symantec™

Norton Internet Security 3.0™

Pour Macintosh®

Guide de l'utilisateur

Guide de l'utilisateur de Norton Internet Security™ pour Macintosh®

Documentation relative à la version 3.0

PN : 10067316

Copyright

Marques commerciales

Imprimé en Irlande.

10 9 8 7 6 5 4 3 2 1

Table des matières

Section 1 Premiers pas

Chapitre 3 Principes de fonctionnement de Norton Internet Security

Chapitre 4 Protection contre les nouvelles menaces

Section 3 Norton AntiVirus

Chapitre 10 Protection des disques, des fichiers et des données contre les virus

Chapitre 11 Que faire en cas de détection de virus ?

1

Premiers pas

A propos de Norton Internet Security pour Macintosh

1

Norton Internet Security pour Macintosh offre :

- Un système complet de prévention, de détection et d'élimination des virus.
- Une protection complète contre les intrusions.
- Le blocage des publicités, la protection des données confidentielles et le blocage des sites Web non autorisés.

Pour ce faire, le logiciel inclut Norton AntiVirus pour Macintosh, Norton Personal Firewall pour Macintosh et Norton Privacy Control en un seul produit.

Nouveautés de Norton Internet Security

La version 3.0 de Norton Internet Security pour Macintosh comprend à présent :

- Une fenêtre principale, à partir de laquelle vous pouvez lancer tous les produits inclus dans le logiciel.
- Un assistant de configuration, qui vous guide dans les paramètres de vos *services* Internet et vous aide à configurer plus facilement le pare-feu, de façon à ce qu'il soit adapté à ces paramètres.
- Un système de configuration automatique de votre pare-feu, pour tous les services actifs. Une fois que vous avez installé Norton Internet Security, lorsque vous exécutez un service, la configuration automatique vérifie les paramètres du pare-feu et vous prévient si l'un d'eux risque d'interférer avec l'utilisation de ce service.

- Le rapport d'utilisateurs connectés, qui vous indique que d'autres ordinateurs sont connectés au vôtre.
- Des options de consignation et de notification des tentatives d'accès, qui peuvent être spécifiées individuellement pour chaque service de votre ordinateur.
- Les paramètres du pare-feu pour les connexions sortantes, afin de vous aider à contrôler l'utilisation de votre ordinateur et à contrer les programmes malveillants qui viseraient à envoyer des données sans votre accord.
- Norton QuickMenu, qui vous permet d'accéder à une barre d'outils pour le démarrage, la désactivation et l'activation de Norton Personal Firewall ; ainsi que pour l'activation et la désactivation de Norton Auto-Protect. Norton QuickMenu apparaît sous la forme du logo Symantec (rond noir et jaune) dans votre barre de menu.
- Des options de protection améliorées, telles que la protection contre les activités suspectes, destinées à bloquer la transmission de données comportant de fausses *adresses IP*, une option pour permettre l'accès aux services essentiels lorsque la protection *UDP* est activée ainsi qu'une option pour désactiver le support *FTP* actif.
- La possibilité de spécifier une adresse IP différente de celle de votre ordinateur pendant l'Autotest.
- Une protection antivirus complète pour Mac OS X et Classic, en une seule version.
- La mise en quarantaine des fichiers infectés qui ne peuvent pas être réparés.
- L'examen au montage des disques amovibles, notamment des CD, Zip et disquettes, pour une meilleure sécurité de vos données
- Un éditeur d'outils sous Norton AntiVirus, qui permet un accès personnalisé et optimisé à vos outils antivirus
- L'identification et la réparation des virus Windows et DOS dans les fichiers et archives, évitant que des virus PC cachés puissent s'implanter dans votre ordinateur et se disséminer vers des ordinateurs Windows
- L'examen et la réparation de fichiers au sein des archives, à l'exclusion de Stuffit, sans sollicitation de l'utilisateur

Menaces sur Internet

Internet offre tout un monde d'informations et de connexions qui paraissaient impossibles auparavant, mais il est également source de nombreux dangers, divers et variés, pour votre ordinateur. Ceux-ci incluent les virus, les attaques de hackers, la perte de données personnelles et les éléments indésirables qui se glissent dans votre navigateur.

Fonctionnement des virus

Un virus informatique est un programme parasite écrit dans le but de modifier à votre insu la façon dont votre ordinateur fonctionne. Un virus se duplique et attache ses propres copies à vos fichiers et, lorsqu'il est activé, peut endommager vos données, causer des pannes intempestives ou afficher des messages inattendus.

Les virus informatiques infectent les fichiers système (fichiers situés dans le dossier Système que le Macintosh utilise pour démarrer) et les documents créés par des logiciels faisant appel à des *macros*. Les extensions système (programmes qui se chargent en mémoire au démarrage d'un Macintosh) et les applications de type Microsoft Office, par exemple, sont considérées comme des fichiers système sous MacOS.

Certains virus sont programmés pour corrompre les programmes, effacer des fichiers ou formater les disques.

Pour plus d'informations sur les virus, consultez l'aide en ligne.

Risques encourus en l'absence de pare-feu

Lorsque vous êtes connecté à Internet ou à un autre réseau, tous les utilisateurs connectés à ce réseau ont la possibilité d'accéder à votre ordinateur. Cette situation peut s'avérer dangereuse si vous avez activé le partage de fichiers ou le lien entre applications, car votre ordinateur devient ainsi une cible privilégiée pour les hackers.

Contrôle des informations stockées dans votre ordinateur

Vous conservez des informations confidentielles sur votre ordinateur, notamment des relevés financiers, des archives bancaires, des numéros d'identification personnelle, etc. Si vous ne protégez pas ces informations, toute personne ayant accès à votre ordinateur, y compris un accès non autorisé, pourra les récupérer.

Lorsque vous êtes sur Internet, vous pouvez recevoir des informations que vous n'avez pas demandées. Celles-ci peuvent être simplement ennuyeuses (publicité) ou véritablement indésirables (sites Web inconvenants). Toutes ces données indésirables exigent une réponse de votre part, sous quelque forme que ce soit, ce qui vous ralentit dans votre navigation.

Norton Internet Security vous aide à éliminer ces menaces

Avec Norton Internet Security, vous installez trois outils puissants de contre-attaque face aux *menaces* Internet : Norton AntiVirus, Norton Personal Firewall et Norton Privacy Control.

Fonctionnement de Norton AntiVirus

Norton AntiVirus recherche la présence de virus connus et inconnus sur votre ordinateur. Un virus connu est un virus qui peut être détecté et identifié par son nom. Un virus inconnu est un virus pour lequel Norton AntiVirus ne possède pas encore de définition.

Norton AntiVirus protège votre ordinateur contre ces deux types de virus, en recourant à des *définitions de virus* pour détecter les virus connus et à la technologie Bloodhound pour détecter les virus inconnus. Les définitions de virus et la technologie Bloodhound sont sollicitées lors des examens programmés et manuels ainsi que par Auto-Protect dans le cadre de la surveillance permanente de votre ordinateur.

Fonctionnement de Norton Personal Firewall

Norton Personal Firewall place un pare-feu entre votre ordinateur et Internet. Les applications pare-feu sont des filtres qui bloquent ou autorisent les connexions sur Internet. En filtrant les connexions, les pare-feu protègent l'ordinateur des activités Internet malveillantes.

Norton Personal Firewall s'appuie sur les paramètres d'accès pour déterminer s'il convient d'autoriser ou de bloquer les connexions, entrantes ou sortantes. Vous pouvez modifier ces paramètres, en autorisant ou en bloquant l'accès à votre ordinateur par d'autres ordinateurs et en autorisant ou en bloquant les connexions sortantes de votre ordinateur.

Vous spécifiez les *services* (partage Web ou partage de fichiers, par exemple) et le type de connexion que vous souhaitez protéger. Vous pouvez autoriser ou refuser tout accès à un service particulier ou encore autoriser ou refuser l'accès à un service à partir de certains ordinateurs ou l'accès d'un service à certains ordinateurs. Vous pouvez bloquer tous les accès au partage de fichiers, par exemple, tout en autorisant les accès au partage Web sur les ordinateurs appartenant aux utilisateurs que vous connaissez.

Comment identifier les ordinateurs bénéficiant d'autorisations d'accès

En règle générale, l'octroi d'autorisations d'accès à votre ordinateur à d'autres utilisateurs est totalement inutile. Certaines configurations et situations de partage de fichiers ou de partage Web exigent cependant l'attribution de droits d'accès, par exemple :

- Vous possédez deux ordinateurs en réseau ou plus et l'un d'eux au moins bénéficie d'un d'accès à Internet. Dans ce cas, une copie de Norton Personal Firewall doit être installée sur chaque ordinateur bénéficiant d'une connexion à Internet, et l'accès doit se limiter aux autres ordinateurs du réseau.
- Vous avez créé sur votre ordinateur un site Web dont vous ne souhaitez autoriser l'accès qu'à certaines personnes. Norton Personal Firewall vous permet dans ce cas d'activer le partage Web pour tous les utilisateurs auxquels vous voulez octroyer un droit d'accès à votre site (les autres membres de votre famille, par exemple).
- Vous faites appel à un fournisseur de services Internet gratuits, et l'établissement de la connexion peut exiger l'accès à un *port* de votre ordinateur. Si le *fournisseur* ne bénéficie pas de cet accès, vous ne pouvez plus l'utiliser.

Se reporter à « Réponse aux tentatives d'accès » à la page 69.

Par défaut, Norton Personal Firewall consigne dans un journal toutes les tentatives d'accès entrant, hormis celles liées au mode silencieux. Vous pouvez consulter la fenêtre Historique des accès à tout moment afin de voir si des utilisateurs indésirables tentent de se connecter à votre ordinateur.

Fonctionnement de Norton Privacy Control

Se reporter à « Utilisation de Norton Privacy Control » à la page 131.

Norton Privacy Control bloque les publicités de sites Web, les données confidentielles et les sites Web indésirables. Vous pouvez activer et personnaliser tout ou partie de ces outils, afin de contrôler de manière précise les éléments entrants et sortants de votre ordinateur. Vous pouvez également consulter des statistiques qui contrôlent que la protection est bien active.

Votre ordinateur contient-il des virus ?

Norton Internet Security installe Norton AntiVirus, Norton Personal Firewall et Norton Privacy Control.

Se reporter à « Procédures de mise à jour » à la page 47.

Une fois que vous avez installé Norton AntiVirus et redémarré l'ordinateur, vous êtes à l'abri des virus. Pour garantir la protection, laissez Auto-Protect activé pour que Norton AntiVirus trouve automatiquement les virus. Utilisez LiveUpdate pour vos protéger contre les nouveaux virus.

Se reporter à « Protection des disques, des fichiers et des données contre les intrusions » à la page 59.

Dès lors que vous avez installé Norton Personal Firewall et redémarré votre ordinateur, le pare-feu est en place et bloque par défaut toutes les tentatives d'accès entrant. Au cours de votre travail dans Norton Personal Firewall, vous pouvez, le cas échéant, ajuster vos paramètres d'accès.

Se reporter à « Utilisation de Norton Privacy Control » à la page 131.

Norton Privacy Control est installé avec l'option Blocage des publicités activée par défaut. Vous devez activer les fonctions Données confidentielles et Contrôle parental, pour que celle-ci prennent effet.

Comment éviter les virus

Procédez à la maintenance de vos fichiers et mettez à jour Norton AntiVirus de façon régulière.

Pour éviter les virus :

- Documentez-vous sur les derniers virus en date en vous connectant au site Web Symantec Security Response (http://www.symantec.fr/region/fr/avcenter/index.html) sur lequel vous trouverez de nombreuses informations, régulièrement mises à jour, sur les virus et sur la protection antivirale.
- Utilisez régulièrement LiveUpdate pour mettre à jour vos programmes et vos fichiers de *définitions de virus*.
- Faites en sorte que Norton AntiVirus Auto-Protect soit activé en permanence, afin d'éviter toute infection de votre ordinateur.
- Programmez des examens automatiques réguliers.

Se reporter à « Protection contre les nouvelles menaces » à la page 43.

A propos des autres produits présents sur le CD

Norton Internet Security inclut également Aladdin iClean, qui libère de l'espace disque et aide au contrôle de votre confidentialité en ligne en supprimant les éléments Web parasites tels que les *cookies*, les *fichiers cache* et les journaux. Aladdin iClean s'installe indépendamment de Norton Internet Security. Pour plus d'informations sur l'installation d'Aladdin iClean, consultez la section « Démarrage rapide d'iClean » à la page 151.

Installation de Norton Internet Security

2

Le programme d'installation de Norton Internet Security place Norton AntiVirus, Norton Personal Firewall et Norton Privacy Control sur votre ordinateur et définit des paramètres de protection par défaut de manière à ce que votre ordinateur soit protégé, après avoir été redémarré.

Vous trouverez sur le CD les versions Mac OS 8.1 à 9.x et Mac OS X de Norton Internet Security. Pour obtenir des instructions sur l'installation et l'utilisation de Norton Internet Security pour Mac OS 8.1 à 9.x, reportez-vous au fichier PDF intitulé *Guide de l'utilisateur de Norton Internet Security*, situé dans le dossier d'installation pour Mac OS 9 du CD.

Configuration requise

Norton Internet Security ne prend pas en charge les versions 10.0 à 10.1 de Mac OS X. Si vous souhaitez installer Norton Internet Security sous Mac OS X, vous devez passer à la version 10.1.5 de Mac OS X.

- Macintosh OS X 10.1.5
- Processeur G3 ou G4
- 128 Mo de RAM
- 150 Mo d'espace disque disponible pour l'installation (80 Mo si vous choisissez de ne pas installer la liste des adresses pour le blocage Web)
- Lecteur de CD-ROM ou de DVD-ROM
- Accès Internet

Avant l'installation

Le fichier Readme du CD Norton Internet Security pour Macintosh fournit des informations de dernière minute et des conseils de dépannage que vous devez lire attentivement avant de procéder à l'installation de Norton Internet Security.

Lecture du fichier Readme

Ce fichier fournit un récapitulatif des nouveautés et des modifications apportées à Norton Internet Security, des versions condensées de procédures clés et des conseils d'ordre technique.

Pour lire le fichier Readme

1. Insérez le CD de Norton Internet Security pour Macintosh dans votre lecteur de CD-ROM.
2. Dans la fenêtre du CD, ouvrez le dossier **Installation pour OS X**.
3. Cliquez deux fois sur le fichier **Readme** pour l'ouvrir.

Installation

Installez Norton Internet Security pour Macintosh à partir du CD fourni.

Norton Internet Security pour Mac OS X protège aussi bien l'environnement Mac OS X que l'environnement Classic.

La procédure d'installation requiert la saisie d'un mot de passe d'administrateur. En cas de doute sur votre type de connexion, vous pouvez le vérifier dans les Préférences Système.

Pour vérifier votre type de connexion

1. Dans le menu Pomme, cliquez sur **Préférences Système**.
2. Choisissez l'une des options suivantes :
   - Dans Mac OS X, version 10.2 et supérieure, cliquez sur **Comptes**.
   - Dans Mac OS X, version 10.1.5, cliquez sur **Utilisateurs**.

   Vos nom et type de connexion s'affichent.

Pour installer Norton Internet Security pour Macintosh

1 Insérez le CD de Norton Internet Security pour Macintosh dans votre lecteur de CD-ROM.
Si la fenêtre du CD ne s'ouvre pas automatiquement, cliquez deux fois sur l'icône de CD pour l'ouvrir.

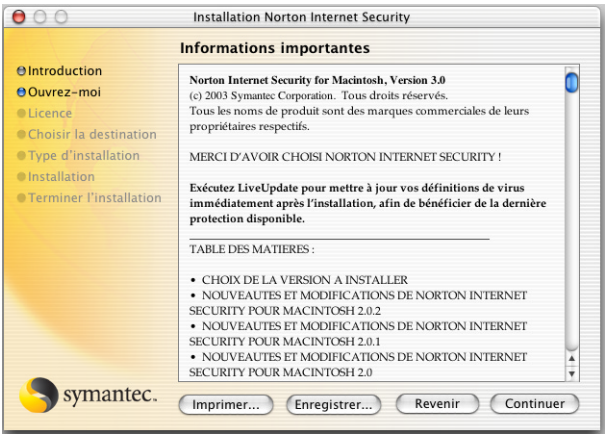
2 Dans la fenêtre du CD, ouvrez le dossier **Installation pour OS X**.

3 Cliquez deux fois sur **Installation de Norton Internet Security**.

Si vous installez Norton Internet Security sous Mac OS X 10.1.5, la fenêtre d'authentification n'apparaît pas automatiquement. Cliquez sur le cadenas dans l'angle inférieur gauche de la fenêtre d'autorisation pour ouvrir la fenêtre d'authentification et poursuivre le reste de la procédure.

4 Dans la fenêtre d'authentification, saisissez votre mot de passe d'administrateur, puis cliquez sur **OK**.

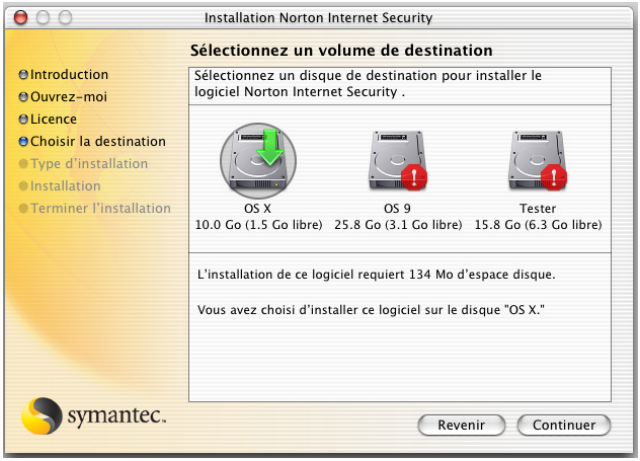
5 Dans la fenêtre de Bienvenue au programme d'installation de Norton Internet Security, cliquez sur **Continuer**.



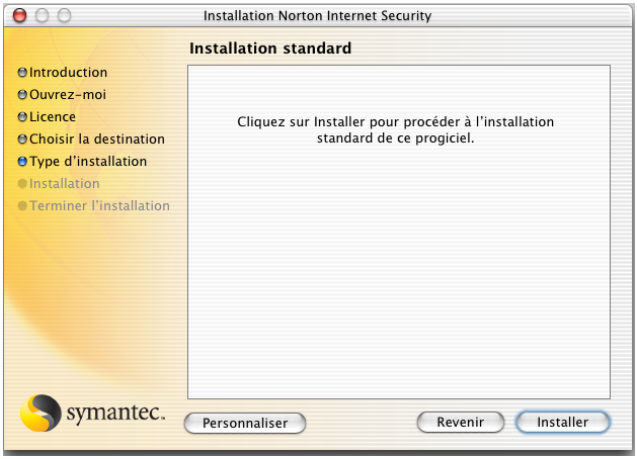
6 Parcourez le fichier Readme, puis cliquez sur **Continuer**.

7 Dans la fenêtre du contrat de licence, cliquez sur **Continuer**.

8 **Acceptez** les termes du contrat de licence.
En cas de refus, vous ne pouvez pas poursuivre l'installation.



9 Sélectionnez le disque sur lequel vous souhaitez installer Norton Internet Security, puis cliquez sur **Continuer**.



10 Dans la fenêtre Type d'installation, vous pouvez choisir divers éléments :

- Pour procéder à une installation complète, choisissez **Installer**. Si vous avez d'autres produits Symantec installés sur votre ordinateur, ce bouton peut indiquer Mise à niveau.
- Pour afficher la liste des composants installés ou pour ne pas installer la liste d'adresses pour le blocage Web, cliquez sur **Personnaliser**.
  Lorsque vous avez fini de parcourir la liste, cliquez sur **Installation**.

11 Dans la zone de dialogue de vérification, cliquez sur **Poursuivre l'installation**.

12 Choisissez si vous souhaitez exécuter LiveUpdate pour vous assurer que le logiciel est à jour.

13 Lorsque l'installation est terminée, cliquez sur **Redémarrer**.

Après l'installation

Après avoir installé Norton Internet Security, différentes possibilités s'offrent à vous :

Tâche	Informations complémentaires
Redémarrer votre ordinateur.	Se reporter à « Redémarrage de votre ordinateur » à la page 25.
Enregistrer votre logiciel.	Se reporter à « Enregistrement de Norton Internet Security » à la page 25.
Consulter les informations de dernière minute sur votre logiciel. Pour ce faire, servez-vous du lien Internet situé dans le dossier de Norton Internet Security.	Se reporter à « Informations de dernière minute » à la page 26.
Découvrir les fonctions et programmes complémentaires fournis sur le CD.	Se reporter à « Contenu du CD » à la page 27.

Redémarrage de votre ordinateur

La protection anti-intrusion et antivirus prend effet dès que vous redémarrez l'ordinateur après avoir installé Norton Internet Security. Norton Auto-Protect et les extensions Norton Personal Firewall et Norton Privacy Control se chargent à chaque démarrage de l'ordinateur, afin d'offrir une protection active, à moins que vous ne choisissiez de les désactiver.

En cas de problème d'éjection du CD

Si vous ne parvenez pas à éjecter le CD après avoir redémarré votre ordinateur, essayez les solutions suivantes :

- Appuyez sur le bouton d'éjection du lecteur de CD-ROM lorsque le carillon correspondant au redémarrage de votre Macintosh retentit.
- Sur les modèles Macintosh équipés d'un lecteur de CD-ROM à fente, appuyez sur le bouton de la souris pendant le démarrage pour éjecter le CD.

Enregistrement de Norton Internet Security

Votre connexion Internet vous permet d'enregistrer Norton Internet Security pour Macintosh par l'intermédiaire d'Internet.

Pour effectuer l'enregistrement sur Internet

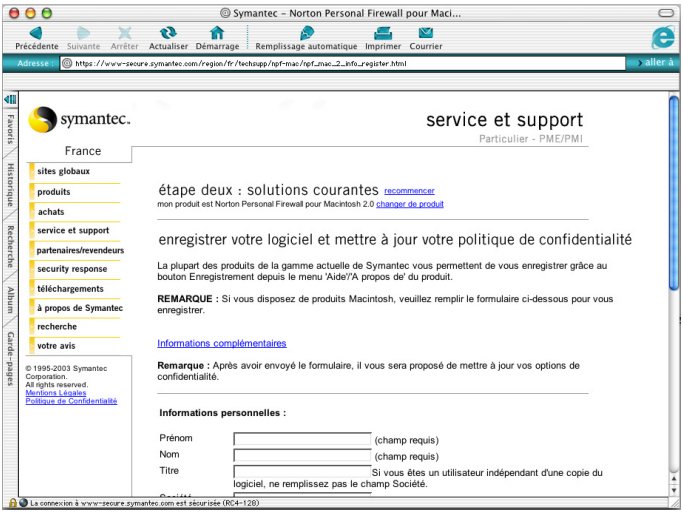
Se reporter à « Si vous vous connectez à Internet via America Online » à la page 27.

1. Connectez-vous à Internet.
   Si vous utilisez America Online (AOL) pour vos connexions Internet, vous devez tout d'abord ouvrir une session AOL.
2. Dans le dossier de Norton Solutions, cliquez deux fois sur **Enregistrer votre logiciel**.

   En principe, votre navigateur Internet par défaut affiche la page Service et support de Symantec.
3. Dans la page Service et support, cliquez sur **Particulier – PME/PMI**.
4. Sur la page d'enregistrement du logiciel, cliquez sur **Norton Internet Security pour Macintosh**.

5 Sélectionnez la version de votre produit

6 Cliquez sur **continuer**.



7 Dans la page d'enregistrement de Norton Internet Security pour Macintosh, saisissez toutes les informations requises.

8 Cliquez sur **Envoyer l'enregistrement**.

Informations de dernière minute

Norton AntiVirus installe un lien vers les informations de dernière minute. Ce lien vous permet de consulter les dernières informations relatives au logiciel que vous avez installé.

Pour consulter les dernières informations

Se reporter à « Si vous vous connectez à Internet via America Online » à la page 27.

1 Connectez-vous à Internet.
Si vous utilisez America Online (AOL) pour vos connexions Internet, vous devez tout d'abord ouvrir une session AOL.

2 Dans le dossier de Norton Solutions, cliquez deux fois sur **Nouvelles de dernière minute**.


Nouvelles de dernière minute

En principe, votre navigateur Internet par défaut affiche la page de produits Symantec.

Si vous vous connectez à Internet via America Online

Si vous utilisez le *fournisseur de services Internet* (*FSI*) America Online (AOL), vous devez vous connecter à AOL avant d'accéder à la page d'enregistrement ou à la page Nouvelles de dernière minute sur le site Web de Symantec.

Pour vous connecter au site Web de Symantec via AOL

1. Connectez-vous sur AOL.
2. Dans la page d'accueil d'AOL, cliquez sur le navigateur Internet AOL.
3. Déplacez le navigateur et toute autre fenêtre AOL ouverte afin de ne pas encombrer l'écran.
4. Dans la fenêtre de Norton Internet Security, effectuez l'une des opérations suivantes :
   - Cliquez deux fois sur **Enregistrer votre logiciel**. Procédez à l'enregistrement. Reportez-vous à la section « Enregistrement de Norton Internet Security » à la page 25.
   - Cliquez deux fois sur **Nouvelles de dernière minute**. Poursuivez la procédure pour prendre connaissance des dernières informations en date. Reportez-vous à la section « Informations de dernière minute » à la page 26.
5. Mettez fin à votre connexion avec AOL.

Contenu du CD

Outre les dossiers des programmes d'installation et les applications Norton Internet Security pour Macintosh, le CD contient un certain nombre d'éléments.

Dossier Aladdin iClean	Contient les programmes d'installation d'Aladdin iClean.
Dossier de documentation	Dans chaque dossier d'installation se trouve un dossier Documentation, qui contient le Guide de l'utilisateur au format PDF correspondant à la version contenue dans le dossier d'installation. En outre, le dossier Documentation pour la version Mac OS 9 contient les fichiers d'installation d'Adobe Acrobat Reader.

Désinstallation de Norton Internet Security

Si vous devez supprimer Norton Internet Security de votre ordinateur, utilisez le programme de désinstallation de Symantec qui se trouve sur le CD de Norton Internet Security pour Macintosh. La procédure est plus rapide si vous refermez tous les autres programmes avant de désinstaller Norton Internet Security.

La procédure de désinstallation exige la saisie d'un mot de passe d'administrateur. En cas de doute sur votre type de connexion, vous pouvez le vérifier dans les Préférences Système.

Pour vérifier votre type de connexion

1. Dans le menu Pomme, cliquez sur **Préférences Système**.
2. Choisissez l'une des options suivantes :
   - Dans Mac OS X, version 10.2 et supérieure, cliquez sur **Comptes**.
   - Dans Mac OS X, version 10.1.5, cliquez sur **Utilisateurs**.

