Guide de l'utilisateur Norton™ Smartphone Security

for Windows Mobile®

symantec™

Norton™ Smartphone Security pour Windows Mobile®

Mention juridique

Symantec, le logo Symantec, LiveUpdate, Symantec AntiVirus, Symantec Client Firewall, Symantec SMS AntiSpam et Norton Smartphone Security sont des marques commerciales ou déposées de Symantec Corporation ou ses sociétés affiliées aux Etats-Unis et dans d'autres pays. Les autres noms peuvent être des marques de leurs détenteurs respectifs.

Windows, Windows Mobile et Windows Vista sont des marques déposées de Microsoft Corporation.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.fr.

Solutions de service et de support

Symantec se consacre à fournir un excellent service dans le monde entier. Notre objectif est de vous apporter une assistance professionnelle pour utiliser nos logiciels et nos services, où que vous vous trouviez.

Les solutions de support technique et de service clientèle varient selon les pays.

Si vous avez des questions sur les services décrits ci-dessous, consultez la section « Informations de service et de support dans le monde ».

Enregistrement et licences

Si vous déployez un produit qui nécessite un enregistrement et/ou une clé de licence, le système le plus rapide et le plus simple consiste à accéder à notre site de licence et d'enregistrement (en anglais) à l'adresse www.symantec.com/certificate.

Si vous avez acheté un abonnement de support, vous êtes habilité à bénéficier d'un support technique par téléphone et sur Internet. Lorsque vous contactez les services de support pour la première fois, vous devez disposer du numéro de votre certificat de licence ou de l'identification de contact fournie lors de l'enregistrement, pour permettre la vérification de vos droits au support. Si vous n'avez pas acheté d'abonnement de support, contactez votre revendeur ou le service clientèle de Symantec pour savoir comment obtenir un support technique auprès de Symantec.

Mises à jour de la sécurité

Pour obtenir les informations les plus récentes sur les virus et les menaces de sécurité, visitez le site de Symantec Security Response (anciennement SARC - Centre de Recherche AntiVirus de Symantec), à l'adresse

http://www.symantec.fr/region/fr/avcenter/index.html.

Ce site contient des informations exhaustives sur la sécurité et les virus, ainsi que les dernières définitions de virus. Vous pouvez également télécharger les définitions de virus en utilisant la fonction LiveUpdate de votre produit.

Renouvellement d'abonnement aux définitions de virus

Votre achat d'un service de support avec un produit vous permet de télécharger gratuitement des définitions de virus pendant la durée de l'abonnement. Si votre abonnement au support a expiré, contactez votre revendeur ou le Service clientèle de Symantec pour savoir comment le renouveler.

Sites Web Symantec :

Page d'accueil Symantec (par langue) :

- Allemand :
  http://www.symantec.de
- Anglais :
  http://www.symantec.com
- Espagnol :
  http://www.symantec.com/region/es
- Français :
  http://www.symantec.fr
- Italien :
  http://www.symantec.it
- Néerlandais :
  http:// www.symantec.nl
- Portugais :
  http://www.symantec.com/br

Symantec Security Response:

- http://www.symantec.fr/region/fr/avcenter/index.html

Page de service et assistance Symantec :

- http://www.symantec.com/region/fr/techsupp/enterprise/index.html

Bulletin d'informations spécifique produit :

- Etats-Unis, Asie-Pacifique :
  http://www.symantec.com/techsupp/bulletin/index.html
- Europe, Moyen-Orient, Afrique/Anglais :
  http://www.symantec.com/region/reg_eu/techsupp/bulletin/index.html
- Allemand :
  http://www.symantec.com/region/de/techsupp/bulletin/index.html
- Français :
  http://www.symantec.com/region/fr/techsupp/bulletin/index.html
- Italien :
  http://www.symantec.com/region/it/techsupp/bulletin/index.html
- Amérique latine/Anglais :
  http://www.symantec.com/techsupp/bulletin/index.html

Support technique

Au sein de Symantec Security Response, l'équipe de support technique internationale gère les centres d'assistance dans le monde entier. Son objectif premier est de répondre aux questions spécifiques sur les fonctionnalités/fonctions, l'installation et la configuration des produits Symantec ainsi que sur le contenu de la Base de connaissances accessible via le Web. Symantec Security Response est en collaboration étroite avec les autres départements de Symantec pour répondre rapidement à vos questions. Nous travaillons par exemple avec notre service d'ingénierie produit et nos centres de recherche en sécurité pour fournir des services d'alertes et des mises à jour des définitions de virus, face aux attaques virales et aux alertes de sécurité. Caractéristiques de nos offres :

- Une panoplie d'options de support vous permet de choisir le service approprié quel que soit le type d'entreprise.
- Le support Web et téléphonique fournit des réponses rapides et des informations de dernière minute.
- Les mises à jour des produits fournissent une protection de mise à niveau automatique.
- Les mises à jour de contenu des définitions de virus et les signatures de sécurité assurent la meilleure protection.
- Le support mondial des experts Symantec Security Response est disponible 24h/24, 7j/7 dans le monde entier et dans différentes langues.
- Les fonctionnalités avancées telles que le Service d'alertes Symantec (Symantec Alerting Service) et le Responsable de compte technique (Technical Account Manager) offrent un support d'intervention et de sécurité proactive.

Rendez-vous sur notre site Web pour obtenir les dernières informations sur les programmes de support.

Coordonnées du support

Les clients disposant d'un contrat de support peuvent contacter l'équipe de support technique par téléphone, sur le site Web suivant ou sur les sites régionaux de Service et Support internationaux.

http://www.symantec.com/region/fr/techsupp/enterprise/index.html

Lorsque vous contactez le support, vérifiez que vous disposez des informations suivantes :

- Version du produit
- Informations sur le matériel

- Mémoire disponible, espace disque et informations sur la carte d'interface réseau
- Système d'exploitation
- Niveau de version et correctif
- Topologie du réseau
- Informations sur le routeur, la passerelle et l'adresse IP
- Description du problème
- Messages d'erreur/fichiers journaux
- Intervention effectuée avant de contacter Symantec
- Modifications récentes de la configuration du logiciel ou du réseau

Service clientèle

Le Centre de service clientèle de Symantec peut vous seconder pour vos questions non techniques :

- Informations générales sur les produits (caractéristiques, langues disponibles, adresse des distributeurs, etc)
- Dépannage de base, par exemple vérification de la version du produit
- Dernières informations sur les mises à jour produit
- Comment mettre votre produit à jour/à niveau
- Comment enregistrer votre produit et/ou votre licence
- Informations sur les programmes de licences de Symantec
- Informations sur les contrats de mise à niveau et de maintenance
- Remplacement des CD et des manuels
- Mise à jour des données d’enregistrement produit en cas de changement de nom ou d'adresse
- Conseil sur les options de support technique de Symantec

Des informations détaillées sur le Service clientèle sont disponibles sur le site Web de l’assistance Symantec. Vous pouvez également contacter le Centre de service clientèle par téléphone. Pour des informations sur les numéros de support clientèle et les sites Web, consultez la section « Informations de service et de contact en bref ».

