à un autre sur un réseau. Ce protocole sert à router les courriers électroniques sur Internet.

SSID (Service Set Identifier)

Nom réseau pour les périphériques d'un sous-système d'un réseau local sans fil. Il s'agit d'une chaîne longue de 32 caractères en texte clair, ajoutée au début de chaque paquet de réseau local sans fil. Le SSID différentie entre eux les réseaux locaux sans fil pour que tous les utilisateurs puissent fournir le même SSID et accéder à un point d'accès donné. Un SSID refuse l'accès à tout périphérique client ne possédant pas de SSID. Par défaut toutefois, un point d'accès diffuse son SSID dans sa balise. Et même si la diffusion du SSID est désactivée, un pirate peut le détecter via une opération de reniflage.

SSL (Secure Sockets Layer)

Protocole développé par Netscape pour transmettre des documents privés sur Internet. SSL utilise une clé publique pour chiffrer des données transférées sur une connexion SSL. Netscape Navigator et Internet Explorer utilisent et acceptent tous deux le SSL et de nombreux sites Web utilisent le protocole pour obtenir des informations confidentielles sur l'utilisateur comme son numéro de carte de crédit. Par convention, les URL nécessitant une connexion SSL commencent par https au lieu de http.

synchroniser

Résoudre les incohérences entre des fichiers sauvegardés et ceux stockés sur votre ordinateur local. La synchronisation des fichiers a lieu lorsque la version du fichier dans le référentiel de sauvegarde en ligne est plus récente que la version du fichier sur d'autres ordinateurs. La synchronisation met à jour la copie du fichier sur l'ordinateur avec la version du fichier se trouvant dans le référentiel de sauvegarde en ligne.

SystemGuard

Les SystemGuards détectent les modifications non autorisées apportées à votre ordinateur et vous en avertissent.

texte brut

Message non chiffré.

texte chiffré

Données qui ont été chiffrées. Le texte chiffré est illisible tant qu'il n'a pas été converti en texte brut (déchiffré) à l'aide d'une clé.

TKIP (Temporal Key Integrity Protocol)

Méthode de réparation rapide pour surmonter les faiblesses inhérentes à la sécurité WEP, notamment pour la réutilisation des clés de chiffrement. TKIP modifie les clés temporaires tous les 10 000 paquets, pour offrir une méthode de distribution dynamique qui améliore considérablement la sécurité du réseau. Le processus TKIP (sécurité) démarre par une clé temporaire à 128 bits partagée entre les clients et les points d'accès. Il associe la clé temporaire à l'adresse MAC (celle de la machine cliente), puis ajoute un vecteur d'initialisation de 16 octets relativement large pour produire la clé qui chiffre les données. Cette procédure permet de s'assurer que chaque station utilise des flux de clé différents pour chiffrer les données. TKIP utilise le RC4 pour procéder au chiffrement. Le WEP utilise aussi le RC4.

types de fichiers de surveillance

Types de fichiers (par exemple, .doc, .xls, etc.) que Data Backup sauvegarde ou archive dans les emplacements surveillés.

URL

Localisateur de ressources universel. L'URL est le format standard d'adresse Internet.

usurpation d'adresse IP

Action de falsifier les adresses IP dans un paquet IP. Ceci est utilisé dans de nombreux types d'attaques, notamment la prise de contrôle des sessions, et sert souvent à falsifier les en-têtes des courriers électroniques de spam pour empêcher leur traçage.

ver

Virus qui se propage automatiquement et qui se fixe dans la mémoire active et peut utiliser les e-mails pour envoyer des copies de lui-même. Les vers reproduisent et consomment les ressources du système, ce qui ralentit les performances ou interrompt les tâches.

VPN (Virtual Private Network)

Réseau conçu pour utiliser les câbles publics afin de réunir des noeuds. Il existe par exemple plusieurs systèmes permettant de créer des réseaux en passant par Internet comme support du transport des données. Ces systèmes utilisent le chiffrement et d'autres mécanismes de sécurité pour s'assurer que seuls les utilisateurs autorisés aient accès au réseau et que les données ne puissent pas être interceptées.

wardriver

Interpolateurs munis d'ordinateurs portables, de logiciels spéciaux et de matériel improvisé, qui passent par les villes, les banlieues et les parcs d'activité pour intercepter le trafic d'un réseau local sans fil.

