

Guide de l'utilisateur Norton™ Smartphone Security

for Symbian OS™



Norton™ Smartphone Security pour Symbian OS™

Avis légal

Copyright © 2007 Symantec Corporation.

Tous droits réservés.

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 de ses sociétés affiliées aux Etats-Unis et dans d'autres pays. Les autres noms sont des marques commerciales de leurs détenteurs respectifs.

Symbian et Symbian OS sont des marques déposées de Symbian Software Ltd. Windows est une marque déposée de Microsoft Corporation.

Le produit décrit dans ce document est distribué selon les termes d'une licence qui en limite son utilisation, sa copie, sa distribution ainsi que sa décompilation ou ingénierie inverse. La reproduction de ce document, sous quelque forme que ce soit, est formellement interdite sans l'accord écrit préalable de Symantec Corporation et de ses concédants de licence, le cas échéant.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET, DANS LES LIMITES AUTORISEES PAR LA LOI, SANS AUCUNE CONDITION, REPRESENTATION NI GARANTIE EXPRESSE OU TACITE, Y COMPRIS LES GARANTIES TACITES LIEES A LA COMMERCIALISATION, A L'ADEQUATION A UN USAGE PARTICULIER OU A LA CONTREFACON. SYMANTEC CORPORATION NE PEUT ETRE TENUE POUR RESPONSABLE DES DOMMAGES DIRECTS OU INDIRECTS RELATIFS AU CONTENU OU A L'UTILISATION DE LA PRESENTE DOCUMENTATION. LES INFORMATIONS CONTENUES DANS CETTE DOCUMENTATION PEUVENT ETRE MODIFIEES SANS PREAVIS.

La documentation et le logiciel sous licence sont considérés comme logiciel informatique commercial conformément aux définitions de la section FAR 12.212, et soumis selon le cas aux droits restreints, conformément aux définitions de la section FAR 52.227-19, "Commercial Computer Software - Restricted Rights", et DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", ainsi qu'à d'éventuelles réglementations successives. Toute utilisation, modification, diffusion d'une reproduction, exécution, affichage ou divulgation de la documentation et du logiciel sous licence par les autorités des Etats Unis doit être strictement conforme aux termes de ce contrat.

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
Número 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. Chucuri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brésil, SA
Número 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
Número 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
Número 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
Taiwan
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

Solutions de service et de support	3
Chapitre 1	Présentation de Norton Smartphone Security 17
	A propos de Norton Smartphone Security 17
	Fonctionnement de Norton Smartphone Security 18
	Protection des périphériques 18
	Mise à jour de Norton Smartphone Security et de la protection contre les menaces 19
	Consignation des activités 19
	Pour plus d'informations 19
Chapitre 2	Installation de Norton Smartphone Security 21
	Configuration requise 21
	Installation de Norton Smartphone Security 22
	Test de l'installation 23
	Mise à niveau de Norton Smartphone Security 23
	Installation de la mise à niveau 24
	Désinstallation de Norton Smartphone Security 24
Chapitre 3	Protection des périphériques grâce à Norton Smartphone Security 25
	Ouvrez Norton Smartphone Security. 25
	A propos des options disponibles dans la vue principale 26
	Analyse et traitement des menaces 27
	Planification d'analyses 27
	A propos des analyses Auto-Protect 27
	Désactivation temporaire d'Auto-Protect 28
	Configuration de la protection par le pare-feu 28
	Désactivation temporaire de la protection par pare-feu 29
	A propos du Journal d'activités 30
	Activités antimenaces 30
	Activités du pare-feu 30
	Activités de LiveUpdate 31
	Saturation du journal 32

- A propos de SMS AntiSpam 32
 - Configuration des règles et conditions pour SMS AntiSpam 33
 - Correspondance de numéros de téléphone 34
- Chapitre 4 Mise à jour des périphériques 35
 - Mise à jour des périphériques 35
 - Planification des mises à jour ou des rappels 36
 - Mise à jour de l'abonnement au produit 37
- Index 39

Présentation de Norton Smartphone Security

Ce chapitre traite des sujets suivants :

- [A propos de Norton Smartphone Security](#)
- [Fonctionnement de Norton Smartphone Security](#)
- [Pour plus d'informations](#)

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 mobiles.

