

# Norton Personal Firewall<sup>TM</sup> pour Macintosh<sup>®</sup> Guide de l'utilisateur

Norton  
**Personal Firewall**<sup>TM</sup>  
Pour Macintosh<sup>®</sup>

# Guide de l'utilisateur de Norton Personal Firewall<sup>TM</sup> pour Macintosh<sup>®</sup>

Le logiciel décrit dans ce manuel est fourni sous accord de licence et doit impérativement être utilisé conformément aux termes de cet accord.

## Copyright

Copyright © 2003 Symantec Corporation. Tous droits réservés.

Certaines parties de ce logiciel sont en Copyright © 1990-2000 Aladdin Systems, Inc.

Documentation relative à la version 1.0.a

Tous les documents techniques édités par Symantec Corporation sont protégés par les droits d'auteur détenus par Symantec Corporation.

**LIMITATION DE GARANTIE.** La documentation technique est fournie en l'état, et Symantec Corporation ne peut se porter garant de la validité ou de l'utilisation des informations qu'elle contient. Toute utilisation de la documentation technique et des informations qu'elle contient relève de la responsabilité de l'utilisateur. Cette documentation peut contenir des erreurs techniques ou autres imprécisions, ainsi que des fautes de frappe. Symantec se réserve le droit d'y apporter toutes les modifications nécessaires sans préavis.

Cette publication ne peut être copiée, en partie ou en totalité, sans l'autorisation écrite de Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, Etats-Unis.

## Marques commerciales

Norton Personal Firewall et LiveUpdate sont des marques commerciales de Symantec Corporation.

Macintosh, Mac OS, Macintosh PowerPC, Macintosh G3 et Finder sont des marques commerciales d'Apple Computer. Tous les autres noms de produit ou marques mentionnés dans ce manuel peuvent être des marques commerciales ou des marques déposées de leur société respective et sont reconnues comme telles dans le présent manuel.

Imprimé en Irlande.

10 9 8 7 6 5 4 3 2 1

# Comment utiliser un pare-feu ?

Installez Norton Personal Firewall.  
Le logiciel est automatiquement activé et configuré pour refuser l'accès à tous les services.

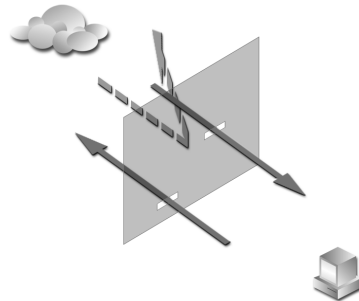
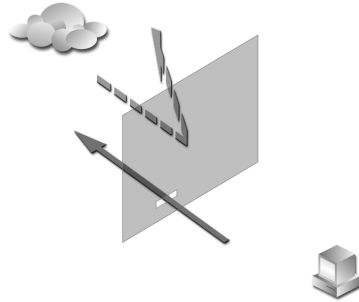
Consultez l'historique des accès.  
Existe-t-il des services Internet non définis et exigeant un accès personnalisé ?  
D'autres ordinateurs ont-ils besoin d'accéder à votre machine ?

Oui

Non

Ajustez la configuration des accès en conséquence.

Consultez régulièrement l'historique des accès afin de vérifier que les réglages sont toujours corrects.





# T A B L E D E S M A T I È R E S

## Comment utiliser un pare-feu ?

### Chapitre 1 A propos de Norton Personal Firewall

Fonctionnement de Norton Personal Firewall .....	9
Identification des ordinateurs bénéficiant d'une autorisation d'accès .....	11
Risques encourus en l'absence de pare-feu .....	11

### Chapitre 2 Installation de Norton Personal Firewall

Configuration du système .....	13
A propos du CD Norton Personal Firewall pour Macintosh .....	14
Installation de Norton Personal Firewall pour Macintosh .....	14
Pour de plus amples informations .....	16
Enregistrement de Norton Personal Firewall pour Macintosh .....	17
Informations de dernière minute .....	18
Connexion au site Web de Symantec via America Online .....	19
Désinstallation de Norton Personal Firewall .....	20

### Chapitre 3 Protection des disques, des fichiers et des données contre les intrusions

Éléments protégés par Norton Personal Firewall .....	21
Configuration des accès à partir des adresses IP .....	22
Protection des numéros de port .....	23
Suivi des tentatives d'accès .....	23
Norton Personal Firewall et AppleTalk .....	24
Utilisateurs multiples .....	24
Sécurité TCP/IP sur Norton Personal Firewall .....	25
AppleTalk et Internet .....	25
Activation et désactivation de la protection pare-feu .....	25
A propos des modes basique et avancé .....	27

---

## Chapitre 4 Réponse aux tentatives d'accès

Surveillance de l'activité du pare-feu .....	29
Activation ou désactivation de la notification des tentatives d'accès .....	30
Test des réglages du pare-feu .....	31
Réponse aux tentatives d'accès .....	33
Informations relatives aux messages d'alerte .....	33
Consultation de l'historique des accès .....	33
Obtention d'informations détaillées sur une tentative d'accès donnée .....	37
Modification des préférences de consignation .....	38
Désactivation de la consignation .....	38
Structure du fichier journal .....	39

## Chapitre 5 Personnalisation de la protection anti-intrusion

Protection des services Internet standard .....	41
Ajout d'adresses IP .....	43
Recherche d'adresses IP .....	44
Ajout d'adresses de sous-réseau .....	45
Définition d'un service personnalisé à protéger .....	46
Modification ou suppression d'un service personnalisé .....	47
Modification des réglages de protection .....	47
Modification du niveau de restriction .....	48
Modification d'une liste d'adresses IP .....	48
Configuration d'une protection UDP .....	49
Fonctionnement de la protection UDP .....	50

## Chapitre 6 Dépannage

Questions fréquentes .....	53
Comment désactiver la protection anti-intrusion ? .....	53
Pourquoi m'est-il impossible de télécharger des fichiers à partir d'un site Web ? .....	54
Pourquoi m'est-il impossible d'accéder aux sites Web ? .....	55
Pourquoi mon serveur FTP ne fonctionne-t-il pas ? .....	55
Pourquoi mon imprimante ne fonctionne-t-elle pas ? .....	56
A quel service correspond ce numéro de port ? .....	56
Comment créer un nouveau fichier journal ? .....	60
Pourquoi Norton Personal Firewall ne se charge-t-il pas ? .....	60
Pourquoi le partage de fichiers ne fonctionne-t-il pas ? .....	60

---

Questions relatives aux réseaux locaux domestiques .....	61
Comment protéger tous les ordinateurs présents sur mon réseau local domestique ? .....	61
Comment spécifier l'accès à un ordinateur dont l'adresse IP est dynamiquement générée ? .....	61
Quelle est l'incidence de la protection anti-intrusion sur le partage de fichiers et d'imprimantes ? .....	61

## **Annexe A      Mise à jour avec LiveUpdate**

A propos de LiveUpdate .....	63
Mise à jour des fichiers de programme .....	64
Consultation du fichier What's New de LiveUpdate .....	66
Vérification des numéros de version et des dates .....	66
Personnalisation d'une session LiveUpdate .....	67
Programmation de LiveUpdate .....	67
Si vous ne pouvez pas utiliser LiveUpdate .....	69
Utilisation de LiveUpdate avec America Online .....	70

## **Glossaire**

## **Index**

---



# A propos de Norton Personal Firewall

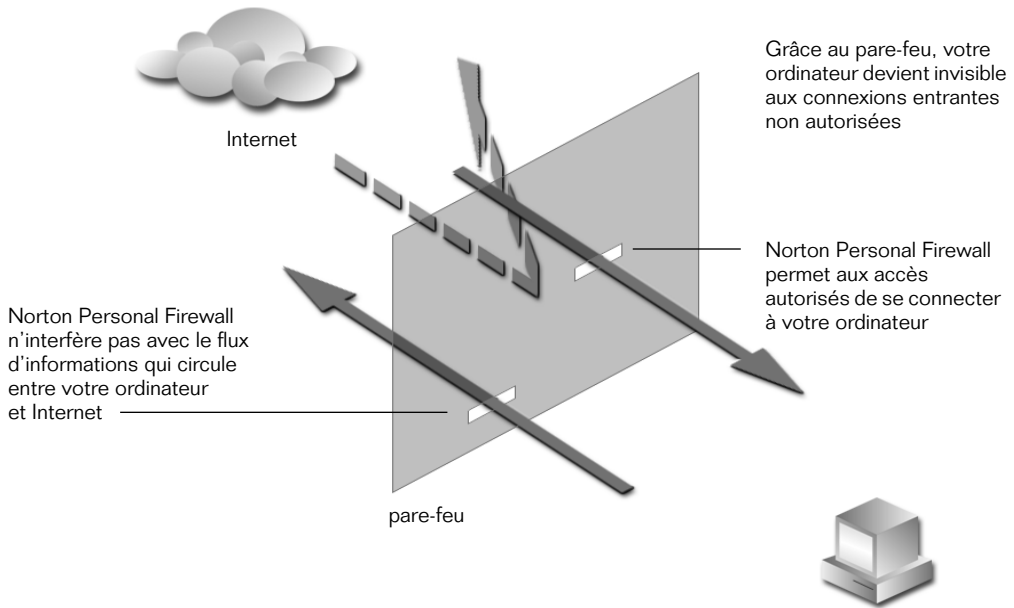
Des millions d'ordinateurs sont connectés à Internet, et leur nombre augmente chaque jour davantage. En vous connectant à Internet, vous avez la possibilité de communiquer avec des millions d'autres ordinateurs. Cependant, ceux-ci peuvent également se connecter à votre ordinateur. En l'absence de protection, votre ordinateur est vulnérable aux attaques de *pirates*, aux *virus*, aux *chevaux de Troie* et autres menaces Internet. Les pirates sont des personnes qui pénètrent dans des systèmes informatiques sans autorisation. Les virus et les chevaux de Troie sont des programmes capables de détériorer les données stockées dans votre ordinateur.

Norton Personal Firewall vous permet de surveiller et de contrôler les connexions établies avec votre ordinateur, et de préserver ainsi la sécurité et la confidentialité de vos données.

## Fonctionnement de Norton Personal Firewall

Norton Personal Firewall place une barrière appelée *pare-feu* entre votre ordinateur et Internet. Les programmes de pare-feu sont des filtres qui bloquent ou autorisent les connexions établies via Internet. En filtrant les connexions, les pare-feu protègent votre ordinateur des activités Internet malveillantes.

Norton Personal Firewall utilise les réglages d'accès pour déterminer s'il doit autoriser ou bloquer les connexions. Vous pouvez modifier ces réglages de façon à permettre ou interdire l'accès d'autres ordinateurs à votre propre machine.



Il vous suffit de spécifier les services que vous souhaitez protéger (par exemple partage Web ou partage de fichiers) et les ordinateurs sur lesquels ils doivent l'être. Vous pouvez autoriser ou refuser l'accès à un service particulier, ou encore autoriser ou refuser l'accès à un service à partir de certains ordinateurs. Vous pouvez par exemple bloquer tous les accès au partage de fichiers, tout en autorisant les accès au partage Web pour des ordinateurs appartenant à des utilisateurs que vous connaissez.

## Identification des ordinateurs bénéficiant d'une autorisation d'accès

En règle générale, vous ne devez pas autoriser quiconque à accéder à votre ordinateur. Toutefois, certaines configurations informatiques et situations de partage de fichiers ou de partage Web exigent que vous définissiez des autorisations d'accès. Par exemple :

- Vous possédez deux ordinateurs ou plus en réseau et l'un d'eux au moins bénéficie d'un 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 (contenant par exemple un album de photos de famille) 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 les utilisateurs auxquels vous souhaitez octroyer un droit d'accès à votre site (les autres membres de votre famille, par exemple).
- Si vous faites appel à un fournisseur d'accès Internet gratuit, vous devrez probablement autoriser l'accès à un port de votre ordinateur pour maintenir la connexion à Internet. Si le fournisseur ne bénéficie pas de cet accès, vous ne pouvez plus l'utiliser.

Lors de l'installation, Norton Personal Firewall est paramétré pour conserver dans un journal toutes les tentatives d'accès. 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.

Pour de plus amples informations sur l'utilisation de la fenêtre Historique des accès, reportez-vous à la section « [Réponse aux tentatives d'accès](#) » à la page 33.