Service et support internationaux

Europe, Moyen-Orient, Afrique et Amérique latine

Sites Web de service et assistance Symantec

- Allemand :
  www.symantec.de/desupport/
- Anglais :
  www.symantec.com/eusupport/
- Espagnol :
  www.symantec.com/region/mx/techsupp/
- Français :
  www.symantec.fr/frsupport
- Italien :
  www.symantec.it/itsupport/
- Néerlandais :
  www.symantec.nl/nlsupport/
- Portugais :
  www.symantec.com/region/br/techsupp/
- FTP Symantec : ftp.symantec.com (téléchargement des notes techniques et des derniers correctifs)

Visitez le site Service et assistance de Symantec pour trouver des informations techniques et non techniques sur votre produit.

Symantec Security Response :

- http://securityresponse.symantec.com

Bulletin d'informations spécifique produit :

- Anglais :
  http://www.symantec.com/techsupp/bulletin/index.html
- Europe, Moyen-Orient, Afrique/Anglais :
  http://www.symantec.com/region/reg_eu/techsupp/bulletin/index.html
- Allemand :
  http://www.symantec.com/region/de/techsupp/bulletin/index.html
- Français :
  http://www.symantec.com/region/fr/techsupp/bulletin/index.html
- Italien :
  http://www.symantec.com/region/it/techsupp/bulletin/index.html

- Amérique latine/Anglais :
  http://www.symantec.com/techsupp/bulletin/index.html

Service Clientèle de Symantec

Fournit des informations non techniques et des conseils par téléphone dans les langues suivantes : anglais, allemand, français et italien.

- Autriche :
  + (43) 1 50 137 5030
- Belgique :
  + (32) 2 2750173
- Danemark :
  + (45) 35 44 57 04
- Espagnol :
  + (34) 91 7456467
- Finlande :
  + (358) 9 22 906003
- France :
  + (33) 1 70 20 00 00
- Allemagne :
  + (49) 69 6641 0315
- Irlande :
  + (353) 1 811 8093
- Italie :
  + (39) 02 48270040
- Luxembourg :
  + (352) 29 84 79 50 30
- Pays-Bas :
  + (31) 20 5040698
- Norvège :
  + (47) 23 05 33 05
- Afrique du Sud :
  + (27) 11 797 6639
- Suède :
  + (46) 8 579 29007
- Suisse :
  + (41) 2 23110001

- Royaume Uni :
  + (44) 20 7744 0367
- Autres pays :
  + (353) 1 811 8093 (service en anglais uniquement)

Service Clientèle Symantec – Adresse postale

- Symantec Ltd
  Customer Service Centre
  Europe, Middle East and Africa (EMEA)
  PO Box 5689
  Dublin 15
  Irlande

En Amérique latine

Symantec dispose d'un support technique et d'un service clientèle internationaux. Les services varient selon les pays et incluent des partenaires internationaux qui représentent Symantec dans les régions où il n'y a pas de bureau Symantec. Pour des informations générales, contactez le service de support de Symantec pour votre région.

ARGENTINE

- Pte. Roque Saenz Peña 832 - Piso 6
  C1035AAQ,
  Ciudad de Buenos Aires
  Argentine
  Numéro principal: +54 (11) 5811-3225
  Site Web: http://www.service.symantec.com/mx
  Gold Support: 0800-333-0306

VENEZUELA

- Avenida Francisco de Miranda. Centro Lido
  Torre D. Piso 4, Oficina 40
  Urbanización el Rosal
  1050, Caracas D.F.
  Dong Cheng District
  Venezuela
  Numéro principal: +58 (212) 905-6327
  Site Web: http://www.service.symantec.com/mx
  Gold Support: 0800-1-00-2543

COLOMBIA

- Carrera 18# 86A-14
  Oficina 407,
  Bogota D.C.
  Colombia
  Numéro principal: +57 (1) 638-6192
  Site Web: http://www.service.symantec.com/mx
  Gold Support: 980-915-5241

BRÉSIL

- Symantec Brasil
  Market Place Tower
  Av. Dr. Chucri Zaidan, 920
  12° andar
  São Paulo - SP
  CEP: 04583-904
  Brésil, SA
  Numéro principal: +55 (11) 5189-6300
  Télécopie: +55 (11) 5189-6210
  Site Web: http://www.service.symantec.com/br
  Gold Support: 000814-550-4172

CHILE

- Alfredo Barros Errazuriz 1954
  Oficina 1403
  Providencia,
  Santiago de Chile
  Chile
  Numéro principal: +56 (2) 378-7480
  Site Web: http://www.service.symantec.com/mx
  Gold Support: 0800-333-0306

MEXIQUE

- Boulevard Adolfo Ruiz Cortines 3642 Piso 8,
  Colonia Jardines del Pedregal,
  01900, Mexico D.F.
  Mexico
  Numéro principal: +52 (55) 5481-2600
  Site Web: http://www.service.symantec.com/mx
  Gold Support: 001880-232-4615

RESTE DE L'AMÉRIQUE LATINE

- 9155 South Dadeland Blvd.
  Suite 1100,
  Miami, FL 33156
  U.S.A
  Site Web: http://www.service.symantec.com/mx
  Gold Support:
  Costa Rica: 800-242-9445
  Panama: 800-234-4856
  Puerto Rico: 800-232-4615

Asie-Pacifique

Symantec dispose d'un support technique et d'un service clientèle internationaux. Les services varient selon les pays et incluent des partenaires internationaux qui représentent Symantec dans les régions où il n'y a pas de bureau Symantec. Pour des informations générales, contactez le service de support de Symantec pour votre région.