WEP (Wired Equivalent Privacy)

Protocole de chiffrement et d'authentification défini dans le cadre de la norme 802.11. Les premières versions sont basées sur des chiffrements RC4 et présentent des faiblesses considérables. WEP tente d'apporter un minimum de sécurité en chiffrant les données sur des ondes radio pour qu'elles soient protégées lors de leur transfert d'un point d'extrémité à un autre. On a toutefois découvert que WEP n'est pas aussi sûr qu'on le pensait.

Wi-Fi (Wireless Fidelity)

Terme générique utilisé pour désigner tout type de réseau 802.11, qu'il s'agisse de 802.11b, 802.11a, double bande, etc. Le terme est utilisé par la Wi-Fi Alliance.

Wi-Fi Alliance

Organisation constituée des principaux fournisseurs d'équipements et logiciels sans fil, avec pour mission de (1) certifier tous les produits basés sur 802.11 à des fins de compatibilité et (2) promouvoir le terme Wi-Fi comme marque internationale sur tous les marchés, pour tous les produits de réseaux locaux sans fil basés sur du 802.11. L'organisation agit comme un consortium, un laboratoire de test et un centre d'informations pour les fournisseurs qui veulent promouvoir la compatibilité et la croissance du marché.

Même si tous les produits 802.11a/b/g sont appelés Wi-Fi, seuls ceux qui ont réussi le test de Wi-Fi Alliance sont autorisés à se qualifier de certifiés Wi-Fi (une marque déposée). Les produits qui réussissent le test doivent avoir un sceau d'identification sur leurs emballages indiquant qu'ils sont certifiés Wi-Fi et précisant la bande de fréquence radio utilisée. Ce groupe était anciennement connu sous le nom WECA (Wireless Ethernet Compatibility Alliance) mais a changé de nom en octobre 2002 pour mieux représenter la marque Wi-Fi qu'il souhaitait créer.

WPA (Wi-Fi Protected Access)

Norme de spécification qui augmente fortement le niveau de protection des données et le contrôle d'accès des systèmes de réseau local sans fil actuels et futurs. Conçu pour fonctionner sur le matériel existant sous la forme d'une mise à niveau du logiciel, le WPA est issu de la norme IEEE 802.11i avec laquelle il est compatible. Lorsqu'il est correctement installé, il offre aux utilisateurs d'un réseau local sans fil un niveau de certitude élevé sur le fait que leurs données sont protégées et que seuls les utilisateurs autorisés à utiliser le réseau y auront accès.

WPA-PSK

Mode WPA spécial, conçu pour les utilisateurs à domicile qui n'ont pas besoin de la sécurité nécessaire aux entreprises et n'ont pas accès à des serveurs d'authentification. Avec ce mode, l'utilisateur à domicile entre manuellement le mot de passe de départ pour activer l'accès Wi-Fi protégé en mode clé pré-partagée et doit régulièrement modifier le mot de passe sur chaque ordinateur sans fil et point d'accès. Voir aussi WPA2-PSK et TKIP.

WPA2

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

WPA2-PSK

Voir aussi WPA-PSK et WPA2. Norme similaire à WPA-PSK, basée sur la norme WPA2. Cette norme établit, parmi ses fonctions générales, que les périphériques acceptent souvent plusieurs modes de chiffrement (comme AES, TKIP) simultanément, tandis que les plus anciens n'acceptaient généralement qu'un mode de chiffrement à la fois (tous les clients devaient 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 offre aux particuliers, aux entreprises, au secteur public et aux prestataires de service la capacité de bloquer les attaques, de prévenir les perturbations et d'assurer et d'améliorer régulièrement leur sécurité.

Copyright

Index

8

A

F

G

I

L

M

N

O

P

Q

R

S

T

U

V

W