

Norton™ Security

Manuel du produit



Prenons soin de notre environnement.

Nous avons décidé de supprimer la couverture de ce manuel afin de réduire l'empreinte écologique de nos produits. Ce manuel est constitué à partir de matériaux recyclés.

Manuel du produit Norton™ Security

Le logiciel décrit dans ce manuel est fourni dans le cadre d'un contrat de licence et ne peut être utilisé qu'en accord avec les conditions de ce contrat.

Documentation version 22.0

Copyright © 2014 Symantec Corporation. Tous droits réservés.

Symantec, le logo Symantec, LiveUpdate, Norton 360 et Norton sont des marques commerciales ou déposées de Symantec Corporation ou de ses sociétés affiliées aux Etats-Unis et dans d'autres pays. Copyright sur les parties de ce produit 1996-2011 Glyph & Cog, LLC. Les autres noms peuvent être des marques de leurs détenteurs respectifs.

Le produit décrit dans ce document est distribué aux termes d'une licence limitant son utilisation, sa copie, sa distribution et sa décompilation/ingénierie inverse. Ce document ne peut, en tout ou partie, être reproduit sous aucune forme et par aucun moyen sans l'autorisation préalable écrite de Symantec Corporation et de ses concédants éventuels.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTE GARANTIE OU CONDITION D'AUCUNE SORTE, EXPRESSE OU IMPLICITE, Y COMPRIS, SANS QUE CELA SOIT LIMITATIF, LES GARANTIES OU CONDITIONS IMPLICITES DE QUALITE MARCHANDE, D'ADEQUATION A UN USAGE PARTICULIER OU DE RESPECT DES DROITS DE PROPRIETE INTELLECTUELLE EST REFUTEE, EXCEPTÉ DANS LA MESURE OÙ DE TELLES EXCLUSIONS SERAIENT TENUES POUR LEGALEMENT NON VALIDES. 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 PRESENTES DANS CETTE DOCUMENTATION SONT SUJETTES A DES MODIFICATIONS SANS PREAVIS.

Le logiciel et la documentation sous licence sont considérés respectivement comme "logiciel informatique commercial", selon les définitions de la section FAR 12.212 et soumis aux restrictions spécifiées dans les sections FAR 52.227-19, "Commercial Computer Software - Restricted Rights" et DFARS 227.7202, et sections suivantes "Commercial Computer Software and Commercial Computer Software Documentation", comme applicable, et à toute réglementation ultérieure. Toute utilisation, modification, reproduction, représentation ou divulgation du logiciel ou de la documentation par le gouvernement des Etats-Unis ne pourra se faire que conformément au présent Contrat.

Symantec Corporation
350 Ellis Street,
Mountain View, CA 94043

<http://www.symantec.fr>

Imprimé en République tchèque.

10 9 8 7 6 5 4 3 2 1

Table des matières

Chapitre 1	Prise en main	8
	L'activation : gage de protection	8
	A propos de la fenêtre principale de Norton Security	12
	Connexion à votre compte Norton	19
	A propos de Norton Bootable Recovery Tool	21
	Démarrage de Norton Security à partir de l'invite de commande	31
	Réaction face aux indicateurs d'état de sécurité	32
	A propos de Norton LiveUpdate	36
	Configuration des paramètres de proxy réseau	43
Chapitre 2	Contrôle des performances de votre système	45
	A propos de Diagnostic du système	45
	Rapport sur 30 jours	78
Chapitre 3	Protection des fichiers et des données	81
	A propos de la protection permanente	81
	A propos des analyses de Norton Security	82