## 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 être très dangereuse, notamment si vous avez activé le partage de fichiers ou le lien entre applications. Les pirates informatiques représentent dans ce cas une menace réelle.

Dans la communauté des programmeurs, un pirate est un individu passionné par l'exploration des ordinateurs et de leurs possibilités ; ce terme n'a aucune connotation négative. Les programmeurs préfèrent utiliser le terme « crackers » pour désigner les pirates malintentionnés. Toutefois, dans le domaine de la sécurité, le terme « cracker » désigne un individu capable de craquer les codes, mais pas nécessairement dans un but malhonnête. Le terme « pirate » étant plus communément employé à l'extérieur de la communauté des programmeurs pour désigner les personnes qui s'introduisent dans des systèmes informatiques pour les endommager, c'est ce terme-là que nous emploierons dans ce manuel.

Les pirates accèdent aux ordinateurs d'autres utilisateurs pour des raisons diverses :

- pour détourner des informations dont ils pourront tirer parti ;
- pour détruire des données ou perturber le fonctionnement de l'ordinateur ;
- pour prouver qu'ils en sont capables, tout simplement.

Les pirates sont aussi nombreux que les motivations qui les animent. Ne partez jamais du principe que vous ne risquez rien parce que vous êtes un utilisateur anonyme. Les pirates ne se préoccupent pas nécessairement de savoir à qui appartient l'ordinateur qu'ils attaquent. Ils recherchent tout simplement un ordinateur non protégé.

# Installation de Norton Personal Firewall

Norton Personal Firewall assure à votre ordinateur Macintosh une protection complète contre les intrusions. Norton Personal Firewall surveille en effet toutes les connexions Internet émises ou reçues par votre ordinateur, les consigne dans un journal et vous prévient en cas de tentatives d'accès non autorisées.

## Configuration du système

Pour pouvoir utiliser Norton Personal Firewall, la configuration minimale de votre ordinateur doit être la suivante :

- Processeur Macintosh Power PC
- Lecteur de CD-ROM
- 24 Mo de mémoire
- 2 Mo d'espace disque libre
- Connexion à Internet
- Mac OS 8.1 ou version supérieure (8.5 ou version supérieure pour la fonctionnalité Barre des réglages)
- Open Transport version 1.3 ou supérieure

## A propos du CD Norton Personal Firewall pour Macintosh

Utilisez le CD Norton Personal Firewall pour Macintosh pour installer votre logiciel. Ce CD contient des versions de Norton Personal Firewall pour Mac OS 8.1-9.x et Mac OS X. Cliquez deux fois sur le dossier d'installation pour OS 9 pour installer la version Mac OS 8.1-9.x.

Outre le programme d'installation de Norton Personal Firewall pour Mac OS 8.1-9.x, le dossier OS 9 contient également un dossier de documentation, dans lequel vous trouverez le *Guide de l'utilisateur de Norton Personal Firewall* au format .pdf, ainsi que les fichiers d'installation d'Adobe Acrobat Reader.

## Installation de Norton Personal Firewall pour Macintosh

Pour obtenir des informations de dernière minute ainsi que des conseils de dépannage et d'installation, consultez le fichier Lisez-moi qui figure sur le CD.

---

**Remarque :** Le fichier Lisez-moi contient des informations qui s'appliquent à la fois aux versions Mac OS 8.1-9.x et Mac OS X de Norton Personal Firewall.

---

### Pour lire le fichier :

- 1 Insérez le CD dans le lecteur de CD-ROM.
- 2 Cliquez deux fois sur le fichier **Lisez-moi**.

Après avoir lu ce fichier, installez Norton Personal Firewall.

Si vous installez Norton Personal Firewall dans un emplacement qui contient déjà une copie du pare-feu DoorStop d'Open Door, les fichiers de DoorStop sont supprimés, mais les paramètres DoorStop existants sont conservés dans Norton Personal Firewall.

**Pour installer Norton Personal Firewall pour Macintosh :**

- 1 Insérez le CD de Norton Personal Firewall pour Macintosh dans le lecteur de CD-ROM.  
Si la fenêtre du CD ne s'ouvre pas automatiquement, cliquez deux fois sur l'icône du **CD** pour l'ouvrir.
- 2 Dans la fenêtre du CD, cliquez deux fois sur le dossier **d'installation pour OS 9**.
- 3 Dans le dossier d'installation pour OS 9, cliquez deux fois sur le programme **d'installation de Personal Firewall**.
- 4 Le programme vous invite à progresser dans les divers écrans d'information qui s'affichent.  
Si vous cliquez sur **Refuser** dans la fenêtre des accords de licence et de garantie, l'installation est annulée.
- 5 Procédez comme suit :
  - Pour procéder à une installation complète, cliquez sur **Installation Standard**.
  - Pour sélectionner des composants individuels, cliquez sur **Installation personnalisée**, puis sélectionnez les composants que vous souhaitez installer.
- 6 Acceptez la destination proposée par défaut ou spécifiez un dossier-cible différent pour l'installation.
- 7 Cliquez sur **Installer**.
- 8 Pour terminer l'installation, suivez les instructions qui s'affichent à l'écran, puis cliquez sur **Redémarrer**.

Après le premier redémarrage de votre ordinateur consécutif à l'installation de Norton Personal Firewall, Norton Personal Firewall s'ouvre et affiche la rubrique Statut de la fenêtre d'installation afin de vérifier que le pare-feu est activé. Quittez le programme pour faire disparaître cette fenêtre. Le pare-feu reste activé.



Si vous ne parvenez pas à éjecter le CD après avoir redémarré votre ordinateur, procédez comme suit :

- Appuyez sur le bouton d'éjection du lecteur de CD-ROM lorsque vous entendez le bip de redémarrage de votre Macintosh.
- Sur les nouveaux ordinateurs Macintosh équipés d'un lecteur de CD-ROM à fente, appuyez sur le bouton de la souris pendant le démarrage pour éjecter le CD.

Après avoir installé Norton Personal Firewall, redémarrez votre ordinateur pour le protéger contre les intrusions. L'extension Norton Personal Firewall se charge systématiquement à chaque démarrage de l'ordinateur pour le protéger contre les intrusions, à moins que vous ne la désactiviez manuellement.

## Pour de plus amples informations

L'application Norton Personal Firewall est fournie avec une aide contextuelle intégrée.

### Pour accéder à l'Aide :

- Cliquez sur **Aide** à partir d'une fenêtre de Norton Personal Firewall.



Votre navigateur Web s'ouvre et affiche une fenêtre d'aide.

Le *Guide de l'utilisateur de Norton Personal Firewall* est disponible sur le CD sous forme de fichier .pdf (Adobe Acrobat) imprimable. Vous pouvez également installer Adobe Acrobat Reader s'il n'est pas présent sur votre ordinateur.

---

**Remarque :** Le fichier Lisez-moi inclus sur le CD Norton Personal Firewall pour Macintosh contient des informations de dernière minute sur votre nouveau logiciel. Nous vous recommandons de le lire avant de poursuivre.

---



# Enregistrement de Norton Personal Firewall pour Macintosh

Votre connexion Internet vous permet d'enregistrer Norton Personal Firewall pour Macintosh via *Internet*.

Si vous travaillez sous Mac OS 8.5 ou une version ultérieure, vous trouverez dans le dossier de Norton Personal Firewall pour Macintosh une icône permettant de lancer votre navigateur et de vous connecter à la page d'enregistrement de logiciels de Symantec. Si vous possédez une version antérieure de Macintosh OS, guidez votre navigateur jusqu'à la page Web de Symantec.

## Pour effectuer l'enregistrement sur Internet :

- 1 Connectez-vous à Internet.  
Si vous utilisez America Online (AOL) pour vous connecter à Internet, reportez-vous à la section « [Pour enregistrer votre logiciel via AOL :](#) » à la page 19.
- 2 Dans le dossier de Norton Personal Firewall pour Macintosh, cliquez deux fois sur **Enregistrer votre logiciel**.

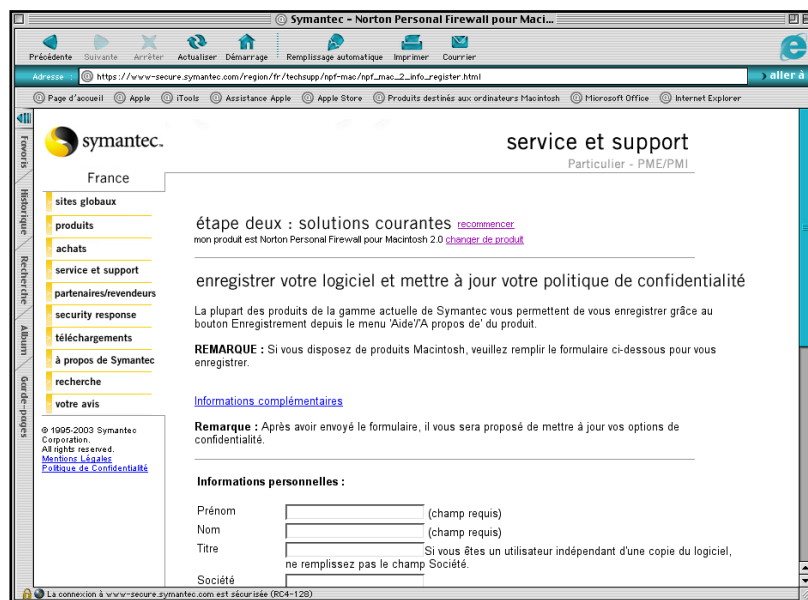


### Enregistrer votre logiciel

Votre navigateur Internet par défaut affiche la page d'enregistrement Service et support de Symantec.

- 3 Si vous utilisez le système d'exploitation Mac OS 8.1, lancez votre navigateur et accédez à la page Service et support de Symantec :  
<http://www.symantec.com/frsupport/>
- 4 Dans la page Service et support, cliquez sur **Particulier – PME/PMI**.
- 5 Dans la page suivante, sélectionnez le produit **Norton Personal Firewall pour Macintosh** et la version **1.0**.

### 6 Cliquez sur **continuer**.



- 7 Dans la page d'enregistrement de Norton Personal Firewall pour Macintosh, saisissez toutes les informations requises.
- 8 Cliquez sur **Envoyer l'enregistrement**.

## Informations de dernière minute

Norton Personal Firewall pour Macintosh installe un lien vers les informations de dernière minute, qui vous permet de consulter les dernières informations relatives au logiciel que vous avez installé.

### Pour consulter les informations de dernière minute :

- 1 Connectez-vous à Internet.

Si vous utilisez America Online (AOL) pour vous connecter à Internet, reportez-vous à la section « [Pour consulter les informations de dernière minute via AOL](#) : » à la page 20.

- 
- 2 Dans le dossier de Norton Personal Firewall pour Macintosh, cliquez deux fois sur **Nouvelles de dernière minute**.



Nouvelles de dernière minute

Votre navigateur Internet par défaut affiche la page Web des informations de dernière minute de Symantec pour votre produit.

- 
- 
- 3 Si vous utilisez le système Mac OS 8.1, lancez votre navigateur et accédez à la page Web de Symantec :

<http://www.symantec.com/region/fr/product/mac.html>

## Connexion au site Web de Symantec via America Online

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

### Pour enregistrer votre logiciel 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, cliquez deux fois sur **Enregistrer votre logiciel**.
- 5 Dans la page Service et support, cliquez sur **Particulier – PME/PMI**.
- 6 Dans la page suivante, sélectionnez le produit **Norton Personal Firewall pour Macintosh** et la version **1.0**.
- 7 Cliquez sur **continuer**.
- 8 Dans la page Service et support, entrez toutes les informations requises.
- 9 Cliquez sur **Envoyer l'enregistrement**.
- 10 Mettez fin à votre connexion avec AOL.

### Pour consulter les informations de dernière minute 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 le dossier de Norton Personal Firewall pour Macintosh, cliquez deux fois sur **Nouvelles de dernière minute**.  
Votre navigateur affiche la page Web des informations de dernière minute de Symantec pour votre produit.
- 5 Lorsque vous avez terminé votre lecture, mettez fin à votre connexion avec AOL.

## Désinstallation de Norton Personal Firewall

Utilisez le CD de Norton Personal Firewall pour supprimer Norton Personal Firewall de votre système.