Service et support

AUSTRALIE

- Symantec Australia
  Level 2, 1 Julius Avenue
  North Ryde, NSW 2113
  Australie
  Numéro principal: +61 2 8879 1000
  Télécopie: +61 2 8879 1001
  Site Web: http://service.symantec.com
  Gold Support: 1800 805 834 gold.au@symantec.com
  Admin. contrats de support: 1800 808 089 contractsadmin@symantec.com

CHINE

- Symantec China
  Unit 1-4, Level 11,
  Tower E3, The Towers, Oriental Plaza
  No.1 East Chang An Ave.,
  Dong Cheng District
  Beijing 100738
  Chine P.R.C.
  Numéro principal: +86 10 8518 3338
  Support technique: +86 10 8518 6923

Télécopie: +86 10 8518 6928
Site Web: http://www.symantec.com.cn

HONG KONG

- Symantec Hong Kong
  Central Plaza
  Suite #3006
  30th Floor, 18 Harbour Road
  Wanchai
  Hong Kong
  Numéro principal: +852 2528 6206
  Support technique: +852 2528 6206
  Télécopie: +852 2526 2646
  Site Web: http://www.symantec.com.hk

INDE

- Symantec India
  Suite #801
  Senteck Centrako
  MMTC Building
  Bandra Kurla Complex
  Bandra (East)
  Mumbai 400051, Inde
  Numéro principal: +91 22 652 0658
  Support technique: +91 22 652 0671
  Télécopie: +91 22 657 0669
  Site Web: http://www.symantec.com/india

COREE

- Symantec Korea
  15,16th Floor
  Dukmyung B/D
  170-9 Samsung-Dong
  KangNam-Gu
  Seoul 135-741
  Corée du Sud
  Numéro principal: +822 3420 8600
  Support technique: +822 3452 1610
  Télécopie: +822 3420 8650
  Site Web: http://www.symantec.co.kr

MALAISIE

- Symantec Corporation (Malaysia) Sdn Bhd
  31-3A Jalan SS23/15
  Taman S.E.A.
  47400 Petaling Jaya
  Selangor Darul Ehsan
  Malaisie
  Numéro principal: +603 7805 4910
  Support technique: +603 7804 9280
  E-mail société: gold.apac@symantec.com
  N° vert société: +1800 805 104
  Site Web: http://www.symantec.com.my

NOUVELLE-ZELANDE

- Symantec New Zealand
  Level 5, University of Otago Building
  385 Queen Street
  Auckland Central 1001
  Nouvelle-Zélande
  Numéro principal: +64 9 375 4100
  Télécopie: +64 9 375 4101
  Site Web de support: http://service.symantec.co.nz
  Gold Support: 0800 174 045 gold.nz@symantec.com
  Admin. contrats de support: 0800 445 450 contractsadmin@symantec.com

SINGAPOUR

- Symantec Singapore
  6 Battery Road
  #22-01/02/03
  Singapour 049909
  Numéro principal: 1800 470 0730
  Télécopie: +65 6239 2001
  Support technique: 1800 720 7898
  Site Web: http://www.symantec.com.sg

TAIWAN

- Symantec Taiwan
  2F-7, No.188 Sec.5
  Nanjing E. Rd.,
  105 Taipei
  Taïwan
  Numéro principal: +886 2 8761 5800
  Corporate Support: +886 2 8761 5800
  Télécopie: +886 2 2742 2838
  Gold Support: 0800 174 045 gold.nz@symantec.com
  Site Web: http://www.symantec.com.tw

L’exactitude des informations contenues dans ce document a fait l’objet de toutes les attentions. Toutefois, les informations fournies ici sont susceptibles d'être modifiées sans préavis. Symantec Corporation se réserve le droit d’apporter ces modifications sans avertissement préalable.

Table des matières

Chapitre 1

Présentation de Norton Smartphone Security

Ce chapitre traite des sujets suivants :

A propos de Norton Smartphone Security

Norton Smartphone Security sécurise l'informatique mobile grâce à une protection complète et fiable contre les attaques malveillantes dirigées vers les périphériques. Norton Smartphone Security protège vos périphériques des attaques malveillantes et des messages SMS indésirables à l'aide d'antivirus, de SMS AntiSpam et d'un pare-feu. Norton Smartphone Security est également intégré à Symantec LiveUpdate pour assurer des mises à jour de produit et de sécurité dans les meilleurs délais.

Les composants et fonctionnalités actuels de Norton Smartphone Security comprennent les éléments suivants :

- Antivirus : protège efficacement les utilisateurs contre les menaces mobiles tout en ayant un impact minimal sur le périphérique mobile.
- AntiSpam pour SMS : les messages SMS indésirables sont placés automatiquement dans le dossier correspondant ou sont supprimés ; vous pouvez configurer les messages qui doivent être traités comme tel.
- Pare-feu : empêche les réseaux sans autorisation d'accéder à votre périphérique mobile.

Norton Smartphone Security comprend un pare-feu dynamique qui bloque le trafic réseau externe indésirable.

Fonctionnement de Norton Smartphone Security

Les composants de Norton Smartphone Security collaborent à la protection des périphériques.

Pour comprendre le fonctionnement de Norton Smartphone Security, lisez les sections suivantes :

- Protection des périphériques
- Mise à jour de Norton Smartphone Security et de la protection contre les menaces
- Consignation des activités

Protection des périphériques

Norton Smartphone Security utilise les fichiers de définitions de virus pour identifier les menaces connues. Lorsque l'utilisateur tente d'ouvrir un fichier du périphérique, Auto-Protect lance automatiquement une analyse antimenace en temps réel. L'utilisateur peut également lancer cette analyse manuellement. Par défaut, lorsque Auto-Protect détecte un fichier suspect, le fichier est mis en quarantaine. Les fichiers infectés sont en sécurité dans la zone Quarantaine et ne peuvent pas propager des menaces vers d'autres zones sur le périphérique.

Que se passe-t-il lorsque le pare-feu détecte une activité non autorisée ?

Lorsque le pare-feu Norton Smartphone Security détecte une activité qui n'est pas autorisée, comme des connexions entrantes et sortantes, il consigne l'activité de pare-feu dans le Journal des activités.

Mise à jour de Norton Smartphone Security et de la protection contre les menaces

Symantec™ Security Response fournit aux utilisateurs des mises à jour régulières des fichiers de définitions de virus, qui permettent de conserver une protection antivirale à jour. Symantec offre également des mises à jour du logiciel Norton Smartphone Security.

Pour obtenir des mises à jour de définitions de virus et de produits, accédez directement au serveur Symantec LiveUpdate.