Chapitre 4	Réponse aux problèmes de sécurité	126
	Maintenir votre ordinateur sécurisé	126
	A propos de la résolution des problèmes de connexion	128
	A propos de la réaction aux urgences	128
	Mesures à prendre en cas de détection d'un virus	130
Chapitre 5	Exécution de tâches de routine	143
	Activation ou désactivation des tâches automatiques	143
	Exécution de tâches personnalisées	144
	Planification des analyses de sécurité et de performances	145
	Indication de la durée du délai d'inactivité	147
Chapitre 6	Protection des activités sur Internet	149
	A propos du pare-feu intelligent	150
	Désactivation et activation de la protection du navigateur	184
	Désactivation ou activation du diagnostic des téléchargements	185
	Configuration de l'option Notifications sur le Diagnostic des téléchargements	187
	Configurer l'option Afficher le rapport au lancement des fichiers	188
	Désactivation ou activation des notifications de la prévention d'intrusion	192
	Exclusion ou inclusion des signatures d'attaque dans la surveillance	194
	Activation ou désactivation d'AutoBlock	195
	Déblocage d'ordinateurs bloqués par AutoBlock	196

	Blocage permanent d'un ordinateur qui a été bloqué par AutoBlock	197
	A propos de la liste d'exclusions de la prévention d'intrusion	198
	Retrait de tous les périphériques de la liste d'exclusion de la Prévention d'intrusion	199
	Ajout d'un périphérique à l'approbation du périphérique	201
	Modification du niveau d'approbation de votre réseau et de vos périphériques	203
	A propos des types de risques de sécurité	207
	A propos de Norton AntiSpam	209
	Ajout de ports POP3 et SMTP aux Ports protégés	222
	Suppression d'un port de messagerie électronique des Ports protégés	223
	Désactivation ou activation de la limitation de l'utilisation réseau	224
	Définir l'utilisation de bande passante de Norton Security	225
Chapitre 7	Sécuriser vos données sensibles	228
	A propos de Norton Safe Web	228
	A propos de l'antiphishing	235
	A propos d'Identity Safe	240
	A propos de la barre d'outils Norton	288
	Norton Identity Safe	296
Chapitre 8	Optimisation des performances de votre ordinateur	301
	A propos de la fragmentation du disque et du fichier	301
	Optimisation manuelle de vos disques permanents	302
	A propos de l'utilisation efficace de l'optimisation	303

	A propos du nettoyage de l'encombrement du disque	304
	Exécution d'une analyse pour nettoyer l'encombrement du disque	305
	Exécution du rapport de diagnostic	306
	Gestion des éléments de démarrage	306
	Désactivation ou activation des éléments de démarrage	307
Chapitre 9	Contrôle des fonctions de protection	309
	A propos de l'Historique de la sécurité	309
Chapitre 10	Personnalisation des fonctions de protection	346
	Résumé des fonctionnalités	346
	A propos de la désactivation des fonctions automatiques	350
Chapitre 11	Personnalisation des paramètres	356
	Personnalisation des paramètres de Norton Security	357
	Activation et désactivation des Commandes rapides	358
	A propos des paramètres de la protection automatique	359
	A propos des paramètres Analyses et risques	366
	A propos des paramètres Antispyware et mises à jour	375
	A propos des paramètres de protection contre les intrusions et de protection du navigateur	378
	Activation ou désactivation de la gestion à distance	380
	Réinitialisation du mot de passe des configurations de votre produit Norton	381

	Désactivation du mot de passe des paramètres du produit Norton	382
	Sécurisation des paramètres de votre produit Norton à l'aide d'un mot de passe	383
	A propos de Protection contre les falsifications du produit Norton	385
Chapitre 12	Recherche de solutions supplémentaires	387
	Recherche du numéro de version de votre produit	387
	Accès au contrat de licence d'utilisateur final	388
	A propos de la mise à niveau de votre produit	388
	Résolutions des problèmes avec Norton Autofix	391
	Raisons expliquant l'échec de l'option Corriger	393
	A propos du support	395
	Désinstallation de votre produit Norton	398
Index		404

Ce chapitre traite des sujets suivants :

- [L'activation : gage de protection](#)
- [A propos de la fenêtre principale de Norton Security](#)
- [Connexion à votre compte Norton](#)
- [A propos de Norton Bootable Recovery Tool](#)
- [Démarrage de Norton Security à partir de l'invite de commande](#)
- [Réaction face aux indicateurs d'état de sécurité](#)
- [A propos de Norton LiveUpdate](#)
- [Configuration des paramètres de proxy réseau](#)

L'activation : gage de protection

Le processus d'activation du produit vérifie que vous êtes autorisé à utiliser le logiciel et marque le début de votre abonnement. Il s'assure que la version du produit Norton installée sur votre ordinateur est authentique. Seuls les produits Norton authentiques peuvent recevoir des mises à jour de Symantec et ainsi vous protéger des menaces. L'activation est un processus simple qui vous protège contre les logiciels piratés ou contrefaits. Les logiciels piratés sont des logiciels copiés ou distribués de manière illégale, sans licence légitime.