### Pour désinstaller Norton Personal Firewall :

- 1 Insérez le CD de Norton Personal Firewall pour Macintosh dans le lecteur de CD-ROM.  
Si la fenêtre du CD ne s'ouvre pas automatiquement, cliquez deux fois sur l'icône du **CD** pour l'ouvrir.
- 2 Dans la fenêtre du CD, cliquez deux fois sur le dossier d'**installation pour OS 9**.
- 3 Dans la fenêtre d'installation pour OS 9, cliquez deux fois sur le programme d'**installation de Personal Firewall**.
- 4 Progressez dans les différents écrans d'information, jusqu'à l'écran de sélection des options d'installation.
- 5 Dans la liste, cliquez sur **Désinstaller**.
- 6 Sélectionnez le dossier à partir duquel vous souhaitez désinstaller Norton Personal Firewall.
- 7 Cliquez sur **Désinstaller**.

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

Norton Personal Firewall protège votre ordinateur contre les intrusions à l'aide des réglages d'accès que vous définissez. 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 ordinateur. Norton Personal Firewall prend en charge le suivi de toutes les tentatives d'accès et fonctionne conjointement avec AppleTalk pour contrôler les accès. Vous pouvez activer et désactiver Norton Personal Firewall à tout moment.

### Éléments 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, éventuellement, *UDP* (User Datagram Protocol). En d'autres termes, lorsque vous êtes connecté à Internet ou à un autre réseau, aucun ordinateur ne peut accéder sans votre autorisation aux fichiers, programmes ou autres informations stockés dans votre ordinateur. Cette autorisation est accordée à un ordinateur et non à un utilisateur spécifique, ce qui permet à tous les utilisateurs de cet ordinateur d'en bénéficier.

Norton Personal Firewall ne permet pas d'exercer un contrôle sur les informations sortantes. Par exemple, vous ne pouvez pas l'utiliser pour bloquer la connexion à des sites Web inconvenants, ni pour chiffrer des informations personnelles telles que le numéro d'une carte de crédit que vous indiquez sur un site Web. Le programme ne bloque pas non plus les connexions *AppleTalk* directes (*AppleTalk* est un protocole de communication propre au système Macintosh).

Pour de plus amples informations sur le fonctionnement de Norton Personal Firewall avec *AppleTalk*, reportez-vous à la section « [Norton Personal Firewall et AppleTalk](#) » à la page 24.

## Configuration des accès à partir des adresses IP

Lorsque vous accordez ou refusez des autorisations d'accès à certains ordinateurs, vous répertoriez 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, séparés par des points (par exemple, 216.35.137.202). 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 à son *nom d'hôte*. Le nom d'hôte identifie un ordinateur sur un réseau. Par exemple, [www.symantec.com](http://www.symantec.com) est le nom d'hôte du site Web de Symantec. Les noms d'hôte sont convertis en adresses IP par le *système de noms de domaine* (DNS, Domain Name System). Vous pouvez entrer un nom d'hôte et rechercher l'adresse IP correspondante à l'aide de Norton Personal Firewall.

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

## Protection des numéros de port

Vous pouvez répertorier des adresses IP pour octroyer ou refuser des 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. Par exemple, le partage Web utilise en général le port 80, tandis que le port 548 est utilisé pour le partage de fichiers sur TCP/IP. Certains services fonctionnent cependant parfois sur d'autres ports. Ainsi, si deux *serveurs Web* (ordinateurs qui acheminent des pages Web vers 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 de ces serveurs. Le choix d'une protection par numéro de port est très utile pour protéger des services non prédéfinis par Norton Personal Firewall ou des services qui utilisent d'autres numéros de port.

Vous pouvez également protéger des services qui utilisent des ports UDP. Cette option est toutefois réservée uniquement 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 peut enregistrer toutes les connexions refusées et/ou autorisées et peut même vous informer immédiatement des accès autorisés ou refusés, si vous le souhaitez.

## Norton Personal Firewall et AppleTalk

Les ordinateurs Macintosh utilisent principalement deux protocoles réseau, AppleTalk et TCP/IP. En règle générale, AppleTalk fournit des services locaux qui ne sont pas disponibles sur Internet, tels que l'impression, le partage de fichiers avec d'autres ordinateurs du même réseau et les applications propres à une entreprise. TCP/IP permet d'accéder à des services plus généraux, notamment les services Internet tels que la messagerie électronique et l'accès aux sites Web. Sous Macintosh OS 9, TCP/IP fournit également des services qui n'étaient jusque là disponibles que par l'intermédiaire d'AppleTalk, notamment le partage de fichiers et le lien entre applications sur Internet ou sur un intranet.

### Utilisateurs multiples

Le fichier Utilisateurs multiples est le principal composant de sécurité réseau intégré au système d'exploitation Macintosh. Ce fichier, accessible à partir du tableau de bord Utilisateurs multiples ou du tableau de bord Partage de fichiers sous Macintosh OS 9, permet au propriétaire d'un ordinateur de configurer des comptes utilisateur et des mots de passe donnant accès aux services réseau intégrés, et de spécifier les services auxquels chaque compte aura accès. Les comptes utilisateur permettent de limiter l'accès à ces services par le biais d'AppleTalk ou de TCP/IP. Il est également possible d'accorder des autorisations d'accès à certains invités (utilisateurs ne possédant pas de mot de passe). Les services qui utilisent la sécurité Utilisateur multiples sont notamment des services de lien entre applications, de partage de fichiers, de partage Web et d'accès distant (permet aux utilisateurs de se connecter à un ordinateur spécifique). L'accès à ces services est généralement configuré par l'intermédiaire de leurs tableaux de bord respectifs.



## 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. Ce mécanisme de sécurité est donc indépendant des mots de passe exigés par Utilisateurs multiples. Par exemple, si vous avez activé le partage de fichiers sur TCP/IP, les mots de passe de partage de fichiers créés dans Utilisateurs multiples sont insuffisants pour permettre aux utilisateurs d'accéder aux fichiers. Vous devez également autoriser l'accès au partage de fichiers pour leurs ordinateurs dans Norton Personal Firewall. Vous pouvez soit autoriser tous les accès dans Norton Personal Firewall et vous contenter d'utiliser les mécanismes de sécurité Utilisateurs multiples, soit autoriser les accès pour certaines adresses IP uniquement, et bénéficier ainsi de deux points de contrôle pour les tentatives d'accès au partage des fichiers.

## AppleTalk et Internet

Lorsque vous démarrez Norton Personal Firewall, vous recevez un avertissement si vos connexions AppleTalk et Internet utilisent le même port. Dans ce cas, il se peut que votre ordinateur soit accessible sur Internet. Si vous recevez un tel avertissement, procédez comme suit :

- Désactivez l'accès accordé aux invités dans le tableau de bord Utilisateurs multiples.
- Désactivez AppleTalk lorsque vous vous connectez à Internet car Norton Personal Firewall ne protège pas les connexions AppleTalk.
- Si vous utilisez un produit tel que Timbuktu, qui permet un accès direct entre deux postes de travail via AppleTalk ou TCP/IP, il est préférable de désactiver les fonctionnalités AppleTalk du produit, car elles ne sont pas protégées par Norton Personal Firewall.

## Activation et désactivation de la protection pare-feu

Par défaut, Norton Personal Firewall refuse l'accès à tous les services TCP/IP. En règle générale, les réglages du logiciel assurent la protection requise, sans gêner les utilisateurs dans leur travail. A moins que vous ne souhaitiez définir des règles d'accès spécifiques, n'effectuez aucune opération après l'installation de Norton Personal Firewall.

Vous pouvez arrêter la protection à tout moment en désactivant Norton Personal Firewall. Par exemple, vous pouvez désactiver temporairement Norton Personal Firewall pour utiliser *FTP* (File Transfer Protocol). Vous pouvez désactiver Norton Personal Firewall pour une période donnée ou jusqu'à ce que vous le réactiviez.

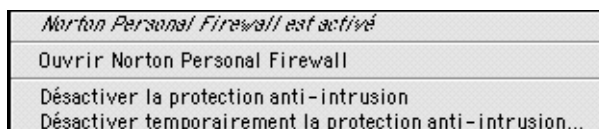
Vous pouvez désactiver (ou activer) Norton Personal Firewall à partir de deux emplacements : à partir de la fenêtre Configuration ou de la barre des réglages (si vous possédez Macintosh OS 8.5 ou une version supérieure).

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

- 1 Lancez Norton Personal Firewall en cliquant deux fois sur l'icône **Norton Personal Firewall**.
- 2 Cliquez sur **Désactiver la protection**.  
Si Norton Personal Firewall est déjà désactivé, ce bouton s'intitule Activer et vous permet de réactiver la protection Norton Personal Firewall.
- 3 Vous êtes invité à confirmer la désactivation de Norton Personal Firewall.
- 4 Fermez Norton Personal Firewall.

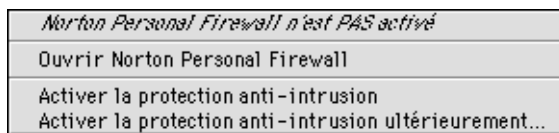
### **Pour désactiver ou activer Norton Personal Firewall à partir de la barre des réglages :**

- 1 Cliquez sur le module Norton Personal Firewall pour ouvrir le menu de la barre des réglages.  
La première ligne du menu indique le statut actuel de Norton Personal Firewall.



- 2 Cliquez sur **Désactiver la protection anti-intrusion** pour désactiver Norton Personal Firewall.  
Si Norton Personal Firewall est déjà désactivé, l'option s'intitule Activer la protection anti-intrusion.

- 3 Vous êtes invité à confirmer la désactivation de Norton Personal Firewall.



Vous pouvez également utiliser le menu de la barre des réglages pour lancer Norton Personal Firewall et pour désactiver la protection pour une période donnée, ou pour la réactiver après un certain laps de temps.

**Pour désactiver et activer Norton Personal Firewall après une période donnée :**

- 1 Cliquez sur le module Norton Personal Firewall pour ouvrir le menu de la barre des réglages.
- 2 Cliquez sur **Désactiver temporairement la protection anti-intrusion** ou sur **Activer la protection anti-intrusion ultérieurement**.
- 3 Indiquez le délai (en minutes) à l'issue duquel Norton Personal Firewall devra démarrer.
- 4 Cliquez sur **OK**.

## A propos des modes basique et avancé

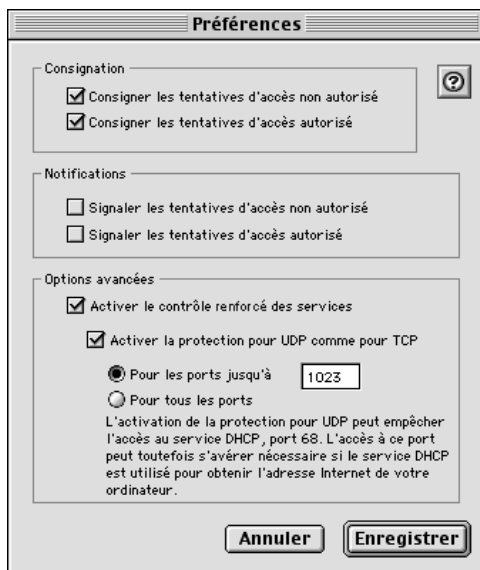
Norton Personal Firewall propose deux modes de fonctionnement : basique et avancé. Le mode basique permet de définir les accès aux services les plus fréquemment utilisés. Norton Personal Firewall est défini par défaut en mode basique.

Utilisez le mode avancé pour :

- définir les réglages d'accès à un service qui n'est pas encore répertorié dans Norton Personal Firewall ;
- spécifier un sous-réseau autre que le vôtre dans une liste d'adresses IP ;
- étendre la protection aux ports UDP ;
- afficher des informations détaillées sur les tentatives d'accès.

Pour passer en mode avancé :

- 1 Dans le menu Edition, cliquez sur **Préférences**.



- 2 Cochez la case **Activer le contrôle renforcé des services**.
- 3 Cliquez sur **Enregistrer**.

## Réponse aux tentatives d'accès

Il n'est pas toujours très facile de déterminer si Norton Personal Firewall remplit bien son rôle : vous continuez en effet à utiliser votre ordinateur comme d'habitude, sans noter aucune différence. C'est exactement le but recherché. Le pare-feu est en place et bloque toutes les intrusions indésirables.

Norton Personal Firewall enregistre dans un journal toutes les tentatives d'accès, qu'elles soient autorisées ou non. Ce journal vous permet de vérifier que Norton Personal Firewall fonctionne correctement.