Norton Smartphone Security propose les composants et fonctionnalités suivants :

- **Protection AntiVirus** : Technologies antivirus Symantec plébiscitées assurant l'analyse, la détection et la mise en quarantaine automatiques des virus et vers à risque.
- **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.
- **Protection par pare-feu** : empêche les intrus d'entrer et d'exporter des données à partir de votre périphérique.
- **Assistance LiveUpdate** : mises à jour de définitions de virus et de produit grâce à des communications sans fil via LiveUpdate ou synchronisation de l'appareil mobile.

- Protection contre les programmes malveillants téléchargés sur le Web, envoyés par courrier électronique ou via une connexion WiFi, ou transmis via Bluetooth® ou ports infrarouges.
- Prend en charge la programmation d'analyses antivirus sur votre périphérique.
- Analyses à la demande permettant de rechercher la présence de virus dans les fichiers, archives et applications désignés.
- Journal d'activités présentant l'ensemble des derniers événements consignés pour que les utilisateurs soient avertis en permanence des dangers éventuels.

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.

Si la première action par défaut échoue (Quarantaine), une deuxième action par défaut (Refuser l'accès) interdit à toute application d'ouvrir le fichier.

Se reporter à [Tableau 3-2](#) à la page 28.

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

En cas de détection d'une activité non autorisée (connexions entrantes ou sortantes, ou tentatives d'analyse de port par exemple), le pare-feu Norton Smartphone Security se comporte comme suit :

- Sur certains périphériques configurés en ce sens, il affiche provisoirement un message avec des informations sur l'activité non autorisée.
- Il consigne l'activité de pare-feu dans le Journal d'activités.
Se reporter à "[A propos du Journal d'activités](#)" à la page 30.
- Il bloque tout le trafic provenant de cette adresse IP par le biais de la détection des analyses de port.

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 35.

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 30.

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.

Installation de Norton Smartphone Security

Ce chapitre traite des sujets suivants :

- [Configuration requise](#)
- [Installation de Norton Smartphone Security](#)
- [Test de l'installation](#)
- [Mise à niveau de Norton Smartphone Security](#)
- [Désinstallation de Norton Smartphone Security](#)

Configuration requise

Le [Tableau 2-1](#) détaille la configuration requise pour les périphériques. 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	Spécifications
Symbian OS 9	<p>Inclut des périphériques Nokia Série 60 Version 3 tels que :</p> <ul style="list-style-type: none"> ■ Nokia E50 ■ Nokia E60 ■ Nokia E61 ■ Nokia E62 ■ Nokia E70 ■ Nokia N71 ■ Nokia N73 ■ Nokia N80 ■ Nokia N91 ■ Nokia N93 ■ Nokia 3250 ■ Nokia 5500 <p>Inclut des périphériques UIQ 3.0 tels que :</p> <ul style="list-style-type: none"> ■ Sony Ericsson P990 ■ Sony Ericsson M600i ■ Sony Ericsson W950
Périphériques	Espace requis pour l'installation : 1,1 Mo
Symantec LiveUpdate Wireless	Prise en charge du matériel Internet sans fil utilisant la pile TCP/IP intégrée.

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 préalablement 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 de Norton Smartphone Security

Bien qu'il soit possible de désinstaller des composants individuels de Norton Smartphone Security, cette opération provoque l'échec de Norton Smartphone Security. Une éventuelle réinstallation de Norton Smartphone Security nécessite la désinstallation préalable de tous les composants.

Pour désinstaller Norton Smartphone Security sur les périphériques :

- 1 Démarrez le gestionnaire d'applications du périphérique.
- 2 Dans la boîte de dialogue à l'écran, sélectionnez **Norton Security**, puis cliquez sur **Supprimer**.
- 3 Redémarrez le périphérique.