Se reporter à "Mise à jour des périphériques" à la page 39.

Consignation des activités

Le logiciel Norton Smartphone Security du périphérique enregistre des informations sur les activités de l'antivirus et du pare-feu effectuées sur le périphérique. Il enregistre également les informations à propos des mises à jour.

L'utilisateur peut afficher ces données directement sur le périphérique.

Se reporter à "A propos du Journal d'activités" à la page 33.

Pour plus d'informations

L'aide en ligne est installée sur les périphériques en même temps que le logiciel du produit.

Outre les dernières mises à jour en matière de protection et de programme, le site Web du support technique Symantec met à votre disposition des correctifs, des didacticiels, des articles issus de la base de connaissances et des outils de suppression de menaces.

Pour explorer le site Web de support technique Symantec

1. Accédez à l'adresse suivante sur Internet :

   http://www.symantec.fr

2. Suivez les liens relatifs aux informations recherchées.

Chapitre 2

Installation de Norton Smartphone Security

Ce chapitre traite des sujets suivants :

Configuration requise du système et du périphérique

Le Tableau 2-1 détaille les périphériques pris en charge et les élements de configuration requis. Les plates-formes de bureau qui prennent Norton Smartphone Security en charge sont Windows XP Edition familiale/Professionnel avec Service Pack 2, ainsi que Windows Vista.

Tableau 2-1 Configuration requise pour les périphériques

Système d'exploitation ou composant	Configuration minimale
Windows Mobile 5.0 et 6.0	■ Pocket PC/Professional : 1,8 Mo ■ Smartphone/Standard : 1,7 Mo ■ Microsoft ActiveSync 4.1 ou version ultérieure ; Gestionnaire pour appareils Windows Mobile 6.0 ou version ultérieure

Système d'exploitation ou composant	Configuration minimale
LiveUpdate	Prise en charge d'internet sans fil utilisant la pile TCP/IP intégrée.

Il existe deux versions de Norton Smartphone Security pour Windows Mobile. La première version a été conçue pour les périphériques de type Smartphone avec écran tactile et stylet comme les périphériques qui exécutent Windows Mobile 6 Professional ou Windows Mobile 5 PocketPC. La seconde version est conçue pour les périphériques sans écran tactile, comme les périphériques exécutant Windows Mobile 6 Standard ou Windows Mobile 5 Smartphone.

Les termes suivants sont utilisés dans le document et font référence aux périphériques exécutant Windows Mobile :

- WM Professional : correspond aux Pocket PC Windows Mobile 6 Professional et Windows Mobile 5.
- WM Standard : correspond aux Smartphone Windows Mobile 6 Standard et Windows Mobile 5.

Installation de Norton Smartphone Security

Après avoir connecté le périphérique à votre ordinateur de bureau, vous pouvez effectuer l'installation à l'aide de l'assistant d'installation sur le CD, puis synchroniser le périphérique à l'ordinateur.

Effectuez ce qui suit sur le périphérique préalablement à l'installation :

- Définissez la date et l'heure de l'horloge du périphérique.
- Fermez tous les fichiers.
- Quittez toutes les applications.
- Redémarrez le périphérique pour vous assurer que les applications précédemment installées le sont complètement et que les données sont enregistrées.

Remarque : L'installation dans le répertoire par défaut est la seule configuration d'installation prise en charge.

Pour installer Norton Smartphone Security

1. Insérez le CD et exécutez le fichier start.exe.
2. Sélectionnez **Installer Norton Smartphone Security**.
3. Suivez les instructions à l'écran pour terminer l'installation.

   Attention de ne pas annuler ou interrompre le processus d'installation. Après l'affichage du message d'installation réussie, vous êtes invité à redémarrer le périphérique. Une icône pour Norton s'affiche sur le périphérique une fois l'installation terminée.

Test de l'installation

Vous pouvez vérifier que Norton Smartphone Security est actif en téléchargeant le fichier de test standard de l'organisme EICAR (European Institute for Computer Anti-Virus Research) et en le copiant vers le périphérique.

Pour tester l'installation

1. Téléchargez le fichier test EICAR à partir de l'URL ci-dessous :

   www.eicar.org

   Vous serez peut-être amené à désactiver temporairement l'analyse antimenace sur votre ordinateur pour pouvoir accéder au fichier de test de l'EICAR. N'oubliez pas de réactiver l'analyse antimenace sur votre ordinateur à l'issue de cette opération.
2. Copiez le fichier de test de l'EICAR sur le périphérique.

   Une fois Norton Smartphone Security correctement installé, une boîte de dialogue s'affiche quand le fichier test EICAR a été copié sur le périphérique.

Mise à niveau de Norton Smartphone Security

Effectuez ce qui suit prélablement à la mise à niveau :

- Définissez la date et l'heure de l'horloge du périphérique.
- Fermez tous les fichiers.
- Quittez toutes les applications.
- Sauvegardez vos données.
- Redémarrez le périphérique pour vous assurer que les applications précédemment installées le sont complètement et que les données sont enregistrées.

Installation de la mise à niveau

La procédure suivante permet d'installer la mise à niveau.

Pour installer la mise à niveau

1. Insérez le CD et exécutez le fichier start.exe.
2. Sélectionnez **Installer Norton Smartphone Security**.
3. Suivez les instructions à l'écran pour terminer l'installation.
4. Si un message s'affiche et indique que la mise à niveau ne parvient pas à supprimer la version précédente du logiciel, cliquez sur **OK** pour continuer.

   Attention de ne pas annuler ou interrompre le processus d'installation.

Désinstallation des composants de Norton Smartphone Security

Norton Smartphone Security Firewall ou Norton Smartphone Security AntiVirus peuvent être désinstallés du périphérique à partir de l'écran Suppression de programmes. La désinstallation d'AntiVirus désinstalle également SMS AntiSpam et LiveUpdate.

Pour désinstaller le pare-feu ou l'antivirus sur un périphérique WM Standard

1. Sélectionnez **Démarrer > Paramètres > Suppression de programmes**.
2. Sélectionnez le composant Norton Firewall ou AntiVirus.
3. Sélectionnez **Menu > Supprimer**.
4. Sélectionnez **Oui** lorsque le message de confirmation s'affiche.