   Vos nom et type de connexion s'affichent.

Pour désinstaller Norton Internet Security

1. Insérez le CD de Norton Internet Security pour Macintosh dans votre lecteur de CD-ROM.
   Si la fenêtre du CD ne s'ouvre pas automatiquement, cliquez deux fois sur l'icône de CD pour l'ouvrir.
2. Dans la fenêtre du CD, ouvrez le dossier **Installation pour OS X**.
3. Ouvrez le dossier **Désinstaller**.
4. Cliquez deux fois sur le programme de **désinstallation de Symantec**.
5. Dans la fenêtre de désinstallation des produits Symantec, cochez les produits que vous souhaitez désinstaller. Pour désinstaller totalement Norton Internet Security, cochez tous les éléments suivants :
   - Norton AntiVirus
   - Norton AntiVirus Auto-Protect
   - Norton Personal Firewall
   - Norton Privacy Control
   - Liste d'adresses de Norton Privacy Control
6. Cliquez sur **Désinstaller**.

7 Confirmez que vous souhaitez supprimer le produit.

8 Dans la fenêtre d'authentification, saisissez votre mot de passe d'administrateur, puis cliquez sur **OK**.

9 Dans la fenêtre qui affiche la liste des éléments supprimés, cliquez sur **Fermer**.

10 Dans la fenêtre de désinstallation des produits Symantec, cliquez sur **Quitter**.

Principes de fonctionnement de Norton Internet Security

3

Ce chapitre aborde les principes du fonctionnement de Norton Internet Security et vous indique comment obtenir des informations complémentaires sur cette application.

Lancement et arrêt de Norton Internet Security

Vous pouvez utiliser Norton Internet Security pour accéder à Norton AntiVirus, Norton Personal Firewall, Norton Privacy Control, Norton Scheduler et LiveUpdate, dans une seule fenêtre.

Si vous avez lancé un programme depuis la fenêtre principale de Norton Internet Security, vous devez arrêter de manière séparée Norton Internet Security et le programme ouvert. Quitter Norton Internet Security n'entraîne pas l'arrêt de l'autre programme.

Vous n'avez pas besoin de lancer les programmes inclus dans le pack Norton Internet Security pour être protégé. Faites-le uniquement lorsque vous souhaitez réaliser une tâche spécifique avec l'un d'eux.

Pour lancer Norton Internet Security

1 Dans le dossier Applications, cliquez deux fois sur **Norton Internet Security**.

2 Pour lancer l'un des programmes répertoriés, cliquez sur son icône.

Pour quitter Norton Internet Security

❖ Choisissez l'une des options suivantes :

- Dans le menu Norton Launcher, cliquez sur **Quitter Norton Launcher**.
- Appuyez sur **Commande-Q.**

Pour quitter un autre programme Symantec

1 Assurez-vous que le programme que vous souhaitez quitter est actif.

2 Appuyez sur **Commande-Q.**

Désactivation et activation des fonctions automatiques

Norton Internet Security charge Norton AntiVirus Auto-Protect et Norton Personal Firewall en mémoire lorsque vous démarrez votre ordinateur. Vous pouvez désactiver ces fonctions à tout moment.

Désactivation temporaire de Norton AntiVirus Auto-Protect

Par défaut, Norton AntiVirus Auto-Protect assure votre protection antivirale dès que vous démarrez votre ordinateur. Il recherche les virus dans les programmes au fur et à mesure de leur exécution et surveille, sur votre ordinateur, toute activité susceptible de trahir la présence d'un virus. Il n'est pas nécessaire de procéder à des examens Norton AntiVirus manuels tant que la fonction Auto-Protect reste activée. L'interception assurée par Auto-Protect empêche les virus de s'introduire sur votre disque.

Pour désactiver temporairement Auto-Protect

- Dans Norton QuickMenu, cliquez sur **Norton Auto-Protect > Désactiver Auto-Protect**.

Désactivation et activation de la protection anti-intrusion

A l'installation, Norton Personal Firewall est défini par défaut pour refuser l'accès à tous les *services TCP/IP*. En règle générale, les paramètres du logiciel assurent la protection requise, sans gêner les utilisateurs dans leur travail. Vous ne devez modifier ces paramètres par défaut que si vous voulez définir des règles d'accès spécifiques.

Vous pouvez interrompre la protection à tout moment en désactivant Norton Personal Firewall. La désactivation peut porter sur un laps de temps précis ou rester en vigueur jusqu'au redémarrage suivant.

La commande permettant de désactiver (ou d'activer) Norton Personal Firewall est accessible à partir de la fenêtre Configuration ou Norton QuickMenu.

Pour désactiver ou activer Norton Personal Firewall à partir de la fenêtre Configuration

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Personal Firewall**.
3. Dans la fenêtre Configuration, vous pouvez lancer diverses opérations :
   - Pour désactiver la protection, désélectionnez **Activer Norton Personal Firewall**.
   - Pour activer la protection, cochez **Activer Norton Personal Firewall**.
4. Ne désélectionnez l'option Activer Norton Personal Firewall que lorsque vous êtes sûr de vouloir désactiver le pare-feu.
5. Quittez Norton Personal Firewall.

Pour désactiver ou activer Norton Personal Firewall à partir de Norton QuickMenu

1. Dans la barre de menus Finder, cliquez sur l'icône Norton QuickMenu.
2. Dans Norton QuickMenu, cliquez sur **Norton Personal Firewall**.
3. Choisissez l'une des options suivantes :
   - Désactiver le pare-feu
   - Activer le pare-feu

Si vous avez besoin de désactiver Norton Personal Firewall temporairement

Vous pouvez également utiliser Norton QuickMenu pour désactiver la protection pendant un laps de temps donné.

Pour désactiver temporairement Norton Personal Firewall

1. Dans la barre de menus Finder, cliquez sur l'icône Norton QuickMenu.
2. Dans Norton QuickMenu, cliquez sur **Norton Personal Firewall > Désactiver temporairement le pare-feu**….
3. Dans la fenêtre Désactiver temporairement le pare-feu, tapez le nombre de minutes que vous souhaitez affecter à la désactivation de Norton Personal Firewall.
4. Cliquez sur **Réparer**.

Vérification des paramètres du pare-feu

Utilisez l'Assistant de configuration pour vérifier les paramètres généraux du pare-feu et les modifier, si nécessaire.

Pour vérifier les paramètres du pare-feu

1. Ouvrez Norton Personal Firewall.
   Lorsque vous ouvrez Norton Personal Firewall pour la première fois après l'installation, l'Assistant de configuration apparaît automatiquement.
2. Si l'Assistant de configuration n'apparaît pas, ouvrez le menu Outils et cliquez sur **Assistant de configuration**.
3. Dans l'écran d'accueil de l'Assistant de configuration, cliquez sur **Continuer**.
   Si des services Internet sont en cours d'exécution sur votre ordinateur, ils apparaissent dans la fenêtre Paramètres d'accès qui vous indique si le pare-feu en autorise ou non l'accès. Vous avez également la possibilité de demander à être averti au cas où les paramètres de votre ordinateur entreraient en conflit avec les paramètres du pare-feu. Par exemple, l'accès en partage de fichiers est refusé par défaut. Si vous avez choisi l'option de notification et que vous activez le partage de fichiers, Norton Personal Firewall vous demandera si vous souhaitez en autoriser l'accès.
4. Modifiez les paramètres dans la fenêtre Paramètres d'accès, si nécessaire.
5. Cliquez sur **Continuer**.
   Si vous choisissez d'autoriser l'accès à des services actifs, une deuxième fenêtre de Paramètres d'accès apparaît et vous donne la possibilité de limiter cet accès aux ordinateurs qui se trouvent sur votre réseau local.
6. Choisissez de limiter ou non l'accès, puis cliquez sur **Continuer**.
   La fenêtre Paramètres de protection vous indique si votre pare-feu est réglé sur une protection minimale, moyenne ou maximale et précise la façon dont ces niveaux sont définis, en fonction des paramètres activés ou non.
7. Dans la fenêtre Paramètres de protection, vous pouvez déplacer le curseur afin de modifier le niveau de protection.
8. Cliquez sur **Continuer**.
9. Dans la dernière fenêtre, cliquez sur **Terminé**.

Si vous souhaitez consulter la liste détaillée des paramètres du pare-feu, utilisez le rapport de synthèse.

Pour afficher le rapport de synthèse

1. Dans le menu Fichier, cliquez sur **Synthèse**.
2. Sélectionnez la façon dont vous souhaitez afficher le rapport de synthèse. Les options possibles sont les suivantes :

Trier la liste.	Cliquez sur l'un des en-têtes de colonne pour trier la colonne correspondante. Pour modifier le sens de tri, cliquez sur le triangle situé à droite de l'en-tête de colonne. Pour rétablir l'ordre d'origine, cliquez sur Restaurer l'ordre par défaut.
Modifier un paramètre.	Cliquez deux fois sur l'une des entrées du rapport de synthèse pour fermer le rapport et ouvrir la fenêtre dans laquelle vous pourrez modifier le paramètre correspondant.
Enregistrer la liste en tant que fichier texte.	Cliquez sur Enregistrer dans un fichier. Spécifiez un nom et un emplacement de fichier, puis cliquez sur Enregistrer.

3. Lorsque vous avez terminé, cliquez sur **Fermer**.

Personnalisation de Norton Internet Security

Vous pouvez personnaliser Norton QuickMenu et certaines barres d'outils de Norton Internet Security afin de les adapter à votre utilisation personnelle du produit.

Personnalisation de Norton QuickMenu

Norton QuickMenu apparaît sous la forme d'un logo Symantec jaune et noir du côté droit de la barre de menus dans le haut de l'écran. Si vous ne souhaitez pas que Norton QuickMenu apparaisse dans la barre de menus, vous pouvez le masquer. Vous pouvez également changer les options du menu.

Pour masquer Norton QuickMenu

1. Dans Norton QuickMenu, cliquez sur **Norton QuickMenu > Préférences**.
2. Dans la fenêtre Norton QuickMenu, désélectionnez **Activer Norton QuickMenu**.
3. Dans le menu Préférences système, cliquez sur **Quitter les préférences système**.

Pour afficher Norton QuickMenu

1. Dans le menu Pomme, cliquez sur **Préférences Système**.
2. Dans la fenêtre des préférences système, cliquez sur **Norton QuickMenu**.
3. Dans la fenêtre Norton QuickMenu, sélectionnez **Activer Norton QuickMenu**.
4. Dans le menu Préférences système, cliquez sur **Quitter les préférences système**.

Pour changer le contenu de Norton QuickMenu

1. Dans Norton QuickMenu, cliquez sur **Norton QuickMenu > Préférences**.
2. Dans la fenêtre de Norton QuickMenu, désélectionnez les options que vous ne voulez pas voir apparaître dans le menu.
3. Dans le menu Préférences système, cliquez sur **Quitter les préférences système**.

Personnalisation de vos barres d'outils

La fenêtre principale de Norton Internet Security et la fenêtre Configuration de Norton Personal Firewall, le journal Historique des accès et le rapport d'utilisateurs connectés disposent de barres d'outils que vous pouvez personnaliser selon vos besoins.

Pour personnaliser vos barres d'outils

1. Ouvrez Norton Internet Security.
2. Si vous souhaitez modifier la barre d'outils de la fenêtre Configuration de Norton Personal Firewall, du journal Historique des accès ou du rapport d'utilisateurs connectés, ouvrez la fenêtre contenant la barre d'outils que vous souhaitez modifier.
3. Dans le menu Fenêtre, cliquez sur **Personnaliser la barre d'outils**.

4 Dans la zone de dialogue de la barre d'outils, faites glisser les icônes à l'intérieur ou à l'extérieur de la barre d'outils, en haut de la fenêtre, jusqu'à obtenir l'ensemble désiré. Vous pouvez modifier l'emplacement d'une icône en la faisant glisser jusqu'à l'emplacement désiré.

5 Si vous souhaitez retrouver la barre d'outils d'origine, faites glisser l'ensemble des icônes par défaut en bas de la zone de dialogue de la barre d'outils.

6 Par défaut, toutes les icônes apparaissent avec un texte descriptif. Pour modifier l'affichage par défaut, sélectionnez l'une des options suivantes :

- Icône et texte
- Icône seule
- Texte seul

7 Lorsque la barre d'outils vous convient, cliquez sur **Terminé**.

Pour de plus amples informations

Les documentations de Norton Internet Security sont proposées dans trois formats différents :

Guide de l'utilisateur	Le Guide de l'utilisateur présente les concepts et procédures de base de toutes les fonctions de Norton Internet Security. Utilisez la copie imprimée du Guide de l'utilisateur si vous ne pouvez pas accéder à la documentation en ligne pour une raison quelconque. Les termes techniques imprimés en italique dans le Guide de l'utilisateur sont définis dans le glossaire, qui figure tant dans le PDF du Guide de l'utilisateur que dans l'Aide.
Aide intégrée	L'aide contient toutes les informations fournies dans le Guide de l'utilisateur, plus des détails sur les concepts et les procédures, ainsi qu'un glossaire pour la définition des termes techniques. Utilisez l'aide pour trouver une réponse aux questions qui se posent à vous pendant l'utilisation de Norton Internet Security. Se reporter à « Accès à l'Aide » à la page 39.
PDF	Le PDF est une version électronique du Guide de l'utilisateur, que vous pouvez utiliser si vous préférez consulter des informations en ligne dans un format livre ou si vous souhaitez des copies supplémentaires du Guide de l'utilisateur. Le PDF contient également un glossaire expliquant les termes techniques. Se reporter à « Accès au fichier PDF du Guide de l'utilisateur » à la page 40.

Outre cette documentation, le CD de Norton Internet Security pour Macintosh contient un fichier Readme. Consultez ce fichier avant d'installer Norton Internet Security afin de prendre connaissance des informations les plus récentes.

Enfin, vous pouvez également vous rendre sur le site Web de Symantec, pour obtenir des informations sur Norton Internet Security.

Accès à l'Aide

Si vous ouvrez l'Aide dans Norton Internet Security, le système d'aide Apple s'affiche, présentant une liste de rubriques. Lorsque vous ouvrez l'aide depuis la fenêtre principale, une liste complète des rubriques apparaît, dans laquelle vous pouvez rechercher celles relatives à Norton Internet Security. Si vous accédez à l'aide à partir d'une fonction spécifique, la liste des rubriques sera restreinte.

Pour accéder à l'aide

❖ Dans le menu Aide, cliquez sur **Aide d'Internet Security**.

Conseils pour visiter l'aide :

- Pour chercher une rubrique spécifique, tapez le terme voulu dans le champ de recherche situé dans le haut de la fenêtre d'aide, puis cliquez sur Demander.
- Les termes affichés en bleu et soulignés dans le texte sont définis dans le glossaire. Cliquez dessus pour en obtenir la définition. Cliquez sur la flèche vers la gauche pour retourner à la rubrique.
- Vous pouvez afficher les mêmes informations, que vous accédiez à l'aide à partir de la fenêtre principale ou d'une fonction spécifique.
- Des liens vers des rubriques connexes apparaissent à la fin de la rubrique.
- Certaines rubriques contiennent des liens qui ouvrent une fenêtre où vous pouvez exécuter la tâche décrite.

Accès au fichier PDF du Guide de l'utilisateur

Le Guide de l'utilisateur est disponible sur le CD sous forme de fichier PDF (Adobe Acrobat) imprimable.

Pour ouvrir le fichier PDF

1. Insérez le CD de Norton Internet Security pour Macintosh dans le lecteur de CD-ROM.
2. Dans la fenêtre du CD, cliquez deux fois sur le dossier **Installation pour Mac OS X**.
3. Dans le dossier d'installation pour OS X, cliquez deux fois sur le dossier **Documentation**.
4. Cliquez deux fois sur le fichier PDF du **Guide de l'utilisateur de Norton Internet Security**.

Vous pouvez également faire glisser le fichier PDF sur votre disque dur.

Conseils pour parcourir le PDF :

- Lorsque vous ouvrez le fichier PDF, la table des matières apparaît dans la colonne de gauche. Dans la table des matières, cliquez sur un titre pour accéder à la rubrique correspondante.
- Pour chercher une rubrique spécifique, utilisez la commande Chercher du menu Edition.
- Les termes affichés en bleu et en italiques dans le texte sont définis dans le glossaire. Cliquez dessus pour en obtenir la définition. Cliquez sur le bouton de retour à la page précédente pour retourner à la rubrique.

Ouverture du fichier Readme

Le fichier Readme inclus sur le CD Norton Internet Security pour Macintosh contient des informations de dernière minute sur votre nouveau logiciel.

Pour ouvrir le fichier Readme

1. Insérez le CD de Norton Internet Security pour Macintosh dans votre lecteur de CD-ROM.
2. Dans la fenêtre du CD, ouvrez le dossier **Installation pour OS X**.
3. Cliquez deux fois sur le fichier **Readme** pour l'ouvrir.

Exploration du site Web de Symantec

Le site Web de support Symantec fournit des informations détaillées Norton Internet Security. Vous pouvez y trouver des mises à jour, des correctifs, des articles de Base de connaissances et des outils d'éradication de virus.

Pour explorer le site de support de Symantec

1. Sur Internet, accédez à www.symantec.com/frsupport
2. Dans la page Service et support, sous Particulier – PME/PMI, cliquez sur **continuer**.
3. Dans la page pour particuliers et PME/PMI, cliquez sur **démarrez avec le support en ligne**.
4. Suivez les instructions du site Web pour obtenir les informations voulues.

Si vous ne trouvez pas ce que vous cherchez dans les pages de support en ligne, essayez une recherche sur le site Web.

Pour effectuer une recherche sur le site de support Symantec

1. Du côté gauche d'une page Web du site, cliquez sur **recherche**.
2. Tapez un mot ou une phrase correspondant le mieux à ce que vous recherchez.
   Pour obtenir des conseils sur la saisie du texte de recherche, cliquez sur **aide** dans le bas de la page.
3. Cochez la partie du site sur laquelle doit porter la recherche.
4. Cliquez sur **rechercher**.

Protection contre les nouvelles menaces

4

La première fois que vous installez votre produit Symantec et exécutez LiveUpdate, vous disposez des versions les plus récentes du produit et des fichiers de protection tels que la liste des sites Web inappropriés pour Norton Internet Security ou la liste des *définitions de virus* pour Norton AntiVirus.

A tout moment, des nouvelles *menaces* peuvent apparaître. De même, certaines mises à jour du système d'exploitation peuvent exiger des modifications d'un programme. Dans ces circonstances, Symantec fournit de nouveaux fichiers. Vous pouvez les obtenir en utilisant LiveUpdate.

En utilisant votre connexion Internet, LiveUpdate accède au serveur LiveUpdate de Symantec, il vérifie si des mises à jour sont disponibles, puis il les *télécharge* et les installe.

A propos des mises à jour de programmes

Les mises à jour de programmes apportent des améliorations mineures à un produit installé et sont généralement disponibles par *téléchargement* à partir d'un site Web. Vous ne devez pas les confondre avec les mises à niveau de produit, qui constituent de nouvelles versions d'un produit complet. Les mises à jour d'un programme qui remplacent certaines sections d'un logiciel existant sont appelées correctifs. Les correctifs sont généralement créés pour assurer la compatibilité d'un programme avec des nouvelles versions d'un système d'exploitation ou d'un matériel, remédier à des problèmes de performances ou corriger des bugs.

LiveUpdate automatise le processus de téléchargement et d'installation des mises à jour de programmes. Il va rechercher les fichiers sur un site Internet, les télécharge, les installe, et supprime ensuite les fichiers inutiles sur votre ordinateur.

A propos de la mise à jour des fichiers de protection

Les mises à jour de protection sont des fichiers disponibles chez Symantec par abonnement et qui assurent l'actualisation de vos produits Symantec pour intégrer la technologie la plus récente contre les menaces. Les mises à jour de protection que vous recevez dépendent des produits que vous utilisez.

Norton AntiVirus, Norton SystemWorks	Les utilisateurs de Norton AntiVirus et Norton SystemWorks reçoivent des mises à jour des services de définitions de virus, qui permettent d'obtenir les signatures de virus et autres technologies les plus récentes de Symantec.
Norton Internet Security	Outre les définitions de virus, les utilisateurs de Norton Internet Security reçoivent des mises à jour des listes d'adresses Web et catégories de sites Web utilisées pour identifier un contenu Web non approprié.

A propos de votre abonnement

Si votre produit Symantec comprend des mises à jour de protection, l'achat de ce produit inclut un abonnement gracieux, limité dans le temps, aux mises à jour utilisées par le produit. Lorsque l'abonnement est près d'expirer, vous êtes invité à le renouveler.

Si vous ne renouvelez pas votre abonnement, vous pouvez toujours utiliser LiveUpdate pour obtenir les mises à jour des programmes. Cependant, vous ne pouvez pas obtenir les mises à jour des fichiers de protection et ne serez donc pas protégé contre les *menaces* nouvellement découvertes.

Quand convient-il d'effectuer une mise à jour ?

Se reporter à « Programmation de mises à jour futures » à la page 50.

Durant l'installation de votre logiciel, vous avez l'option d'exécuter LiveUpdate. Faites-le pour vous assurer que vous avez les fichiers de protection les plus à jour. Après l'installation, si vous avez Norton AntiVirus, Norton Personal Firewall, Norton Internet Security ou Norton SystemWorks, des mises à jour mensuelles vous garantiront de toujours disposer des *définitions* de virus et/ou de la protection anti-intrusion les plus récentes.

Tâches préalables à la mise à jour

Dans certains cas, l'exécution de LiveUpdate exige un certain nombre de tâches préalables. Par exemple, si votre *fournisseur de services Internet* est America Online (AOL), vous devez ouvrir une session sur AOL avant d'utiliser LiveUpdate.

Si vous vous connectez via America Online

Si votre *fournisseur de services Internet* est America Online (AOL), vous devrez peut-être ouvrir une session sur AOL avant d'utiliser LiveUpdate.

Pour utiliser LiveUpdate avec AOL

1. Connectez-vous sur AOL.
2. Dans la page d'accueil d'AOL, cliquez sur le navigateur Internet AOL.
3. Ouvrez LiveUpdate.
4. Suivez les instructions données dans la section « Procédures de mise à jour » à la page 47.
5. Lorsque la session LiveUpdate est terminée, fermez le navigateur AOL.
   Si la session LiveUpdate nécessite le redémarrage de l'ordinateur, commencez par vous déconnecter d'AOL.

Si vous effectuez la mise à jour par le biais d'un réseau interne

Si vous exécutez LiveUpdate sur un Macintosh connecté à un réseau d'entreprise protégé par un pare-feu, l'administrateur a la possibilité de configurer un serveur LiveUpdate interne sur ce réseau. Une fois que votre administrateur l'a configuré, LiveUpdate devrait trouver cet emplacement automatiquement.

Si vous rencontrez des difficultés pour la connexion à un serveur LiveUpdate interne, veuillez vous adresser à votre administrateur réseau.

Si vous ne pouvez pas utiliser LiveUpdate

Dès que de nouvelles mises à jour sont disponibles, Symantec poste des messages sur son site Web. Si vous ne pouvez pas exécuter LiveUpdate, vous pouvez obtenir les nouveaux fichiers de mise à jour à partir du site Web de Symantec.

Votre abonnement doit être à jour pour que vous puissiez obtenir les nouvelles mises à jour de protection sur le site Web de Symantec.

Pour obtenir des définitions de virus depuis le site Web de Symantec :

1. Ouvrez votre navigateur Internet et connectez-vous au site suivant : securityresponse.symantec.com/avcenter/defs.download.html
   Si vous ne parvenez pas à charger cette page, rendez-vous sur le site securityresponse.symantec.com et cliquez sur **Mise à jour des définitions de virus**, puis sur **Download Virus Definitions (Intelligent Updater Only)**.
2. Sur la page Security Response, sélectionnez **Norton AntiVirus for Macintosh**.
3. Cliquez sur **Download Updates**.
4. Sur la page Security Response, sélectionnez le fichier à télécharger. Assurez-vous que vous sélectionnez les fichiers correspondant à la version de votre produit.
   Les fichiers téléchargeables sont accompagnés d'informations relatives à la mise à jour.

Pour obtenir des fichiers de mise à jour depuis le site Web de Symantec :

1. Ouvrez votre navigateur Internet et connectez-vous au site suivant : securityresponse.symantec.com/downloads/
2. Sur la page des téléchargements, sélectionnez, dans la liste des mises à jour, le produit que vous souhaitez mettre à jour.
3. Dans la page Service et support, sélectionnez la version de votre produit.
4. Cliquez sur **continuer**.
5. Dans la page des produits, sélectionnez le fichier à télécharger. Les fichiers téléchargeables sont accompagnés d'informations relatives à la mise à jour.

Procédures de mise à jour

Se reporter à « Programmation de mises à jour futures » à la page 50.

Vous pouvez laisser LiveUpdate chercher toutes les mises à jour en même temps, ou sélectionner des mises à jour précises. Vous avez également la possibilité de programmer à l'avance l'exécution d'une session LiveUpdate.

Sélectionne les éléments à mettre à jour lors de cette session.

Met à jour tous les composants installés

Permet de programmer des mises à jour spécifiques

Indique la dernière activité de mise à jour

Mise à jour complète et immédiate

La mise à jour de tous les fichiers disponibles est sans aucun doute la méthode la plus rapide pour s'assurer que tous les produits Symantec bénéficient de la protection la plus récente.

Pour procéder à une mise à jour complète et immédiate

1. Dans la barre de menus Norton Internet Security, cliquez sur **LiveUpdate**.
2. Cliquez sur **Tout mettre à jour**.
   A tout moment, une zone de dialogue vous informe du déroulement des opérations.

Personnalisation d'une session LiveUpdate

Si vous souhaitez ne mettre à jour que certains éléments, vous avez la possibilité de les sélectionner en omettant les autres.

Pour personnaliser une session LiveUpdate

1. Dans la fenêtre LiveUpdate, cliquez sur **Personnaliser cette mise à jour**.
   LiveUpdate présente la liste des mises à jour disponibles. Par défaut, toutes les mises à jour sont sélectionnées et incluses dans la session. Si vos fichiers sont déjà à jour, vous ne pouvez sélectionner aucun élément.
2. Désélectionnez les éléments que vous ne souhaitez pas mettre à jour.
3. Cliquez sur **Mise à jour**.
   Le transfert des fichiers ne prend que quelques minutes. Lorsque le transfert est terminé, la fenêtre de synthèse de LiveUpdate apparaît.

Se reporter à « Affichage de la synthèse de LiveUpdate » à la page 49.

A l'issue de la mise à jour

Au terme d'une session LiveUpdate, une liste des éléments mis à jour accompagnée de quelques brèves remarques s'affiche dans la fenêtre Synthèse LiveUpdate.

Affichage de la synthèse de LiveUpdate

La zone de dialogue Synthèse LiveUpdate affiche un récapitulatif des activités réalisées ainsi que la liste des produits mis à jour dans le cadre de la session.