### Surveillance de l'activité du pare-feu

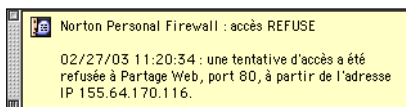
Par défaut, Norton Personal Firewall consigne dans un journal aussi bien les tentatives d'accès refusées que les tentatives d'accès autorisées. Ces tentatives sont répertoriées dans la fenêtre Historique des accès, que vous pouvez consulter à tout moment.

Vous pouvez recevoir une notification immédiate des tentatives d'accès dans des circonstances particulières. Par exemple, lorsque vous installez Norton Personal Firewall pour la première fois, vous pouvez évaluer immédiatement chaque tentative d'accès afin de vous assurer que le logiciel remplit bien son rôle. Vous pouvez également choisir de recevoir une notification immédiate si vous avez modifié certains réglages et souhaitez vous assurer qu'ils ont effectivement généré les résultats escomptés.

Pour vérifier les réglages de protection ou les modifications apportées à ces réglages avant de vous connecter, utilisez la fonction d'autotest de Norton Personal Firewall. L'autotest simule une connexion TCP, consigne dans le journal une tentative d'accès et déclenche une notification si vous avez activé cette option.

## Activation ou désactivation de la notification des tentatives d'accès

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



Pour savoir comment procéder lors de la réception d'une alerte, reportez-vous à la section « [Informations relatives aux messages d'alerte](#) » à la page 33.

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.

### Pour activer ou désactiver la notification des accès :

- 1 Cliquez deux fois sur l'icône de **Norton Personal Firewall** ou, dans le menu de la barre des réglages, cliquez sur **Ouvrir Norton Personal Firewall** pour lancer Norton Personal Firewall.
- 2 Dans le menu Edition, cliquez sur **Préférences**.
- 3 Indiquez les options de notification souhaitées.
- 4 Cliquez sur **Enregistrer**.

## Test des réglages du pare-feu

L'autotest contrôle la protection anti-intrusion en simulant une tentative d'accès à un service. Vous pouvez exécuter l'autotest en mode basique ou avancé. Avant de commencer, assurez-vous que la consignation est activée.

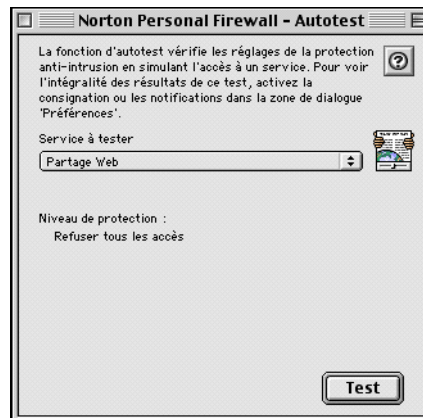
En mode basique, vous pouvez tester les services répertoriés dans la fenêtre Configuration, qu'ils soient prédéfinis ou personnalisés. Le test utilise l'adresse IP de votre ordinateur. Si l'ordinateur utilise une connexion PPP (Point-to-Point protocol) et qu'il n'est pas connecté lors du test, ou si votre ordinateur ne possède pas d'adresse IP, l'autotest utilise l'adresse IP 127.0.0.1.

En mode avancé, vous pouvez tester une liste étendue de services et spécifier pour le test une adresse IP autre que celle de votre ordinateur. Vous pouvez par exemple entrer une adresse IP pour laquelle vous aviez défini une interdiction d'accès.

Pour consulter les résultats de l'autotest, affichez la fenêtre Historique des accès. Si vous avez activé les notifications pour le type de tentative d'accès testé, l'autotest génère une alerte. Si Norton Personal Firewall n'est pas activé, l'accès à tous les services est autorisé et l'autotest vous l'indique.

### Pour effectuer un autotest en mode basique :

- 1 Cliquez deux fois sur l'icône de **Norton Personal Firewall** ou, dans le menu de la barre des réglages, cliquez sur **Ouvrir Norton Personal Firewall** pour lancer Norton Personal Firewall.
- 2 Dans le menu Fenêtre, cliquez sur **Autotest**.



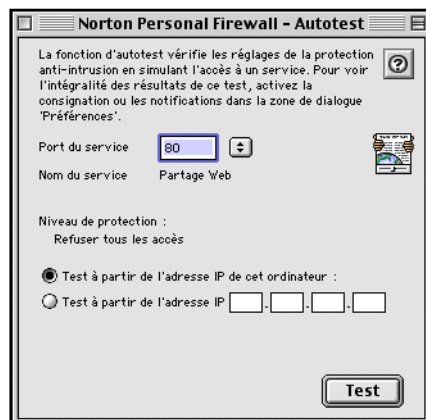
- 3 Sélectionnez un port de service.

Le niveau de protection défini pour le service choisi s'affiche sous le nom de service.

- 4 Cliquez sur **Test**.

### Pour exécuter l'autotest en mode avancé :

- 1 Dans le menu Fenêtre, cliquez sur **Autotest**.



- 2 Spécifiez le numéro de port du service.

Le niveau de protection défini pour le service choisi s'affiche sous le nom de service.

- 3 Indiquez si vous souhaitez utiliser l'adresse IP de votre ordinateur ou une adresse IP différente pour le test.

Si aucune adresse IP n'a été attribuée à votre ordinateur, l'option Test à partir de l'adresse IP de cet ordinateur est estompée.

- 4 Le cas échéant, entrez une adresse IP.

- 5 Cliquez sur **Test**.

En modes basique et avancé, seuls les services TCP sont testés. Il se peut que la protection définie pour un service UDP spécifique diffère de celle du service TCP correspondant selon la configuration de Norton Personal Firewall.



# Réponse aux tentatives d'accès

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

## Informations relatives aux messages d'alerte

Si vous avez activé la notification des tentatives d'accès, des messages d'alerte s'affichent à l'écran à chaque tentative d'accès.



Les messages d'alerte fournissent des informations détaillées sur les tentatives d'accès. Si une tentative vous semble suspecte, consultez la fenêtre Historique des accès. Pour obtenir des informations plus précises sur une tentative d'accès répertoriée dans cette fenêtre, cliquez deux fois sur la ligne correspondante.

La notification des tentatives d'accès ne reprend qu'après la fermeture du message d'alerte en cours. De plus, avec les systèmes d'exploitation antérieurs à OS 9, l'exécution des autres applications peut être suspendue jusqu'à la fermeture du message d'alerte. En votre absence, n'activez pas la notification sous ces systèmes d'exploitation si d'autres applications sont actives.

## Consultation de l'historique des accès

Toutes les tentatives d'accès consignées apparaissent dans la fenêtre 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 :

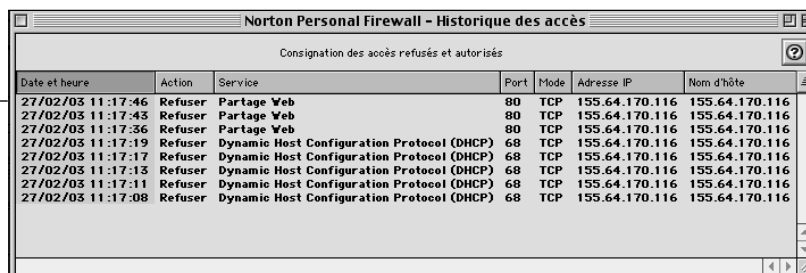
- refus d'accès récurrents, en particulier pour une adresse IP cliente habituelle ;
- succession de numéros de port sollicités par une même adresse IP cliente, indiquant probablement un examen des ports (un intrus passe en revue les différents ports de votre ordinateur jusqu'à ce qu'il trouve un port accessible).

Il est normal que certaines tentatives d'accès soient refusées de façon aléatoire (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 propre ordinateur, telles que la connexion à un serveur FTP et l'envoi de messages électroniques.

### Pour afficher la fenêtre Historique des accès :

- 1 Cliquez deux fois sur l'icône de **Norton Personal Firewall** ou, dans le menu de la barre des réglages, cliquez sur **Ouvrir Norton Personal Firewall** pour lancer Norton Personal Firewall.
- 2 Dans le menu Fenêtre, cliquez sur **Historique des accès**.

Présentation en  
mode avancé



Date et heure	Action	Service	Port	Mode	Adresse IP	Nom d'hôte
27/02/03 11:17:46	Refuser	Partage Web	80	TCP	155.64.170.116	155.64.170.116
27/02/03 11:17:43	Refuser	Partage Web	80	TCP	155.64.170.116	155.64.170.116
27/02/03 11:17:36	Refuser	Partage Web	80	TCP	155.64.170.116	155.64.170.116
27/02/03 11:17:19	Refuser	Dynamic Host Configuration Protocol (DHCP)	68	TCP	155.64.170.116	155.64.170.116
27/02/03 11:17:17	Refuser	Dynamic Host Configuration Protocol (DHCP)	68	TCP	155.64.170.116	155.64.170.116
27/02/03 11:17:13	Refuser	Dynamic Host Configuration Protocol (DHCP)	68	TCP	155.64.170.116	155.64.170.116
27/02/03 11:17:11	Refuser	Dynamic Host Configuration Protocol (DHCP)	68	TCP	155.64.170.116	155.64.170.116
27/02/03 11:17:08	Refuser	Dynamic Host Configuration Protocol (DHCP)	68	TCP	155.64.170.116	155.64.170.116

La fenêtre Historique des accès peut être consultée en mode basique ou en mode avancé. En mode basique, les colonnes Port, Mode et Adresse IP n'apparaissent pas.

Vous trouverez des instructions sur le passage en mode avancé à la section « [Pour passer en mode avancé](#) : » à la page 28

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
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	Protocole utilisé (TCP ou UDP)
Adresse IP	Adresse IP de l'ordinateur à l'origine de la tentative d'accès
Nom d'hôte	Nom d'hôte de l'ordinateur à l'origine de la tentative d'accès

Les lignes en gras datent de moins de 15 minutes.

## **Tri des colonnes**

Par défaut, les lignes sont triées par date. Les lignes les plus récentes apparaissent en début de liste.

### **Pour effectuer un tri en fonction d'autres colonnes :**

- Cliquez sur l'en-tête de la colonne.  
L'en-tête en gris foncé identifie la colonne à partir de laquelle le tri est actuellement effectué.

Modifiez l'ordre du tri (croissant ou décroissant) en cliquant sur le triangle situé à droite des en-têtes de colonne.

## Exportation des informations de la fenêtre Historique des accès

Vous pouvez exporter le contenu de la fenêtre Historique des accès dans un fichier texte délimité par des tabulations. L'exportation n'est possible que si la fenêtre Historique des accès est ouverte.

### Pour exporter les informations affichées dans la fenêtre Historique des accès :

- 1 Dans le menu Fichier, cliquez sur **Exporter**. Pour pouvoir utiliser cette fonction, la fenêtre Historique des accès doit être ouverte.
- 2 Dans la zone de dialogue d'exportation, indiquez l'emplacement et le nom du fichier.  
Pour créer un nouveau dossier pour ce fichier, sélectionnez **Nouveau**.
- 3 Cliquez sur **Enregistrer**.

## Effacement du contenu de la fenêtre Historique des accès

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

### Pour effacer le contenu de la fenêtre Historique des accès :

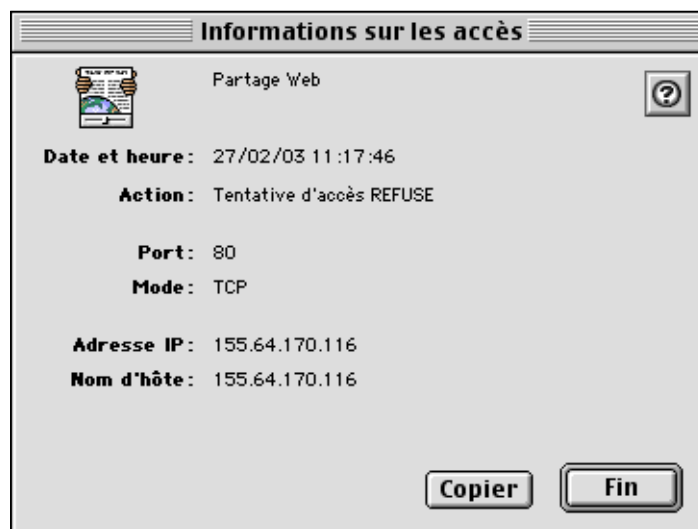
- Dans le menu Edition, cliquez sur **Purger l'historique des accès**.  
Pour pouvoir utiliser cette fonction, la fenêtre Historique des accès doit être ouverte.  
Cette opération n'a aucune incidence sur le fichier journal ; toutes les tentatives d'accès qui y sont consignées sont préservées.