Pour désinstaller le pare-feu ou l'antivirus sur un périphérique WM Professional

1. Sélectionnez **Démarrer > Paramètres**.
2. Sélectionnez l'onglet **Système**.
3. Sélectionnez **Suppression de programmes**.
4. Sélectionnez le composant Norton Firewall ou AntiVirus.
5. Sélectionnez **Supprimer**.
6. Sélectionnez **Oui** lorsque le message de confirmation s'affiche.

Chapitre 3

Protection des périphériques grâce à Norton Smartphone Security

Ce chapitre traite des sujets suivants :

A propos du pare-feu

Norton Smartphone Security vous permet de sélectionner quatre niveaux de pare-feu différents. Chaque niveau applique une politique définissant les types de trafic réseau autorisés ou bloqués sur le périphérique. La politique sélectionnée reste en place tant que vous n'en sélectionnez pas une autre.

En fonction de la version de Windows Mobile en cours d'exécution sur votre périphérique, comme Windows Mobile 6 Standard et Windows Mobile 5

Smartphone, la fonctionnalité de pare-feu vous permet d'afficher et d'actualiser les statistiques d'événements.

Sur les périphériques qui exécutent Windows Mobile 6 Professional et Windows Mobile 5 Pocket PC, la fonctionnalité de pare-feu vous permet d'effectuer les opérations suivantes :

- Sur l'écran Résumé des événements, afficher les statistiques qui suivent le nombre d'événements détectés dans la dernière minute, heure et journée.
- Sur l'écran Liste des événements, afficher tous les événements contenus dans le journal d'événements actif. Cette liste indique la date, l'heure, le type de l'événement ainsi qu'une brève description de l'événement.
- Dans l'écran Détail des événements, afficher des données détaillées à propos de chaque événement.

A propos des niveaux de pare-feu

Les niveaux de pare-feu sont décrits comme suit :

Sécurité maximale	Cette politique bloque tout trafic entrant et sortant, y compris la synchronisation de bureau via ActiveSync ou le Gestionnaire pour appareils Windows Mobile. Tout le trafic bloqué est consigné.
Sécurité élevée	Cette politique autorise les connexions réseau TCP et UDP courantes établies par les utilisateurs, comme la navigation Web ou l'utilisation du courrier électronique. DHCP, la résolution de nom DNS, le trafic IPsec VPN, le transfert de fichiers FTP/FTPS et la synchronisation de bureau via ActiveSync ou le Gestionnaire pour appareils Windows Mobile sont autorisés. Le datagramme NETBIOS et le service de noms NETBIOS sont bloqués sans être consignés. Tout le trafic autorisé est consigné à l'exception de la synchronisation de bureau. Se reporter à Tableau 3-1 à la page 27.
Sécurité moyenne	Cette politique est le niveau de pare-feu par défaut lors de l'installation initiale de Norton Smartphone Security. Le niveau Sécurité moyenne autorise toutes les connexions TCP et UDP établies par l'utilisateur, y compris la synchronisation de bureau via ActiveSync ou le Gestionnaire pour appareils Windows Mobile. Les requêtes Ping entrantes et sortantes sont autorisées pour tester la connectivité de réseau. Le datagramme NETBIOS et le service de noms NETBIOS sont bloqués sans être consignés. Tout le trafic autorisé est consigné à l'exception de la synchronisation de bureau.
Sécurité basse	Cette politique autorise tout le trafic entrant et sortant et ne consigne aucun événement.

Le Tableau 3-1 décrit les règles de filtrage.

Tableau 3-1 Politique Sécurité élevée avec le pare-feu Norton Smartphone Security

Nom de règle	Protocole	Port distant	Port local
Autoriser le client DHCP	UDP	67	68
Autoriser les requêtes DNS	UDP	53	Tout
Autoriser HTTP	TCP	80	Tout
Autoriser le proxy Web HTTP 8080	TCP	8080	Tout
Autoriser HTTP Alternate 8008	TCP	8008	Tout
Autoriser HTTPS TCP	TCP	443	Tout
Autoriser FTP-control	TCP	21	Tout
Autoriser FTPS	TCP	990	Tout
Autoriser POP3	TCP	110	Tout
Autoriser POP3-SSL	TCP	995	Tout
Autoriser SMTP	TCP	25	Tout
Autoriser SMTP-SSL	TCP	465	Tout
Autoriser IMAP4	TCP	143	Tout
Autoriser IMAP4-SSL	TCP	993	Tout
Autoriser IKE	UDP	Tout	500
Autoriser IPsecNAT-T 4500	UDP	Tout	4500
Autoriser IPsecNAT-T 4502	UDP	Tout	4502

Définition du niveau du pare-feu

Vous pouvez définir le niveau de pare-feu sur les périphériques qui exécutent Windows Mobile Professional ou Windows Mobile Standard.

Pour définir le niveau de pare-feu sur un périphérique WM Standard

1. Sélectionnez **Démarrer > Norton Security > Norton Firewall**.
2. Sélectionnez **Menu >** et l'une des options suivantes : **Sécurité basse, Sécurité moyenne, Sécurité élevée** ou**Sécurité maximale**.

   Les règles de politique associées à ce niveau de sécurité sont appliquées.

Pour définir le niveau de pare-feu sur un périphérique WM Professional

1. Sélectionnez **Démarrer > Programmes > Norton Security > Norton Firewall**.
2. Sélectionnez l'une des options suivantes : **Sécurité maximale, Sécurité élevée, Sécurité moyenne** ou **Sécurité basse**.

   Les règles de politique associées à ce niveau de sécurité sont appliquées.

Consignation d'événements

Norton Smartphone Security crée un journal des événements de pare-feu. Lorsqu'un événement est détecté, il est automatiquement consigné dans le journal. Le journal de pare-feu actif est supprimé lorsqu'il atteint les 500 enregistrements. Un nouveau journal enregistre les événements suivants.

Sur un périphérique WM Standard, les statistiques d'événement de pare-feu pour la dernière minute, heure et journée s'affichent directement dans l'interface du pare-feu.

Sur un périphérique WM Professional, les événements s'affichent dans les écrans Liste d'événements et Détail de l'événement. L'écran Résumé des événements permet d'obtenir un résumé de tous les événements.

Affichage d'événements récents

Vous pouvez afficher les événements récents sur votre périphérique WM Standard ou WM Professional.

Pour afficher les événements récents sur un périphérique WM Standard

1. Ouvrez **Démarrer > Norton Security > Norton Firewall**.
2. Sélectionnez **Menu > Actualiser**.

Pour afficher les événements récents sur un périphérique WM Professional

1. Ouvrez **Démarrer > Programmes > Norton Security > Norton Firewall**.
2. Sélectionnez **Options**, puis sélectionnez soit **Résumé des événements**, soit **Liste d'événements**.
3. Sélectionnez un élément de l'écran **Liste d'événements** afin d'afficher les informations détaillées sur celui-ci.