Certaines mises à jour exigent que vous redémarriez l'ordinateur. Lorsque cette recommandation apparaît dans la description récapitulative, le bouton Redémarrer est disponible.

Pour redémarrer l'ordinateur après une session LiveUpdate

- Dans la fenêtre Synthèse LiveUpdate, cliquez sur **Redémarrer**.

Vidage de la Corbeille au terme d'une session LiveUpdate

Après la mise à jour des fichiers de programme, LiveUpdate place les anciens fichiers devenus inutiles dans la Corbeille. Si vous n'avez pas encore redémarré à la suite de la mise à jour, vous risquez de voir un message indiquant que ces fichiers sont utilisés. Vous pourrez vider la Corbeille après avoir redémarré votre ordinateur.

Vérification des numéros de version et des dates

Les derniers numéros de version et les dates des mises à jour les plus récentes s'affichent dans la fenêtre LiveUpdate.

Vous pouvez aussi vérifier les numéros de version et les dates dans la fenêtre A propos de l'application, accessible à partir du menu du produit, pour vous assurer que vous avez la version la plus récente.

Pour afficher la fenêtre A propos d'une application

1. Ouvrez votre application.
2. Dans le menu du produit, cliquez sur **A propos de <nom du produit>**.
   La fenêtre A propos de indique le numéro de version et les dates de copyright.
3. Lorsque vous avez fini de consulter la fenêtre A propos, fermez-la.

Programmation de mises à jour futures

L'utilisateur qui a programmé l'événement doit être connecté pour que cet événement se produise. Sinon, l'événement se produit la prochaine fois que l'utilisateur correct est connecté.

Vous pouvez programmer l'exécution de certains événements à un moment déterminé, sans aucune intervention de votre part. Si votre Macintosh est éteint au moment où l'événement doit se produire, il survient lors de la mise sous tension suivante de votre ordinateur. Avant de programmer une mise à jour, testez-la manuellement une fois au moins. Se reporter à « Mise à jour complète et immédiate » à la page 48 et « Personnalisation d'une session LiveUpdate » à la page 48.

Pour des instructions sur la programmation de mises à jour futures, reportez-vous à la section « Programmation d'événements LiveUpdate » à la page 52.

Programmation d'événements futurs

5

Utilisez Norton Scheduler pour veiller à l'exécution régulière des tâches essentielles à la protection de votre ordinateur et de vos données.

A propos de Norton Scheduler

Les tâches disponibles dans Norton Scheduler dépendent des produits installés.

Si votre Macintosh est éteint au moment où l'événement doit se produire, il survient lors de la mise sous tension suivante de votre ordinateur.

Ouverture de Norton Scheduler

Vous pouvez ouvrir Norton Scheduler à partir du programme actuellement ouvert.

Pour ouvrir Norton Scheduler à partir de Norton Internet Security

1. Ouvrez Norton Internet Security.
2. Dans la barre de menus Norton Internet Security, cliquez sur **Norton Scheduler**.

Pour ouvrir Norton Scheduler à partir de LiveUpdate

Se reporter à « Procédures de mise à jour » à la page 47.

1. Ouvrez LiveUpdate.
2. Dans la fenêtre LiveUpdate, cliquez sur **Norton Scheduler**.

Programmation d'événements LiveUpdate

Dans Norton Scheduler, les événements LiveUpdate vérifient s'il existe des mises à jour pour les produits installés. Si Norton AntiVirus est installé, une mise à jour des *définitions de virus* est également programmée.

Pour programmer des événements LiveUpdate

Se reporter à « Ouverture de Norton Scheduler » à la page 51.

1. Ouvrez Norton Scheduler.
2. Dans la fenêtre Norton Scheduler, cliquez sur **Nouveau**.
3. Cliquez sur **Mise à jour des produits**.
4. Attribuez un nom suffisamment explicite à la tâche LiveUpdate.
5. Dans la liste Produit à mettre à jour, sélectionnez le produit à mettre à jour. Les options possibles sont les suivantes :

Tous les produits	Met à jour tous les produits installés.
Définitions de virus	Met à jour les définitions de virus.
LiveUpdate	Met à jour les fichiers programme de LiveUpdate.
<Nom du produit>	Met à jour le produit sélectionné. Les noms des produits Symantec installés apparaissent dans la liste.

6. Dans la liste Fréquence, choisissez la fréquence à laquelle la mise à jour doit avoir lieu.
Les options proposées sont les suivantes :

Tous les mois	Lance l'événement tous les mois, au jour et à l'heure indiqués. Vous pouvez choisir une date comprise entre le 1er et le 28 du mois.
Toutes les semaines	Lance la mise à jour une fois par semaine, aux jour et à l'heure indiqués.
Tous les jours	Lance l'événement une fois par jour, à l'heure indiquée.
Tous les ans	Lance l'événement une fois par an, à la date et à l'heure indiquées. Vous pouvez programmer l'événement jusqu'à un an à l'avance.

7 Si vous choisissez une fréquence autre que quotidienne, spécifiez la date ou le jour de la semaine où la mise à jour doit se faire.

Se reporter à « Définition de l'heure de début » à la page 54.

8 Définissez une heure de début pour l'événement.

9 Cliquez sur **Enregistrer**.

Programmation d'examens Norton AntiVirus

Si vous avez installé Norton AntiVirus, vous pouvez programmer des examens partiels ou exhaustifs du système.

Pour programmer des examens Norton AntiVirus

Se reporter à « Ouverture de Norton Scheduler » à la page 51.

1 Ouvrez Norton Scheduler.

2 Dans la fenêtre Norton Scheduler, cliquez sur **Nouveau**.

3 Cliquez sur **Examen antivirus**.

4 Dans la fenêtre d'ajout d'une tâche d'examen antivirus, tapez un nom évocateur pour la tâche, par exemple, Examen du disque OS X.

5 Choisissez l'une des options suivantes :

- Faites glisser l'élément à examiner depuis le Finder vers la fenêtre d'ajout de tâche d'examen antivirus.
- Cliquez sur **Naviguer** pour sélectionner l'élément à examiner.

Se reporter à « Sélection d'un élément en vue d'un examen programmé » à la page 54.

6 Dans la liste Fréquence, choisissez la fréquence à laquelle l'examen doit avoir lieu.
Les options possibles sont les suivantes :

Tous les mois	Lance l'événement tous les mois, au jour et à l'heure indiqués. Vous pouvez choisir une date comprise entre le 1er et le 28 du mois.
Toutes les semaines	Lance la mise à jour une fois par semaine, aux jour et à l'heure indiqués.
Tous les jours	Lance l'événement une fois par jour, à l'heure indiquée.
Tous les ans	Lance l'événement une fois par an, à la date et à l'heure indiquées. Vous pouvez programmer l'événement jusqu'à un an à l'avance.

7 Si vous choisissez une fréquence autre que quotidienne, spécifiez la date ou le jour de la semaine où l'examen doit se faire.

8 Définissez l'heure à laquelle l'événement doit avoir lieu.

9 Cliquez sur **Enregistrer**.

Se reporter à « Définition de l'heure de début » à la page 54.

Sélection d'un élément en vue d'un examen programmé

Vous pouvez sélectionner un disque, un dossier ou un fichier à examiner.

Pour sélectionner un élément à examiner

1 Dans la fenêtre d'ajout d'une tâche d'examen antivirus, cliquez sur **Naviguer**.

2 Dans la fenêtre de sélection de la cible, localisez le disque, dossier ou fichier à examiner.

3 Cliquez sur **Sélectionner**.

4 Le nom de l'élément et son emplacement apparaissent dans la fenêtre d'ajout de tâche d'examen antivirus.

Définition de l'heure de début

Vous pouvez définir l'heure exacte à laquelle vous voulez que commence l'événement programmé.

Pour définir l'heure de début

1 Dans la fenêtre des tâches, section de réglage de l'heure, effectuez l'une des opérations suivantes :

- Tapez l'heure exacte dans les zones heure et minute.
- Sélectionnez la zone heure ou minute, puis cliquez sur la flèche vers le haut ou vers le bas pour changer l'heure affichée.

2 Si votre ordinateur est réglé pour un affichage de l'heure au format 12 heures, un indicateur AM/PM apparaît à côté de l'heure. Cliquez sur l'indicateur pour en faire basculer la valeur.

3 Lorsque vous avez terminé, cliquez sur **Enregistrer**.

Gestion des événements programmés

Vous pouvez modifier, supprimer, désactiver et réinitialiser des événements programmés.

Modification d'événements programmés

Vous pouvez modifier les événements que vous programmez.

Pour modifier un événement programmé

1. Ouvrez Norton Scheduler.
2. Dans la liste Evénements programmés, sélectionnez l'événement programmé que vous voulez modifier.
3. Cliquez sur **Modifier**.
4. Apportez les modifications voulues.
   Vous trouverez une description des options de programmation dans la section « Programmation d'événements LiveUpdate » à la page 52.
5. Pour changer le nom de l'événement, tapez un autre nom dans le champ prévu à cet effet.
6. Cliquez sur **Enregistrer**.

Suppression d'événements programmés

Vous pouvez supprimer les événements programmés dont vous n'avez plus l'utilité.

Pour supprimer un événement programmé

1. Ouvrez Norton Scheduler.
2. Dans la liste Evénements programmés, sélectionnez l'événement programmé que vous voulez supprimer.
3. Cliquez sur **Supprimer**.
4. Dans la zone de dialogue qui apparaît, cliquez sur **Supprimer** pour confirmer la suppression du service.

Désactivation d'événements programmés

Vous pouvez désactiver des événements programmés sans les supprimer, de façon à garder la possibilité de les réactiver ultérieurement.

Pour désactiver un événement programmé

1. Dans la liste Evénements programmés, sous Activé, désélectionnez l'événement programmé que vous voulez désactiver.
2. Pour activer l'événement, sélectionnez-le à nouveau.

Rétablissement de tâches programmées

Vous pouvez rétablir les réglages d'origine de toutes les tâches programmées.

Produit	Réglages installés
Norton Personal Firewall	Aucun.
Norton AntiVirus	Tâche LiveUpdate mensuelle pour rechercher de nouvelles définitions de virus. Exécution programmée le 1er du mois.
Norton Internet Security	Tâche LiveUpdate mensuelle pour rechercher de nouvelles définitions de virus. Exécution programmée le 1er du mois.
Norton Utilities	Image FileSaver quotidienne pour procéder à la mise à jour des répertoires du disque. Exécution programmée à minuit. Défragmentation Speed Disk quotidienne. Exécution programmée à minuit.
Norton SystemWorks	Tâche LiveUpdate mensuelle pour rechercher de nouvelles définitions de virus. Exécution programmée le 1er du mois. Défragmentation Speed Disk quotidienne. Exécution programmée à minuit. Image FileSaver quotidienne pour procéder à la mise à jour des répertoires du disque. Exécution programmée à minuit.

Pour rétablir des tâches programmées

1. Dans le menu Norton Scheduler, cliquez sur **Réinitialiser les tâches programmées**.
2. Dans la zone de dialogue qui apparaît, cliquez sur **Réinitialiser**.

2

Norton Personal Firewall

Protection des disques, des fichiers et des données contre les intrusions

6

Norton Personal Firewall protège votre ordinateur contre les intrusions en se référant aux paramètres d'accès que vous spécifiez. Vous pouvez ainsi accorder des autorisations d'accès à certains ordinateurs, en les répertoriant en fonction de leur *adresse IP*, et définir d'autres *services* à protéger sur votre machine.

Eléments protégés par Norton Personal Firewall

Norton Personal Firewall protège votre ordinateur contre les intrusions externes, grâce à des connexions *TCP/IP (Transmission Control Protocol/Internet Protocol)* et, de manière facultative, *UDP (User Datagram Protocol)*. En d'autres termes, lorsque vous êtes connecté à Internet ou à un autre réseau, aucun ordinateur ne peut accéder aux fichiers, programmes ou autres informations stockés sur votre machine sans votre autorisation. Cette autorisation est accordée à un ordinateur, et pas à un utilisateur spécifique, ce qui permet à tous les utilisateurs de l'ordinateur en question d'en bénéficier. Vous pouvez également bloquer les requêtes *ICMP*.

Norton Personal Firewall ne permet pas d'exercer un contrôle sur les informations sortantes. Par exemple, il ne peut être utilisé pour crypter des informations personnelles, telles qu'un numéro de carte de crédit, que vous fournissez à un site Web. Il ne bloque pas non plus le trafic Bluetooth (la technologie Bluetooth fournit des connexions sans fil entre des périphériques numériques qui ont été spécifiquement activés. Elle est intégrée dans certains ordinateurs Macintosh).

Spécification de l'accès par adresse IP ou par nom d'hôte

Se reporter à « Ajout d'adresses IP » à la page 83.

Lorsque vous accordez ou refusez des autorisations d'accès à certains ordinateurs, vous pouvez répertorier ces ordinateurs en fonction de leur adresse IP (Internet Protocol : les protocoles sont des ensembles de règles qui régissent la transmission des données). Les adresses IP se composent de quatre nombres compris entre 0 et 255 et reliés par des points (206.204.212.3, par exemple). Chaque ordinateur présent sur Internet possède une adresse IP unique.

Si vous ne connaissez pas l'adresse IP d'un ordinateur, vous pouvez l'identifier grâce au nom d'hôte qui l'identifie sur un réseau. www.symantec.com est le nom d'hôte du site Web de Symantec, par exemple. Les noms d'hôte sont convertis en adresses IP par le *système de noms de domaine* (DNS, Domain Name System). Vous pouvez saisir un nom d'hôte ou une adresse IP dans une liste d'accès.

Les adresses IP peuvent être spécifiées individuellement, sous la forme d'une plage commençant par une valeur précise, ou sous la forme d'une plage correspondant à un sous-réseau. Un sous-réseau est un réseau local qui fait partie intégrante d'un intranet de plus grande taille ou d'Internet.

Protection de numéros de port

Se reporter à « Définition d'un service personnalisé à protéger » à la page 84.

Dressez une liste des *adresses IP* en vue de l'octroi ou du refus d'autorisations d'accès à chacun des *services* installés sur votre ordinateur. Les services les plus courants sont déjà définis dans la fenêtre Configuration. Pour ceux qui ne sont pas répertoriés, vous pouvez créer une entrée dans la liste des services, en spécifiant le nom et le *numéro de port* correspondants.

Les services Internet communiquent par l'intermédiaire de *ports*, chaque service utilisant un numéro de port unique. Le partage Web s'effectue par l'intermédiaire du port 80, par exemple, tandis que le port 548 est utilisé pour le partage de fichiers *TCP/IP*. Il peut cependant arriver que ces services soient exécutés sur d'autres ports. Ainsi, si deux serveurs Web (ordinateurs qui acheminent des pages Web jusqu'à votre ordinateur) sont actifs sur un même ordinateur, ils ne peuvent utiliser le même numéro de port : un autre numéro de port est donc attribué à l'un des serveurs. Le choix d'une protection par numéro de port s'avère très utile pour protéger des services non prédéfinis par Norton Personal Firewall, ou encore des services qui utilisent d'autres numéros de port.

Se reporter à « Activation de la protection UDP » à la page 90.

Vous avez également la possibilité de protéger des services qui transitent par des ports *UDP*. Cette option doit toutefois être réservée aux utilisateurs qui maîtrisent parfaitement les *protocoles* Internet, car si vous refusez des autorisations d'accès à des ports UDP qui doivent impérativement en bénéficier, votre ordinateur risque de ne pas fonctionner correctement sur Internet.

Suivi des tentatives d'accès

Norton Personal Firewall génère un historique complet de toutes les tentatives d'accès à votre ordinateur. Il est en mesure de consigner toutes les connexions refusées ou/et autorisées, et peut même vous adresser une notification immédiate des accès autorisés ou refusés.

Norton Personal Firewall et AppleTalk

Les ordinateurs Macintosh utilisent principalement deux *protocoles* réseau : *AppleTalk* et *TCP/IP*. AppleTalk assure des *services* locaux qui ne sont pas disponibles sur Internet : impression, partage de fichiers avec d'autres ordinateurs du réseau et applications propres à une entreprise, par exemple.
TCP/IP fournit des services Internet tels que la messagerie électronique et l'accès aux sites Web ainsi que le partage de fichiers et le lien entre applications, sur Internet ou sur un intranet.

Sécurité TCP/IP sur Norton Personal Firewall

Norton Personal Firewall ajoute un niveau de protection à toute application qui utilise le *protocole* TCP en accordant des autorisations d'accès à des groupes d'ordinateurs limités sur Internet, en fonction de leur *adresse IP*. Par exemple, si vous avez activé le partage de fichiers sur *TCP/IP*, vous devez également autoriser l'accès aux fichiers partagés dans Norton Personal Firewall. Vous pouvez autoriser tous les accès, dans Norton Personal Firewall, ou restreindre l'accès à certaines adresses IP.

Sous Mac OS X, *AppleTalk* fait appel au protocole TCP/IP pour se connecter aux *services* de partage de fichiers et de liens entre applications exécutés sur d'autres ordinateurs Mac OS X. Norton Personal Firewall détecte de ce fait ces connexions et les bloque si vous n'avez pas accordé d'autorisations d'accès spécifiques.

Se reporter à « Personnalisation de la protection anti-intrusion » à la page 81.

Pour éviter le blocage d'AppleTalk, configurez les services de partage de fichiers et de lien entre applications dans Norton Personal Firewall de façon à autoriser les accès aux ordinateurs auxquels vous vous connectez par l'intermédiaire d'AppleTalk.

Surveillance des tentatives d'accès

7

Norton Personal Firewall consigne toutes les tentatives d'accès entrantes, qu'elles soient autorisées ou non. Vous pouvez également consigner les tentatives d'accès sortantes. Le journal généré vous permet de vérifier que Norton Personal Firewall fonctionne correctement.

Surveillance de l'activité du pare-feu

Par défaut, Norton Personal Firewall consigne dans un journal aussi bien les tentatives d'accès refusées que les tentatives d'accès autorisées. Ces tentatives sont répertoriées dans le journal Historique des accès, que vous pouvez consulter à tout moment.

Vous avez la possibilité de recevoir une notification immédiate des tentatives d'accès dans des circonstances particulières. Lorsque vous installez Norton Personal Firewall pour la première fois, par exemple, vous pouvez évaluer chaque tentative d'accès pour vous assurer que le logiciel remplit bien son rôle. Vous pouvez également choisir de recevoir une notification immédiate si vous avez modifié certains paramètres afin de vous assurer qu'ils ont bien produit les résultats escomptés.

Se reporter à « Test des paramètres du pare-feu » à la page 65.

Pour vérifier les paramètres de protection ou les modifications qui leur ont été apportées avant de vous connecter, faites appel à la fonction Vérification rapide de Norton Personal Firewall. La Vérification rapide simule une connexion TCP, consigne une tentative d'accès et déclenche une notification si vous avez activé cette option.

Vous pouvez également tester la sécurité de votre ordinateur grâce à un lien vers le site Web Symantec Security Check. Les résultats du test vous permettent ensuite de déterminer si les paramètres de votre pare-feu sont adéquats.

Une fois votre pare-feu configuré, vous pouvez effectuer une dernière vérification des résultats obtenus en consultant le rapport d'utilisateurs connectés. Si votre pare-feu est configuré pour bloquer toutes les connexions, ce rapport sera vide. Si vous l'avez configuré de façon à autoriser l'accès de votre ordinateur à certains utilisateurs, vous pourrez, grâce au rapport, vérifier qu'ils ont bien pu se connecter.

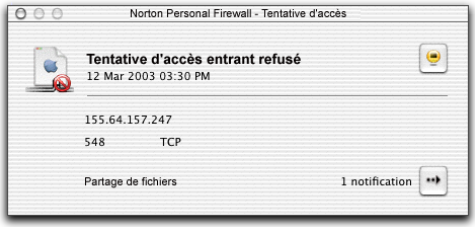
Activation ou désactivation de la notification des tentatives d'accès

Se reporter à « A propos des messages d'alerte » à la page 69.

Pour les connexions entrantes et sortantes, vous pouvez choisir de recevoir une notification de toutes les tentatives d'accès refusées et/ou de toutes celles autorisées. Si vous avez activé la notification, une *alerte* se déclenche lors de chaque tentative d'accès correspondant au type spécifié.

Vous pouvez également demander une notification si les paramètres de votre ordinateur entrent en conflit avec les paramètres du pare-feu. Vous pouvez, par exemple, avoir configuré Norton Personal Firewall de façon à ce que tout accès au partage de fichiers soit refusé, puis avoir activé le partage de fichiers dans les préférences système. Du fait que le pare-feu en bloque l'accès, le partage de fichiers est inutilisable. Norton Personal Firewall peut vous signaler ce conflit et modifier les paramètres du pare-feu pour vous.

Les options de notification d'accès peuvent être configurées individuellement pour chaque *service* répertorié dans la fenêtre Configuration. Les services pour lesquels aucune option de notification n'a été définie utilisent les options générales définies dans les préférences.



L'activation ou la désactivation de la notification n'a aucune incidence sur la consignation. De même, la désactivation de la consignation n'a aucune conséquence sur la notification, mais dans ce cas, l'alerte de notification constitue le seul enregistrement des tentatives d'accès dont vous disposez.

Pour activer ou désactiver les notifications d'accès à un service

1. Ouvrez Norton Personal Firewall.
2. Dans la fenêtre Configuration, sélectionnez le service pour lequel vous souhaitez définir les options de notification.
3. Cliquez sur **Modifier**.
4. Dans la zone de dialogue de configuration du serveur, cliquez sur **Notifications**.
5. Indiquez les options de notification souhaitées.
6. Cliquez sur **Enregistrer**.

Pour activer ou désactiver la notification d'accès générale

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Personal Firewall, cliquez sur **Préférences**.
3. Dans la fenêtre Préférences de Personal Firewall, cliquez sur **Notifications**.
4. Indiquez les options de notification souhaitées.
5. Fermez la fenêtre de préférences.
   Vos modifications sont automatiquement enregistrées.

Test des paramètres du pare-feu

Il existe deux façons de tester les paramètres du pare-feu : à l'aide de l'option Vérification rapide pour simuler l'accès à un *service* ou par le biais de l'option Vérification de sécurité, pour vous connecter au site Web de Symantec et analyser la vulnérabilité de votre ordinateur aux *menaces* en provenance d'Internet.

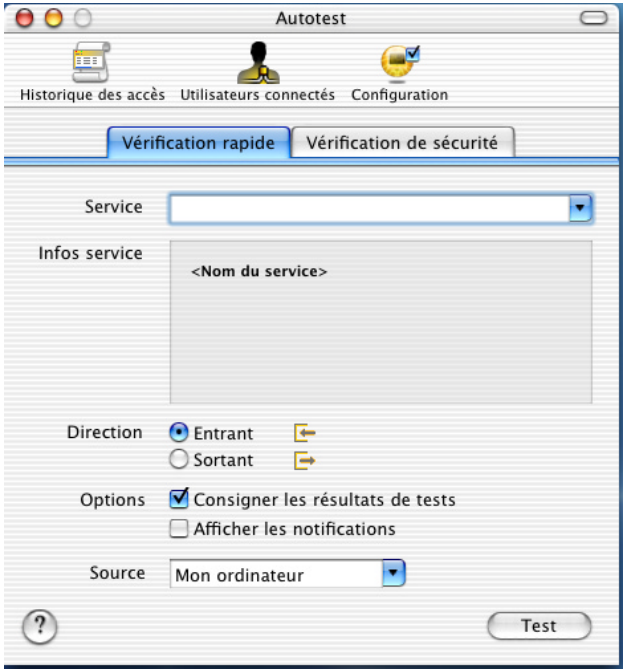
Simulation d'accès avec l'option Vérification rapide

Par défaut, l'option Vérification rapide utilise l'*adresse IP* de votre ordinateur pour simuler l'accès à l'un des services répertoriés dans la fenêtre Configuration. Vous pouvez également spécifier une adresse IP particulière, à utiliser pour le test. Si votre ordinateur ne possède pas d'adresse IP, vous devez vous connecter à Internet avant d'utiliser l'option Vérification rapide.

L'option Vérification rapide ne fonctionne que si Norton Personal Firewall est actif.

Pour simuler un accès avec l'option Vérification rapide

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Outils, cliquez sur **Autotest**.
3. Dans la fenêtre d'autotest, cliquez sur **Vérification rapide**.



4. Sélectionnez un service à tester.
   Le niveau de protection défini pour le service spécifié s'affiche en dessous.
5. Dans Direction, choisissez l'une des options suivantes :
   - Entrant
   - Sortant

6 Dans Options, choisissez l'endroit où vous souhaitez voir apparaître les résultats du test. Les options possibles sont les suivantes :

Consigner les résultats de tests	La tentative d'accès apparaît dans le journal Historique des accès.
Afficher les notifications	La tentative d'accès apparaît dans l'option Tentatives d'accès récentes du menu Dock.

Vous pouvez sélectionner l'une et/ou l'autre des options, ou aucune. Les résultats du test apparaissent toujours dans la fenêtre Autotest.

7 Pour spécifier une adresse IP différente de celle de votre ordinateur, tapez-la dans le champ Source.

8 Cliquez sur **Test**.

Analyse de la vulnérabilité par le biais du site Symantec Security Check

Recourez au site Symantec Security Check pour tester la vulnérabilité de votre ordinateur aux intrusions. Le lien Symantec Security Check disponible dans Norton Personal Firewall vous connecte au site Web de Symantec. Vous trouverez sur ce site des informations détaillées sur les données analysées durant une vérification de sécurité, ainsi que les instructions à suivre pour exécuter l'analyse.

Si votre ordinateur est protégé par un pare-feu d'entreprise, Symantec Security Check peut donner des résultats incorrects.

Pour évaluer la vulnérabilité en recourant au site Symantec Security Check

1 Ouvrez Norton Personal Firewall.

2 Dans le menu Outils, cliquez sur **Autotest**.

3 Dans la fenêtre d'autotest, cliquez sur **Vérification de sécurité**.

4 Cliquez sur **Examen**.
La page Web Symantec Security Check s'ouvre dans votre navigateur.

5 Pour plus d'informations sur les opérations effectuées, cliquez sur **A propos de l'analyse des risques en matière de sécurité** dans la page Web.

6 Pour exécuter l'analyse, cliquez sur **Analyse des risques en matière de sécurité**.

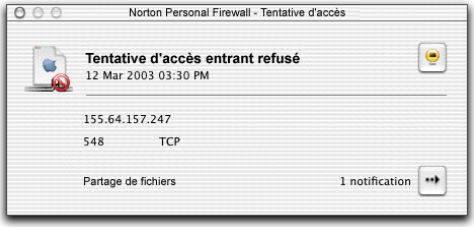
Au terme de l'analyse, toutes les zones vérifiées sont répertoriées avec leur degré de vulnérabilité respectif dans la page des résultats. Pour toutes les zones signalées comme vulnérables, vous pouvez obtenir des informations détaillées sur la nature du problème et sur les solutions envisageables.