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

Vous avez la possibilité d'obtenir des informations détaillées sur chacune des entrées répertoriées dans la fenêtre Historique des accès.

### Pour ouvrir la zone de dialogue Informations sur les accès :

- Dans la fenêtre Historique des accès, cliquez deux fois sur une ligne ou sélectionnez une ligne, puis cliquez sur **Lire les informations** dans le menu Edition.



### Pour copier les informations dans le Presse-papiers afin de pouvoir les utiliser dans une autre application :

- Dans la zone de dialogue Informations sur les accès, cliquez sur **Copier**.

## Accès à la page Web de détails sur les accès

La page Web de détails sur les accès de Norton Personal Firewall fournit 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 (le champ Nom d'hôte) des tentatives d'accès.

**Pour accéder à la page Web de détails sur les accès de Norton Personal Firewall :**

- Dans la zone de dialogue Informations sur les accès, cliquez sur **Apprendre**.

## **Modification des préférences de consignation**

La consignation de toutes les tentatives d'accès est activée par défaut. Conservez ce paramètre 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. C'est pourquoi vous pouvez limiter les données à consigner.

**Pour modifier les préférences de consignation :**

- 1 Cliquez deux fois sur l'icône de **Norton Personal Firewall** ou, dans le menu de la barre des réglages, cliquez sur **Ouvrir Norton Personal Firewall** pour lancer Norton Personal Firewall.
- 2 Dans le menu Edition, cliquez sur **Préférences**.
- 3 Indiquez les options de consignation souhaitées.
- 4 Cliquez sur **Enregistrer**.

## **Désactivation de la consignation**

La consignation et la protection des services sont totalement indépendantes l'une de l'autre. Par exemple, si vous consignez les accès autorisés puis désactivez Norton Personal Firewall, ce dernier continue à consigner 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.

**Pour désactiver la consignation :**

- 1 Cliquez deux fois sur l'icône de **Norton Personal Firewall** ou, dans le menu de la barre des réglages, cliquez sur **Ouvrir Norton Personal Firewall** pour lancer Norton Personal Firewall.
- 2 Dans le menu Edition, cliquez sur **Préférences**.
- 3 Désactivez les deux options de consignation.
- 4 Cliquez sur **Enregistrer**.

# Structure du fichier journal

Le journal est un fichier texte délimité par des tabulations, appelé Journal Norton Personal Firewall et placé dans le dossier Préférences de votre ordinateur. Il est enregistré au format WebSTAR étendu, lisible par la plupart des traitements de texte et des tableurs, ainsi que par certaines applications d'analyse des journaux.

Les tentatives d'accès sont consignées à l'aide des éléments suivants (inclus dans la ligne !!LOG\_FORMAT à chaque démarrage de Norton Personal Firewall ou lors de la création d'un nouveau fichier journal) :

DATE, TIME	Date et heure d'accès au format WebSTAR standard
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 à un port particulier
SERVER_PORT	Port auquel un client donné tente d'accéder
METHOD	Protocole utilisé pour la tentative d'accès (TCP ou UDP)

L'exportation du journal dans un tableur, puis 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 pour lesquelles le champ RESULT prend la valeur ERR!, observez les adresses IP dans le champ HOSTNAME. 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 pour lesquelles 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. Des séries de différents numéros de port associés à une même adresse IP peuvent en effet indiquer une tentative d'analyse des ports.

Pour plus d'informations sur une adresse IP répertoriée dans le fichier journal (ou dans une alerte de notification), consultez la fenêtre Historique des accès. Pour de plus amples informations sur la consultation de la fenêtre Historique des accès, reportez-vous à la section « [Pour afficher la fenêtre Historique des accès :](#) » à la page 34.





## Personnalisation de la protection anti-intrusion

A mesure que vous utilisez Norton Personal Firewall, vous devrez peut-être ajuster vos réglages d'accès. Par exemple, vous souhaiterez peut-être autoriser le partage de fichiers pour un collègue qui travaille sur un autre site. Il peut également arriver qu'un service présent sur votre ordinateur et non répertorié dans la fenêtre Configuration exige une protection personnalisée. Vous pouvez ajouter ce service à la liste. Vous pouvez également étendre la protection aux ports UDP de l'ordinateur.

Les modifications apportées aux réglages 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 interruption de la connexion. Par exemple, si 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 se déconnecte 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 prédéfinis dans la fenêtre Configuration de Norton Personal Firewall. Les services non répertoriés sont protégés en fonction des réglages définis pour l'entrée Autres. Tous les accès sont refusés par défaut. Vous pouvez modifier les réglages de protection pour tous les services répertoriés.

### Pour ouvrir la fenêtre Configuration :

- 1 Cliquez deux fois sur l'icône de **Norton Personal Firewall** ou, dans le menu de la barre des réglages, cliquez sur **Ouvrir Norton Personal Firewall** pour lancer Norton Personal Firewall.
- 2 Si la fenêtre Configuration n'apparaît pas, ouvrez le menu Fenêtre et cliquez sur **Configuration**.
- 3 Si la fenêtre Configuration ne s'affiche que partiellement, cliquez sur **Réglages** pour l'agrandir.



Lorsque vous ouvrez la fenêtre Configuration pour la première fois, les réglages de protection situés à droite n'apparaissent pas. Pour afficher les réglages associés à l'un des services répertoriés dans le volet gauche de la fenêtre, cliquez sur ce service.

Pour chaque service répertorié dans la fenêtre Configuration, 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 réglages sont classés par ordre de restriction décroissante. Pour refuser ou autoriser tout accès à un service, cliquez sur ce service puis activez l'option souhaitée.

Pour autoriser ou refuser tout accès à une liste d'adresses IP, cliquez sur le service, activez l'option souhaitée, puis définissez les adresses IP à inclure dans la liste.

**Pour définir une liste d'adresses auxquelles vous souhaitez accorder ou refuser l'accès :**

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

La zone de dialogue Nouvelle adresse apparaît.

## Ajout d'adresses IP

Les deux premières options de la zone de dialogue Nouvelle adresse vous permettent d'ajouter une seule adresse ou une plage d'adresses à la liste des accès autorisés ou refusés.

**Pour ajouter une seule adresse :**

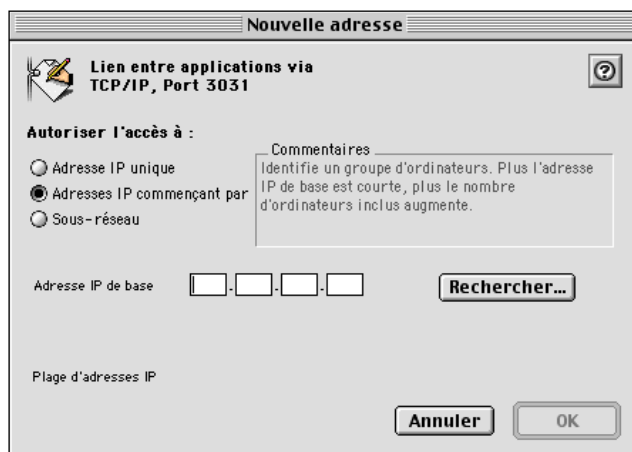
- 1 Dans la zone de dialogue Nouvelle adresse, cliquez sur **Adresse IP unique**.



- 2 Dans le champ Adresse IP, indiquez l'adresse souhaitée.
- 3 Cliquez sur **OK**.

### Pour ajouter une plage d'adresses :

- 1 Dans la zone de dialogue Nouvelle adresse, cliquez sur **Adresses IP commençant par**.



- 2 Entrez une partie suffisante de l'adresse dans le champ Adresse IP de base pour obtenir la plage d'adresses souhaitée.

A mesure que vous entrez les chiffres d'une adresse IP de base, Norton Personal Firewall détermine la fin de la plage et l'affiche dans la partie de la zone de dialogue Nouvelle adresse réservée à la plage d'adresses IP.

- 3 Cliquez sur **OK**.

## Recherche d'adresses IP

Que vous entriez une seule adresse ou une plage d'adresses, vous ne pouvez rechercher une adresse que si vous connaissez son nom d'hôte.

### Pour rechercher une adresse :

- 1 Dans la zone de dialogue Nouvelle adresse, cliquez sur **Rechercher**.
- 2 Dans la zone de dialogue Recherche d'une adresse IP, tapez le nom d'hôte.
- 3 Cliquez sur **Rechercher**.
- 4 Cliquez sur **OK** pour entrer l'adresse IP trouvée dans le champ de la zone de dialogue Nouvelle adresse.

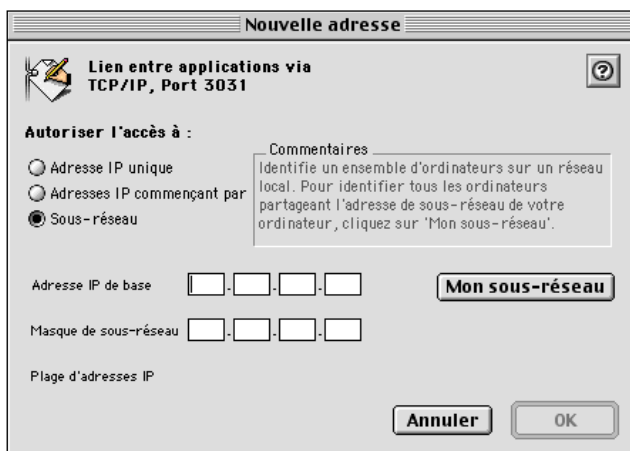
## Ajout d'adresses de sous-réseau

Vous pouvez ajouter des sous-réseaux à votre liste d'accès refusés ou autorisés. En mode basique, vous ne pouvez spécifier que votre propre sous-réseau. En mode avancé, vous pouvez spécifier votre sous-réseau ou un sous-réseau différent.

Pour obtenir des instructions sur le passage en mode avancé, reportez-vous à la section « [Pour passer en mode avancé](#) : » à la page 28

### Pour ajouter des adresses pour votre propre sous-réseau :

- 1 Dans la zone de dialogue Nouvelle adresse, cliquez sur **Sous-réseau**.



- 2 Cliquez sur **Mon sous-réseau**.

L'adresse IP de base et le *masque de sous-réseau* de votre sous-réseau s'inscrivent automatiquement. Un masque de sous-réseau définit la proportion d'une adresse IP qui identifie le sous-réseau.

- 3 Cliquez sur **OK**.

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

- 1 Dans la zone de dialogue Nouvelle adresse, cliquez sur **Sous-réseau**.
- 2 Entrez l'adresse IP de base et le masque de sous-réseau dans les champs prévus à cet effet.
- 3 Pour utiliser les valeurs définies pour votre propre sous-réseau, cliquez sur **Mon sous-réseau**.

Norton Personal Firewall renseigne automatiquement les champs appropriés.

- 4 Cliquez sur **OK**.

## Définition d'un service personnalisé à protéger

Pour configurer l'accès à un service non répertorié dans la fenêtre Configuration, vous devez définir ce service dans Norton Personal Firewall. Vous ne pouvez effectuer cette opération qu'en mode avancé.

Pour de plus amples informations sur le passage en mode avancé, reportez-vous à la section « [Pour passer en mode avancé :](#) » à la page 28

### Pour définir un nouveau service :

- 1 Dans la liste des services, cliquez sur **Nouveau**.



- 2 Spécifiez le numéro de port du service.
- 3 Tapez le nom du service.  
Si vous avez sélectionné un nom de port dans la liste, le nom du service apparaît automatiquement.  
Une icône s'affiche automatiquement pour le service.
- 4 Vous pouvez la remplacer par l'icône de votre choix, que vous copiez puis collerez sur l'icône existante dans la zone de dialogue Nouveau service.
- 5 Cliquez sur **OK**.

Le nouveau service apparaît dans la liste de la fenêtre Configuration. Vous pouvez à présent définir les réglages d'accès à ce service.

Pour de plus amples informations, reportez-vous à la section « [Protection des services Internet standard](#) » à la page 41.

## Modification ou suppression d'un service personnalisé

Vous ne pouvez pas modifier ou supprimer un service prédéfini, mais vous pouvez modifier ou supprimer les services personnalisés que vous avez ajoutés à la liste.