Vous vous exposez à des risques de virus, de faille de sécurité, de pannes système, et bien plus encore si vous utilisez des logiciels piratés.

Pour activer le produit, vous avez besoin des éléments suivants :

- une licence ou une clé de produit ;
- un compte Norton ;
- une connexion Internet.

Lorsque vous activez Norton Security, vous êtes invité à vous connecter à votre compte Norton. Si vous souhaitez créer un compte ou si vous avez des difficultés pour accéder au compte, Se reporter à "[Connexion à votre compte Norton](#)" à la page 19.

Le compte Norton stocke toutes les licences enregistrées que vous pouvez utiliser avec les produits Norton. Une fois connecté, vous pouvez effectuer l'une des opérations suivantes pour activer le produit :

- Entrez une clé de produit. Pour une assistance sur la localisation de la clé de produit, Se reporter à "[Où trouver la clé ou le code PIN de votre produit ?](#)" à la page 10.
- Utilisez une licence existante pour ce produit. Votre licence est automatiquement enregistrée dans le compte Norton si vous avez acheté le produit dans la Boutique Norton ou si vous avez déjà activé le produit.



Par ailleurs, vous pouvez très facilement transférer une licence d'un appareil vers un autre. Si vous transférez une licence, l'appareil duquel la licence est supprimée n'est plus protégé.

- Achetez un nouvel abonnement.

Des alertes d'activation commencent à s'afficher quelques jours avant la date d'expiration du produit. Si vous n'activez pas le produit dans le délai indiqué dans les alertes, il cesse de fonctionner. Toutefois, vous pouvez procéder à l'activation après ce délai, mais vous

ne bénéficiez pas de la protection tant que cela ne sera pas fait.

Activation de Norton Security

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Activer**.
Vous pouvez également cliquer sur **Activer** dans l'alerte d'activation.
- 2 Si vous y êtes invité, connectez-vous à votre compte Norton en utilisant vos informations d'authentification Norton.
- 3 Effectuez l'une des opérations suivantes :
 - Si vous disposez d'une clé de produit, cliquez sur **Entrez une clé**, tapez la clé de produit et suivez les instructions à l'écran.
 - Si des licences sont disponibles, sélectionnez l'abonnement et suivez les instructions à l'écran.
 - Si vous voulez acheter une licence, cliquez sur **S'abonner**. Vous êtes redirigé vers le site Web de la Boutique Norton où vous pourrez finaliser votre achat.

Où trouver la clé ou le code PIN de votre produit ?

Il existe différentes manières de localiser votre clé de produit selon la façon dont vous avez acheté le produit. La clé de produit est une clé unique dont vous avez besoin pour activer le produit Norton sur votre ordinateur. La clé de produit est une chaîne de 25 caractères alphanumériques, composée de cinq groupes de cinq caractères chacun, séparés par un trait d'union.

Si vous avez acheté le produit auprès d'un fournisseur de services, vous devez disposer d'un code PIN d'activation. Un code PIN est un code alphanumérique à 13 caractères que vous a fourni votre fournisseur de services. Pour localiser votre code PIN, Se reporter à [la section intitulée « Recherche de votre code PIN »](#) à la page 12..

Recherche de votre clé de produit Norton Security

- Si vous avez acheté votre produit Norton dans une boutique Norton ou si votre produit est enregistré sur votre compte Norton, vous pouvez vous connecter à votre compte Norton pour obtenir la clé de produit.
- Si vous avez acheté Norton Security sur un site Web ou un magasin tiers, Se reporter à [la section intitulée « Autres manières de trouver la clé de produit »](#) à la page 11..