Réponse aux tentatives d'accès

Consultez régulièrement le journal Historique des accès pour détecter des activités inhabituelles ou des problèmes éventuels, tels qu'un refus d'accès à un utilisateur autorisé.

A propos des messages d'alerte

Si vous avez activé la notification des tentatives d'accès, une fenêtre d'*alerte* apparaît à l'écran, à chaque tentative d'accès. Le nombre d'alertes reçues est indiqué dans le coin inférieur droit de la fenêtre d'alerte. Vous pouvez passer les alertes en revue en cliquant sur la flèche droite.



Les alertes fournissent des détails sur les tentatives d'accès. Si une tentative vous semble suspecte, consultez le journal Historique des accès.

Affichage du journal Historique des accès

Toutes les tentatives d'accès consignées apparaissent dans le journal Historique des accès. Ce journal vous permet de repérer les éventuelles violations de sécurité. Lors de la lecture du journal, recherchez la présence d'éléments récurrents, tels que :

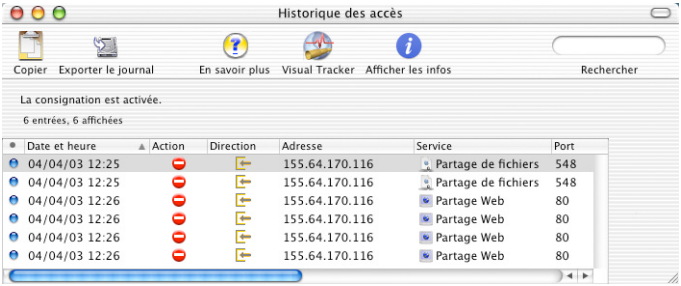
- Refus d'accès à répétition, en particulier pour une *adresse IP* cliente habituelle
- Succession de numéros de *port* sollicités par une même adresse IP cliente, indiquant un risque d'analyse des ports (un intrus passe en revue les différents ports de votre ordinateur jusqu'à ce qu'il trouve un port accessible).

Il est normal que certaines tentatives d'accès soient aléatoirement refusées (tentatives ne provenant pas de la même adresse IP, et ne sollicitant pas une succession de numéros de ports). Dans certains cas, des tentatives d'accès sont effectuées suite à des activités sur votre ordinateur, comme la connexion à un serveur *FTP* et l'envoi de messages électroniques.

Pour afficher le journal Historique des accès

1 Ouvrez Norton Personal Firewall.

2 Dans le menu Rapports, cliquez sur **Journal Historique des accès**.



Contenu de l'historique des accès

Le type d'accès faisant l'objet d'une consignation est indiqué dans la partie supérieure de la fenêtre. La fenêtre comprend les champs suivants :

Date et heure	Date et heure de la tentative d'accès
Action	Indique si la tentative d'accès a été autorisée ou refusée
Direction	Indique si la tentative d'accès était entrante ou sortante.
Adresse	Adresse IP de l'ordinateur à l'origine de la tentative d'accès
Service	Nom du service Internet ayant fait l'objet de la tentative d'accès, le cas échéant.
Port	Numéro du port ayant fait l'objet de la tentative d'accès.
Mode	Mode de communication par lequel la tentative d'accès à été effectuée. Les modes possibles sont TCP, UDP et ICMP.

Type	Raison pour laquelle l'entrée apparaît dans le fichier journal.
Hôte	Nom d'hôte de l'ordinateur à l'origine de la tentative d'accès. Si le nom d'hôte ne peut pas être déterminé, c'est l'adresse IP de l'ordinateur qui apparaît.

Les tentatives d'accès marquées d'un point bleu dans la première colonne se sont produites au cours des 15 dernières minutes.

Modification de l'apparence du journal Historique des accès

Vous pouvez modifier l'apparence du journal Historique des accès en fonction de vos besoins.

Pour modifier l'apparence du journal Historique des accès

❖ Personnalisez le journal Historique des accès. Les options possibles sont les suivantes :

Tri par colonne.	Cliquez sur l'en-tête de la colonne à trier. Pour modifier le sens de tri, cliquez sur le triangle situé à droite de l'en-tête de colonne. Par défaut, le journal est trié par date, les entrées les plus récentes se trouvant à la fin.
Réorganisation des colonnes.	Faites glisser les en-têtes de colonne vers la position à laquelle vous souhaitez faire apparaître les colonnes.
Redimensionnement des colonnes.	Faites glisser la bordure de l'en-tête de colonne jusqu'à obtention des dimensions voulues.
Suppression de colonnes.	Dans le menu Rapports, cliquez sur Options d'affichage pour obtenir une liste des colonnes affichées. Désélectionnez les colonnes que vous ne souhaitez pas afficher, puis cliquez sur Enregistrer.

Exportation des informations de l'historique des accès

Vous pouvez exporter le contenu du journal Historique des accès dans un fichier texte délimité par tabulations. Vous pouvez exporter l'intégralité du journal ou seulement les entrées sélectionnées. L'exportation n'est possible que si le journal Historique des accès est ouvert.

Pour exporter les informations affichées dans la fenêtre Historique des accès

1. Dans le menu Rapports, cliquez sur **Journal Historique des accès**.
2. Vous pouvez exporter individuellement les entrées de votre choix.
3. Dans le menu Fichier, cliquez sur **Exporter**.
4. Dans la zone de dialogue d'exportation, indiquez un nom et un emplacement pour le fichier.
5. Si vous exportez des entrées sélectionnées, cochez l'option **Exporter uniquement les entrées sélectionnées**.
6. Cliquez sur **Enregistrer**.

Effacement du contenu du journal Historique des accès

Si la liste affichée dans le journal Historique des accès est trop longue, vous pouvez l'effacer.

Pour effacer le contenu du journal Historique des accès

1. Dans le menu Rapports, cliquez sur **Journal Historique des accès**.
2. Dans le menu Edition, cliquez sur **Effacer le journal**.
3. Confirmez l'effacement de l'Historique des accès.

Obtention d'informations détaillées sur une tentative d'accès donnée

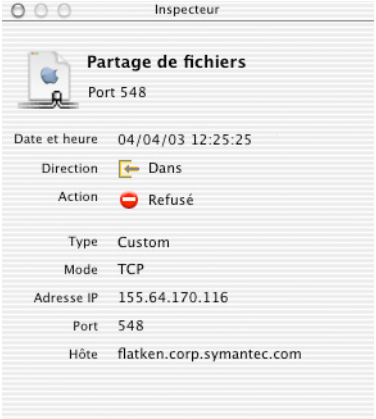
Vous pouvez obtenir des informations complémentaires sur une entrée du journal Historiques des accès dans la fenêtre Inspecteur, dans la page Web En savoir plus ou dans la page Web Visual Tracking.

Ouvrez la fenêtre Inspecteur

La fenêtre Inspecteur vous donne, dans une seule fenêtre, toutes les informations relatives à une tentative d'accès consignées dans le journal Historique des accès.

Pour ouvrir la fenêtre Inspecteur :

- Dans le journal Historique des accès, cliquez deux fois sur la ligne pour laquelle vous souhaitez obtenir des informations complémentaires.



Accès à la page Web En savoir plus

La page Web En savoir plus de Norton Personal Firewall donne des informations détaillées sur chaque tentative d'accès, ainsi que des liens vers d'autres sites susceptibles de vous apporter des précisions sur la source (champ Nom d'hôte) des tentatives d'accès.

Pour accéder à la page Web En savoir plus

1. Dans le journal Historique des accès, sélectionnez la tentative d'accès pour laquelle vous souhaitez obtenir des informations complémentaires.
2. Dans le menu Outils, cliquez sur **En savoir plus**.

Accès à la page Web Visual Tracking

La page Web Visual Tracking vous indique, sur une carte, l'endroit où se trouve le propriétaire de l'*adresse IP* source d'une tentative d'accès. Elle vous indique également le nom du fournisseur d'accès Internet de cette adresse IP, ainsi que des liens vers plus de détails concernant le propriétaire correspondant.

Pour accéder à la page Web Visual Tracking

1. Dans le journal Historique des accès, sélectionnez la tentative d'accès pour laquelle vous souhaitez obtenir des informations complémentaires.
2. Dans le menu Outils, cliquez sur **Visual Tracking**.

Modification des préférences de consignation

La consignation de toutes les tentatives d'accès entrantes et de toutes les activités suspectes est activée par défaut. Conservez ces paramètres jusqu'à ce que vous ayez la certitude que la configuration de Norton Personal Firewall donne les résultats escomptés. La consignation de toutes les tentatives d'accès entraîne très rapidement la création d'un fichier journal volumineux, raison pour laquelle vous pouvez limiter les données à consigner.

Vous avez également la possibilité de consigner les tentatives d'accès en provenance uniquement de certains *services*. Vous pouvez ainsi définir les informations à consigner pour chaque service. Les paramètres définis dans les préférences sont appliqués aux services pour lesquels vous n'avez défini aucun paramètre de consignation.

Pour modifier les préférences de consignation par défaut

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Personal Firewall, cliquez sur **Préférences**.
3. Dans la fenêtre Préférences de Personal Firewall, cliquez sur **Consignation**.
4. Précisez les options de consignation souhaitées.
5. Fermez la fenêtre de préférences.
   Vos modifications sont automatiquement enregistrées.

Pour définir les préférences de consignation pour un service

1. Ouvrez Norton Personal Firewall.
2. Dans la fenêtre Configuration, sélectionnez le service pour lequel vous souhaitez définir les préférences de consignation.
3. Cliquez sur **Modifier**.
4. Dans la zone de dialogue de configuration du service, cliquez sur **Consignation**.
5. Indiquez les préférences de consignation désirées pour ce service.
6. Cliquez sur **Enregistrer**.

Désactivation de la consignation

La consignation et la protection des *services* sont totalement indépendantes l'une de l'autre. Si vous consignez les accès autorisés puis désactivez la protection anti-intrusion, par exemple, Norton Personal Firewall poursuit la consignation de tous les accès, puisqu'ils sont tous autorisés. Certaines situations, telles que la création d'un nouveau fichier journal, exigent cependant la désactivation de la consignation. Cette désactivation n'a aucune incidence sur la protection assurée par Norton Personal Firewall.

Si vous avez défini des préférences de consignation individuelles pour un service, vous devez également les désactiver pour arrêter toutes les consignations.

Pour désactiver les options de consignation par défaut

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Personal Firewall, cliquez sur **Préférences**.
3. Dans la fenêtre Préférences de Personal Firewall, cliquez sur **Consignation**.
4. Désactivez toutes les options de consignation.
5. Fermez la fenêtre de préférences.
   Vos modifications sont automatiquement enregistrées.

Pour désactiver la consignation pour un service

1. Ouvrez Norton Personal Firewall.
2. Dans la fenêtre Configuration, sélectionnez le service pour lequel vous souhaitez désactiver la consignation.
3. Cliquez sur **Modifier**.
4. Dans la zone de dialogue de configuration du service, cliquez sur **Consignation**.
5. Désactivez toutes les options de consignation.
6. Cliquez sur **Enregistrer**.

Structure du fichier journal

Le fichier journal est un fichier texte délimité par tabulations, intitulé Norton Personal Firewall Log. Il peut être lu par toutes les applications de traitement de texte ou de tableur, ainsi que par certains analyseurs de journal.

Le fichier journal est situé dans Library:Application Support:Norton Solutions Support:Norton Personal Firewall.

Les tentatives d'accès sont consignées à l'aide des jetons suivants (ajoutés à la ligne !!LOG_FORMAT à chaque démarrage de Norton Personal Firewall ou lors de la création d'un nouveau fichier journal) :

DATE	Date, heure et fuseau horaire de la tentative d'accès
RESULT	Prend la valeur OK pour un accès autorisé et la valeur ERR! pour un accès refusé
HOSTNAME	Adresse IP du client qui tente d'accéder au port en question
SERVER_PORT	Port auquel le client considéré tente d'accéder
METHOD	Protocole utilisé pour la tentative d'accès (TCP ou UDP)
DIRECTION	IN pour les tentatives d'accès entrantes, OUT pour les tentatives d'accès sortantes
TYPE	Raison pour laquelle l'entrée apparaît dans le fichier journal

L'exportation du journal dans un tableur et le tri des données peuvent faciliter l'identification d'éléments récurrents susceptibles d'indiquer une violation de sécurité. Par exemple :

- Effectuez un tri par résultat (champ RESULT) puis par nom d'hôte (champ HOSTNAME). Sur les lignes dont le champ RESULT prend la valeur ERR!, observez les *adresses IP* dans le champ HOSTNAME. L'existence d'un grand nombre de lignes ERR! pour une adresse IP donnée peut indiquer une tentative de violation de sécurité.
- Effectuez un tri par résultat (champ RESULT), puis par nom d'hôte (champ HOSTNAME) et enfin par port serveur (champ SERVER_PORT). Sur les lignes dont le champ RESULT prend la valeur ERR!, recherchez dans le champ SERVER_PORT les séries de numéros de *port* pour lesquelles une adresse IP identique figure dans le champ HOSTNAME. Les séries de numéros de port associées à une adresse IP donnée peuvent en effet indiquer une tentative d'analyse des ports.

Se reporter à « Pour afficher le journal Historique des accès » à la page 70.

Pour obtenir des précisions sur une adresse IP répertoriée dans le fichier journal (ou dans une *alerte* de notification), consultez le journal Historique des accès.

Utilisation du rapport d'utilisateurs connectés

Le rapport d'utilisateurs connectés indique tous les ordinateurs actuellement connectés au vôtre. Toutes les connexions effectuées par un ordinateur sont affichées séparément. Vous pouvez utiliser le rapport d'utilisateurs connectés pour vérifier que les utilisateurs qui ont le droit d'être connectés à votre ordinateur ont la possibilité de le faire et qu'aucun de ceux qui devraient être bloqués n'est parvenu à s'infiltrer.

Lorsque vous consultez le rapport d'utilisateurs connectés, vous avez la possibilité d'ajouter l'*adresse IP* d'un ordinateur connecté à la liste d'accès autorisé ou refusé, de déconnecter cet ordinateur du vôtre, d'obtenir des informations complémentaires sur cet ordinateur et d'exporter la liste dans un fichier texte.

Pour consulter le rapport d'utilisateurs connectés

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Rapports, cliquez sur **Utilisateurs connectés**.
   Le rapport d'utilisateurs connectés s'affiche :

Connexion récente	Un point bleu apparaît dans la première colonne si la connexion s'est produite au cours des 15 dernières minutes.
Etat de la connexion	Dans la deuxième colonne, un point vert apparaît si l'utilisateur est encore connecté. Un point rouge apparaît lorsque vous déconnectez l'utilisateur.
Heure de début de connexion	Heure à laquelle la connexion a commencé.
Service	Service par lequel la connexion a été effectuée.
Adresse	Adresse IP de l'ordinateur qui effectue la connexion.
Application	Application utilisée pour effectuer la connexion.
Hôte	Nom d'hôte de l'ordinateur connecté. Si le nom d'hôte ne peut pas être déterminé, c'est l'adresse IP de l'ordinateur qui apparaît.

Modification de l'affichage du rapport d'utilisateurs connectés

Vous pouvez modifier l'affichage du rapport d'utilisateurs connectés en fonction de vos besoins.

Pour modifier l'affichage du rapport d'utilisateurs connectés

Personnalisez le rapport d'utilisateurs connectés. Les options possibles sont les suivantes :

Tri par colonne.	Cliquez sur l'en-tête de la colonne à trier. Pour modifier le sens de tri, cliquez sur le triangle situé à droite de l'en-tête de colonne. Par défaut, le rapport est trié par heure de début de connexion, les entrées les plus récentes se trouvant à la fin.
Réorganisation des colonnes.	Faites glisser les en-têtes de colonne vers la position à laquelle vous souhaitez faire apparaître les colonnes.
Redimensionnement des colonnes.	Faites glisser la bordure de l'en-tête de colonne jusqu'à obtention des dimensions voulues.
Suppression de colonnes.	Dans le menu Rapports, cliquez sur Options d'affichage pour obtenir une liste des colonnes affichées. Désélectionnez les colonnes que vous ne souhaitez pas afficher, puis cliquez sur Enregistrer.

Déconnexion d'un utilisateur connecté

Se reporter à « Modification de la durée de déconnexion des utilisateurs » à la page 80.

Vous pouvez déconnecter tout utilisateur répertorié dans le rapport d'utilisateurs connectés. Par défaut, l'utilisateur en question ne pourra plus se reconnecter à votre ordinateur pendant 30 minutes. Vous pouvez modifier ce laps de temps dans les Préférences.

Certains *services* effectuent plus d'une connexion à la fois. *FTP*, par exemple, effectue souvent deux connexions et certains navigateurs Web en font jusqu'à huit. Toutes ces connexions apparaissent séparément dans le rapport, sous la forme de doublons d'entrées, mais la déconnexion d'une seule de ces entrées les déconnecte toutes.

Pour empêcher de façon permanente un utilisateur de se reconnecter à votre ordinateur, ajoutez son *adresse IP* à la liste d'accès refusés pour ce service.

Pour déconnecter un utilisateur connecté

1. Dans le rapport d'utilisateurs connectés, sélectionnez l'ordinateur que vous souhaitez déconnecter.
2. Dans la barre d'outils, cliquez sur **Déconnecter l'utilisateur**.
3. Dans la zone de dialogue de confirmation, cliquez sur **Déconnecter**.

Obtention d'informations complémentaires sur un utilisateur connecté

Vous pouvez obtenir des informations complémentaires sur un utilisateur connecté en affichant :

La fenêtre Afficher les infos	La fenêtre Afficher les infos vous donne toutes les informations consignées dans le rapport d'utilisateurs connectées relatives à la connexion, dans une seule fenêtre.
La page Web En savoir plus	La page Web En savoir plus de Norton Personal Firewall fournit des informations détaillées sur chaque utilisateur connecté, ainsi que des liens vers d'autres sites susceptibles de vous apporter des précisions sur la source de la connexion.
La page Web Visual Tracking	La page Web Visual Tracking vous indique, sur une carte, l'emplacement du propriétaire de l'adresse IP indiquée dans le rapport. Elle vous indique également le nom du fournisseur d'accès Internet de cette adresse IP, ainsi que des liens vers plus de détails concernant le propriétaire correspondant.

Pour obtenir des informations complémentaires sur un utilisateur connecté

1. Dans le rapport d'utilisateurs connectés, sélectionnez les connexions pour lesquelles vous souhaitez obtenir des informations complémentaires.
2. Dans la barre d'outils, sélectionnez l'une des options suivantes :
   - Afficher les infos
   - En savoir plus
   - Visual Tracking

Exportation de la liste des utilisateurs connectés

Vous pouvez exporter le contenu du rapport d'utilisateurs connectés sous forme de fichier texte.

Pour exporter la liste des utilisateurs connectés

1. Dans la barre d'outils du rapport d'utilisateurs connectés, cliquez sur **Exporter la liste**.
2. Dans la zone de dialogue Enregistrer sous, entrez le nom que vous souhaitez donner au rapport.
3. Choisissez l'emplacement où vous souhaitez enregistrer le rapport.
4. Cliquez sur **Enregistrer**.

Modification de la durée de déconnexion des utilisateurs

Lorsque vous déconnectez un utilisateur à partir du rapport d'utilisateurs connectés, celui-ci ne pourra plus se connecter à votre ordinateur pendant un certain temps, défini dans les préférences.

Pour modifier la durée de déconnexion des utilisateurs

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Personal Firewall, cliquez sur **Préférences**.
3. Dans la fenêtre des préférences, cliquez sur **Utilisateurs connectés**.
4. Modifiez à votre convenance la durée pendant laquelle l'utilisateur devra rester déconnecté.
5. Fermez la fenêtre de préférences.
   Vos modifications sont automatiquement enregistrées.

Personnalisation de la protection anti-intrusion

8

A mesure que vous utilisez Norton Personal Firewall, il se peut que vous deviez ajuster vos paramètres d'accès. Vous pouvez être amené à autoriser le partage de fichiers pour un collègue qui travaille sur un site distant, par exemple. Il peut également arriver qu'un *service* non répertorié dans la fenêtre Configuration exige une protection personnalisée. Vous pouvez ajouter ce service à la liste. Vous avez également la possibilité d'étendre la protection aux *ports UDP* de votre ordinateur.

Se reporter à « Déconnexion d'un utilisateur connecté » à la page 78.

Les modifications apportées aux paramètres d'accès n'ont aucune incidence sur les ordinateurs connectés à votre machine au moment de la modification. Les changements effectués n'entrent en vigueur qu'après l'interruption de la connexion. Si, par exemple, un ordinateur est connecté à votre machine pour partager des fichiers et que vous interdisez l'accès aux fichiers partagés, cet ordinateur reste connecté jusqu'à ce que son utilisateur ferme la session ou jusqu'à ce que vous interrompiez explicitement la connexion.

Protection des services Internet standard

Les services *Internet* intégrés au système d'exploitation Macintosh sont définis dans la fenêtre Configuration de Norton Personal Firewall. Les services non répertoriés sont protégés en fonction des paramètres définis pour l'entrée Autres. Tous les accès sont refusés par défaut. Vous pouvez modifier les paramètres de protection pour tous les services répertoriés.

Pour chaque service affiché dans la fenêtre Configuration, pour les connexions entrantes et sortantes, vous pouvez :

- refuser tous les accès ;
- autoriser l'accès aux adresses figurant dans la liste ;
- refuser l'accès aux adresses figurant dans la liste ;
- autoriser tous les accès.

Ces paramètres sont classés par ordre de restriction décroissante.

Pour refuser ou autoriser tous les accès à un service

1. Sélectionnez le service auquel vous souhaitez refuser ou autoriser tous les accès.
2. Sélectionnez les connexions entrantes ou sortantes.
3. Sélectionnez les options voulues.

Se reporter à « Utilisation du rapport d'utilisateurs connectés » à la page 77.

Si vous interdisez tout accès à un service auquel un utilisateur est déjà connecté, la modification n'entre en vigueur qu'à l'interruption de la connexion. Vous pouvez voir qui est connecté à un service dans le rapport d'utilisateurs connectés.

Pour refuser ou autoriser l'accès à une liste d'adresses IP

1. Sélectionnez le service auquel vous souhaitez refuser ou autoriser l'accès.
2. Sélectionnez les connexions entrantes ou sortantes.
3. Sélectionnez les options voulues.
4. Spécifiez les adresses IP à inclure dans la liste.

Se reporter à « Utilisation du rapport d'utilisateurs connectés » à la page 77.

Si vous refusez l'accès à une *adresse IP* déjà connectée, la modification n'entre en vigueur qu'à l'interruption de la connexion. Vous pouvez voir les adresses IP déjà connectées à votre ordinateur dans le rapport d'utilisateurs connectés.

Pour établir une liste d'adresses auxquelles accorder ou refuser des accès

1. Sélectionnez le service Internet pour lequel vous souhaitez définir des accès.
2. Sélectionnez les connexions entrantes ou sortantes.
3. Choisissez d'autoriser ou de refuser les accès pour une liste d'adresses IP.
4. Cliquez sur **Nouveau** pour ajouter une adresse ou une plage d'adresses à la liste.

Ajout d'adresses IP

Vous pouvez ajouter une *adresse IP* spécifique ou une plage d'adresses à la liste des accès autorisés ou refusés. Lors de l'ajout d'une plage d'adresses, vous saisissez seulement le début de la plage. Norton Personal Firewall détermine la fin de la plage en fonction du nombre de segments saisis pour l'adresse IP de départ.

Pour ajouter une adresse précise

1. Dans la zone de dialogue Configuration de l'adresse, cliquez sur **une adresse spécifique**.
2. Dans le champ Adresse, saisissez l'adresse IP ou le nom d'hôte approprié.
   Pour choisir un ordinateur sur votre réseau, cliquez sur **Naviguer**.
3. Cliquez sur **Enregistrer**.
   L'adresse saisie apparaît dans la liste de la fenêtre Configuration.

Pour ajouter une plage d'adresses

1. Dans la zone de dialogue Configuration de l'adresse, cliquez sur **Adresses commençant par**.
2. Dans le champ Adresse IP de base, tapez une partie suffisante de l'adresse pour obtenir la plage d'adresses voulues.
   Au fur et à mesure que vous entrez les chiffres d'une adresse IP de base, Norton Personal Firewall détermine la fin de la plage et l'affiche en regard de l'intitulé Plage d'adresses dans la partie inférieure de la zone de dialogue Configuration de l'adresse.
3. Cliquez sur **Enregistrer**.

Ajout d'adresses de sous-réseau

Vous pouvez ajouter votre propre *sous-réseau* ou un sous-réseau différent à votre liste d'accès refusés ou autorisés. Si vous utilisez votre propre sous-réseau, le *masque de sous-réseau* est automatiquement complété. Si vous spécifiez un sous-réseau distinct, vous devez indiquer son masque de sous-réseau.

Pour ajouter des adresses pour votre propre sous-réseau

1. Dans la zone de dialogue Configuration de l'adresse, cliquez sur **Tous les ordinateurs d'un réseau** dans la liste Autoriser l'accès à.
2. Cliquez sur **Mon sous-réseau**.
   L'adresse IP de base et le masque de sous-réseau de votre sous-réseau s'inscrivent automatiquement.
3. Cliquez sur **Enregistrer**.

Pour ajouter des adresses pour un sous-réseau autre que le vôtre

1. Dans la zone de dialogue Configuration de l'adresse, cliquez sur **Tous les ordinateurs d'un réseau** dans la liste Autoriser l'accès à.
2. Indiquez l'adresse IP de base et le masque de sous-réseau dans les champs prévus à cet effet.
3. Cliquez sur **Enregistrer**.

Définition d'un service personnalisé à protéger

Vous pouvez ajouter des *services* qui ne sont pas répertoriés dans la fenêtre Configuration. Vous avez la possibilité de faire votre choix dans une liste de services prédéfinis, ou de spécifier vos propres services.

Pour définir un service personnalisé

1. Sous la liste des services, cliquez sur **Nouveau**.

2. Sélectionnez un nom de service. Si le nom du service à ajouter n'apparaît pas dans la liste, saisissez-le dans le champ Nom.
   Si vous sélectionnez un service dans la liste, le numéro de port s'affiche automatiquement.

3 Si vous le souhaitez, saisissez une description du service.

4 Si vous devez définir une plage de ports pour le service ou si vous avez saisi un nom de service, cliquez sur **Nouveau** pour spécifier le numéro ou la gamme de ports.
Une icône par défaut s'affiche aussi pour le service.

5 Vous pouvez remplacer cette icône par celle de votre choix en la collant ou en la faisant glisser sur l'icône existante dans la zone de dialogue Nouveau service.