### Pour modifier un service personnalisé :

- 1 Dans la fenêtre Configuration, sélectionnez le service souhaité.
- 2 Cliquez sur **Modifier**.
- 3 Dans la zone de dialogue Modifier, modifiez le nom du service ou son icône (en coupant et en collant une nouvelle icône).
- 4 Pour modifier le numéro de port, supprimez le service et ajoutez-en un nouveau, avec le numéro de port souhaité.
- 5 Cliquez sur **OK**.

### Pour supprimer un service personnalisé :

- 1 Dans la fenêtre Configuration, sélectionnez le service souhaité.
- 2 Cliquez sur **Supprimer**.
- 3 Dans la zone d'avertissement qui apparaît, cliquez sur **Supprimer** pour confirmer la suppression du service.

## Modification des réglages de protection

Vous pouvez modifier les réglages de protection d'un service à deux niveaux. Vous pouvez modifier le niveau de restriction (par exemple, passer du niveau « Refuser tous les accès » au niveau « Autoriser l'accès aux adresses IP de la liste uniquement ») ou modifier la liste des adresses associées à un niveau de restriction. Vous pouvez effectuer ces modifications dans la fenêtre Configuration.

## 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 souhaité.
- 2 Cliquez sur 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.

Pour de plus amples informations sur la création d'une liste d'adresses IP, reportez-vous à la section « [Protection des services Internet standard](#) » à la page 41.
  - Si vous sélectionnez l'option Refuser tous les accès ou Autoriser tous les accès à la place d'une option comportant une liste d'adresses IP, la suppression de ces adresses n'est pas indispensable. Elles restent visibles mais sont estompées dans la fenêtre Configuration.

## Modification d'une liste d'adresses IP

Pour les options de restriction qui exigent une liste d'adresses, vous pouvez ajouter des adresses à la liste ou modifier et supprimer les adresses de la liste de la fenêtre Configuration.

Avant de modifier une liste, assurez-vous que celle-ci est bien affichée en cliquant sur le service correspondant.

### Pour ajouter des éléments à une liste :

- 1 Dans la fenêtre Configuration, cliquez sur **Nouveau**.
- 2 Ajoutez les adresses IP souhaitées.
- 3 Cliquez sur **OK**.

Pour de plus amples informations sur l'ajout d'adresses IP, reportez-vous à la section « [Ajout d'adresses IP](#) » à la page 43. Pour de plus amples informations sur l'ajout d'adresses de sous-réseau, reportez-vous à la section « [Ajout d'adresses de sous-réseau](#) » à la page 45.



**Pour modifier une adresse ou une plage d'adresses dans une liste :**

- 1 Dans la fenêtre Configuration, sélectionnez l'adresse ou la plage souhaitée.
- 2 Cliquez sur **Modifier**.
- 3 Dans la zone de dialogue Modifier l'adresse, effectuez les modifications souhaitées.
- 4 Cliquez sur **OK**.

**Pour supprimer une adresse ou une plage d'adresses :**

- 1 Dans la fenêtre Configuration, sélectionnez l'adresse ou la plage souhaitée.
- 2 Cliquez sur **Supprimer**.
- 3 Dans la zone d'avertissement qui apparaît, cliquez sur **Supprimer** pour confirmer votre requête.

## Configuration d'une protection UDP

Le protocole UDP (User Datagram Protocol) est un protocole relativement simple utilisé pour certaines opérations Internet. Par exemple, le système DNS (Domain Name System) utilise le protocole UDP pour convertir des noms d'hôtes en adresses IP.

La protection des ports UDP est généralement inutile. Toutefois, si vous devez protéger un port UDP pour une raison particulière, faites-le avec circonspection, car le refus d'accès à des services UDP peut entraîner des problèmes de connexion à Internet.

Dans la plupart des cas, il suffit de protéger les ports UDP inférieurs au numéro 1023. Ces numéros de ports UDP sont utilisés pour des services standard tels que *DHCP* (Dynamic Host Configuration Protocol, protocole qui permet d'obtenir l'adresse IP d'un ordinateur) et *NTP* (Network Time Protocol, protocole qui peut être utilisé par le tableau de bord Date et 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 donné.

**Pour activer la protection UDP :**

- 1 Cliquez deux fois sur l'icône de **Norton Personal Firewall** ou, dans le menu de la barre des réglages, cliquez sur **Ouvrir Norton Personal Firewall** pour lancer Norton Personal Firewall.
- 2 Dans le menu Edition, cliquez sur **Préférences**.
- 3 Cochez la case **Activer le contrôle renforcé des services**.
- 4 Cochez la case **Activer la protection pour UDP comme pour TCP**.
- 5 Spécifiez la plage de ports à protéger.
- 6 Cliquez sur **Enregistrer**.

## Fonctionnement de la protection UDP

Une fois activée, la protection UDP fonctionne sur le même principe que la protection TCP. Norton Personal Firewall utilise la même liste de services pour UDP et pour TCP. Un service utilise en général 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 par connexion* (l'envoi d'un message exige une connexion préalable). Avec TCP, Norton Personal Firewall peut autoriser ou refuser uniquement la tentative de connexion, 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 ou notifiées, et ne sont pas répertoriées dans la fenêtre Historique des accès.

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. Par exemple, étant donné que le système DNS utilise un port UDP, le journal contiendrait une entrée pour chaque tentative de connexion à un site Web.

Même si vous vous contentez de protéger les ports UDP dont les numéros sont les plus faibles, il est préférable de créer des entrées spécifiques pour certains services. Par exemple, si votre ordinateur utilise le protocole DHCP pour obtenir son adresse IP, vous pouvez choisir l'option Autoriser tous les accès (ou l'option Autoriser l'accès aux adresses IP de la liste, en précisant l'adresse IP du serveur DHCP) pour le service DHCP, port 68. Norton Personal Firewall crée automatiquement une entrée pour ce service lorsque vous activez la protection UDP. Pour une sécurité maximum, l'accès à ce service prend par défaut la valeur Refuser tous les accès.



# Dépannage

## Questions fréquentes

### Comment désactiver la protection anti-intrusion ?

Vous pouvez désactiver la protection à partir de la fenêtre Configuration ou du menu de la barre des réglages (si vous êtes équipé de Mac OS 8.5 ou version supérieure).

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

- 1 Cliquez deux fois sur l'icône de **Norton Personal Firewall**.
- 2 Si la fenêtre Configuration n'apparaît pas, ouvrez le menu Fenêtre et cliquez sur **Configuration**.
- 3 Cliquez sur **Désactiver la protection**.

#### **Pour désactiver la protection anti-intrusion à partir de la barre des réglages :**

- 1 Dans la barre des réglages, cliquez sur le module **Norton Personal Firewall** pour ouvrir le menu correspondant.
- 2 Cliquez sur **Désactiver la protection anti-intrusion**.

Vous pouvez également utiliser le menu de la barre des réglages pour interrompre la protection assurée par Norton Personal Firewall pendant une période donnée.

### **Pour désactiver Norton Personal Firewall pendant une période donnée :**

- 1 Dans la barre des réglages, cliquez sur le module **Norton Personal Firewall** pour ouvrir le menu correspondant.
- 2 Cliquez sur **Désactiver temporairement la protection anti-intrusion**.
- 3 Indiquez le délai (en minutes) à l'issue duquel la protection Norton Personal Firewall sera de nouveau activée.
- 4 Cliquez sur **OK**.

## **Pourquoi m'est-il impossible de télécharger des fichiers à partir d'un site Web ?**

Vous utilisez peut-être le protocole FTP pour transférer vos fichiers. Pour de nombreuses opérations du protocole FTP, le serveur FTP établit une connexion TCP avec votre ordinateur et utilise cette connexion comme port de données pour aller rechercher des données sur votre ordinateur. Le problème provient du fait que le numéro de port utilisé comme port de données est généralement sélectionné de façon aléatoire, ce qui permet difficilement de déterminer à l'avance les autorisations d'accès à accorder au serveur FTP.

### **Pour résoudre les problèmes relatifs au protocole FTP, procédez comme suit :**

- Dans le menu de la barre des réglages, cliquez sur **Désactiver temporairement la protection anti-intrusion**.  
La désactivation de Norton Personal Firewall n'est nécessaire qu'au début d'un transfert de fichiers. Si vous transférez simultanément plusieurs fichiers, veillez à ce que Norton Personal Firewall reste désactivé jusqu'au début du téléchargement du dernier fichier. Si votre ordinateur est doté du système d'exploitation Mac OS 8.1, désactivez puis réactivez Norton Personal Firewall dans la fenêtre Configuration.
- Sélectionnez l'entrée Autres dans la liste des services, puis autorisez les accès en provenance du serveur FTP (utilisez l'adresse IP indiquée dans la fenêtre Historique des accès).
- Si votre application cliente FTP vous permet de spécifier un port de données, créez une entrée de service pour le port que vous souhaitez utiliser et autorisez les accès pour le serveur FTP.

- Si votre application cliente FTP autorise les transferts FTP en mode passif (le port de données est dans ce cas inutile), sélectionnez cette option. Assurez-vous que le mode passif est activé dans l'onglet Avancé du tableau de bord Internet (sur les systèmes Mac OS 8.5 et versions supérieures).

## 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 pour l'exécution d'activités Internet quotidiennes. Dans ce cas, procédez comme suit :

- DHCP : Dans le tableau de bord TCP/IP, vérifiez si votre ordinateur est configuré pour obtenir son adresse IP au moyen du protocole 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 la fenêtre Historique des accès.
- DNS : La plupart des opérations Internet sortantes utilisent le système DNS, qui convertit les noms d'hôte en adresses IP. Assurez-vous de ne pas bloquer les ports dynamiques utilisés par DNS (il s'agit en général des ports dont le numéro est supérieur ou égal à 32768).

Pour de plus amples informations sur l'identification des numéros de port bloqués, reportez-vous à la section « [Consultation de l'historique des accès](#) » à la page 33. Pour de plus amples informations sur la modification d'une entrée de la liste des services pour attribuer une autorisation d'accès, reportez-vous à la section « [Ajout d'adresses IP](#) » à la page 43.

## Pourquoi mon serveur FTP ne fonctionne-t-il pas ?

Si vous exécutez un serveur FTP sur votre ordinateur, il se peut que certains clients rencontrent des difficultés de connexion au serveur, même si vous avez autorisé les accès au port 21. Si un client utilise le protocole FTP en mode passif, il peut ouvrir dynamiquement une deuxième connexion au serveur pour un port de données. Faites en sorte que le client n'utilise pas le mode passif, ou donnez-lui accès au nouveau port ouvert par le serveur.

Pour de plus amples informations sur l'octroi d'autorisations d'accès à un port, reportez-vous à la section « [Définition d'un service personnalisé à protéger](#) » à la page 46.

## Pourquoi mon imprimante ne fonctionne-t-elle pas ?

Vous avez peut-être désactivé AppleTalk en réponse à l'avertissement qui vous signalait qu'AppleTalk utilisait le même port que votre connexion Internet. Réactivez AppleTalk pour effectuer vos impressions.

## A quel service correspond ce numéro de port ?

Voici les numéros de port TCP et UDP généralement utilisés par les services Macintosh.

### Numéros de port TCP

Port	Utilisation	Commentaires
20	Données FTP	Utilisé uniquement 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 UDP et non TCP
70	Gopher	
79	Finger	
80	HTTP (Web)	
88	Kerberos	
105	PH (répertoire)	
106	Poppass (modification de mot de passe)	
110	POP3 (courrier électronique)	
111	RPC (Appel de procédure à distance)	Utilisé pour les programmes Java
113	AUTH	
119	NNTP (informations)	



Port	Utilisation	Commentaires
139	Session NETBIOS	Accès Windows (ASIP 6)
143	IMAP (nouveau système de courrier électronique)	
311	AppleShare Web Admin	ASIP versions 6.1 et supérieures
384	ARNS (tunnellisation)	
387	AURP (tunnellisation)	
389	LDAP (répertoire)	
407	Timbuktu version 5.2 ou supérieures	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 également les ports UDP 6970+
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 supérieures
666	Désormais serveur de contact	Viola l'affectation de port existante
687	Port U&G partagé ASIP	ASIP versions 6.2 et supérieures
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

<b>Port</b>	<b>Utilisation</b>	<b>Commentaires</b>
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)	Macintosh OS 9 et versions supérieures
4000	Désormais serveur d'événements public	
4199	EIMS Admin	
4347	Répondeurs LANsurveyor	Utilise également les ports UDP
5003	FileMaker Pro	Accès direct et non via le 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	
5501	Serveur Hotline	
6699	Client Napster/Macster	Utilisé lorsque le serveur est en mode pare-feu
7070	Real Player	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
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	Protocole de transfert uniquement, antérieur à la version 5.2
458	QuickTime TV	
497	Retrospect	Recherche de clients sur le réseau
514	Syslog	
554	Protocole de diffusion multimédia (QuickTime)	
2049	Système de gestion de fichiers en réseau (NFS, Network File System)	
3283	Assistant réseau Apple	
5003	FileMaker Pro	Pour obtenir 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 nécessaire ; 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. Le nouveau fichier est ensuite créé.