Protection des périphériques grâce à Norton Smartphone Security

Ce chapitre traite des sujets suivants :

- [Ouvrez Norton Smartphone Security.](#)
- [Analyse et traitement des menaces](#)
- [A propos des analyses Auto-Protect](#)
- [Configuration de la protection par le pare-feu](#)
- [A propos du Journal d'activités](#)
- [A propos de SMS AntiSpam](#)

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

- ◆ Ouvrez le raccourci **Norton** de votre périphérique.

A propos des options disponibles dans la vue principale

Le [Tableau 3-1](#) décrit la vue principale de Norton Smartphone Security permettant d'accéder aux composants du programme et de modifier les paramètres. L'option du menu AntiVirus permet d'accéder aux éléments figurant dans le tableau. Le contenu du menu est le même, quelle que soit l'application (AntiVirus, pare-feu, LiveUpdate, SMS AntiSpam) choisie.

Tableau 3-1 Options de la vue principale

Option	Description
AntiVirus	
- Analyse	Analyser manuellement les périphériques pour la recherche de virus
- Journal d'activités	Consulter les informations sur l'analyse
- Liste d'éléments en quarantaine	Afficher la liste de quarantaine
- Liste des menaces	Afficher la liste des menaces contre lesquelles le périphérique est actuellement protégé
- Paramètres	Activer ou désactiver Auto-Protect et le pare-feu, et personnaliser la configuration du pare-feu et de LiveUpdate
Analyse	Analyser manuellement les périphériques pour la recherche de virus
Rech. des mises à jour	Rechercher les mises à jour de produits et de définitions de virus
Journal d'activités	
- AntiVirus	Consulter les informations sur les analyses antivirus.
- Pare-feu	Consulter les informations sur le pare-feu
- LiveUpdate	Consulter les informations sur la planification LiveUpdate
Paramètres	
- AntiVirus	Consulter et définir les paramètres pour l'analyse AntiVirus ; activer/désactiver Auto-Protect
- Pare-feu	Personnaliser les paramètres du pare-feu
- LiveUpdate	Planification LiveUpdate
- SMS AntiSpam	Définition de règles pour SMS AntiSpam

Option	Description
Abonnement	Mettre à jour votre abonnement produit
A propos	Afficher des informations sur le produit, la version et la licence
Accord de licence	Afficher les informations relatives à l'accord de licence
Aide	Afficher l'aide en ligne de Norton Smartphone Security
Quitter	Quitter Norton Smartphone Security

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.

Planification d'analyses

Les analyses planifiées vérifient automatiquement la présence de virus sur votre périphérique. Les rappels que vous définissez, ainsi que les rappels par défaut, vous invitent à exécuter une analyse.

Vous pouvez activer les analyses planifiées et les configurer selon un intervalle spécifié.

Pour planifier une analyse

- 1 Ouvrez le raccourci **Norton** de votre périphérique.
- 2 En fonction de votre périphérique, effectuez l'une des opérations suivantes :
 - Sélectionnez **Options > Paramètres > AntiVirus > Analyse planifiée**.
 - Sélectionnez **AntiVirus > Paramètres > Analyse planifiée**.
- 3 Dans la boîte de dialogue, parcourez les options jusqu'à ce que l'option souhaitée s'affiche, puis définissez l'heure et la date si nécessaire.

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 3-2](#) détaille les actions automatiques disponibles.

Tableau 3-2 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.
Réparer	Indique s'il est possible ou non d'écarter une menace.
Signaler	Affiche une demande d'action.

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 3-2](#) à la page 28. est effectuée.

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

Pour désactiver temporairement Auto-Protect

- Ouvrez le raccourci **Norton** de votre périphérique.
- En fonction de votre périphérique, effectuez l'une des opérations suivantes :
 - Sélectionnez **Options > Paramètres > AntiVirus > Auto-Protect**.
 - Sélectionnez **AntiVirus > Paramètres > Auto-Protect**.
- Sélectionnez **Désactivé**.