6 Si, pour ce service, vous souhaitez spécifier des préférences de consignation ou de notification des accès, différentes des préférences par défaut, utilisez les onglets Consignation et Notifications. Se reporter à « Activation ou désactivation de la notification des tentatives d'accès » à la page 64 et « Modification des préférences de consignation » à la page 74.

7 Cliquez sur **Enregistrer**.
Le nouveau service apparaît dans la liste de la fenêtre Configuration. Pour configurer l'accès à ce service, reportez-vous à la section « Protection des services Internet standard » à la page 81.

Modification ou suppression d'un service personnalisé

Pour les *services* prédéfinis, vous pouvez modifier les seuls paramètres de consignation et de notification. Vous ne pouvez pas supprimer des services prédéfinis. Vous pouvez modifier ou supprimer un service personnalisé que vous avez ajouté à la liste.

Vous n'avez pas la possibilité de modifier le numéro de *port* en intervenant sur le service personnalisé. Pour modifier le numéro de port, supprimez le service et ajoutez-en un nouveau avec le numéro de port correct.

Pour modifier un service personnalisé

1 Dans la fenêtre Configuration, sélectionnez le service à modifier.

2 Cliquez sur **Modifier**.

3 Dans la zone de dialogue Configuration du service, effectuez les modifications souhaitées.

4 Cliquez sur **Enregistrer**.

Pour supprimer un service personnalisé

1. Dans la fenêtre Configuration, sélectionnez le service à supprimer.
2. Cliquez sur **Supprimer**.
3. Dans la zone de dialogue Avertissement qui apparaît, confirmez la suppression du service.

Modification des paramètres de protection

Vous pouvez modifier les paramètres de protection d'un *service* à deux niveaux. Vous pouvez intervenir sur le niveau de restriction (passer du niveau Refuser tous les accès au niveau Autoriser l'accès aux adresses IP de la liste, par exemple) ou sur la liste des adresses associées à un niveau de restriction. Ces modifications peuvent être apportées dans la fenêtre Configuration.

Si vous modifiez les paramètres de protection d'un service dans le sens d'un refus d'accès à un utilisateur déjà en cours de connexion à ce service, la modification n'entre en vigueur qu'après la déconnexion de l'utilisateur, soit à son initiative, soit par une interruption de votre part.

Modification du niveau de restriction

Vous pouvez modifier le niveau de restriction d'un *service* à tout moment.

Pour modifier le niveau de restriction

1. Dans la fenêtre Configuration, sélectionnez le service à modifier.
2. Sélectionnez les connexions entrantes ou sortantes.
3. Sélectionnez la nouvelle option de restriction :
   - Si vous sélectionnez une option de restriction qui fait référence à une liste d'adresses IP, vous devez créer cette liste. Se reporter à « Protection des services Internet standard » à la page 81.
   - Si vous sélectionnez l'option Refuser tous les accès ou Autoriser tous les accès à la place d'une option pour laquelle vous avez spécifié une liste d'adresses IP, la suppression de ces adresses n'est pas indispensable. Elles restent visibles dans la fenêtre Configuration, mais sont inaccessibles.

Modification d'une liste d'adresses IP

Dans le cas des options de restriction qui exigent une liste d'*adresses IP*, vous pouvez compléter la liste en ajoutant d'autres entrées, ou modifier et supprimer les adresses déjà répertoriées dans la fenêtre Configuration.

Avant de modifier une liste, assurez-vous que celle-ci est bien affichée, en cliquant sur le *service* correspondant et la bonne direction pour les connexions.

Pour ajouter une adresse IP à une liste

1. Dans la fenêtre Configuration, cliquez sur **Nouveau**.
2. Ajoutez les adresses IP voulues.
3. Cliquez sur **Enregistrer**.

Pour modifier une adresse ou une plage d'adresses IP dans une liste

1. Dans la fenêtre Configuration, sélectionnez l'adresse ou la plage d'adresses voulue.
2. Cliquez sur **Modifier**.
3. Dans la zone de dialogue Configuration de l'adresse IP, apportez les modifications voulues.
4. Cliquez sur **Enregistrer**.

Pour supprimer une adresse IP d'une liste

1. Dans la fenêtre Configuration, sélectionnez l'adresse ou la plage d'adresses voulue.
2. Cliquez sur **Supprimer**.

Support FTP actif

Norton Personal Firewall fournit un support *FTP* actif, qui permet le *téléchargement* de fichiers depuis un serveur FTP, sans bloquer la connexion.

Le support FTP actif est activé par défaut. Si vous utilisez votre ordinateur comme serveur FTP ou si vous ne souhaitez pas que votre ordinateur télécharge des fichiers à l'aide de FTP, vous pouvez désactiver le support FTP actif.

Pour désactiver le support FTP actif

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Outils, cliquez sur **Paramètres de protection**.
3. Dans la zone de dialogue Paramètres de protection, cliquez sur **Configuration personnalisée**.
4. Décochez la case **Activer la prise en charge de FTP actif**.
5. Cliquez sur **Enregistrer**.

Mode silencieux

En règle générale, lorsque Norton Personal Firewall refuse une tentative d'accès à votre ordinateur, le système demandeur reçoit un message l'informant de ce refus. Si vous activez le mode silencieux, aucun message n'est envoyé, et votre ordinateur reste ainsi invisible aux auteurs des tentatives d'accès.

Avantages du mode silencieux

Lorsque vous activez le mode silencieux, les requêtes TCP, *UDP* et la majorité des requêtes *ICMP* adressées à des *services* dont vous avez refusé l'accès sont neutralisées. Les seules exceptions concernent les requêtes ICMP de type 0 (réponses écho pour les requêtes Ping envoyées), 3 (impossible d'atteindre la destination) et 11 (dépassement du délai). Votre ordinateur reste en outre invisible aux utilitaires Traceroute (ces utilitaires permettent d'identifier le chemin emprunté par un *paquet* jusqu'à sa destination finale). L'activation du mode silencieux entraîne également la consignation des messages ICMP dans l'historique des accès.

Vous pouvez également choisir d'activer le mode silencieux pour la mise en réseau Rendezvous. Cela bloquera toutes les communications basées Rendezvous.

Désactivation du mode silencieux

Le mode silencieux est activé par défaut. A moins que vous ne subissiez des attaques du type *refus de service*, nous vous conseillons de ne pas l'activer, car les messages *ICMP* s'utilisent à des fins tout à fait légitimes sur les réseaux et notamment dans le cadre du partage de fichiers.

Pour désactiver le mode silencieux

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Outils, cliquez sur **Paramètres de protection**.
3. Dans la zone de dialogue Paramètres de protection, cliquez sur **Configuration personnalisée**.
4. Désélectionnez l'option **Activer le mode silencieux**.
5. Cliquez sur **Enregistrer**.

Bloquer toute activité suspecte

Une activité suspecte est définie par Norton Personal Firewall comme une transmission de *paquets de données* dont les *adresses IP* sources ont été usurpées (et qui ressemblent donc à un hôte connu).

Vous pouvez vous protéger contre les activités suspectes en entrée et en sortie. La protection contre les activités suspectes sortantes évite que votre ordinateur ne contamine d'autres ordinateurs. La protection contre les activités suspectes entrantes empêche ce genre d'attaques d'atteindre votre ordinateur.

Pour bloquer les activités suspectes

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Outils, cliquez sur **Paramètres de protection**.
3. Dans la zone de dialogue Paramètres de protection, cliquez sur **Configuration personnalisée**.
4. Sélectionnez l'option **Activer la protection contre les activités suspectes**.
5. Choisissez si vous souhaitez refuser tout trafic sortant suspect, tout trafic entrant suspect ou les deux.
6. Cliquez sur **Enregistrer**.

A propos du protocole UDP

Le protocole *UDP (User Datagram Protocol)* est un *protocole* relativement simple, utilisé pour certaines opérations Internet. Le système DNS (*Domain Name System*) fait appel au protocole UDP pour la conversion des *noms d'hôtes* en *adresses IP*, par exemple.

La protection des *ports* UDP est généralement inutile. Si vous devez toutefois protéger un port UDP pour une raison précise, faites-le avec circonspection. Le refus d'accès à des *services* UDP peut entraîner des problèmes de connexion à Internet.

Activation de la protection UDP

Dans la plupart des cas, vous n'aurez à protéger que les *ports UDP* jusqu'à 1023. Les ports UDP de numéro inférieur sont utilisés pour les *services* standard tels que *DHCP (Dynamic Host Configuration Protocol)*, généralement utilisé pour obtenir l'*adresse IP* d'un ordinateur, ou NTP (Network Time Protocol), qui peut être utilisé par le panneau de configuration de la date et de l'heure. Les numéros de port supérieurs sont utilisés dynamiquement par certains services UDP tels que *DNS*. Le refus d'accès à ces ports désactive les services correspondants, puisque rien ne permet de déterminer le port qui sera utilisé par un service précis.

Pour éviter tout problème lié à l'activation de la protection UDP, vous pouvez autoriser l'accès à des services essentiels. Cette option implique que des services tels que DHCP et DNS peuvent continuer à fonctionner librement.

Pour activer la protection UDP

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Outils, cliquez sur **Paramètres de protection**.
3. Dans la zone de dialogue Paramètres de protection, cliquez sur **Configuration personnalisée**.
4. Sélectionnez l'option **Activer la protection UDP**.
5. Cochez les options UDP comme vous le souhaitez. Les options possibles sont les suivantes :
   - Protéger les connexions UDP sortantes
   - Autoriser l'accès aux services essentiels
   - Protéger tout ou partie des ports UDP
6. Cliquez sur **Enregistrer**.

Principes du fonctionnement de la protection UDP

Une fois activée, la protection *UDP* fonctionne sur le même principe que la protection TCP. Norton Personal Firewall s'appuie sur la même liste de *services* pour les ports UDP et TCP. Un service utilise normalement soit un *port* TCP, soit un port UDP, mais Norton Personal Firewall protège les deux types de ports pour un service donné (si la protection UDP est active pour ce port).

La protection UDP diffère de la protection TCP car le protocole UDP est un *protocole* sans connexion (l'envoi d'un message n'exige pas de connexion), tandis que TCP est un protocole orienté connexion (l'envoi d'un message exige une connexion préalable). Avec TCP, Norton Personal Firewall peut autoriser ou refuser la tentative de connexion exclusivement, sans incidence sur les informations qui suivent. Avec UDP, Norton Personal Firewall doit autoriser ou refuser chaque élément d'information destiné à un service particulier. Par conséquent, il ne peut pas bloquer uniquement les tentatives de connexions entrantes, mais doit bloquer toutes les communications associées au service.

Les autres différences par rapport au protocole UDP concernent la consignation et la notification. Avec TCP, même si aucun service n'est actif sur un port donné, Norton Personal Firewall reçoit une notification des tentatives d'accès à ce port et peut alors les consigner. En règle générale, Norton Personal Firewall ne reçoit pas de notification des tentatives d'accès aux ports UDP inactifs. Ces tentatives ne sont pas consignées et ne sont pas répertoriées dans le journal Historique des accès.

Si vous activez la protection UDP, celle-ci crée une entrée de journal pour les tentatives d'accès UDP, même si les ports UDP sont inactifs.

Se reporter à « Modification des préférences de consignation » à la page 74.

UDP étant un protocole sans connexion, Norton Personal Firewall crée une entrée de journal et une notification pour chaque *paquet* UDP transmis sur les ports actifs protégés (à condition que les options appropriées aient été configurées). Vous pouvez choisir de ne pas consigner les accès autorisés si vous avez activé la protection UDP, car le nombre d'entrées de journal généré serait considérable. Le système *DNS* utilisant un port UDP, par exemple, le journal contiendrait une entrée pour chaque tentative de connexion à un site Web.

Problèmes et solutions dans Norton Personal Firewall

9

Forum aux questions

Cette section aborde les questions les plus fréquentes liés à l'utilisation d'un pare-feu.

Comment désactiver la protection anti-intrusion ?

Désactivez la protection anti-intrusion à partir de la fenêtre Configuration.

Pour désactiver la protection anti-intrusion à partir de la fenêtre Configuration

1. Ouvrez Norton Personal Firewall.
2. Si la fenêtre Configuration n'apparaît pas, ouvrez le menu Outils et cliquez sur **Configuration**.
3. Dans la fenêtre Configuration, désélectionnez **Activer Norton Personal Firewall**.

Pour désactiver Norton Personal Firewall pendant un laps de temps spécifié

1. Dans la barre de menus Finder, cliquez sur l'icône Norton QuickMenu.
2. Dans Norton QuickMenu, cliquez sur **Norton Personal Firewall > Désactiver temporairement le pare-feu**….
3. Dans la fenêtre Désactiver temporairement le pare-feu, tapez le nombre de minutes que vous souhaitez affecter à la désactivation de Norton Personal Firewall.
4. Cliquez sur **Réparer**.

Pourquoi m'est-il impossible d'accéder aux sites Web ?

Vous avez probablement activé la protection *UDP* et affecté un *service* de bas niveau requis par votre ordinateur à l'exécution d'activités Internet. Dans ce cas, procédez comme suit :

- *DHCP* : Vérifiez les paramètres *TCP/IP* dans la zone de dialogue Préférences Système du réseau pour voir si la configuration de votre ordinateur permet d'obtenir son *adresse IP* en utilisant DHCP. Si c'est le cas, Norton Personal Firewall a créé une entrée de service pour le protocole DHCP. Modifiez cette entrée de service pour faire en sorte que le serveur DHCP puisse accéder à votre ordinateur. Utilisez l'adresse IP du serveur DHCP indiquée dans le fichier journal Historique des accès.
- *DNS* : La plupart des opérations Internet sortantes s'appuient sur le système DNS qui convertit les *noms d'hôte* en adresses IP. Assurez-vous de ne pas bloquer les *ports* dynamiques utilisés par le service DNS (ports 32768 et supérieurs, en règle générale).
- Assurez-vous d'avoir sélectionné l'option permettant l'accès aux services essentiels, dans vos paramètres de protection. Cette option évite les interférences avec les services DHCP et DNS ainsi qu'avec les autres services Internet standard.

A quel service correspond ce numéro de port ?

Vous trouverez ci-dessous les numéros de *port* TCP et *UDP* généralement utilisés par les *services* Macintosh.

Numéros de port TCP

Port	Utilisation	Commentaires
20	Données FTP	Exclusivement utilisé en tant que port source
21	Contrôle FTP	
23	Telnet	Port par lequel s'effectuent généralement les attaques
25	SMTP (courrier électronique)	
53	DNS	Utilise principalement des ports UDP et pas TCP
70	Gopher	

Port	Utilisation	Commentaires
79	Finger	
80	HTTP (Web)	
88	Kerberos	
105	PH (service d'annuaire)	
106	Poppass (modification de mot de passe)	
110	POP3 (courrier électronique)	
111	RPC (Appel de procédure à distance)	Utilisé pour de nombreux programmes UNIX
113	AUTH	
119	NNTP (news)	
139	Session NETBIOS	Accès Windows (ASIP 6)
143	IMAP (nouveau système de courrier électronique)	
311	AppleShare Web Admin	ASIP versions 6,1 et ultérieures
384	ARNS (tunnellisation)	
387	AURP (tunnellisation)	
389	LDAP (service d'annuaire)	
407	Timbuktu version 5.2 ou ultérieure	Les versions antérieures utilisent d'autres ports
427	SLP (recherche de services)	Utilise exclusivement TCP pour les réponses volumineuses
443	SSL (HTTPS)	
497	Retrospect	UDP pour la recherche de clients
510	Serveur FirstClass	
515	LPR (impression)	
548	AFP (AppleShare)	
554	RTSP (serveur QuickTime)	Utilise aussi les ports UDP 6970+

Port	Utilisation	Commentaires
591	FileMaker Pro Web	Alternative recommandée pour le port 80
626	IMAP Admin	Extension Apple dans ASIP 6
660	ASIP Remote Admin	ASIP versions 6.3 et ultérieures
666	Désormais serveur de contact	Viole l'affectation de port existante
687	Port U&G partagé ASIP	ASIP versions 6,2 et ultérieures
1080	WebSTAR Admin	Numéro de port WebSTAR supérieur à 1000
1417	Contrôle Timbuktu (antérieur à la version 5.2)	La connexion s'effectue par l'intermédiaire du port UDP 407
1418	Examen Timbuktu (antérieur à la version 5.2)	La connexion s'effectue par l'intermédiaire du port UDP 407
1419	Envoi de fichiers Timbuktu (antérieur à la version 5.2)	La connexion s'effectue par l'intermédiaire du port UDP 407
1420	Echange Timbuktu (antérieur à la version 5.2)	La connexion s'effectue par l'intermédiaire du port UDP 407
1443	WebSTAR/SSL Admin	Numéro de port WebSTAR supérieur à 1000
3031	Lien entre applications (événements Apple)	Mac OS 9 et versions ultérieures
4000	Désormais serveur d'événements public	
4199	EIMS Admin	
4347	Répondeurs LANsurveyor	Les ports UDP sont également utilisés
5003	FileMaker Pro	Accès direct et non pas accès Web ; port UDP pour la liste des hôtes
5190	AOL Instant Messenger	
5498	Tracker Hotline	Port UDP 5499 pour la recherche de serveurs
5500	Serveur Hotline	

Port	Utilisation	Commentaires
5501	Serveur Hotline	
7070	RealPlayer	Utilise également les ports UDP 6970-7170
7648	CuSeeMe (vidéo)	Connexions clientes ; ports UDP pour les services audio/vidéo
7649	CuSeeMe (vidéo)	Etablissement de connexions
8080	Alternative HTTP courante	
19813	Serveur 4D	Précédemment port 14566 (versions 6.0 et antérieures)

Numéros de ports UDP

Port	Utilisation	Commentaires
53	DNS	Utilise parfois des ports TCP
68	DHCP (Dynamic Host Configuration Protocol)	Généralement utilisé pour obtenir l'adresse IP d'un ordinateur
69	TFTP (Trivial File Transfer Protocol)	
123	Network Time Protocol	
137	Service de noms Windows	
138	Service de datagrammes Windows	
161	SNMP (Simple Network Management Protocol)	
407	Timbuktu	Négociation seulement, antérieur à la version 5.2
458	QuickTime TV	
497	Retrospect	Recherche de clients sur le réseau
514	Syslog	
554	Real Time Streaming Protocol (QuickTime)	
2049	NFS (Network File System)	

Port	Utilisation	Commentaires
3283	Assistant réseau Apple	
5003	FileMaker Pro	Pour l'obtention de la liste des hôtes
6970 +	QuickTime et RealPlayer	
7070	Alternative à RTSP (RealPlayer)	

Comment créer un nouveau fichier journal ?

Si votre fichier journal s'avère difficilement maniable en raison de sa taille, vous pouvez en créer un nouveau. La suppression de l'ancien fichier journal n'est pas obligatoire ; vous pouvez l'enregistrer et l'archiver.

Si vous ne désactivez pas la consignation avant de renommer ou de déplacer le fichier journal, Norton Personal Firewall poursuit la consignation des événements dans ce fichier jusqu'à ce que la consignation soit désactivée ou l'ordinateur redémarré, après quoi le nouveau fichier est créé.

Pour créer un nouveau fichier journal

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Personal Firewall, cliquez sur **Préférences**.
3. Dans la fenêtre Préférences de Personal Firewall, cliquez sur **Consignation**.
4. Désactivez la consignation.

Se reporter à « Désactivation de la consignation » à la page 75.

5. Choisissez l'une des options suivantes :
   - Renommez le fichier journal (intitulé Journal Norton Personal Firewall, à l'origine).
   - Sortez le fichier journal du dossier Library:Application Support:Norton Solutions Support:Norton Personal Firewall.
6. Réactivez la consignation.

Se reporter à « Modification des préférences de consignation » à la page 74.

Pourquoi le chargement de Norton Personal Firewall est-il impossible ?

Le système est peut-être bloqué. Essayez de supprimer le fichier de préférences, intitulé com.symantec.NPF.plist, dans Library:Preferences.

Pourquoi le partage de fichiers est-il inopérant ?

Se reporter à "Protection des services Internet standard" à la page 81.

Vous avez peut-être activé le partage de fichiers via *TCP/IP*. Par défaut, tous les *services* TCP/IP sont initialement protégés contre tout accès. Vous devez autoriser l'accès au partage de fichiers avant de pouvoir y recourir.

Pourquoi m'est-il impossible d'installer Norton Personal Firewall pour Mac OS X ?

Vous devez posséder un mot de passe administrateur pour installer Norton Personal Firewall sous Mac OS X.

Pourquoi m'est-il impossible de créer un alias pour Norton Personal Firewall ?

Si Norton Personal Firewall a été installé sous un identifiant de connexion Mac OS différent de celui que vous utilisez, vous n'avez pas la possibilité de créer d'*alias* à cause des autorisations d'accès définies sous Mac OS X. Demandez à la personne qui a installé le logiciel de créer un alias et de le placer dans une zone qui vous est accessible. Faites ensuite glisser l'alias jusqu'à l'emplacement de votre choix.

Les entrées que je crée dans IPFW disparaissent systématiquement

Norton Personal Firewall utilise ses propres paramètres pour les opérations d'écriture dans IPFW. Toutes les entrées créées indépendamment sont écrasées.

Questions relatives aux réseaux locaux domestiques

Consultez cette section si vous possédez un réseau local domestique.

Comment protéger tous les ordinateurs présents sur mon réseau local domestique ?

Installez une copie de Norton Personal Firewall sur les ordinateurs qui ont accès à Internet. La présence de Norton Personal Firewall est inutile sur tous les autres ordinateurs du réseau.

Une copie de Norton Personal Firewall doit cependant être installée sur tous les ordinateurs connectés à un module Airport.

Comment spécifier l'accès à un ordinateur dont l'adresse IP est générée de façon dynamique?

Se reporter à « Pour afficher le journal Historique des accès » à la page 70.

Des *adresses IP* différentes sont généralement attribuées aux ordinateurs qui obtiennent leur adresse IP par le biais du protocole *DHCP (Dynamic Host Configuration Protocol)* chaque fois qu'ils se connectent à un réseau. Leurs adresses IP se situent toutefois dans une plage précise. Déterminez cette plage à partir du fichier journal Historique des accès, en recherchant les accès refusés à cet ordinateur et en notant les adresses IP utilisées.

Se reporter à « Pour ajouter une plage d'adresses » à la page 83.

Vous pouvez ensuite spécifier cette plage dans la liste d'adresses IP du *service* pour lequel vous devez définir des accès.

Quelle est l'incidence de la protection anti-intrusion sur le partage de fichiers et d'imprimantes ?

Se reporter à « Protection des services Internet standard » à la page 81.

Norton Personal Firewall assure la sécurité des connexions *TCP/IP*. Il n'affecte en aucune façon les connexions *AppleTalk* sous Mac OS 8.1 à 9.x. Si vous souhaitez que d'autres ordinateurs aient accès au partage de fichiers sur votre ordinateur via TCP/IP, indiquez leurs *adresses IP* dans la liste des accès autorisés pour le partage de fichiers.

Sous Mac OS X, AppleTalk utilise aussi TCP/IP pour le partage de fichiers et le lien entre applications. Assurez-vous que les accès aux services de partage de fichiers et de lien entre applications sont autorisés pour les ordinateurs auxquels vous vous connectez par l'intermédiaire d'AppleTalk.

3

Norton AntiVirus

Protection des disques, des fichiers et des données contre les virus

10

Bien que Auto-Protect surveille votre ordinateur à la recherche de virus en examinant les fichiers créés ou copiés et en examinant tous les disques et supports amovibles lors de leur montage, il se peut qu'Auto-Protect ne détecte pas des nouveaux virus. Avec Norton AntiVirus, vous pouvez rechercher les virus dans n'importe quel fichier, dossier ou disque.

Examen des disques, des dossiers et des fichiers

Lancez le programme principal de Norton AntiVirus pour examiner vos disques.

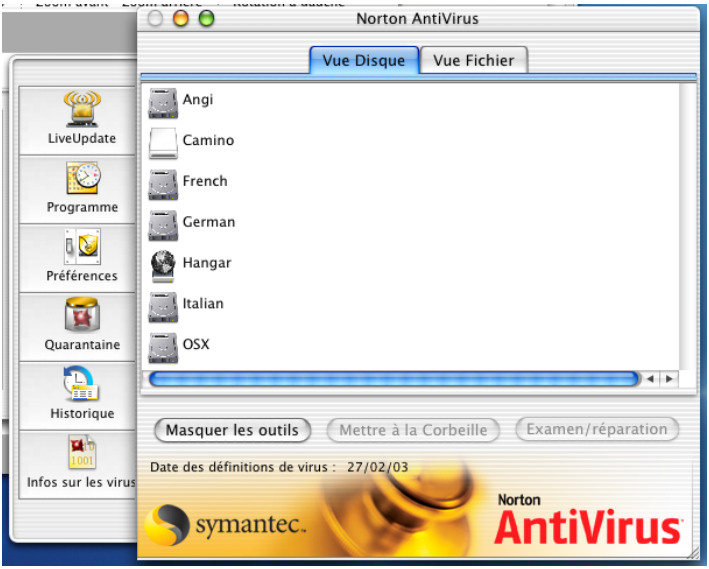
Norton AntiVirus examine les seuls fichiers pour lesquels vous disposez de privilèges d'accès. Même si vous êtes connecté en tant qu'Administrateur, l'analyse de certains répertoires et fichiers système est impossible. Ces fichiers ne peuvent être examinés que si vous êtes connecté en tant qu'utilisateur racine. Toutefois, à moins que vous ne soyez connecté en tant qu'utilisateur racine pour travailler sur votre ordinateur, les risques d'infection de ces fichiers sont pratiquement inexistants, car le compte racine est désactivé par défaut sous Mac OS X. Si vous ne vous connectez jamais en tant qu'utilisateur racine, exécutez les analyses lorsque vous travaillez en tant qu'Administrateur pour détecter d'éventuels virus.

Se reporter à « Pour vérifier votre type de connexion » à la page 20.

Vous pouvez personnaliser le mode d'examen de Norton AntiVirus. Norton AntiVirus peut rechercher des virus dans des fichiers *compressés*, mais non dans des fichiers cryptés. Les fichiers cryptés dont l'ouverture est soumise à un mot de passe doivent être décryptés avant d'être examinés.

Pour examiner des disques, des dossiers et des fichiers

1 Lancez Norton AntiVirus.



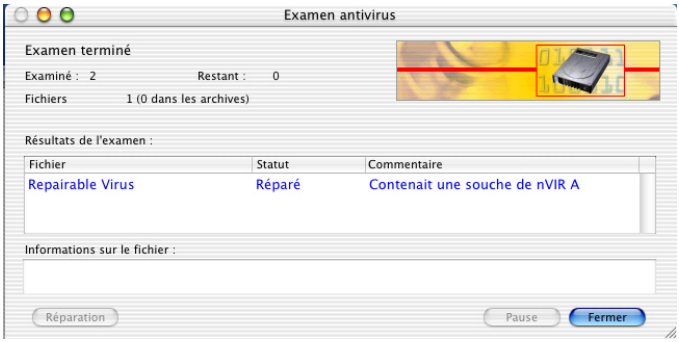
2 Dans la fenêtre de Norton AntiVirus, effectuez l'une des opérations suivantes:

- Dans la vue des disques, sélectionnez le disque à examiner.
- Dans la vue des fichiers, sélectionnez les dossiers ou fichiers spécifiques à examiner.