### Pour créer un nouveau fichier journal :

- 1 Cliquez deux fois sur l'icône de **Norton Personal Firewall** ou, dans le menu de la barre des réglages, cliquez sur **Ouvrir Norton Personal Firewall** pour lancer Norton Personal Firewall.
  - 2 Dans le menu Edition, cliquez sur **Préférences**.
  - 3 Désactivez la consignation.
  - 4 Renommez le fichier journal (nommé Journal Norton Personal Firewall) ou retirez-le du dossier Préférences.
  - 5 Activez la consignation.
- Norton Personal Firewall crée un nouveau fichier journal dans le dossier Préférences.

## Pourquoi Norton Personal Firewall ne se charge-t-il pas ?

Il y a peut-être un conflit d'extensions si vous possédez un grand nombre d'extensions et que la mémoire virtuelle est désactivée. Essayez d'activer la mémoire virtuelle ou de supprimer les extensions inutiles.

## Pourquoi le partage de fichiers ne fonctionne-t-il pas ?

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 accéder.

## Questions relatives aux réseaux locaux domestiques

### 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. Vous n'avez pas besoin d'installer Norton Personal Firewall sur les autres ordinateurs du réseau.

Toutefois, vous devez installer une copie de Norton Personal Firewall sur tous les ordinateurs connectés à un module Airport.

### Comment spécifier l'accès à un ordinateur dont l'adresse IP est dynamiquement générée ?

Les ordinateurs qui obtiennent leur adresse IP par le biais du protocole DHCP (Dynamic Host Configuration Protocol) ont en général une adresse IP différente chaque fois qu'ils se connectent à un réseau. Toutefois, ces adresses IP se situent dans une plage précise. Vous pouvez déterminer cette plage à partir de la fenêtre Historique des accès en recherchant les accès refusés à cet ordinateur et en notant les adresses IP utilisées. Vous pouvez ensuite spécifier cette plage dans la liste d'adresses IP du service pour lequel vous devez définir des accès.

Pour de plus amples informations sur la consultation de la fenêtre Historique des accès, reportez-vous à la section « [Pour afficher la fenêtre Historique des accès :](#) » à la page 34. Pour de plus amples informations sur la spécification d'une plage d'adresses IP pour la configuration des accès, reportez-vous à la section « [Pour ajouter une plage d'adresses :](#) » à la page 44.

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

Norton Personal Firewall assure la sécurité des connexions TCP/IP. Cette protection n'a aucune incidence sur les connexions AppleTalk. 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.

Pour de plus amples informations sur l'octroi d'autorisations d'accès à un service, reportez-vous à la section « [Ajout d'adresses IP](#) » à la page 43.





## Mise à jour avec LiveUpdate

LiveUpdate vous permet de mettre à jour vos fichiers de programme. Si vous disposez d'une connexion Internet, LiveUpdate est la méthode la plus efficace pour la mise à jour de vos fichiers.

Si votre fournisseur d'accès à Internet est America Online (AOL), vous devez vous connecter sur AOL avant d'utiliser LiveUpdate. Pour de plus amples informations, reportez-vous à la section « [Utilisation de LiveUpdate avec America Online](#) » à la page 70.

### A propos de LiveUpdate



Symantec fournit un accès en ligne aux mises à jour des fichiers de programme dans le cadre de votre abonnement.

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

## Mise à jour des fichiers de programme

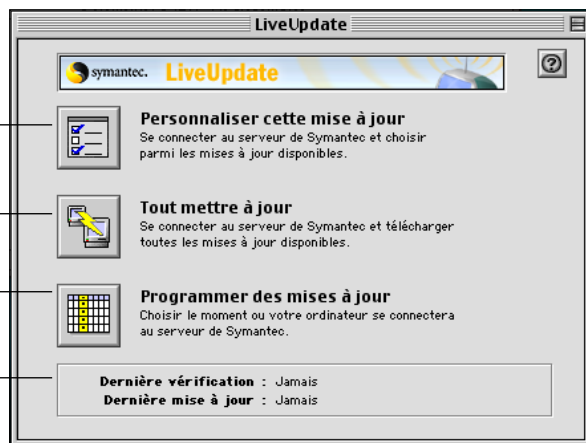
Vous pouvez laisser LiveUpdate rechercher simultanément les mises à jour de tous les fichiers, choisir vous-même les mises à jour qui vous intéressent ou programmer une future session LiveUpdate.

Permet de sélectionner les éléments à mettre à jour lors de cette session

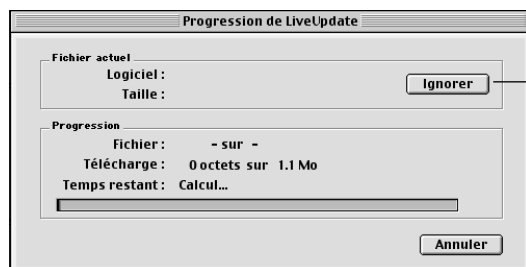
Met à jour tous les composants installés

Permet de programmer des mises à jour spécifiques

Indique la dernière activité de mise à jour



LiveUpdate télécharge et installe les mises à jour disponibles. Une zone de dialogue vous informe du déroulement du transfert de fichiers.

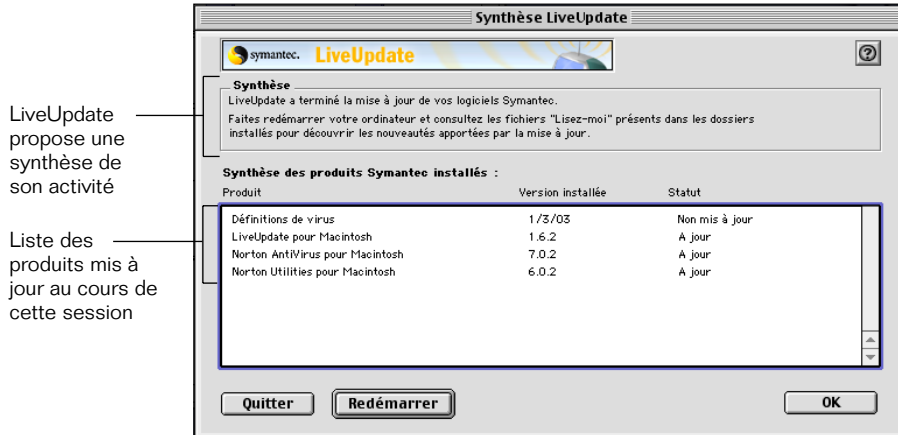


Cliquez pour ignorer l'élément en cours de téléchargement



Le transfert des fichiers s'effectue en quelques minutes. LiveUpdate vous informe de la fin du transfert des fichiers.

Si vos fichiers sont déjà à jour, LiveUpdate vous en informe.



### Pour mettre à jour les fichiers de programme avec LiveUpdate :

- 1 Dans le dossier Norton Personal Firewall, cliquez sur LiveUpdate.
- 2 Procédez comme suit :
  - Pour mettre tous les fichiers à jour, cliquez sur Tout mettre à jour.
  - Pour spécifier les éléments à mettre à jour dans la session en cours, cliquez sur Personnaliser cette mise à jour.

Pour de plus amples informations, reportez-vous à la section « [Pour personnaliser une session LiveUpdate](#) : » à la page 67.

- Pour ouvrir la fenêtre de programmation de LiveUpdate et programmer des événements LiveUpdate, cliquez sur Programmer des mises à jour.

Pour de plus amples informations, reportez-vous à la section « [Pour programmer un événement LiveUpdate](#) : » à la page 68.
- 3 Cliquez sur Fermer.
- 4 Si LiveUpdate vous recommande de redémarrer l'ordinateur, cliquez sur Redémarrer.
- 5 Dans le menu Fichier, cliquez sur Quitter.

## Vider la Corbeille à la fin d'une session LiveUpdate

Après une mise à jour des fichiers de programme avec LiveUpdate, la Corbeille contient des éléments. LiveUpdate y place en effet les fichiers périmés. Videz la Corbeille. Si vous n'avez pas encore redémarré votre ordinateur après l'installation de l'application, vous recevrez peut-être un message indiquant que ces fichiers sont en cours d'utilisation. Vous pourrez vider la Corbeille après avoir redémarré votre ordinateur.

## Consultation du fichier What's New de LiveUpdate

LiveUpdate place un fichier intitulé What's New sur le bureau. Celui-ci comprend le détail des fichiers qui ont été mis à jour par LiveUpdate.

### Pour consulter le fichier What's New :

- Cliquez deux fois sur le fichier pour connaître le contenu des fichiers mis à jour.  
Le fichier s'ouvre dans SimpleText.

### Pour fermer le fichier What's New :

- Appuyez sur Commande-Q pour quitter SimpleText.

### Pour supprimer le fichier What's New :

- Faites-le glisser vers la Corbeille.

## Vérification des numéros de version et des dates

LiveUpdate vous permet de savoir si vos fichiers de programme sont à jour en affichant les numéros de version et l'état. Vous pouvez également vérifier le fichier de programme et les définitions de virus dans la fenêtre A propos de l'application, accessible à partir du menu Pomme.

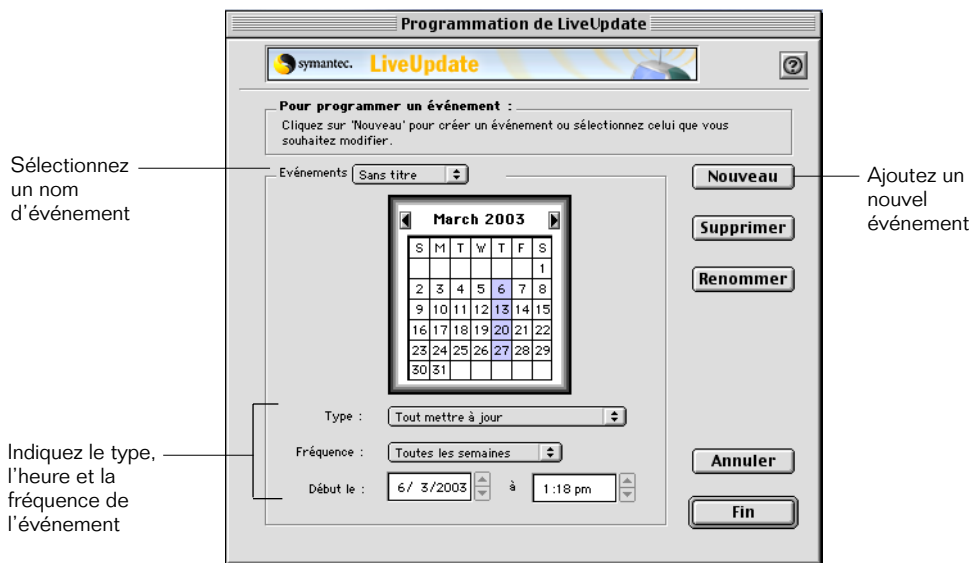
### Pour afficher la fenêtre A propos de application :

- 1 Lancez Norton Personal Firewall.
- 2 Dans le menu Pomme, cliquez sur A propos de Norton Personal Firewall.  
La fenêtre A propos indique le numéro de version et les dates de copyright.
- 3 Lorsque vous avez fini de consulter la fenêtre A propos de, cliquez sur OK.

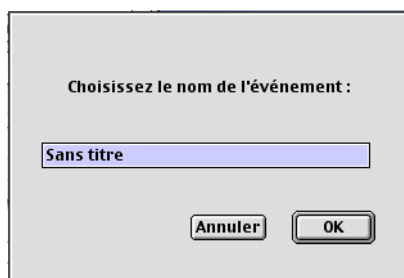


### Pour programmer un événement LiveUpdate :

- 1 Dans la fenêtre principale de LiveUpdate, cliquez sur Programmer des mises à jour.