Résumé des événements (WM Professional)

L'écran Résumé des événements affiche le nombre d'événements détectés dans la dernière minute, heure et journée. L'écran Résumé des événements présente deux vues des événements : Evénements par gravité et Evénements par catégorie. Le nombre total d'événements accumulés est également affiché.

La vue Evénements par gravité affiche les statistiques d'événements pour la dernière minute, heure et journée pour trois niveaux de gravité. Les événements dits informatifs comme la modification du niveau de pare-feu ne sont pas comptabilisés dans ces statistiques.

La vue Evénements par catégorie affiche toutes les statistiques d'événement pour la dernière minute, heure et journée par catégorie signalée par les abréviations PF (pare-feu) et Séc (sécurité). Les événements informatifs sont comptés dans Evénements par catégorie, par conséquent, les totaux accumulés en fonction de la sévérité et de la catégorie peuvent ne pas être les mêmes.

Pour accéder à l'écran Résumé des événements

1. Naviguez vers le composant Pare-feu.
2. Sélectionnez **Options > Résumé des événements**.

Liste d'événements (WM Professional)

La liste d'événements se compose de tous les événements contenus dans le journal des événements actif. Elle comprend la date, l'heure, le type de l'événement ainsi qu'une brève description de l'événement. Vous pouvez trier les événements en sélectionnant l'en-tête d'une colonne.

Pour accéder à l'écran Liste d'événements

1. Naviguez vers le composant Pare-feu.
2. Sélectionnez **Options > Liste d'événements**.

Détail de l'événement (WM Professional)

Vous pouvez afficher des informations détaillées, notamment le port et le protocole, pour chaque événement de pare-feu dans la liste d'événements.

Pour afficher un détail d'événement

1. Naviguez vers le composant Pare-feu.
2. Sélectionnez **Options > Liste d'événements**.
3. Sélectionnez un événement pour afficher des informations supplémentaires à propos de celui-ci.

Ouvrez Norton Smartphone Security.

Norton Smartphone Security protège le périphérique sur lequel il est installé. Il n'est pas nécessaire de lancer le programme pour activer la protection.

Pour ouvrir Norton Smartphone Security

1. Sur le périphérique, ouvrez le composant **AntiVirus**.
2. Sélectionnez **Menu**.

   Pour obtenir des informations sur les options du menu AntiVirus, voir Tableau 3-2.

A propos des options disponibles dans la vue principale

Tableau 3-2 décrit la vue principale de Norton Smartphone Security du composant AntiVirus, qui vous permet de modifier les paramètres.

Tableau 3-2 Options de la vue principale

Option	Description
Options	Activer ou désactiver Auto-Protect et le pare-feu, et personnaliser la configuration du pare-feu et de LiveUpdate
Journal d'activités	Consulter les informations sur les événements d'analyse, de pare-feu et de LiveUpdate
Définitions de menaces	Afficher la liste des menaces contre lesquelles le périphérique est actuellement protégé
LiveUpdate	Rechercher les mises à jour de produits et de définitions de virus
A propos de l'AntiVirus	Afficher des informations sur le produit, la version et la licence

Option	Description
Quarantaine	Afficher le fichier journal de quarantaine
Abonnement	Mettre l'abonnement à jour lorsque cela s'avère nécessaire

Analyse et traitement des menaces

Lorsque Norton Smartphone Security détecte une menace, l'utilisateur peut agir en conséquence. Le type d'action dépend de la nature de la menace.

Il existe plusieurs options d'analyse permettant de rechercher des menaces, en fonction de la configuration requise :

Analyser après une synchronisation	Exécutez cette analyse après avoir synchronisé votre périphérique mobile avec votre bureau.
Analyser après une insertion de la carte	Exécutez cette analyse après avoir installé une carte de stockage dans votre périphérique mobile.
Analyse après màj	Exécutez cette analyse après avoir mis votre périphérique mobile à jour.

Pour exécuter une analyse

1. Sélectionnez **Démarrer > Norton Security > Norton AntiVirus**.
2. Effectuez l'une des opérations suivantes :
   - Sur un périphérique WM Standard, sélectionnez **Menu > Options > Options AntiVirus**.
   - Sur un périphérique WM Professional, passez à l'étape 3.
3. Sélectionnez l'option d'analyse que vous souhaitez exécuter.

Planification d'analyses

Vous pouvez planifier des analyses pour les menaces de virus à des intervalles spécifiés.

Tableau 3-3 dresse la liste des paramètres d'analyse.

Tableau 3-3 Paramètres d'analyse

Paramètre	Description
Fréquence	Jamais : désactive la tâche planifiée. Quotidien : la tâche s'effectue tous les jours. Chaque {jours de la semaine \ Lundi, Mardi,...} : la tâche se produit le jour de la semaine spécifié. {##} de chaque mois : la tâche se produit le jour du mois spécifié. Une fois : la tâche se produit une fois, à la date et à l'heure spécifiées.
Heure de démarrage	Spécifie l'heure initiale à laquelle la tâche se produit ou se reproduit. L'effet de ce paramètre peut varier en fonction du paramètre Fréquence.
Date de démarrage	Spécifie la date initiale à laquelle la tâche se produit ou se reproduit. L'effet de ce paramètre peut varier en fonction du paramètre Fréquence. Par exemple, si la fréquence est définie sur Chaque <jour de la semaine> et la date de départ est définie sur le lundi 1er janvier 2007, l'action planifiée se produira chaque lundi à partir du 1er janvier 2007.

Pour planifier une analyse

1. Sélectionnez **Démarrer** et naviguez vers **Norton AntiVirus**.
2. Effectuez l'une des opérations suivantes :
   - Sur un périphérique WM Professional, sélectionnez **Menu > Options**, puis sélectionnez l'onglet **Analyses**.
   - Sur un périphérique WM Standard, sélectionnez **Menu > Options > Planification d'analyse**.
3. Dans la boîte de dialogue, sélectionnez les paramètres de votre choix et spécifiez la fréquence, l'heure et la date de démarrage pour la planification d'une analyse.