3 Cliquez sur **Examiner et réparer**.

4 Cliquez sur **Pause** pour interrompre un examen.
Pour reprendre l'examen, cliquez sur **Continuer**.

5 Pour afficher les informations détaillées sur un fichier sélectionné, consultez le volet de résultats de l'examen.



6 Pour afficher les informations détaillées sur un fichier sélectionné, consultez le volet d'informations sur les fichiers.

En cas de détection de problèmes lors d'un examen

Norton AntiVirus est conçu pour garder votre ordinateur exempt de virus. Dans la plupart des cas, un fichier infecté peut être réparé automatiquement. Votre intervention peut toutefois s'avérer nécessaire dans certains cas.

Sous Mac OS X, le fichier est automatiquement réparé si le paramètre Réparation est défini sur Automatique dans l'onglet Générales de la fenêtre Préférences.

Si le fichier n'est pas réparable, il peut être mis en quarantaine. La mise en quarantaine permet d'éviter la réinfection de votre ordinateur ou la détérioration d'autres fichiers.

Examen des pièces jointes au courrier électronique

Se reporter à « Réglage des préférences d'examen » à la page 121.

Norton AntiVirus Auto-Protect procède à un examen automatique des messages e-mail. Lorsque Auto-Protect et l'examen des *fichiers compressés* sont activés, l'examen du courrier électronique est entièrement fonctionnel.

Examen et réparation dans des archives

L'application Norton AntiVirus examine et répare automatiquement les fichiers contenus dans des archives. Par exemple, si vous ouvrez un fichier zip, Norton AntiVirus exemine et, le cas échéant, répare les fichiers sans intervention de l'utilisateur.

L'examen des archives Stuffit est limité à l'application Norton AntiVirus. Auto-Protect, le module d'examen de ligne de commande, l'examen au montage et l'examen programmé ne traitent pas les archives Stuffit. Tous les autres formats de fichiers compressés et d'archives sont examinés.

Affichage et impression de l'historique des examens

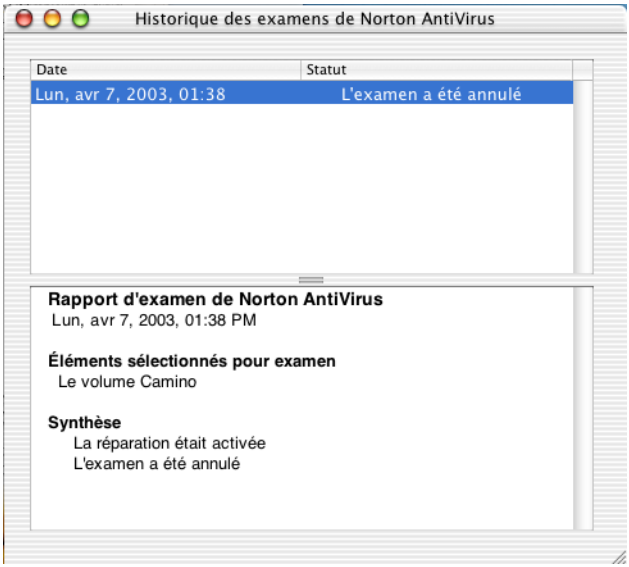
Norton AntiVirus enregistre automatiquement un rapport pour chaque examen. Vous pouvez afficher et imprimer ces résultats à la fin de chaque examen. Vous pouvez également consulter des examens précédents, grâce au fichier d'historique.

Enregistrement et impression de rapports d'examen

A la fin d'un examen, vous pouvez enregistrer les résultats dans un fichier de données. Vous pouvez indiquer le format du fichier dans les Préférences. L'enregistrement d'un rapport sous un format spécifique l'associe au traitement de texte correspondant. Vous pouvez imprimer un rapport d'examen à partir de la fenêtre des résultats de l'examen ou de la fenêtre Historique des examens.

Pour sélectionner un rapport en vue de son enregistrement ou de son impression

1 Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Historique**.



2 Dans le volet supérieur de la fenêtre Historique des examens de Norton AntiVirus, sélectionnez le rapport à afficher.
Les détails apparaissent dans le volet inférieur de la fenêtre.

Pour enregistrer le rapport d'examen sélectionné

1. Dans le menu Fichier, cliquez sur **Enregistrer le rapport**.
2. Dans la zone de dialogue qui apparaît, indiquez un nom et un emplacement pour le fichier. Le nom de fichier par défaut est <Rapport sans titre>.

3. Cliquez sur **Enregistrer**.

Pour imprimer le rapport d'examen sélectionné

1. Choisissez l'une des options suivantes :
   - Si les résultats de l'examen sont toujours affichés, cliquez sur **Imprimer**.
   - Si vous avez sélectionné un rapport dans la fenêtre Historique des examens, cliquez sur **Imprimer** dans le menu Fichier.
2. Dans la zone de dialogue d'impression, sélectionnez les options voulues pour imprimer le rapport.
3. Cliquez sur **Imprimer**.

Examen à partir de la ligne de commande

Command Line Scanner vous permet d'exécuter des examens à partir de la ligne de commande, d'obtenir des rapports d'examen et de les enregistrer. Vous pouvez créer des scripts à intégrer à d'autres scripts de maintenance UNIX.

Vous pouvez personnaliser les fonctions de Command Line Scanner pour effectuer les examens de votre choix. Voici quelques exemples d'examens de ligne de commande que vous pouvez exécuter :

- navx/
  Permet d'examiner votre disque système avec les options par défaut.
- navx -a -r /Users/philippe/
  Permet d'examiner, sans les réparer, tous les fichiers présents dans le dossier Départ de l'utilisateur Philippe, et d'obtenir un rapport sur leur état.
- navx -ar /Users/philippe/
  Permet d'examiner, sans les réparer, tous les fichiers présents dans le dossier Départ de l'utilisateur Philippe, et d'obtenir un rapport sur leur état.
- navx -o ~/myReportFile /tmp
  Permet d'examiner les fichiers placés dans le dossier /tmp, et d'enregistrer le rapport dans votre dossier Départ.
- navx -a -o ~/myReportFile /tmp > <fichier.log>
  Vous permet d'examiner les fichiers placés dans le dossier /tmp et d'enregistrer le rapport complet dans votre dossier Départ et dans un fichier journal.

Pour examiner un fichier à l'aide de Command Line Scanner

1. Ouvrez Terminal.
2. A l'invite, tapez **navx**.
3. Précisez la commande voulue. Les options possibles sont les suivantes :

-a	Répertorie tous les fichiers examinés, indépendamment de leur détérioration ou de la menace qu'ils représentent.
-c	Examine le contenu de fichiers compressés.
-f	Force l'exécution de l'examen en cas d'échec de création ou d'ouverture du fichier de sortie spécifié avec le commutateur -o.
-h	Dresse la liste des fichiers inaccessibles dont l'examen a été impossible.
-Q	Met en quarantaine les fichiers qui ne peuvent pas être réparés

-r	Ne répare pas les fichiers présentant des symptômes définis.
-v	Affiche le numéro de version.
-o <nom du fichier de sortie>	Ajoute les résultats au fichier <nom du fichier de sortie>. Si ce commutateur est associé au commutateur -Q, seule la synthèse s'affiche à l'écran, mais le rapport complet est ajouté au fichier <nom du fichier de sortie>.

4 Tapez le nom du fichier à examiner.

5 Appuyez sur **Entrée**.

Que faire en cas de détection de virus ?

11

Si Norton AntiVirus rapporte un problème, suivez les instructions fournies pour ce problème spécifique.

Il se peut que le message qui apparaît ne soit pas abordé dans ce chapitre. Pour de plus amples informations sur les messages, reportez-vous à la section « Problèmes et solutions dans Norton AntiVirus » à la page 123.

Auto-Protect détecte un virus

Norton AntiVirus Auto-Protect assure votre protection antivirale dès que vous démarrez votre ordinateur. Il recherche les virus dans les programmes au fur et à mesure de leur exécution et surveille, sur votre ordinateur, toute activité susceptible de trahir la présence d'un virus. Auto-Protect vous alerte en cas d'activité virale.

Par défaut, Auto-Protect est activé. Avec les réglages par défaut, Auto-Protect répare automatiquement les fichiers ou les met en quarantaine s'ils ne sont pas réparables.

Lorsqu'une *alerte* de virus apparaît sur votre écran, du fait de Norton AntiVirus Auto-Protect, l'opération en cours s'affiche ainsi que les possibilités d'intervention. Lisez le message avec attention pour savoir si vous devez effectuer une opération quelconque.

Auto-Protect détecte un virus et répare le fichier

Lorsque Norton AntiVirus Auto-Protect indique qu'il a réparé un fichier contaminé, vous n'avez plus rien à faire.

Même une fois qu'Auto-Protect a réparé le fichier contaminé, assurez-vous qu'il n'y a pas d'autres virus sur votre ordinateur en relançant un examen à l'aide de Norton AntiVirus.

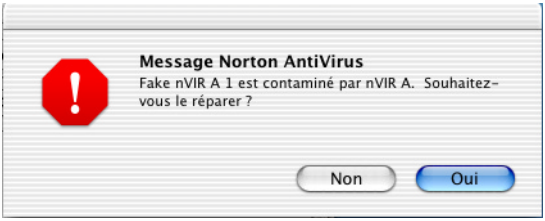
Auto-Protect détecte un virus mais ne répare pas le fichier

Se reporter à « A propos des préférences utilisateur » à la page 121.

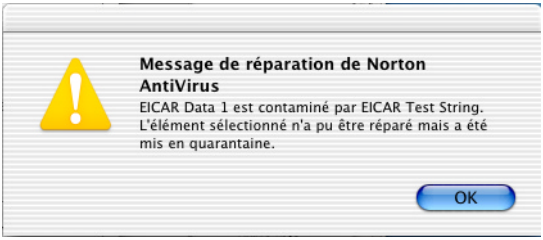
Si vous avez choisi l'option de réparation manuelle dans les préférences d'examens, Auto-Protect vous signale les fichiers infectés, mais ne les répare pas.

Pour réparer manuellement un fichier identifié comme infecté mais non réparé

1 Parcourez tout le message.
Recherchez les mots qui identifient le type du problème.



2 Cliquez sur **Oui**.
Si le fichier n'est pas réparable, il est automatiquement mis en quarantaine. Pour de plus amples informations sur les paramètres de mise en quarantaine, reportez-vous à la section « A propos des préférences utilisateur » à la page 121.



3 Cliquez sur **OK**.

Auto-Protect détecte un virus mais n'est pas en mesure de réparer le fichier

Dans de rares cas, Auto-Protect peut s'avérer incapable de réparer ou mettre en quarantaine un fichier infecté, que les préférences indiquent une réparation automatique ou non.

Pour supprimer un fichier identifié comme infecté mais dont la réparation est impossible

Se reporter à « Examen des disques, des dossiers et des fichiers » à la page 103.

❖ Cliquez sur **Oui** pour exécuter Norton AntiVirus et examiner le fichier ou le dossier contenant le virus.
Dans la fenêtre d'examen, vous pouvez afficher des informations supplémentaires sur le fichier infecté. Se reporter à « Si Norton AntiVirus ne peut pas réparer un fichier » à la page 115.

Un virus a été détecté à l'insertion du support amovible

Si Auto-Protect détecte un virus lorsqu'un *support amovible* est connecté à votre ordinateur, une *alerte* s'affiche, indiquant ce qui s'est passé et quelles options sont disponibles. Se reporter à « Auto-Protect détecte un virus » à la page 111 et « Un virus est détecté lors d'un examen manuel » à la page 114.

Réparation, suppression et restauration de fichiers en quarantaine

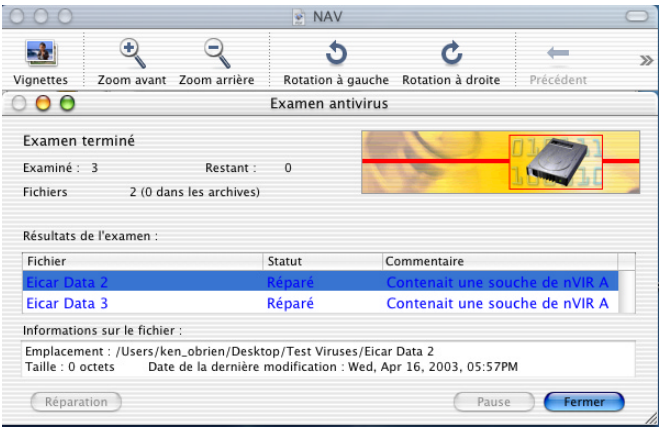
Une fois que des fichiers ont été mis en quarantaine, vous pouvez tenter de les réparer, les supprimer ou les restaurer.

Un virus est détecté lors d'un examen manuel

Si vous procédez à un examen avec Norton AntiVirus et qu'un virus est détecté, une *alerte* s'affiche dans la fenêtre d'examen. Généralement, les fichiers infectés sont réparés ou mis en quarantaine automatiquement et vous n'avez pas à intervenir. Pour déterminer si le fichier a été réparé ou si vous devez prendre d'autres mesures, vérifiez l'état du fichier dans la fenêtre d'examen.

Pour vérifier l'état des fichiers infectés dans la fenêtre d'examen

- Dans la fenêtre de Virus Scan, sélectionnez le fichier infecté parmi les résultats d'examen.



Réparation des fichiers infectés

Si un fichier infecté répertorié dans la fenêtre d'examen n'a pas été réparé parce que l'option de réparation automatique est désactivée dans les Préférences et que l'option de mise en quarantaine des fichiers irréparables est désactivée, procédez à une réparation manuelle.

Pour réparer des fichiers infectés

1. Dans la fenêtre des résultats d'examen, sélectionnez les fichiers à réparer.
2. Cliquez sur **Réparer**.
3. Après avoir réparé tous les fichiers infectés, effectuez un nouvel examen de vos disques pour vous assurer que tous les fichiers sont sains.
4. Vérifiez que les fichiers réparés sont bien utilisables.
   Par exemple, si vous avez réparé un fichier de traitement de texte, ouvrez-le, modifiez-le et enregistrez-le.

Si Norton AntiVirus ne peut pas réparer un fichier

Se reporter à « Vérification des numéros de version et des dates » à la page 49.

Si Norton AntiVirus ne peut pas réparer le fichier infecté, assurez-vous d'abord que vous avez utilisé pour l'examen les dernières *définitions de virus*. Si vous n'en êtes pas sûr, exécutez LiveUpdate. Examinez ensuite votre disque dur à partir des dernières définitions de virus en date.

Si un support amovible est infecté

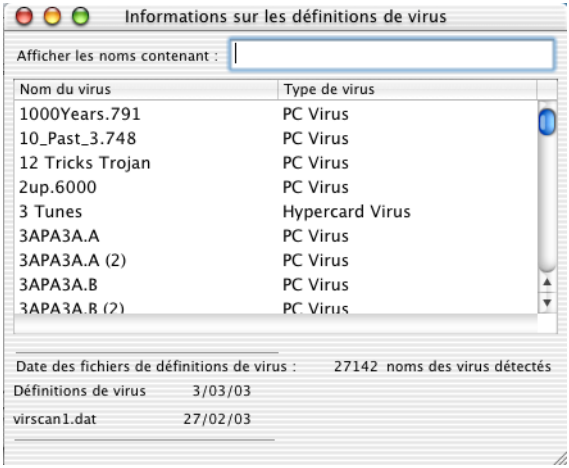
Pour réparer le support infecté, examinez-le avec Norton AntiVirus et exécutez les actions préconisées.

Pour réparer un support amovible infecté

1. Lancez Norton AntiVirus.
2. Dans la fenêtre principale de Norton AntiVirus, sélectionnez le support à examiner.
3. Cliquez sur **Examiner et réparer**.

Recherche des noms et des définitions de virus

Vous pouvez rechercher un nom de virus à partir de l'application Norton Antivirus. La zone de dialogue d'informations sur les définitions de virus répertorie les virus placés dans le fichier de *définition de virus* en cours. Pour être sûr que vous disposez bien des dernières définitions de virus, exécutez LiveUpdate. Vous pouvez exporter la liste dans un fichier texte. Vous avez également la possibilité de rechercher un virus spécifique.



Pour rechercher des noms de virus

1. Dans le menu Outils, cliquez sur **Infos sur les virus**.
2. Tapez le nom du virus ou une partie de celui-ci.

Recherche de définitions de virus sur le site Web de Symantec

Les virus étant très nombreux, le fichier d'informations sur les définitions de virus ne propose pas une description pour chacun d'eux. Le site Web de Symantec Security Response propose une liste complète de tous les virus connus accompagnés de leur code malveillant ainsi que d'une description.

Pour rechercher des définitions de virus

1. Pointez sur le site Web Symantec Security Response dans votre navigateur : http://www.symantec.fr/region/fr/avcenter/index.html
2. Cliquez sur **Liste à jour des menaces**.
3. Choisissez l'une des options suivantes :
   - Saisissez le nom du virus à rechercher.
   - Parcourez la liste alphabétique pour localiser le virus recherché.
4. Cliquez sur un virus pour lire sa description.

Personnalisation de Norton AntiVirus

12

Norton AntiVirus offre les meilleures conditions de détection et de suppression de virus avec les réglages par défaut. Si vous souhaitez modifier ces réglages parce que vous souhaitez extraire des données d'un fichier avant sa suppression ou sa réparation suite à une infection, vous pouvez le faire.

Il y a trois types de préférences à définir. Les options possibles sont les suivantes :

Examiner et réparer	Réglages qui régissent le comportement de Norton AntiVirus et réglages que les utilisateurs peuvent spécifier séparément
Auto-Protect	Réglages régissant le comportement global de la protection antivirus et de la réparation pour votre ordinateur
Rappel	Réglages pour les préférences de Virus Definition Alert

A propos des préférences d'Auto-Protect

Les réglages Auto-Protect actifs offrent une protection antivirus continue. Vous pouvez cependant changer les réglages de la protection antivirus automatique si vous souhaitez réparer ou supprimer manuellement un fichier ou examiner manuellement un *support amovible* lors de son insertion.

Vous pouvez changer une série de réglages relatifs à la façon dont Norton AntiVirus Auto-Protect répare les fichiers.

Pour une protection maximale, laissez Auto-Protect activé et ne changez pas les préférences par défaut dans la fenêtre de Norton Auto-Protect.

Réglage des préférences d'Auto-Protect

Déterminez la façon dont vous voulez que Norton Auto-Protect surveille les virus et répare les fichiers infectés.

Pour régler les préférences d'Auto-Protect

1. Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Préférences**.
2. Dans la fenêtre des préférences, cliquez sur l'onglet **Auto-Protect**.
3. Cliquez sur **Lancer les préférences d'Auto-Protect**.
4. Dans la fenêtre de Norton Auto-Protect, cliquez sur le cadenas pour pouvoir apporter des modifications.
5. Dans la zone de dialogue d'authentification, indiquez vos nom et mot de passe d'administrateur.
6. Cliquez sur **OK**.
7. Sélectionnez les options Auto-Protect voulues. Les options possibles sont les suivantes :

Auto-Protect	Fournit une surveillance automatique des virus. Si vous désactivez Auto-Protect, toutes les autres options automatiques sont indisponibles.
Réparation automatique	Répare automatiquement les fichiers infectés trouvés.
Quarantaine	Met automatiquement en quarantaine les fichiers qui ne peuvent pas être réparés.
Examiner les disques au montage	Examine automatiquement les supports amovibles tels que CD, disques Zip ou iPod lors de leur insertion dans l'ordinateur.
Examiner les fichiers compressés	Examine automatiquement les fichiers compressés.

8. Refermez la fenêtre pour enregistrer vos modifications.

A propos des préférences utilisateur

Vous pouvez modifier les préférences configurées au moment de l'installation de Norton AntiVirus pour Macintosh. Les utilisateurs individuels peuvent en outre spécifier leur propres réglages Norton AntiVirus.

Pour assurer une protection maximale, ne changez pas les préférences par défaut des onglets Examiner, Reparer et Rappel.

Réglage des préférences d'examen

Déterminez la façon dont Norton AntiVirus doit examiner les disques et les fichiers.

Pour régler les préférences d'examen

1. Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Préférences**.
2. Dans la fenêtre Préférences, onglet Examiner, sélectionnez les options voulues. Les options possibles sont les suivantes :

Examiner les fichiers compressés	Examine les fichiers compressés. L'examen d'un disque peut être plus long si vous examinez les fichiers compressés.
Résultats	Détermine les fichiers à énumérer dans le volet de résultats d'examen de la fenêtre Examiner.
Alertes d'examen programmé	Spécifie si vous voulez toujours une alerte d'examen ou uniquement lorsque des fichiers infectés sont trouvés.
Format du rapport	Sélectionne le programme dans lequel les rapports antivirus enregistrés seront visualisés.

3. Cliquez sur **Enregistrer**.

Réglage des préférences de réparation

Déterminez la façon dont Norton AntiVirus doit réparer les fichiers infectés trouvés lors d'un examen manuel.

Pour régler les préférences de réparation

1. Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Préférences**.
2. Dans la fenêtre des préférences, cliquez sur l'onglet **Réparer**.
3. Sélectionnez les options de réparation voulues. Les options possibles sont les suivantes :

Réparation	Pendant un examen manuel, choisissez si les fichiers infectés doivent être réparés automatiquement ou manuellement.
Mettre en quarantaine les fichiers qui ne peuvent pas être réparés	Pendant un examen manuel, choisissez si les fichiers qui ne peuvent pas être réparés doivent être automatiquement mis en quarantaine.

4. Cliquez sur **Enregistrer**.

Définition d'un rappel

Vous pouvez faire en sorte de recevoir un rappel émis par Norton AntiVirus lorsque vos *définitions de virus* sont périmées. Vous devez impérativement vous procurer les dernières définitions de virus en date pour préserver votre ordinateur de toute contamination.

Problèmes et solutions dans Norton AntiVirus

13

Les problèmes présentés ne sont pas directement liés aux activités virales. Si vous ne pouvez pas résoudre votre problème, consultez le fichier Readme sur le CD Norton Internet Security pour Macintosh.

Vous trouverez la liste complète des derniers conseils en date sur le site Service et Support technique de Symantec, à l'adresse suivante : www.symantec.com/frsupport/

Problèmes d'installation

Si vous rencontrez des problèmes lors de l'installation de Norton Internet Security, essayez de redémarrer et de réinstaller Norton Internet Security. Ou bien, faites une copie du programme d'installation Mac OS X à partir du CD Norton Internet Security pour Macintosh, collez-la sur votre ordinateur et effectuez l'installation à partir de là.

Installation impossible de Norton Internet Security

Vous devez démarrer l'ordinateur sous Mac OS X pour pouvoir exécuter le programme d'installation de Norton Internet Security pour Mac. Vous devez en outre connaître le mot de passe d'administrateur.

Problèmes de démarrage

Les problèmes de démarrage peuvent être liés à votre ordinateur, à Norton AntiVirus ou aux paramètres que vous avez définis.

Norton AntiVirus Auto-Protect ne se charge pas au démarrage

Si Auto-Protect ne se charge pas, assurez-vous que tous les fichiers du moteur et toutes les définitions de virus sont installés. Norton AntiVirus Auto-Protect ne fonctionne pas sans eux.

Norton AntiVirus indique qu'un fichier est endommagé au lancement ou à l'activation d'un examen, ou à l'allumage du Macintosh

Ceci indique que l'un des fichiers de *définitions de virus* est endommagé ou non valide.

Pour réparer un fichier de définitions de virus endommagé sous Mac OS X

1. Désinstallez Norton Internet Security
2. Réinstallez Norton Internet Security.
3. Lancez LiveUpdate et mettez à jour vos définitions de virus. Les versions actuelles des éléments placés dans le dossier Norton AntiVirus Additions sont restaurées.

Se reporter à « Installation » à la page 20.

Norton AntiVirus ne trouve pas le fichier des définitions de virus

Réinstallez Norton Internet Security.

Pourquoi m'est-il impossible de créer un alias pour Norton AntiVirus ?

Si vous n'avez pas installé vous-même Norton AntiVirus, vous n'avez pas la possibilité de créer d'alias pour le logiciel à cause des autorisations d'accès définies sous Mac OS X. Demandez à la personne qui a installé le logiciel de créer un alias et de le placer dans une zone qui vous est accessible. Faites ensuite glisser l'alias jusqu'à l'emplacement de votre choix.

Problèmes de protection

Un fichier est endommagé, Norton AntiVirus n'a plus de place en mémoire, ou une erreur s'est produite lors de l'examen.

Pour déterminer si le problème est imputable à un fichier

1. Lancez Norton AntiVirus.
2. Dans l'onglet Vue Fichier, cliquez sur le triangle en regard du disque pour afficher les dossiers qu'il contient.
3. Examinez les dossiers l'un après l'autre pour tenter d'isoler le problème.
4. Relancez l'examen du disque depuis la fenêtre principale de Norton AntiVirus. Vous pouvez aussi tester l'intégrité du disque avec un utilitaire tel que Norton Disk Doctor, intégré aux Norton Utilities pour Macintosh.

Examen et privilèges d'accès des comptes

Norton AntiVirus examine uniquement les fichiers pour lesquels votre compte dispose de privilèges d'accès. S'il vous arrive parfois de vous connecter et de travailler en tant qu'utilisateur racine, effectuez l'examen à ce moment-là. Si vous ne vous connectez jamais en tant qu'utilisateur racine, effectuez l'examen lorsque vous travaillez en tant qu'administrateur pour analyser tous les fichiers susceptibles d'être infectés. Si vous ne souhaitez pas afficher la liste des fichiers dont l'analyse est impossible à cause d'un refus d'accès, cochez la case Ignorer les erreurs de permissions dans la zone de dialogue Préférences.

Je dois réexaminer des fichiers déjà analysés

Le fichier QuickScan de Norton AntiVirus indique si vous avez déjà examiné un fichier à partir des définitions de virus et bibliothèques installées. Si ce n'est pas le cas, le fichier est examiné. Si vous souhaitez malgré tout réexaminer l'ensemble des fichiers, faites appel à Norton AntiVirus pour supprimer le fichier QuickScan à la racine de chaque disque. Le fichier est nommé NAVMac800QSFile.

Pour supprimer le fichier QuickScan

1. Dans la fenêtre de Norton AntiVirus, cliquez sur l'onglet Vue Fichier et assurez-vous que la case Afficher les fichiers invisibles est cochée.
2. Sélectionnez le disque dur.
3. Cliquez sur le fichier QuickScan.
   Sélectionnez également les fichiers QuickScan des versions antérieures de Norton AntiVirus, le cas échéant.
4. Cliquez sur **Corbeille**.