- 2 Dans la zone de dialogue Programmation de LiveUpdate, cliquez sur Nouveau.



- 3 Saisissez le nom de l'événement.
- 4 Cliquez sur OK.
- 5 Indiquez le type d'événement, sa fréquence et l'heure du lancement des mises à jour.

Les jours auxquels les mises à jour doivent être exécutées apparaissent en surbrillance dans le calendrier. Les dates soulignées correspondent aux autres événements programmés.

- 6 Pour terminer la programmation des mises à jour, entrez la date et l'heure de déclenchement.
  - Cliquez sur la zone de saisie Heure et utilisez les touches fléchées de votre clavier pour définir l'heure de lancement des mises à jour.
  - Cliquez sur la zone de saisie Minute pour définir l'heure de lancement à la minute près.

Votre ordinateur doit être allumé pour que LiveUpdate puisse s'exécuter à l'heure prévue. Si ce n'est pas le cas, LiveUpdate s'exécute dès que vous redémarrez votre ordinateur.

- 7 Cliquez sur Fin.

## Si vous ne pouvez pas utiliser LiveUpdate

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

### **Pour télécharger des mises à jour de produits à partir du site Web de Symantec :**

- 1 Ouvrez votre navigateur Internet et rendez-vous sur le site suivant : <http://securityresponse.symantec.com/downloads/>  
Si vous ne parvenez pas à charger cette page, rendez-vous sur le site <http://securityresponse.symantec.com> et cliquez sur téléchargements.
- 2 Sur la page des téléchargements, sélectionnez, dans la liste des mises à jour, le produit que vous souhaitez mettre à jour.
- 3 Cliquez sur Browse.
- 4 Sur la page du produit, sélectionnez la version de votre produit.
- 5 Cliquez sur Continue.
- 6 Sur la page des mises à jour, sélectionnez le fichier que vous souhaitez télécharger.  
Les fichiers téléchargeables sont accompagnés d'informations relatives à la mise à jour.

## Utilisation de LiveUpdate avec America Online

Si votre fournisseur d'accès Internet est America Online (AOL), vous devrez peut-être vous connecter à 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 Lancez LiveUpdate.
- 4 Observez la procédure décrite dans la section « [Pour mettre à jour les fichiers de programme avec LiveUpdate :](#) » à la page 65.
- 5 Lorsque la session LiveUpdate est terminée, quittez AOL.

Si la session LiveUpdate vous demande de redémarrer votre ordinateur, déconnectez-vous tout d'abord d'AOL.

# G L O S S A I R E

Lorsqu'ils sont mentionnés pour la première fois dans le texte, les termes suivants apparaissent en *italique*.

<b>Adresse IP (Internet protocol)</b>	Numéro identifiant votre ordinateur de façon unique sur Internet.
<b>AppleTalk</b>	Protocole utilisé par certains périphériques réseau, tels que les imprimantes et les serveurs, pour communiquer.
<b>Cheval de Troie</b>	Programme présenté sous une forme attrayante (une application connue, par exemple) et qui effectue des opérations inattendues en réaction à un événement déclencheur.
<b>DHCP</b>	Dynamic Host Configuration Protocol. Le protocole DHCP attribue dynamiquement des adresses IP aux périphériques d'un réseau.
<b>FTP</b>	File Transfer Protocol. Protocole d'application utilisé pour le transfert de fichiers entre ordinateurs.
<b>Internet</b>	Réseau mondial décentralisé qui connecte des millions d'ordinateurs.
<b>Masque de sous-réseau</b>	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.
<b>Nom d'hôte</b>	Nom identifiant un ordinateur sur un réseau. Par exemple, <a href="http://www.symantec.com">www.symantec.com</a> est le nom d'hôte du site Web de Symantec. Les noms d'hôte sont convertis en adresses IP par le service DNS.
<b>Pare-feu</b>	Filtre qui bloque ou autorise les connexions et la transmission de données sur Internet.
<b>Pirate</b>	Personne qui tente d'accéder frauduleusement aux ordinateurs d'autres utilisateurs dans le but de détourner des informations ou de détériorer des données.

---

<b>PPP</b>	Point-to-Point Protocol. Méthode de connexion à Internet qui offre des fonctions de contrôle des erreurs.
<b>Protocole</b>	Ensemble de règles régissant les communications et le transfert de données entre ordinateurs. HTTP et FTP sont deux exemples de protocoles.
<b>Protocole par connexion</b>	Protocole exigeant une connexion pour la transmission de paquets d'informations.
<b>Protocole sans connexion</b>	Protocole capable de transmettre des informations jusqu'à une adresse de destination sans établir de connexion.
<b>Serveur proxy</b>	Serveur qui tente de répondre aux requêtes qu'un client a adressées à un autre serveur. S'il n'y parvient pas, il transmet la requête au serveur destinataire. Les serveurs proxy permettent d'accélérer les accès au Web et de filtrer les requêtes.
<b>Serveur Web</b>	Ordinateur équipé d'un logiciel serveur chargé d'envoyer les pages Web requises à votre navigateur.
<b>Sous-réseau</b>	Réseau local qui fait partie d'un intranet de plus grande taille ou d'Internet.
<b>Système de noms de domaine (DNS, Domain Name System)</b>	Service convertissant les noms d'hôte en adresses IP.
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol. Protocoles développés par le Département de la Défense américain pour prendre en charge la construction des réseaux internationaux. Le protocole TCP est utilisé pour le contrôle et la correction des erreurs de transmission tandis que le protocole IP est utilisé pour la transmission des données.
<b>UDP</b>	User Datagram Protocol. Protocole simple utilisé pour l'échange d'informations sans accusé de réception ni garantie de livraison.
<b>Virus</b>	Petit programme conçu pour se reproduire et se propager, généralement à l'insu de l'utilisateur.



# I N D E X

## A

### accès

- autorisation et refus 10
- détermination avec
  - Norton Personal Firewall 11
- réponse aux tentatives 31, 33
- restriction 42
- restriction pour les sous-réseaux 45
- suivi des tentatives, avec
  - Norton Personal Firewall 23
- surveillance 29
- types 35

### activation de la protection

- Norton Personal Firewall 25

### adresse IP

- adresse par défaut pour l'autotest 31
- recherche avec Norton Personal Firewall 22
- restriction d'accès 42

### adresses de noms de domaine 22

### adresses IP 22

- modification de la liste 48
- restriction ou autorisation d'accès 43

### affichage, dernière mise à jour de programme 66

### alertes dans Norton Personal Firewall 33

### America Online

- connexion au site Web de Symantec 19
- enregistrement de
  - Norton Personal Firewall 19
- utilisation de LiveUpdate 70

### AppleTalk

- et Norton Personal Firewall 24
- et TCP/IP, problèmes de sécurité 24

### application

- enregistrement 17
- enregistrement avec America Online 19

### autotest

- exécution en mode avancé 32
- exécution en mode basique 31
- mode basique et mode avancé 31
- protection anti-intrusion 31

## B

### Barre des réglages

- pour désactiver Norton Personal Firewall 26

### Barre des réglages, pour désactiver Norton Personal Firewall 26

## C

### CD

- contenu 14
- guide de l'utilisateur au format PDF 16

### chevaux de Troie 9, 21

### configuration de LiveUpdate 67

### configuration du système, dans le fichier

- Lisez-moi 14

### connexion réseau PPP 31

### connexions

- blocage avec Norton Personal Firewall 10
- TCP/IP 21
- UDP 21

### consignation, préférences dans

- Norton Personal Firewall 38

### Crackers et pirates, définition 12

## D

### dépannage, dans Norton Personal Firewall 53

### désactivation de la protection Norton Personal Firewall 25

### DNS 22

## E

### enregistrement de votre produit 17

### exécution de l'autotest en mode avancé 32

## F

### fenêtre Configuration, dans

- Norton Personal Firewall 42

### fichier Lisez-moi 14, 16

### fichiers de programme, mise à jour 63-65

---

## H

- Historique des accès
  - consultation dans Norton Personal Firewall 33
- exportation des données 36
- fenêtre 11, 33
- journal 3

## I

- installation
  - Norton Personal Firewall 14
  - options 15
- Installation personnalisée 15
- Installation standard 15
- Internet
  - adresses IP 22
  - configuration de la protection 42
  - connexions, blocage avec Norton Personal Firewall 10
  - détection des intrusions 11
  - noms d'hôte 22
  - noms de domaine 22
  - pare-feu 9
  - protection à l'aide de numéros de port 23
  - protection contre les intrusions 9, 21
  - types de tentatives d'accès 35
  - utilisation pour enregistrer des produits Symantec 17
- introduction à Norton Personal Firewall 9
- intrusions
  - protection 9, 21
  - réponse aux tentatives 29

## L

- liens Internet, nouvelles de dernière minute 18
- LiveUpdate
  - configuration 67
  - fichier What's New 66
  - personnalisation d'une session 67
  - programmation des mises à jour 67-69
  - utilisation avec America Online 70

## M

- mise à jour des fichiers de programme 63-65
- Mise à jour des fichiers de programme avec LiveUpdate 65
- mode avancé, autotest de Norton Personal Firewall 31
- mode basique, autotest de Norton Personal Firewall 31

## N

- noms d'hôte, Internet 22
- noms de domaine, Internet 22
- Norton Personal Firewall 26, 47
  - activation et désactivation de la protection 25
  - activation ou désactivation de la notification 30
  - autotest 30
  - autotest en mode avancé 32
  - autotest en mode basique 31
  - consultation de l'historique des accès 33
  - dépannage 53
  - détermination des accès 11
  - éléments protégés 9, 21
  - et AppleTalk 24
  - fenêtre Configuration 42
  - installation 14
  - introduction 9
  - lancement à partir de la barre des réglages 27
  - messages d'alerte 33
  - modalités d'utilisation 3
  - mode basique et mode avancé 42
  - page Web de détails sur les accès 37
  - paramètres par défaut 11
  - personnalisation 41
  - personnalisation de la protection 46
  - préférences de consignment 38
  - recherche d'adresses IP 22
  - réponses aux accès 33
  - services personnalisés 47
  - structure du journal 39
  - sui des tentatives d'accès 23
  - surveillance de l'activité 29
  - types d'accès 35

---

notification, tentatives d'accès 30  
nouvelles de dernière minute 18  
numéros de port, protection 23

## O

obtention d'informations, affichage des tentatives d'accès 37  
ordinateurs  
    adresses IP 22  
    noms d'hôte 22  
    protection contre les intrusions 9, 21

## P

page Web de détails sur les accès 37  
paramètres  
    dans Norton Personal Firewall 11  
    notification d'accès 30  
pare-feu  
    à propos de 9  
    activation et désactivation de la protection 25  
    avantages 11  
    dépannage 53  
    modalités d'utilisation 3  
    personnalisation 41  
    surveillance de l'activité 29, 31  
personnalisation  
    Norton Personal Firewall 41  
    services 47  
pirate  
    attaques 9, 21  
    et cracker, définition 12  
préférences  
    consignation, dans Norton Personal Firewall 38  
    notification d'accès 30  
programmation, mises à jour de programmes 67-69  
protection  
    à l'aide de numéros de ports 23  
    assurée par Norton Personal Firewall 21  
    avec Norton Personal Firewall 9  
protocoles réseau Macintosh 24

## Q

Questions fréquentes 53

## R

redémarrage, après installation 15  
réponse aux tentatives d'accès 29  
restriction des accès aux adresses IP 43

## S

services personnalisés  
    définition 46  
    modification ou suppression 47  
site Web de Symantec 19  
    connexion via America Online 19  
    enregistrement 17  
    nouvelles de dernière minute 18  
sous-réseaux 22  
    restriction d'accès 45  
structure du journal, Norton Personal Firewall 39

## T

tableau de bord du partage de fichiers 24  
tableau de bord Utilisateurs multiples 24  
tableaux de bord, partage de fichiers 24  
TCP/IP  
    connexions 21  
    et AppleTalk, problèmes de sécurité 24  
test de Norton Personal Firewall 30

## U

UDP  
    activation de la protection 50  
    connexions 21  
    protection des adresses 23

## V

versions, vérification avec LiveUpdate 66  
virus 9, 21