A propos des analyses Auto-Protect

Lorsque l'utilisateur ouvre un fichier du périphérique, Auto-Protect lance une analyse antimenace en temps réel. Par défaut, lorsque Auto-Protect détecte un fichier suspect, le fichier est mis en quarantaine. Les fichiers infectés sont en sécurité dans la zone Quarantaine et ne peuvent pas propager des menaces vers d'autres zones sur le périphérique.

En cas d'échec de l'action automatique, l'action suivante consiste à refuser l'accès.

Le Tableau 3-4 détaille les actions automatiques disponibles.

Tableau 3-4 Actions automatiques

Action	Description
Refuser l'accès	Interdit à toute application d'ouvrir le fichier infecté.
Supprimer	Supprime le fichier infecté. Cette action est recommandée.
Quarantaine	(Par défaut) Déplace le fichier vers la zone de quarantaine.

Désactivation temporaire d'Auto-Protect

Auto-Protect surveille et analyse les fichiers auxquels accède le périphérique. Lorsqu'une menace ou une activité de nature menaçante sont détectées, le fichier potentiellement malveillant est bloqué et l'action que vous avez sélectionnée dans le Tableau 3-4 à la page 33. est effectuée.

Par défaut, cette fonction est activée. Il est recommandé de laisser Auto-Protect activé en permanence.

Pour désactiver temporairement Auto-Protect

1. Naviguez vers le composant AntiVirus.
2. Effectuez l'une des opérations suivantes :
   - Sur un périphérique WM Standard, sélectionnez **Menu > Options > Options AntiVirus**.
   - Sur un périphérique WM Professional, sélectionnez **Menu > Options** .
3. Décochez la case **Auto-Protect**.

A propos du Journal d'activités

Le périphérique gère un historique local des activités de l'antivirus, du pare-feu et de LiveUpdate.

Activités antimenaces

Le périphérique enregistre les activités antimenaces suivantes :

Analyse partielle — Une entrée d'analyse s'ajoute lorsque l'utilisateur annule une analyse ou s'il n'analyse qu'une partie du périphérique.

Analyse complète	Une entrée d'analyse complète est ajoutée lorsque tout le périphérique est analysé, y compris ses cartes de stockage.
Menace détectée	Une entrée de menace détectée est ajoutée chaque fois que Norton Smartphone Security identifie un fichier infecté par une menace. Cette entrée inclut l'action effectuée sur le fichier infecté.

Norton Smartphone Security consigne les événements de quarantaine suivants :

- Mise en quarantaine
- Efface quarantaine
- Restaure Quarantaine

Pour chaque événement de Quarantaine, les renseignements suivants sont fournis :

- Date
- Heure
- Evénement (ajout, suppression ou restauration par exemple)
- Source (analyseur, Auto-Protect ou Quarantaine par exemple)
- Fichier
- Statut (réussi ou échoué par exemple)

Activités de LiveUpdate

Le périphérique enregistre les activités LiveUpdate suivantes :

Mise a jour de l'appl.	Fournit des informations sur les mises à jour des composants de l'antivirus, du pare-feu et de LiveUpdate. Inclut également des informations sur SMS AntiSpam, comme la date et l'heure, le nom du composant, les numéros des versions précédente et suivante, ainsi que l'état de l'opération.
Mise à jour de définitions de virus	Fournit des informations sur l'ancienne version de définitions de virus et la nouvelle version de définitions de virus. Les détails incluent la date et l'heure, le numéro de séquence précédent et suivant, et l'état de l'opération.

Activités du pare-feu

Le périphérique enregistre les activités de pare-feu suivantes :

Connexion sortante bloquée	Une entrée est ajoutée en cas de tentative de connexion TCP ou UDP sortante bloquée.
Connexion entrante bloquée	Une entrée est ajoutée en cas de tentative de connexion TCP ou UDP entrante bloquée.

Pour chaque activité du pare-feu, le journal fournit les renseignements suivants :

- Date
- Heure
- Protocole impliqué (TCP ou UDP)
- Direction (connexions TCP et UDP)
- Adresse IP de l'attaquant
- Port de l'attaquant
- Adresse IP de la victime
- Port de la victime

A propos de SMS AntiSpam

SMS AntiSpam permet à l'utilisateur de gérer une liste de numéros de téléphone autorisés ou une liste de numéros de téléphone bloqués en fonction desquelles les messages entrants sont filtrés. Si l'utilisateur exécute une liste de numéros bloqués et qu'un message entrant provient d'un numéro de cette liste, ou s'il exécute une liste de numéros autorisés et que le message entrant provient d'un numéro qui n'y figure pas, les messages sont acheminés vers un dossier spécial.

L'utilisateur peut gérer une liste de numéros autorisés et une liste de numéros bloqués ; les deux listes ne peuvent pas être actives en même temps.

Remarque : SMS AntiSpam filtre les SMS, non le courrier électronique, indésirables.

Configuration de SMS AntiSpam

Vous pouvez ajouter et supprimer des numéros ou encore importer des numéros à partir de la liste de contacts ou de la carte de stockage sur le périphérique. En outre, dans le Centre de message sur le périphérique, le numéro de message actuel peut être bloqué ou autorisé.

Pour configurer SMS AntiSpam

1. Sélectionnez **Démarrer** et accédez à **Norton AntiVirus**.
2. Effectuez l'une des opérations suivantes :
   - Sur un périphérique WM Professional, sélectionnez l'onglet **Menu > Options > AntiSpam**.
   - Sur un périphérique WM Standard, sélectionnez **Menu > Options > Options AntiSpam**.
3. Configurez les éléments suivants à partir de la liste située en haut de l'écran :
   - Numéros bloqués : bloque les messages provenant des numéros répertoriés dans cette liste.
     Si Bloquer les numéros est sélectionné, vous pouvez également sélectionner Bloquer SMS sans numéros. Cet élément bloque tous les messages entrants dont le numéro n'est pas spécifié. Cette fonctionnalité dépend des porteuses ; en effet, certains porteuses attribuent aux messages sans numéro le numéro 000-0000.
   - Numéros acceptés : accepte uniquement les messages provenant des numéros de la liste.
   - Désactiver SMS AntiSpam : désactive la fonctionnalité anti-spam.
4. Effectuez l'une des opérations suivantes :
   - Sur un périphérique WM Professional, sélectionnez **Importer**. Les numéros figurant déjà dans la liste de filtres AntiSpam sont vérifiés.
   - Sur un périphérique VM Standard, sélectionnez **Menu > Modifier les numéros > Menu > A partir des contacts**.
5. Pour ajouter un numéro du carnet d'adresses à la liste de filtres AntiSpam, placez une coche à côté du numéro, puis sélectionnez **Fini**.