5 Cliquez sur **OK**.

6 Quittez Norton AntiVirus.

7 Dans le Finder, videz la Corbeille.

Après la suppression du fichier QuickScan, la première analyse effectuée à partir des nouvelles *définitions de virus* est plus lente.

Je ne parviens pas à mettre à jour mes définitions de virus avec LiveUpdate

Dans certains cas relativement rares, notamment juste après l'apparition d'un nouveau virus, il se peut que le serveur LiveUpdate soit encombré. N'hésitez pas, dans ce cas, à renouveler souvent votre tentative de connexion.

Avant d'utiliser LiveUpdate, vérifiez que votre connexion à Internet est opérationnelle, à l'aide par exemple d'un navigateur Web.

Autres solutions

Voici quelques suggestions supplémentaires qui vous aideront à régler d'éventuels problèmes.

- Réinstallez le Système ou passez à une version plus récente. Pour de plus amples informations, consultez la documentation du Système Macintosh.
- Réinstallez Norton AntiVirus.
- Réinitialisez la PRAM (RAM des paramètres). Pour de plus amples informations, consultez la documentation du Système Macintosh.

Messages d'erreur

Cette annexe regroupe la majorité des messages qui peuvent s'afficher lors de l'utilisation de Norton Antivirus et de Norton Antivirus Auto-Protect.

Norton AntiVirus utilise la mémoire vive pour stocker les éléments à consigner dans le rapport d'examen. Si vous avez trop de fichiers, vous ne pourrez pas tous les consigner dans le rapport. Vous pouvez modifier les préférences de rapports pour ne répertorier que les fichiers infectés.

Message d'erreur Auto-Protect

Si le moteur d'examen produit un message d'erreur, vous avez peut-être encore des fichiers incompatibles issus d'une version précédente de Norton AntiVirus pour Macintosh. Désinstallez, puis réinstallez Norton AntiVirus.

Mot de passe et messages d'administrateur

Le code d'abonnement est erroné. Veuillez le ressaisir.

Vous avez entré un mauvais code d'abonnement aux mises à jour de définitions de virus. Saisissez à nouveau le code.

Les deux mots de passe sont différents. Veuillez recommencer.

Le second mot de passe saisi est différent du premier.

Mot de passe incorrect. Veuillez recommencer.

Vous avez tapé un mot de passe incorrect. Si vous l'avez oublié, reportez-vous à la section « Installation » à la page 20.

Le logiciel à installer exige des privilèges d'administration au minimum.

Saisissez votre mot de passe d'administrateur.

4

Norton Privacy Control

Utilisation de Norton Privacy Control

14

Norton Privacy Control vous offre trois fonctions permettant de sécuriser votre navigation en ligne et de vous tranquilliser. En outre, Norton Privacy Control propose un rapport statistique pour ces fonctions.

Blocage des publicités	Empêche l'affichage de publicités indésirables lors de la connexion à des sites Web.
Données confidentielles	Empêche la récupération des données personnelles stockées sur votre ordinateur, sans votre permission.
Contrôle parental	Interdit l'accès à des sites Web inconvenants, depuis votre ordinateur.
Statistiques	Fournit des informations relatives aux activités de blocage des publicités, aux données confidentielles et au contrôle parental, sur votre ordinateur.

A propos du blocage des publicités

Cette fonction empêche le *téléchargement* des publicités en ligne sur votre ordinateur. Elle vous permet de réduire le temps de téléchargement d'une page Web.

Les publicités qui apparaissent sur les sites Web possèdent un nom et un emplacement uniques. Lorsque la fonction Blocage des publicités est activée et que vous vous connectez à un site Web, Norton Privacy Control utilise deux listes de noms et d'emplacements pour examiner les pages Web, afin de rechercher les publicités au moment de leur téléchargement :

- Une liste par défaut de noms et d'emplacements que Norton Privacy Control bloque automatiquement.
- Une liste de publicités spécifiques que vous avez créée lors des blocages précédents. Vous pouvez apporter des modifications à cette liste.

La fonction de blocage peut également remplacer les publicités par une icône de publicité bloquée, qui vous permet de voir combien de publicités ont été bloquées pour un site Web donné.

Activation du blocage des publicités

Lorsque le blocage des publicités est activé, Norton Privacy Control utilise la liste de noms et d'emplacements par défaut pour bloquer la plupart des publicités qui apparaissent sur Internet.

Le blocage des publicités est activé par défaut. Observez les instructions suivantes si vous avez désactivé le blocage des publicités et que vous souhaitez le réactiver. Pour obtenir des instructions sur la désactivation du blocage des publicités, consultez la section « Désactivation du blocage des publicités » à la page 137.

Pour activer le blocage des publicités

Se reporter à « Lancement et arrêt de Norton Internet Security » à la page 31.

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.
3. Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Blocage des publicités**.
4. Dans l'onglet Blocage des publicités, cochez l'option **Activer le blocage des publicités**.
5. Pour afficher une icône à la place d'une publicité, cochez l'option **Remplacer les publicités bloquées par**.
   La fonction de blocage ne peut pas toujours remplacer une publicité par une icône, mais elle en empêchera toujours l'affichage.

Blocage de publicités spécifiques

Pour la plupart des utilisateurs, il suffit d'activer le blocage des publicités pour bloquer toutes les publicités qu'ils ne souhaitent pas afficher. Toutefois, de nouvelles publicités peuvent apparaître sur les sites auxquels vous vous connectez fréquemment et vous aurez peut être à les bloquer également.

Se reporter à « Modification d'une entrée du blocage des publicités » à la page 136.

Lorsque vous bloquez une publicité spécifique, Norton Privacy Control tente de bloquer toutes les publicités apparaissant dans cette zone du site Web. Si d'autres publicités apparaissent dans cette zone, vous pouvez choisir de les ajouter à la liste ou de modifier le texte identifiant la publicité, afin d'en élargir la portée. Par exemple, si la publicité est identifiée par le texte ads.web.aol.com/link/12345678, vous pouvez modifier ce texte au niveau de /link et entrer l'adresse du site Web, afin de bloquer toutes les publicités de cette zone du site Web.

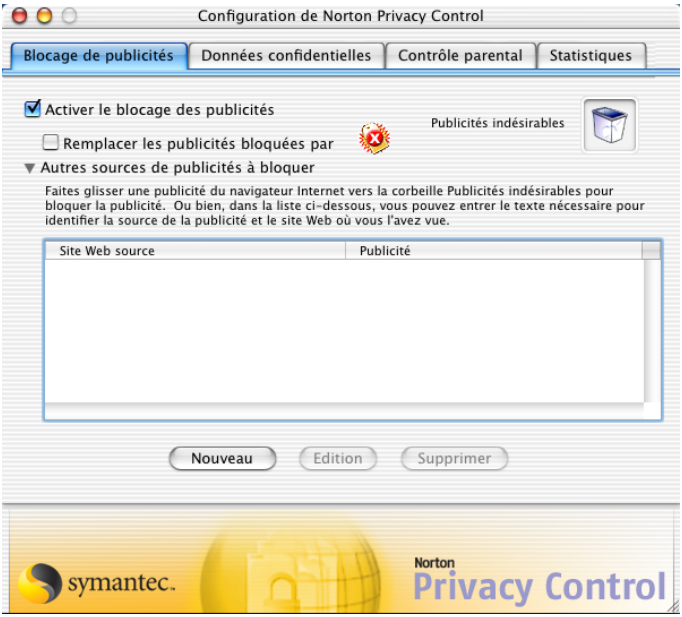
Vous pouvez bloquer des publicités spécifiques uniquement si le blocage des publicités est activé.

Les instructions suivantes permettent de faire glisser une publicité à partir d'un site Web. Si votre navigateur ne prend pas en charge la fonction glisser-déposer, utilisez le menu contextuel de votre navigateur pour copier le lien vers la publicité.

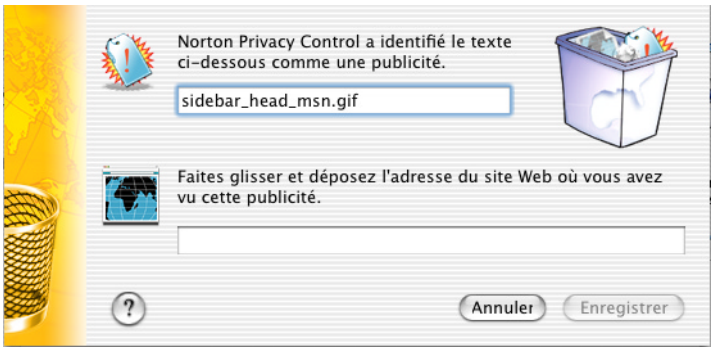
Pour bloquer des publicités spécifiques

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.

3 Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Blocage des publicités**.



4 Faites glisser la publicité à partir du site Web jusqu'à la **Corbeille des publicités**, dans l'onglet Blocage des publicités.



5 Dans la boîte de dialogue Blocage des publicités, si le champ de l'adresse du site Web est vierge, faites glisser l'adresse depuis votre navigateur jusqu'à ce champ. Vous pouvez également saisir l'adresse du site directement dans le champ.

6 Cliquez sur **Enregistrer**.

Vous pouvez également saisir directement le texte identifiant une publicité.

Pour identifier manuellement la publicité à bloquer

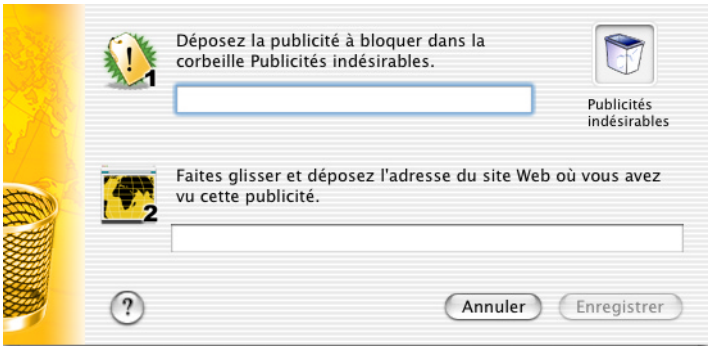
1 Ouvrez Norton Internet Security.

2 Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.

3 Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Blocage des publicités**.

4 Dans l'onglet Blocage des publicités, cliquez sur **Sources supplémentaires de publicités à bloquer**.

5 Cliquez sur **Nouvelle**.



6 Dans la boîte de dialogue de blocage des publicités, saisissez le texte identifiant la publicité que vous souhaitez bloquer, par exemple /ad_banner. Vous pouvez utiliser le menu contextuel de votre navigateur pour copier le lien de la publicité, si vous préférez. De même, vous pouvez faire glisser la publicité vers la **corbeille Publicités indésirables**, dans la boîte de dialogue Configuration.

7 Saisissez l'adresse du site Web dans le champ prévu à cet effet. Vous pouvez également faire glisser l'adresse vers le champ, depuis le site.

8 Cliquez sur **Enregistrer**.

Pour vérifier que la publicité a été bloquée

- ❖ Dans votre navigateur, maintenez enfoncée la touche **Option**, puis cliquez sur **Actualiser**.

Modification d'une entrée du blocage des publicités

Vous pouvez modifier le texte identifiant une publicité à bloquer.

Pour modifier une entrée du blocage des publicités

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.
3. Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Blocage des publicités**.
4. Dans l'onglet Blocage des publicités, cliquez sur **Sources supplémentaires de publicités à bloquer**.
5. Sélectionnez la publicité dont vous souhaitez modifier le texte.
6. Cliquez sur **Modifier**.
7. Saisissez les modifications.
8. Appuyez sur **Entrée** lorsque vous avez terminé une entrée ou pour vous déplacer entre les colonnes.
9. Lorsque vous avez terminé, appuyez sur **Echap**.
   Si vous appuyez sur Echap avant d'appuyer sur Entrée, les entrées que vous avez modifiées ne seront pas enregistrées.

Suppression d'une entrée du blocage des publicités

Vous pouvez annuler le blocage d'une publicité répertoriée en la supprimant de la liste.

Pour supprimer une entrée du blocage des publicités

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.
3. Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Blocage des publicités**.
4. Dans l'onglet Blocage des publicités, cliquez sur **Sources supplémentaires de publicités à bloquer**.

5 Sélectionnez la publicité que vous souhaitez supprimer de la liste.

6 Cliquez sur **Supprimer**.

Désactivation du blocage des publicités

Vous pouvez désactiver le blocage des publicités à tout moment. Si vous avez identifié des publicités spécifiques, la désactivation du Blocage n'entraîne pas la suppression de la liste. Lorsque vous réactivez le blocage des publicités, les publicités de votre liste continueront à être bloquées ainsi que celles de la liste par défaut.

Pour désactiver le blocage des publicités

1 Ouvrez Norton Internet Security.

2 Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.

3 Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Blocage des publicités**.

4 Dans l'onglet Blocage des publicités, désélectionnez l'option **Activer le blocage des publicités**.

Protection des données confidentielles

Vous stockez peut-être, sur votre ordinateur, des informations que vous ne souhaitez pas communiquer sans autorisation. Il est également possible que vous ne souhaitiez pas que ces données soient diffusées sur Internet sans votre autorisation. Ces informations confidentielles peuvent être : un numéro de carte de crédit, des numéros de téléphone, des mots de passe ou toute autre information que vous considérez comme confidentielle.

Si vous êtes connecté à un autre ordinateur lors de la définition de vos données confidentielles, il est possible que celui-ci puisse toujours accéder aux données, jusqu'à ce que la connexion prenne fin. Utilisez le rapport d'utilisateurs connectés de Norton Personal Firewall pour mettre fin à la connexion. Se reporter à « Déconnexion d'un utilisateur connecté » à la page 78.

Pour protéger vos données personnelles, activez les Données confidentielles, puis définissez les informations que vous souhaitez protéger. Si Norton Privacy Control détecte que ces informations quittent votre ordinateur, il affiche un message vous demandant d'autoriser la transmission.

Vous devez saisir votre nom d'administrateur pour déverrouiller l'onglet Données confidentielles et effectuer des modifications. Lorsque vous quittez Norton Privacy Control, la fonction Données confidentielles se verrouille automatiquement. Un verrouillage automatique se produit également après 15 minutes d'inactivité.

Pour protéger vos données confidentielles

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.
3. Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Données confidentielles**.
4. Dans l'onglet Données confidentielles, cliquez sur le cadenas.
5. Saisissez votre nom et votre mot de passe d'administrateur, puis cliquez sur **OK**.
6. Dans l'onglet Données confidentielles, cochez l'option **Activer le blocage des données confidentielles**.
7. Dans la boîte de dialogue vous indiquant une possibilité d'augmentation des temps de transfert, cliquez sur **OK**.
8. Dans le volet Données confidentielles, cliquez sur **Nouveau**.
9. Sélectionnez la catégorie que vous souhaitez utiliser pour identifier l'information.
10. Dans la zone Entrer les données ici, saisissez les données que vous souhaitez protéger.
11. Lorsque vous avez terminé, appuyez sur **Entrée**.
12. Lorsque vous avez saisi toutes vos données confidentielles, cliquez sur le cadenas pour masquer les informations si vous ne prévoyez pas de quitter Norton Privacy Control.

Se reporter à « Conseils pour la saisie de données confidentielles » à la page 142.

Modification des données confidentielles

Vous pouvez modifier tout ou partie des données que vous avez définies comme confidentielles.

Pour modifier des données confidentielles

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.

3 Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Données confidentielles**.

4 Dans l'onglet Données confidentielles, cliquez sur le cadenas.

5 Saisissez votre nom et votre mot de passe d'administrateur, puis cliquez sur **OK**.

6 Sélectionnez les données que vous souhaitez modifier.

7 Cliquez sur **Modifier**.

8 Saisissez les modifications.

9 Lorsque vous avez terminé, appuyez sur **Entrée**.

10 Lorsque vous avez terminé vos modifications, cliquez sur le cadenas pour masquer les informations si vous ne prévoyez pas de quitter Norton Privacy Control.

Suppression de données confidentielles

Vous pouvez supprimer tous les éléments signalés comme données confidentielles.

Pour supprimer des données confidentielles

1 Ouvrez Norton Internet Security.

2 Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.

3 Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Données confidentielles**.

4 Dans l'onglet Données confidentielles, cliquez sur le cadenas.

5 Saisissez votre nom et votre mot de passe d'administrateur, puis cliquez sur **OK**.

6 Sélectionnez les données que vous souhaitez supprimer.

7 Cliquez sur **Supprimer**.

8 Lorsque vous avez terminé, cliquez sur le cadenas pour masquer les informations si vous ne prévoyez pas de quitter Norton Privacy Control.

Définition d'exceptions

Il est possible que vous souhaitiez envoyer certaines données confidentielles à des sites Web spécifiques, sans demander une autorisation préalable. Par exemple, votre serveur de messagerie doit connaître votre adresse électronique. Si votre adresse électronique est classée comme donnée confidentielle, vous aurez peut-être envie de vous connecter à votre serveur de messagerie sans avoir à renvoyer à chaque fois votre adresse. La fonction Données confidentielles vous permet de définir des exceptions pour chaque information personnelle que vous avez spécifiée.

Norton Privacy Control ne bloque pas les données confidentielles cryptées. Par exemple, si vous envoyez votre numéro de carte de crédit à un site Web sécurisé, Norton Privacy Control ne bloquera pas la transmission. Il n'est donc pas nécessaire de définir ce site comme exception.

Pour définir des exceptions

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.
3. Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Données confidentielles**.
4. Dans l'onglet Données confidentielles, cliquez sur le cadenas.
5. Saisissez votre nom et votre mot de passe d'administrateur, puis cliquez sur **OK**.
6. Sélectionnez les données pour lesquelles vous souhaitez définir une exception.
7. Dans la liste des sites Web, cliquez sur **Nouveau**.
8. Saisissez le nom du site Web auquel les données spécifiées peuvent être envoyées. Saisissez uniquement le nom du site, et non pas le chemin complet d'une page particulière. Par exemple, saisissez www.symantec.com, et non pas www.symantec.com/custserv.
9. Lorsque vous avez terminé, appuyez sur **Entrée**.
   Norton Privacy Control vérifie que l'adresse entrée est valide.
10. Lorsque vous avez terminé, cliquez sur le cadenas pour masquer les informations si vous ne prévoyez pas de quitter Norton Privacy Control.

Modification des exceptions

Vous pouvez modifier les adresses de site Web définies comme exceptions.

Pour modifier des exceptions

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.
3. Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Données confidentielles**.
4. Dans l'onglet Données confidentielles, cliquez sur le cadenas.
5. Saisissez votre nom et votre mot de passe d'administrateur, puis cliquez sur **OK**.
6. Sélectionnez les données confidentielles pour lesquelles le site Web est défini comme exception.
7. Sélectionnez le site Web que vous souhaitez modifier.
8. Cliquez sur **Modifier**.
9. Saisissez les modifications.
10. Lorsque vous avez terminé, appuyez sur **Entrée**.
11. Lorsque vous avez terminé vos modifications, cliquez sur le cadenas pour masquer les informations si vous ne prévoyez pas de quitter Norton Privacy Control.

Suppression des exceptions

Vous pouvez supprimer les sites Web définis comme exceptions.

Pour supprimer des exceptions

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.
3. Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Données confidentielles**.
4. Dans l'onglet Données confidentielles, cliquez sur le cadenas.
5. Saisissez votre nom et votre mot de passe d'administrateur, puis cliquez sur **OK**.

6 Sélectionnez les données confidentielles pour lesquelles le site Web est défini comme exception.

7 Sélectionnez le site Web que vous souhaitez supprimer.

8 Cliquez sur **Supprimer**.

9 Lorsque vous avez terminé vos modifications, cliquez sur le cadenas pour masquer les informations si vous ne prévoyez pas de quitter Norton Privacy Control.

Conseils pour la saisie de données confidentielles

Norton Privacy Control bloque les données personnelles uniquement sous la forme exacte dans laquelle vous les avez saisies dans le programme ; c'est pourquoi il est préférable de saisir uniquement des numéros partiels. Par exemple, un numéro de téléphone peut être entré sous la forme 888-555-1234, mais également sans les tirets (8885551234), avec des espaces (888 555 1234) ou encore dans deux zones séparées. Le dénominateur commun de ces différents formats est que les quatre derniers chiffres du numéro (1234) sont toujours regroupés. De ce fait, votre protection sera plus efficace si vous protégez ces quatre chiffres au lieu du numéro tout entier.

La saisie de données partielles présente deux avantages. Tout d'abord, vous ne saisissez pas votre numéro de carte de crédit en entier, il y aura donc moins de chances que quelqu'un le découvre. Ensuite, cela permet à Norton Privacy Control de bloquer vos données personnelles sur des sites utilisant plusieurs cases pour les numéros de carte de crédit.

Réponse à une alerte relative aux données confidentielles

Si Norton Privacy Control détecte que des données confidentielles sont diffusées depuis votre ordinateur, il affiche une *alerte*, indiquant la catégorie de données transmises. Si vous ne répondez pas à cette alerte dans les 60 secondes suivantes, les données seront bloquées automatiquement.

Le temps que vous passez à prendre connaissance des données transmises, dans le menu Détails, n'est pas pris en compte dans le délai de réponse de 60 secondes.

Pour répondre à une alerte relative aux données confidentielles

1 Si vous souhaitez obtenir plus d'informations sur les données transmises, cliquez sur **Détails**. Les informations suivantes s'affichent :

ID de processus	ID de processus du programme qui envoie les données. Vous pouvez utiliser l'utilitaire Process Viewer d'Apple pour savoir à quel programme cet ID correspond, si vous souhaitez essayer d'arrêter le programme.
Codage des données	Indique le mode de codage des données envoyées (par exemple, ASCII ou Unicode). Vous pouvez utiliser cette information si vous pensez que Norton Privacy Control a mal interprété des données confidentielles.
Contexte	Les 10 octets de données qui apparaissent avant les données identifiées comme confidentielles.

2 Choisissez l'une des options suivantes :

Bloquer	Arrêter la transmission des données. C'est la meilleure chose à faire si vous n'avez pas envoyé les données délibérément.
Toujours autoriser	Ajoute la destination à la liste d'exceptions de ces données.
Autoriser une fois	Autorise la transmission des données vers cette destination pour cette fois uniquement. Si la destination requiert ces données plusieurs fois, vous devez en autoriser la transmission à chaque fois.

Désactivation du blocage des données confidentielles

Vous pouvez désactiver le blocage des données confidentielles à tout moment. La liste de vos données confidentielles n'est pas effacée lorsque vous la désactivez. Lorsque vous réactivez le blocage des données confidentielles, votre liste est de nouveau protégée.

Pour désactiver le blocage des données confidentielles

1 Ouvrez Norton Internet Security.

2 Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.

3 Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Données confidentielles**.

4 Dans l'onglet Données confidentielles, cliquez sur le cadenas.

5 Saisissez votre nom et votre mot de passe d'administrateur, puis cliquez sur **OK**.

6 Dans l'onglet Données confidentielles, désélectionnez **Activer le blocage des données confidentielles**.

Blocage des sites Web indésirables

Vous pouvez contrôler à quels sites Web peut accéder votre ordinateur en activant le Blocage Web dans l'onglet Contrôle parental de Norton Privacy Control. Une fois le Blocage Web activé, vous pouvez définir de manière plus précise les sites Web à bloquer, en spécifiant des catégories de site et des sites spécifiques à bloquer ou à autoriser.

Vous devez saisir votre nom d'administrateur pour déverrouiller l'onglet Contrôle parental et effectuer des modifications. Lorsque vous quittez Norton Privacy Control, la fonction Contrôle parental se verrouille automatiquement. Un verrouillage automatique se produit également après 15 minutes d'inactivité.

Activation du blocage Web

Pour activer le blocage de sites Web, vous devez tout d'abord activer la fonction de blocage, puis sélectionner les catégories de site à bloquer

Pour activer le blocage Web

1 Ouvrez Norton Internet Security.

2 Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.

3 Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Contrôle parental**.

4 Dans l'onglet Contrôle parental, cliquez sur le cadenas.

5 Saisissez votre nom et votre mot de passe d'administrateur, puis cliquez sur **OK**.

6 Cochez l'option **Activer le blocage Web**.

7 Dans la liste des catégories de pages Web, cochez celles que vous souhaitez bloquer et désélectionnez celles que vous souhaitez autoriser.

8 Dans la section Pages Web inconnues, indiquez les instructions à suivre lorsqu'un site Web ne correspond à aucune des catégories répertoriées. Choisissez l'une des options suivantes :

- Interdire l'accès au site
- Autoriser l'accès au site

9 Lorsque vous avez terminé vos sélections, cliquez sur le cadenas pour empêcher toute modification ultérieure, si vous ne prévoyez pas de quitter Norton Privacy Control.

Définition d'une exception

Une fois le blocage Web en place, il est possible que l'accès à un site Web indésirable soit autorisé et que l'accès à un site Web autorisé soit bloqué. Vous pouvez définir ces sites comme exceptions, dans la fonction Contrôle parental.

Pour définir une exception

1 Ouvrez Norton Internet Security.

2 Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.

3 Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Contrôle parental**.

4 Dans l'onglet Contrôle parental, cliquez sur le cadenas.

5 Saisissez votre nom et votre mot de passe d'administrateur, puis cliquez sur **OK**.

6 Choisissez l'une des options suivantes :

- Pour bloquer un site, cliquez sur **Nouveau** dans la liste des pages Web à bloquer.
- Pour autoriser l'accès à un site, cliquez sur **Nouveau** dans la liste des pages Web à autoriser.

7 Saisissez l'adresse du site Web à bloquer ou à autoriser, puis appuyez sur **Entrée**.

8 Lorsque vous avez terminé, cliquez sur le cadenas pour empêcher toute modification ultérieure, si vous ne prévoyez pas de quitter Norton Privacy Control.

Modification de vos listes d'exceptions

Vous pouvez modifier ou supprimer les adresses Web répertoriées dans votre liste d'exceptions.

Pour modifier une adresse de site Web

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.
3. Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Contrôle parental**.
4. Dans l'onglet Contrôle parental, cliquez sur le cadenas.
5. Saisissez votre nom et votre mot de passe d'administrateur, puis cliquez sur **OK**.
6. Sélectionnez l'adresse que vous souhaitez modifier.
7. Cliquez sur **Modifier**.
8. Saisissez vos modifications, puis appuyez sur **Entrée**.
9. Lorsque vous avez terminé vos modifications, cliquez sur le cadenas pour empêcher toute modification ultérieure, si vous ne prévoyez pas de quitter Norton Privacy Control.

Pour supprimer une adresse de site Web

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.
3. Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Contrôle parental**.
4. Dans l'onglet Contrôle parental, cliquez sur le cadenas.
5. Saisissez votre nom et votre mot de passe d'administrateur, puis cliquez sur **OK**.
6. Sélectionnez l'adresse que vous souhaitez supprimer.
7. Cliquez sur **Supprimer**.
8. Lorsque vous avez terminé, cliquez sur le cadenas pour empêcher toute modification ultérieure, si vous ne prévoyez pas de quitter Norton Privacy Control.