Configuration de la protection par le pare-feu

Norton Smartphone Security inclut des options préconfigurées pour une protection immédiate. Vous pouvez également personnaliser cette protection en précisant le mode de gestion du trafic entrant et sortant sur votre périphérique.

Les options préconfigurées suivantes conviendront à la plupart des utilisateurs :

- Faible (par défaut) : Tous les services sortants sont autorisés ; tous les services entrants sont autorisés.

- **Moyen** : Tous les services sortants sont autorisés ; tous les services entrants sont bloqués.
- **Elevé** : Tous les services sortants communs sont autorisés ; tous les services entrants sont bloqués.

Pour sélectionner une option de pare-feu préconfigurée

- 1 Ouvrez le raccourci **Norton** de votre périphérique.
- 2 En fonction de votre périphérique, effectuez l'une des opérations suivantes :
 - Sélectionnez **Options > Paramètres > Pare-feu**.
 - Sélectionnez **Pare-feu > Paramètres**.
- 3 Dans la boîte de dialogue, sélectionnez le niveau de pare-feu de votre choix.

Désactivation temporaire de la protection par pare-feu

Le pare-feu protège votre périphérique contre les attaques Internet, le contenu Web dangereux, les analyses de ports et autres comportements suspects.

Le pare-feu est activé par défaut. Il est recommandé de conserver ce réglage à tout moment.

Cependant, vous souhaitez peut-être, dans certains cas, désactiver temporairement la protection par pare-feu. Par exemple, vous pouvez vérifier si celui-ci empêche l'affichage d'une page Web.

Remarque : La désactivation du pare-feu annule tous les réglages personnalisés. De plus, le périphérique ne sera plus à l'abri des attaques issues d'Internet.

Pour désactiver la protection par pare-feu

- 1 Ouvrez le raccourci **Norton** de votre périphérique.
- 2 Effectuez l'une des opérations suivantes :
 - Sélectionnez **Options > Paramètres > Pare-feu**.
 - Sélectionnez **Pare-feu > Paramètres**.
- 3 Sélectionnez **Niveau de protection > Aucun**.

Pour activer la protection par pare-feu

- 1 Ouvrez le raccourci **Norton Security** de votre périphérique.
- 2 Effectuez l'une des opérations suivantes :
 - Sélectionnez **Options > Paramètres > Pare-feu**.

- Sélectionnez **Pare-feu > Paramètres**.
- 3 Sélectionnez **Niveau de protection > Faible, Moyen ou Elevé**.

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

Activités du pare-feu

Le périphérique enregistre les activités de pare-feu suivantes :

Connexion TCP sortante bloquée	Une entrée est ajoutée en cas de tentative de connexion TCP sortante bloquée.
Connexion TCP entrante bloquée	Une entrée est ajoutée en cas de tentative de connexion TCP entrante bloquée.
Tentative d'analyse de port	Une entrée est ajoutée en cas de tentative d'analyse de port.

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

- Date
- Heure
- Protocole impliqué (TCP uniquement)
- Direction (sortante/entrante)
- Adresse IP source
- Port source
- Adresse IP de destination
- Port de destination

Remarque : Le nombre d'entrées consignées dans le journal du pare-feu pour une durée spécifiée est limité. Si un nombre important d'événements se produisent dans un court laps de temps, seule une partie de ces événements sera consignée.

Activités de LiveUpdate

Le périphérique enregistre les activités LiveUpdate suivantes :

Mise à 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.

Saturation du journal

Lorsque la taille du Journal d'activités atteint 300 Ko, Norton Smartphone Security libère de l'espace en le compressant. Si la compression du fichier journal ne libère pas suffisamment d'espace, certaines entrées sont supprimées (en commençant par les plus anciennes) jusqu'à ce que la taille soit inférieure à 300 Ko.

A propos de SMS AntiSpam

SMS AntiSpam vous permet de classer les messages SMS entrants en tant que messages indésirables et de les déplacer dans un dossier réservé, le cas échéant. Vous pouvez créer une ou plusieurs règles permettant d'identifier un message SMS répondant à certaines conditions et de prendre les mesures nécessaires, le cas échéant.