Numéros et correspondance de numéros

Les numéros de téléphone aux Etats-Unis et dans d'autres pays du monde se composent généralement d'un préfixe et d'un numéro principal. Dans certaines régions, le préfixe n'est pas nécessaire à l'envoi d'un message au périphérique. Si par exemple, votre périphérique est enregistré aux Etats-Unis avec le code régional (818), l'appel est acheminé au même endroit, que vous composiez le (818) 555-1212 ou le 555-1212. Les messages entrants suivent la même règle, en fonction de la porteuse. Si un message est envoyé à partir du (818) 555-1212, le numéro peut s'afficher sous les formes suivantes sur le périphérique de destination : 555-1212, 818-555-1212 ou 1-818-555-1212.

Le processus de filtrage tente de résoudre ce problème en commençant par obtenir le numéro de téléphone du périphérique actuel, puis en recherchant les préfixes existants dans le numéro du périphérique, afin de compléter les composants de préfixe manquants si le numéro du message est trop court. Par exemple, un message entrant est émis à partir du 555-1212 et le périphérique est enregistré avec le code régional (818). Ce numéro correspond donc aux numéros 1-818-555-1212, 818-555-1212 ou 555-1212 de la liste AntiSpam des numéros bloqués.

Remarque : Si le programme ne peut pas obtenir le numéro du périphérique utilisé, les numéros sont comparés lors de leur réception. Un message entrant en provenance du 555-1212 ne correspond qu'au 555-1212, mais pas au 1-818-555-1212, car le code régional n'a pas pu être obtenu.

Pour les messages internationaux où le nombre de chiffres des numéros de téléphone varient selon le pays, un message en provenance d'un pays où les numéros sont plus courts risque de perturber la routine de comparaison de chaînes d'un pays utilisant des numéros de téléphone plus longs.

Chapitre 4

Mise à jour des périphériques

Ce chapitre traite des sujets suivants :

Mise à jour des périphériques

Vous pouvez régulièrement télécharger et installer les définitions de virus les plus récentes sur votre périphérique afin de le protéger contre les menaces du moment.

Si le périphérique ne dispose pas d'une connexion Internet active, LiveUpdate tente d'établir une connexion réseau. Si le périphérique ne possède aucun point d'accès à Internet, la connexion échoue.

Norton Smartphone Security prend en charge les types de mise à jour suivants :

Mise à jour des fichiers de définitions de virus	Les produits Symantec utilisent les fichiers de définitions de virus pour identifier les menaces. Symantec Security Response recherche de nouvelles menaces, y répond et fournit aux clients des fichiers de définitions de virus actualisés au fur et à mesure de l'émergence de nouvelles menaces.
Mises à jour des logiciels	Symantec fournit occasionnellement des mises à jour pour Norton AntiVirus, le pare-feu, AntiSpam pour SMS et LiveUpdate.

Mise à jour des moteurs	Symantec fournit occasionnellement des mises à jour des moteurs d'analyse antivirus intégrant les nouveaux types de menaces identifiés.

Pour rechercher des mises à jour

1 Depuis votre périphérique, ouvrez **Norton Security > Norton AntiVirus**.

2 Sélectionnez **Menu > LiveUpdate**.

LiveUpdate se connecte au serveur Symantec LiveUpdate pour vérifier l'existence de mises à jour des fichiers de définitions de virus, des logiciels et des moteurs.

La mise à jour de votre périphérique avec les fichiers de définitions de virus les plus récents le protège contre les menaces du moment.

Planification des mises à jour LiveUpdate

Vous pouvez activer et configurer les mises à jour LiveUpdate selon des intervalles spécifiques.

Le Tableau 4-1 présente les paramètres de planification de LiveUpdate.

Tableau 4-1 Paramètres de planification LiveUpdate

Paramètre	Description
Fréquence	Jamais : désactive la tâche planifiée. Quotidienne : la tâche s'effectue tous les jours. Chaque {jours de la semaine \ Lundi, Mardi,...} : la tâche se produit le jour de la semaine spécifié. {##} de chaque mois : la tâche se produit le jour du mois spécifié.
Action	Rappel : invite l'utilisateur à exécuter LiveUpdate. Mise à jour : se produit automatiquement au moment planifié.
Heure de démarrage	Spécifie l'heure initiale à laquelle la tâche se produit ou se reproduit. L'effet de ce paramètre peut varier en fonction du paramètre Fréquence.
Date de démarrage	Spécifie la date initiale à laquelle la tâche se produit ou se reproduit. L'effet de ce paramètre peut varier en fonction du paramètre Fréquence. Par exemple, si la fréquence est définie sur Chaque <jour de la semaine> et la date de départ est définie sur le lundi 1er janvier 2007, l'action planifiée se produira chaque lundi à partir du 1er janvier 2007.

Pour planifier les mises à jour

1. Sélectionnez **Démarrer** et naviguez vers **Norton AntiVirus**.
2. Effectuez l'une des opérations suivantes :
   - Sur un périphérique WM Professional, sélectionnez **Menu > Options**, puis sélectionnez l'onglet **Mises à jour**.
   - Sur un périphérique WM Standard, sélectionnez **Menu > Options > Planification LiveUpdate**.
3. Dans la boîte de dialogue, sélectionnez les paramètres de votre choix et spécifiez la fréquence, l'action, l'heure et la date de démarrage pour la planification des mises à jour LiveUpdate.

Mise à jour de l'abonnement au produit

Vous pouvez mettre à jour l'abonnement à Norton Smartphone Security simplement à partir du menu principal. Lorsque l'abonnement expire, vous recevez un message sur votre téléphone vous invitant à renouveler la licence.

Remarque : Assurez-vous d'avoir configuré le service Internet sur le téléphone avant de continuer. Contactez votre fournisseur d'accès sans fil pour en savoir plus.

Pour mettre à jour l'abonnement au produit

1. Ouvrez le raccourci **Norton** de votre périphérique.
2. Sélectionnez **Activer**.
3. Sélectionnez **OK** pour mettre à jour l'abonnement.
4. Sélectionnez votre connexion Internet dans la liste. La connexion au serveur Internet peut prendre un certain temps.
5. Sélectionnez l'option de paiement.
6. Suivez les instructions de l'assistant pour effectuer la procédure de renouvellement.

Index

N

P

Q

R

S