Contrôle des résultats de Norton Privacy Control

Vous pouvez vérifier que Norton Privacy Control fonctionne correctement à l'aide de l'onglet Statistiques. Ces statistiques incluent :

Statistique	Description
Nombre de connexions contrôlées	Nombre de connexions Internet actuellement contrôlées par Norton Privacy Control
Nombre de publicités bloquées	Nombre de publicités de site Web bloquées depuis le dernier démarrage de votre ordinateur
Estimation économie espace	Volume d'octets n'ayant pas été téléchargé grâce au blocage des publicités depuis le dernier démarrage de votre ordinateur
Tentatives de connexion à des sites bloqués	Nombre de tentatives d'accès, sur votre ordinateur, à des sites Web bloqués, depuis le dernier démarrage de votre ordinateur
Données confidentielles bloquées Données confidentielles autorisées	Nombre d'autorisations ou de blocages de transmission, pour des données définies comme confidentielles, depuis le dernier démarrage de votre ordinateur

Pour contrôler les résultats de Norton Privacy Control

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Norton Internet Security, cliquez sur **Norton Privacy Control**.
3. Dans la fenêtre de configuration de Norton Privacy Control, cliquez sur **Statistiques**.

5

Aladdin iClean

Démarrage rapide d'iClean

15

Aladdin iClean permet de localiser et de supprimer rapidement les fichiers découlant de la navigation Internet. iClean nettoie les *fichiers cache* Web, l'historique Internet, les *cookies* du navigateur et vide la corbeille. Il répare également les *alias*.

Ce chapitre présente la configuration système requise et les instructions d'installation. Pour une documentation complète, consultez le *Guide de l'utilisateur iClean*, situé dans le dossier iClean de votre ordinateur, une fois l'installation d'iClean terminée. Il s'agit d'un fichier PDF à lire dans Adobe Acrobat.

Configuration requise

La configuration système suivante est requise pour l'exécution d'Aladdin i Clean :

- Processeur PowerPC
- Lecteur de CD-ROM
- 8 Mo de RAM
- 13 Mo d'espace disque
- Macintosh OS 8.6 à 9.x (iClean pour Classic)
- Macintosh OS X 10.1 ou supérieure (iClean pour OS X)

Installation d'iClean

Le logiciel iClean du de CD Norton Internet Security pour Macintosh vous permet d'installer le programme iClean sur un ordinateur Macintosh doté d'un lecteur de CD-ROM. Les programmes d'installation d'iClean pour OS X et d'iClean pour Classic sont inclus. Vous pouvez observer les instructions suivantes pour ces deux versions.

Pour installer iClean

1. Dans la fenêtre du CD Norton Internet Security pour Macintosh, cliquez deux fois sur le dossier **Aladdin iClean**.
2. Choisissez l'une des options suivantes :
   - Si vous installez iClean pour OS X, cliquez deux fois sur le dossier **Programme d'installation Mac OS X**.
   - Si vous installez iClean pour Classic, cliquez deux fois sur le dossier **Programme d'installation Mac OS 8.6 à 9.x**.
3. Choisissez l'une des options suivantes :
   - Si vous installez iClean pour OS X, cliquez deux fois sur **Installer iClean 5.0.1 pour OS X**.
   - Si vous installez iClean pour Classic, cliquez deux fois sur **Programme d'installation iClean 5.0 SY**.
4. Si vous installez iClean pour OS X, saisissez votre mot de passe administrateur dans la fenêtre Authentification, puis cliquez sur **OK**.
5. Dans l'écran iClean, cliquez sur **Continuer**.
6. Cliquez sur **Continuer** après avoir pris connaissance du fichier Readme iClean.
   Si vous souhaitez enregistrer le fichier Readme, cliquez sur **Enregistrer**. Si vous souhaitez imprimer le fichier Readme, cliquez sur **Imprimer**.
7. Prenez connaissance du contrat de licence et acceptez-en les termes en cliquant sur **Accepter**.
   Si vous refusez les termes du contrat, vous ne pouvez pas poursuivre l'installation.
8. Dans la fenêtre du programme d'installation, cliquez sur **Installer**.

9 Dans la fenêtre prévue à cet effet, sélectionnez l'emplacement dans lequel vous souhaitez installer iClean.
Si vous ne souhaitez pas installer iClean à l'emplacement par défaut affiché, utilisez les boutons pour rechercher un autre dossier.

10 Cliquez sur **Choisir** pour terminer l'installation.

6

Annexes

Utilisation de Norton AntiVirus en réseau

A

Vous pouvez exécuter Norton Antivirus sur tout serveur ATP (AppleTalk Transaction Protocol) tel qu'AppleShare ou TOPS.

Notes à l'attention de l'administrateur

En environnement réseau, configurez Norton AntiVirus de la façon suivante :

- Ouvrez Norton AntiVirus Auto-Protect et Norton AntiVirus sur votre ordinateur.
- Assurez-vous que Norton AntiVirus Auto-Protect est activé sur tous les postes du réseau.
- Utilisez la commande Programmation du menu Outils de Norton AntiVirus pour programmer l'examen des disques en réseau.

Examen des unités en réseau

Lorsque vous examinez des unités en réseau depuis un poste, le serveur est ralenti pour les autres utilisateurs. Si certaines personnes créent, suppriment ou déplacent des fichiers sur une unité en réseau pendant un examen de Norton AntiVirus, il se peut que certains fichiers ne soient pas examinés.

Pour empêcher l'examen de certains fichiers, procédez comme suit :

- Assurez-vous que vous êtes le seul connecté au serveur lorsque vous examinez des unités en réseau.
- Eteignez le serveur, redémarrez, réinstallez Norton AntiVirus puis effectuez l'examen.

Préparation d'un plan d'urgence

Afin d'être paré pour l'éventualité d'une infection virale sur un poste, pensez à distribuer à l'avance un plan d'urgence à suivre par toutes les personnes connectées à votre réseau. Ceci empêchera toute panique indue en cas d'infection.

Complétez votre plan en fonction des activités et des exigences de votre organisation.

Avant l'apparition d'un virus

Organisez une réunion avec les utilisateurs de votre réseau pour leur communiquer des informations sur la nature et le comportement des virus informatiques. Insistez sur le fait que la présence d'un virus informatique dans votre système réclame une intervention immédiate, mais qu'il est inutile de s'affoler. Précisez que de nombreux virus se multiplient à partir de copies de logiciels illégales, et interdisez l'utilisation de tels logiciels dans votre entreprise. Enfin, expliquez que vous avez configuré Norton AntiVirus pour parer à d'éventuelles attaques.

Demandez aux utilisateurs de :

- Lancer un examen de tout nouveau logiciel avant son utilisation. Cet examen doit être exécuté aussi bien pour les applications téléchargées sur Internet que pour tous les nouveaux logiciels.
- Signaler tout fonctionnement erratique : blocages fréquents, pertes de données, affichages incohérents, etc.
- Faire des sauvegardes de leurs logiciels et de leurs données.
- Ne pas exécuter d'applications depuis une disquette non examinée par Norton AntiVirus.
- Protéger en écriture les supports amovibles avant de les utiliser sur l'ordinateur d'un collègue.

Pour protéger les postes de travail :

- Lancez un examen complet de chaque poste afin de vérifier l'absence de virus.
- Incitez les utilisateurs à faire fréquemment appel à des programmes de sauvegarde.
- Demandez-leur de mettre régulièrement à jour leurs fichiers de définitions virales.

Pour protéger le réseau :

- Protégez par mot de passe tous les répertoires en réseau contenant des exécutables (vous seul y aurez accès en écriture).
- A l'aide de Norton AntiVirus, examinez tout Macintosh nouvellement arrivé dans l'entreprise.
- Programmez un examen régulier des serveurs du réseau.
- Si vous faites appel à des serveurs Novell NetWare ou Windows NT, recourez aux composants de Norton AntiVirus Enterprise Solution pour protéger vos serveurs des infections virales.

Si un virus est détecté

En cas de détection d'un virus sur votre réseau, vous devez l'éradiquer sur tous les ordinateurs connectés au réseau.

Pour éradiquer un virus

1. Déconnectez physiquement du réseau le poste incriminé.
2. Supprimez le virus avant de reconnecter le poste au réseau.
3. Demandez à tous les utilisateurs du réseau de lancer un examen de leurs disques.
4. Effectuez un examen complet de vos serveurs de réseau.

Glossaire

ActiveSync	Logiciel de synchronisation pour les Pocket PC basés sur Microsoft Windows.
ActiveX	Méthode d'incorporation de programmes interactifs dans des pages Web. Les programmes, appelés contrôles, s'exécutent lorsque vous affichez la page.
Adresse IP (Internet Protocol)	Nombre identifiant un ordinateur de façon unique sur Internet. Les adresses IP sont généralement affichées sous la forme de quatre groupes de chiffres séparés par des points. Exemple : 206.204.52.71.
Adresse réseau	Partie d'une adresse IP commune à tous les ordinateurs d'un réseau ou sous-réseau. Par exemple, 10.0.1.1 et 10.0.1.8 font partie de l'adresse réseau 10.0.1.0.
Alerte	Message qui apparaît pour signaler qu'une erreur s'est produite ou qu'une tâche exige une intervention immédiate, par exemple un blocage du système ou une alerte virale.
Alias	Objet symbolique représentant un élément original (fichier, dossier, disque ou disquette).
AppleTalk	Protocole auquel certains périphériques du réseau (imprimantes et serveurs, par exemple) font appel pour communiquer.

Attaque de refus de service	Utilisateur ou programme qui accapare toutes les ressources du système en lançant une multitude de requêtes, ne laissant ainsi aucune ressource et donc aucun service aux autres utilisateurs.
Attribut masqué	Attribut d'un fichier qui le rend plus difficile d'accès et plus difficile à supprimer que les autres fichiers. Il les empêche également d'apparaître dans une liste de répertoire DOS ou Windows.
Cache	Emplacement du disque où des données sont stockées en vue d'être réutilisées. Le cache d'un navigateur Web stocke des pages Web et des fichiers (tels que des images) à mesure que vous les visualisez.
Caractères génériques	Caractères spéciaux (comme *, $ et ?) qui remplacent un ou plusieurs caractères. Ils permettent de chercher plusieurs éléments à la fois.
Cheval de Troie	Programme contenant un code malicieux déguisé ou se cachant sous les traits d'un code bénin, tel qu'un jeu ou un utilitaire.
Chiffrement	Codage des informations d'une manière telle que seule une personne possédant le mot de passe ou la clé de cryptographie correcte puisse les lire. Ce codage empêche les utilisateurs non autorisés de visualiser ou altérer les données.
Cookie	Fichier que certains serveurs Web placent sur votre disque lorsque vous visualisez des pages à partir de ces serveurs. Ils servent à mémoriser des préférences, créer des paniers d'achat en ligne et identifier les pages déjà visitées.
Définition de virus	Informations utilisées par un programme antivirus afin d'identifier la présence d'un virus spécifique et de vous en alerter.
DHCP (Dynamic Host Configuration Protocol)	Protocole qui attribue une adresse IP temporaire à chacun des périphériques d'un réseau. Les routeurs DSL et câble utilisent DHCP pour permettre à plusieurs ordinateurs de partager une même connexion Internet.

Disque amorçable	Disque qui peut être utilisé pour faire démarrer un ordinateur.
Domaine	Adress Internet commune pour une entreprise ou organisation (comme symantec.com). Voir aussi nom d'hôte.
Ethernet	Méthode commune de mise en réseau d'ordinateurs dans un LAN (réseau local). Les câbles Ethernet, qui ressemblent à des câbles téléphoniques en plus grand, transportent les données à une vitesse de 10 Mbits/s ou 100 Mbits/s.
Extension	Terminaison de trois lettres du nom d'un fichier, qui associe ce fichier à une activité ou un programme. Exemples : .txt (texte) et .exe (programme exécutable).
FAT (table d'allocation des fichiers)	Table du système (utilisée essentiellement par DOS et Windows 9x/Me) qui organise l'emplacement exact de tous les fichiers sur un disque dur.
Fenêtre DOS	Méthode d'accès au système d'exploitation MS-DOS en vue d'exécuter des programmes DOS au travers de l'environnement graphique de Windows.
Fichier compressé	Fichier dont le contenu a été réduit de taille de sorte que les données occupent moins d'espace physique sur le disque.
Fichier de cache	Fichier utilisé pour améliorer les performances de Windows.
Fichier exécutable	Fichier contenant un code logiciel pouvant être exécuté. Cela couvre généralement tout fichier qui est un programme, une extension ou un fichier système se terminant par .bat, .exe ou .com.
Finder	Programme qui gère l'activité et l'affichage des disques et fichiers du Macintosh.
Fournisseur de services Internet	Société qui fournit un accès Internet aux particuliers et aux entreprises. La plupart des FSI offrent des services de connectivité Internet supplémentaires, comme l'hébergement de sites Web.

Fragmenté	Se dit des données qui composent un fichier et sont stockées dans des clusters non contigus sur un disque. Un fichier fragmenté est plus long à lire sur le disque qu'un fichier non fragmenté.
FTP (File Transfer Protocol)	Protocole d'application utilisé pour transférer des fichiers entre ordinateurs sur des réseaux TCP/IP tels que l'Internet.
HotSync	Logiciel de synchronisation pour portables Palm OS.
HTML (Hypertext Markup Language)	Langage utilisé pour créer des pages Web.
ICMP (Internet Control Message Protocol)	Extension du protocole Internet Protocol (IP) de base, qui fournit des informations sur des problèmes réseau.
IGMP (Internet Group Management Protocol)	Extension du protocole Internet Protocol (IP) de base, utilisée pour diffuser des informations multimédias sur l'Internet.
IMAP4 (Internet Message Access Protocol version 4)	Un des deux protocoles les plus populaires pour la réception de messages électroniques. IMAP permet de lire et gérer les messages sans les télécharger sur votre ordinateur.
IP (Internet Protocol)	Protocole sous-jacent à la plus grand partie du trafic Internet. IP détermine la façon dont les données passent d'un ordinateur à un autre. Les ordinateurs connectés à l'Internet ont des adresses IP qui les identifient de manière unique.
Java	Langage de programmation utilisé pour créer des petits programmes dits « applets ». Les applets Java peuvent servir à créer du contenu interactif sur des pages Web.
JavaScript	Langage de script utilisé pour améliorer les pages Web. La plupart des sites utilisent JavaScript pour donner une interactivité élémentaire à leurs pages, mais certains l'utilisent pour ouvrir des publicités dans des fenêtres locales et redéfinir la page de démarrage de leurs visiteurs.

Ligne commutée	Connexion dans laquelle un ordinateur appelle un serveur et opère comme poste de travail local sur le réseau.
Macro	Simple programme qui peut être lancé avec une combinaison de touches spécifique. Les macros peuvent servir à automatiser des tâches répétitives.
Masque de sous-réseau	Code se présentant sous la forme d'une adresse IP, que les ordinateurs utilisent pour déterminer la portion d'une adresse IP identifiant le sous-réseau et la portion identifiant un ordinateur spécifique sur ce sous-réseau.
Menace	Programme pouvant endommager un ordinateur par la destruction, la divulgation ou la modification de données, ou par un refus de service.
NAT (network address translation)	Méthode de conversion d'adresses IP privées en une adresse IP publique unique. NAT permet à plusieurs ordinateurs de partager une adresse IP publique. La plupart des routeurs DSL et câble prennent en charge NAT.
Nom d'hôte	Nom utilisé par les utilisateurs pour faire référence à un site Web. www.symantec.com est le nom d'hôte du site Web de Symantec, par exemple. Les noms d'hôte sont convertis en adresses IP par le service DNS.
NTFS (système de fichiers)	Table du système (utilisée essentiellement par Windows 2000/XP) qui organise l'emplacement exact de tous les fichiers sur un disque dur.
Numéro de port	Numéro utilisé pour identifier un service Internet particulier. Les paquets Internet comprennent un numéro de port pour aider les ordinateurs récepteurs à déterminer le programme à utiliser pour traiter les données.
Paquet IP fragmenté	Paquet IP divisé en plusieurs parties. Les paquets sont fragmentés s'ils dépassent la taille de paquet maximale du réseau, mais des utilisateurs malveillants les fragmentent également pour masquer des attaques Internet.

Paquet	Unité de base des données sur l'Internet. Outre les données, chaque paquet comprend un en-tête qui décrit la destination du paquet et la façon dont les données doivent être traitées.
Partition	Partie d'un disque préparée et placée à part par un utilitaire de disque pour fonctionner comme un disque distinct.
Pilote	Instructions logicielles visant à interpréter des commandes de transfert entre un périphérique et un ordinateur.
POP3 (Post Office Protocol version 3)	Un des deux protocoles les plus populaires pour la réception de messages électroniques. POP3 exige de télécharger les messages pour pouvoir les lire.
Port	Connexion entre deux ordinateurs. TCP/IP et UDP utilisent des ports pour indiquer le type de programme serveur qui doit traiter la connexion. Chaque port est identifié par un numéro.
Port infrarouge (IR)	Port de communication d'un portable permettant de l'interfacer avec un périphérique reconnaissant l'infrarouge. Les ports infrarouges n'utilisent pas de câbles.
PPP (Point-to-Point Protocol)	Protocole de communication entre deux ordinateurs sur une connexion commutée. Le protocole PPP offre des mécanismes de contrôle des erreurs.
Privilèges d'accès	Types d'opérations qu'un utilisateur peut effectuer sur une ressource système. Par exemple, un utilisateur peut être autorisé à accéder à un certain répertoire et à en ouvrir, modifier ou supprimer le contenu.
Protocole	Ensemble de règles régissant les communications et le transfert de données entre ordinateurs. HTTP et FTP sont deux exemples de protocoles.
Protocole orienté connexion	Protocole exigeant une connexion pour la transmission de paquets d'informations.

Protocole sans connexion	Protocole capable de transmettre des informations jusqu'à une adresse de destination sans établir de connexion.
Proxy	Ordinateur ou programme qui redirige le trafic entrant et sortant entre des ordinateurs ou des réseaux. Les proxys sont souvent utilisés pour protéger les ordinateurs et réseaux contre les menaces extérieures.
Registre	Catégorie de données stockées dans la base de registres Windows pour décrire des préférences de l'utilisateur, des réglages matériels et d'autres données de configuration. Les données d'un registre s'utilisent à l'aide d'une clé de registre.
Règle de filtrage	Paramètres qui définissent la façon dont un pare-feu réagit à des données ou des communications réseau spécifiques. Une règle de filtrage contient généralement un schéma de données et une action à exécuter si ce schéma est détecté.
Routeur	Périphérique qui transfère des informations entre ordinateurs et réseaux. Les routeurs servent à gérer les trajectoires suivies par les données sur un réseau. De nombreux modems câble et DSL intègrent un routeur.
Script	Programme, écrit dans un langage de scripts tel que VBScript ou JavaScript, composé d'une série d'instructions qui peuvent s'exécuter sans intervention de l'utilisateur.
Serveur DNS (Domain Name System)	Ordinateur qui fait correspondre des noms de domaines à des adresses IP. Lorsque vous visitez www.symantec.com, votre ordinateur contacte un serveur DNS qui convertit le nom de domaine en une adresse IP (206.204.212.71).
Service	Terme général pour désigner le fait d'offrir à d'autres ordinateurs l'accès à des informations. Des services courants sont les services Web et FTP. Les ordinateurs offrant des services sont appelés serveurs.

Signature d'attaque	Schéma de données caractéristique d'une attaque Internet. Intrusion Detection utilise ces signatures pour distinguer les attaques du trafic licite.
Sous-réseau	Réseau local qui fait partie intégrante d'un intranet de plus grande taille ou d'Internet.
SSL (Secure Sockets Layer)	Protocole de sécurisation des communications en ligne. Les messages envoyés via SSL sont chiffrés afin d'empêcher une visualisation non autorisée. SSL est souvent utilisé pour protéger des informations financières.
Support amovible	Disque dont le retrait est possible, par opposition aux disques fixes. Les disquettes, CD, DVD et disques Zip sont des exemples supports amovibles.
Sync	Processus de transfert de programmes et données d'un ordinateur vers un portable.
Synchronisation	Processus par lequel un portable et un ordinateur comparent leurs fichiers afin de s'assurer qu'ils contiennent les mêmes données.
Système de noms de domaine (DNS, Domain Name System)	Système de dénomination utilisé sur l'Internet. DNS convertit les noms de domaines (comme www.symantec.com) en adresses IP que les ordinateurs peuvent comprendre (comme 206.204.212.71).
TCP/IP (Transmission Control Protocol/ Internet Protocol)	Protocole standard utilisé pour la plus grande partie du trafic Internet. TCP établit des connexions entre ordinateurs et vérifie que les données sont correctement reçues. IP détermine le mode de routage des données.
Télécharger	Transférer une copie d'un fichier ou programme à partir de l'Internet, d'un serveur ou d'un ordinateur vers un autre serveur ou ordinateur.
Transfert infrarouge	Méthode de transfert de certains programmes et données entre deux portables selon une technologie infrarouge intégrée.
Type de fichier	Code associant le fichier à un programme ou une activité, souvent exprimé par l'extension du nom du fichier, comme .txt ou .jpeg.

UDP (User Datagram Protocol)	Protocole couramment utilisé pour la diffusion en continu. A la différence de TCP, UDP n'établit pas de connexion avant d'envoyer les données ni ne vérifie si les données sont correctement reçues.
Ver	Programme qui se duplique sans infecter d'autres programmes. Certains vers se reproduisent en s'autocopiant d'un disque à l'autre, tandis que d'autres ne se reproduisent que dans la mémoire afin de ralentir l'ordinateur. A ce jour, il n'existe pas de ver en environnement Macintosh.
Zone amorce	Secteur situé au début d'un disque et décrivant ce disque (taille de secteur, taille de cluster, etc.). Sur les disques de démarrage, la zone amorce contient également un programme qui charge le système d'exploitation.

Index

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

Solutions de service et de support EMEA

Service Clientèle - vous aide pour les questions non techniques telles que les commandes, les mises à jour, les échanges et les remises.

Support technique - vous aide pour les questions techniques telles que l'installation, la configuration ou le dépannage des produits Symantec.

Les systèmes de support technique et de service clientèle varient en fonction des pays. Pour vous renseigner sur les offres de service dans votre région, visitez le site Web approprié.

Si ce produit vous a été fourni lors de l'achat de votre ordinateur, le fabricant du système prend la responsabilité du support, sauf indication contraire.

Service Clientèle

Le site de support Web vous indique comment :

- localiser des revendeurs et des consultants dans votre région ;
- remplacer des CD défectueux et des manuels ;
- mettre à jour l'enregistrement de votre produit ;
- vous informer sur les commandes, les retours et les remises ;
- accéder à la Foire aux questions (FAQ) du service Clientèle ;
- adresser une question à un agent du Service Clientèle ;
- obtenir des informations une documentation produit ou un logiciel d'essai.

Pour les commandes de mises à jour produit, consultez les informations correspondant à votre région.

Royaume-Uni, Irlande :
http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/eedocid/199991585523

Allemagne, Autriche et Suisse :
http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/gdocid/20000531114300925

France, Belgique, Luxembourg :
http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/fdocid/20000530164002925

Pays-Bas, Belgique :
http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/ddocid/20000531114633925

Italie :
http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/idocid/20001114142714925

Espagne :
http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/sdocid/20000531113344925

Suède, Norvège, Danemark, Finlande :
http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/swdocid/20000531113940925

Autres pays :
http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/eedocid/199991585523

Support technique

Symantec propose deux options de support technique pour vous aider à installer, configurer ou dépanner des produits Symantec.

Service et support en ligne

Connectez-vous au site Web de service et de support Symantec pour votre région. Spécifiez un type d'utilisateur puis sélectionnez votre produit et sa version pour :

- accéder aux rubriques d'actualité ;
- consulter la base de connaissances ;
- suivre des didacticiels en ligne ;
- vous informer sur les options de contact ;
- adresser une question à un agent du support technique en ligne.

Support téléphonique

Des services de support payants par téléphone sont accessibles à tous les utilisateurs enregistrés. Visitez le site de support de votre pays pour obtenir des informations de contact.

Prise en charge des anciennes versions et des versions abandonnées

Lorsque Symantec annonce qu'un produit n'est plus commercialisé, le support téléphonique est assuré pendant 60 jours suivant cette annonce. Certaines informations techniques restent cependant disponibles sur le site de support Symantec.

Politique d'abonnement

Si votre produit Symantec inclut une protection antivirus, un pare-feu (firewall) ou une protection de contenu de site, vous pouvez avoir droit à des mises à jour via LiveUpdate. La durée de l'abonnement dépend de votre produit Symantec.

Quand l’abonnement initial expire, vous devez le renouveler pour continuer à actualiser votre protection. Ces mises à jour limitent votre vulnérabilité aux attaques.

Lorsque vous exécutez LiveUpdate vers la fin de votre abonnement, un message vous rappelle de vous réabonner pour un coût réduit. Suivez simplement les instructions affichées à l'écran.

Pour d'autres informations, visitez le site Web de service et de support Symantec pour votre région.

Bureaux Service et support :

Europe, Moyen Orient et Afrique

Symantec Authorised Service Centre
Postbus 1029
3600 BA Maarssen
Pays-Bas
http://www.symantec.com/region/reg_eu/

Sites Web de service et de support

Europe/Anglais :
http://www.symantec.com/eusupport

Allemagne, Autriche et Suisse :
http://www.symantec.de/desupport/

France :
http://www.symantec.fr/frsupport/

Pays-Bas :
http://www.symantec.nl/nlsupport/

Italie :
http://www.symantec.it/itsupport/

Espagne :
http://www.symantec.com/region/mx/techsupp/index.html

Suède :
http://www.symantec.com/region/se/techsupp/index.html

Norvège :
http://www.symantec.com/region/no/techsupp/index.html

Danemark :
http://www.symantec.com/region/dk/techsupp/index.html

Finlande :
http://www.symantec.com/region/fi/techsupp/index.html

Pologne :
http://www.symantec.com/region/pl/techsupp/index.html

République tchèque :
http://www.symantec.com/region/cz/techsupp/index.html

République slovaque :
http://www.symantec.com/region/cz/techsupp/index.html

Russie :
http://www.symantec.com/region/ru/techsupp/index.html

Hongrie :
http://www.symantec.com/region/hu/techsupp/index.html

Pour les solutions de service et de support dans d'autres pays, visitez le site suivant et sélectionnez votre région.

http://www.symantec.com/globalsites.html

Tous les efforts ont été fournis pour garantir la précision de ces informations. Celles-ci peuvent toutefois faire l'objet de modifications sans préavis. Symantec Corporation se réserve le droit d'apporter de telles modifications sans avertissement préalable.