L'affichage principal des paramètres AntiSpam est une liste de règles que vous créez. La liste contient le nom que vous avez créé pour chaque règle ainsi qu'une petite icône indiquant l'action de la règle.

La dernière règle correspondant à un message entrant est celle qui s'applique au message. Si aucune règle n'est établie, le message est acheminé dans la boîte de réception.

Tableau 3-3 dresse la liste des options permettant de créer et de modifier les règles.

Tableau 3-3 Options de règles

Options de règles	Description
Ouvrir	Modifier la règle sélectionnée
Nouvelle règle	Ajouter une nouvelle règle
Déplacer vers le haut	Déplacer la règle sélectionnée d'un cran vers le haut de la liste
Déplacer vers le bas	Déplacer la règle sélectionnée d'un cran vers le bas de la liste
Supprimer	Supprimer la règle sélectionnée
Aide	Afficher l'application d'aide pour l'affichage
Quitter	Quitter l'application

Après avoir établi une règle pour un contact, vous pouvez spécifier certains détails pour cette règle. Vous pouvez donner un nom à la règle, définir une condition et spécifier une action si la condition est remplie.

Tableau 3-4 dresse la liste des options de détails que vous pouvez appliquer aux règles que vous avez créées.

Tableau 3-4 Options de détails de règles

Options de détails	Description
Nom	Créer un nom pour la règle.
Condition	<p>Dans les contacts : message provenant de toute personne ou entreprise dans la base de données de contacts.</p> <p>Pas dans les contacts : message provenant de toute personne ou entreprise ne figurant pas dans la base de données de contacts.</p> <p>D'un contact : message d'une personne ou entreprise spécifiée que vous avez sélectionnée à partir de la base de données de contacts.</p> <p>D'un groupe (ou catégorie ou dossier) : message d'une personne ou entreprise spécifiée que vous avez identifiée en tant que groupe dans la base de données de contacts.</p> <p>De partout : message provenant de n'importe quel numéro de téléphone.</p> <p>D'un numéro : message provenant d'un numéro de téléphone que vous spécifiez.</p> <p>Anonyme : le message ne comporte pas de numéro de téléphone.</p> <p>Contient du texte : le message contient du texte que vous spécifiez. Le texte n'est pas sensible à la casse.</p> <p>Sans correspondance : le message ne correspond à aucune règle.</p>
Action	<p>Accepter le message sans aucune action supplémentaire ; il reste dans la boîte aux lettres.</p> <p>Déplacer vers : accepter le message et le déplacer dans le dossier spécifié.</p> <p>Supprimer : supprimer le message.</p>

Configuration des règles et conditions pour SMS AntiSpam

Vous pouvez établir des règles pour les messages SMS et définir des conditions pour chaque règle. Vous pouvez également éditer ou modifier les règles et conditions existantes dans la boîte de dialogue des règles.

Pour configurer les règles et conditions SMS AntiSpam

- 1 Ouvrez le raccourci **Norton** de votre périphérique.
- 2 En fonction de votre périphérique, effectuez l'une des opérations suivantes :

- Sélectionnez **Options > Paramètres > SMS AntiSpam > Options > Nouvelle règle**.
 - Sélectionnez **SMS AntiSpam > Plus > Nouvelle règle**.
- 3 Saisissez le nom, la condition et l'action de la règle dans la boîte de dialogue des détails de la règle.
 - 4 Répétez les étapes 2 et 3 autant de fois que nécessaire pour créer des règles et des conditions.

Correspondance de numéros de téléphone

Le filtre anti-spam compare le numéro de téléphone du message entrant aux numéros de téléphone de la liste de contacts, de droite à gauche. Le processus de comparaison peut mettre plusieurs numéros de téléphone en correspondance. A partir d'une correspondance détectée, la règle AntiSpam est appliquée.

Mise à jour des périphériques

Ce chapitre traite des sujets suivants :

- [Mise à jour des périphériques](#)
- [Planification des mises à jour ou des rappels](#)
- [Mise à jour de l'abonnement au produit](#)

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.

Norton Smartphone Security prend en charge les mises 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.

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.
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 Ouvrez le raccourci **Norton** de votre périphérique.
- 2 En fonction de votre périphérique, effectuez l'une des opérations suivantes :
 - Sélectionnez **Options > Rech. des mises à jour**.
 - Sélectionnez **LiveUpdate > Rech. des mises à jour**.

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 ou des rappels

Les mises à jour planifiées recherchent et installent automatiquement les mises à jour pour chaque composant du périphérique, y compris les fichiers de définitions de virus. Les rappels que vous définissez ainsi que les rappels par défaut vous invitent à vérifier les mises à jour.

Pour planifier les mises à jour

- 1 Ouvrez le raccourci **Norton** de votre périphérique.
- 2 En fonction de votre périphérique, effectuez l'une des opérations suivantes :
 - Sélectionnez **Options > Paramètres > LiveUpdate**.
 - Sélectionnez **LiveUpdate > Paramètres**.
- 3 Dans la boîte de dialogue, parcourez les options jusqu'à ce que l'option souhaitée s'affiche, puis définissez l'heure et la date si nécessaire.

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 Selon votre périphérique, effectuez l'une des opérations suivantes :
 - Sélectionnez **Options > Abonnement**.
 - Sélectionnez **Abonnement** dans le menu principal.
- 3 Sélectionnez **Oui** 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

A

- abonnement, renouvellement 37
- actions, en cas de menace 27
- Activation, protection par pare-feu 29
- Analyse
 - mise à jour 35
 - planification 27
- AntiSpam
 - configuration 32
 - règle 32
 - règle, détails 32
- Auto-Protect 27–28

C

- configuration requise 21
- correctif 35

D

- Définitions de virus, fichier 35
- Demander, action en cas de menace 27
- dépannage
 - site Web de support technique Symantec 19
- Désactivation, protection par pare-feu 29
- Désinstallation 24

E

- EICAR, fichier de test 23
- événement antivirus 30
- événement de journal 30
- Événement, journal
 - complet 30
 - partiel 30
- événements de pare-feu 30

I

- informations sur la version 26
- Installation
 - Norton Smartphone Security 22
- installation 21
 - désinstallation 24

- test 23

- Internet, site Web de support technique Symantec 19

J

- Journal d'activités 19
 - à propos 19
 - activités du pare-feu 30
 - événement 30
- Journal, événement de fichier 30

L

- LiveUpdate
 - activités 31
 - événement 30
 - Paramètres de proxy 36
 - planification 36

M

- Menaces, journal 30
- mise à jour
 - à propos 19
 - définitions de virus, fichier 19
 - logiciel 19
- mise à jour logicielle 35
- Mise à niveau, Norton Smartphone Security 23
- Mises à jour
 - définitions de virus, fichier 36
 - logiciel 35
 - moteur d'analyse 35
 - périphérique 35
 - planification 36

N

- Norton Smartphone Security
 - désinstallation 24
 - informations sur la version 26
 - installation 22
 - installation, test 23
 - lancement 25

option 26

Numéros de téléphone, correspondance 34

P

Périphérique

conditions requises 21

mise à jour 35

port

à propos des tentatives d'analyse 18, 31

Ports

Port de destination 31

Port source 31

Protection par pare-feu

activation 29

consignation des activités 30

désactivation 29

par défaut 28

personnalisation 28

préconfigurée 28

protection par pare-feu

configuration 28

désactivation 29

Q

Quarantaine

action en cas de menace 27

événement 30

R

Refuser l'accès, action en cas de menace 27

renouvellement de l'abonnement 37

Réparer, action en cas de menace 27

S

sécurité 25

Service

autorisés 28

bloqués 28

entrants 28

services

autorisés 28

site Web de support technique Symantec 19

Site Web, support technique Symantec 19

Supprimer, action en cas de menace 27

Symantec Security Response 19, 35

V

Virus, consignation des activités antivirus 19

Vue principale, options 26