Obtention de la clé de produit auprès de Norton

- 1 Connectez-vous au site Web Norton.
- 2 Dans la page qui s'affiche, cliquez sur **Services**.
- 3 Cliquez sur le produit Norton pour lequel vous souhaitez recevoir une clé de produit.
- 4 Notez ou copiez la clé de produit.

Autres manières de trouver la clé de produit

- Si vous avez acheté Norton Security auprès d'un site Web tiers, la clé de produit se trouve dans le message électronique de confirmation de la commande. Si vous ne retrouvez pas le message électronique dans votre boîte de réception, vérifiez le dossier de spam.
- Si vous avez acheté Norton Security dans sa version boîte, la clé de produit est imprimée sur un autocollant au dos de la boîte ou sur une carte à l'intérieur de la boîte.
- Si le produit était préinstallé sur votre appareil, la clé de produit peut se trouver dans le fichier texte sous Program Files > Symantec. Si vous ne trouvez pas le fichier texte, vous pouvez contacter le fabricant de votre appareil afin d'obtenir la clé de produit. Certains fabricants peuvent fournir la clé de produit sur une carte d'activation.

Recherche de votre code PIN

- Votre fournisseur de services peut vous envoyer le code PIN à l'adresse électronique que vous avez spécifiée. Si vous ne retrouvez pas le message électronique, vérifiez votre dossier de spam. Si vous ne parvenez toujours pas à trouver votre code PIN, contactez votre fournisseur de services.
- Vous pouvez également trouver le code PIN dans le dossier **Symantec** sous **Mes documents**.

A propos des problèmes au cours de l'activation

Si vous ne parvenez pas à vous connecter aux serveurs Symantec pour activer le produit, vérifiez d'abord votre connexion Internet. Vous devez ensuite vérifier d'avoir un logiciel de contrôle parental, soit installé ou par votre FAI, susceptible de bloquer la connexion.

Un problème de connexion peut se produire si un logiciel de contrôle parental est utilisé. Si vous pensez que ce logiciel de contrôle parental pourrait bloquer la connexion, configurez-le pour qu'il ne bloque pas la procédure d'activation. Vous devez vous connecter au logiciel de contrôle parental ou à l'Internet via votre ISP en tant qu'administrateur pour modifier votre configuration.

Si vous utilisez un serveur proxy pour vous connecter à Internet, vous devez configurer les paramètres proxy. Pour configurer les paramètres proxy, ouvrez la fenêtre principale de Norton Security, puis cliquez sur **Paramètres > Paramètres administratifs > Paramètres proxy de réseau > Configurer**.

A propos de la fenêtre principale de Norton Security

La fenêtre principale du produit Norton opère comme une interface de gestion de la sécurité. Vous pouvez accéder aux fonctionnalités principales et surveiller les

A propos de la fenêtre principale de Norton Security

performances de votre ordinateur depuis la fenêtre principale.

Pendant que vous utilisez l'ordinateur, le produit Norton surveille la protection de votre ordinateur et de vos activités contre les menaces, les risques et les dommages. Le produit Norton affiche le niveau de protection de votre ordinateur dans la fenêtre principale.

Selon l'état de sécurité de votre ordinateur, le produit Norton affiche l'état **Sécurisé**, **Attention requise** ou **Vulnérable**. Si l'état du système est **Attention** ou **Vulnérable**, cliquez sur **Corriger** au bas de la fenêtre principale pour résoudre toutes les menaces portant sur la sécurité de votre ordinateur.

Les options disponibles dans la fenêtre principale récapitulent les principaux problèmes de sécurité et de productivité que les utilisateurs rencontrent. Elles sont les suivantes :

Sécurité	Inclut toutes les fonctions de sécurité relatives aux virus, spywares et autres.
Identité	Inclut la protection contre le phishing et les sites Web frauduleux.
Performances	Inclut les fonctions d'optimisation des performances, telles que le nettoyage des fichiers indésirables.

Vous pouvez utiliser le lien **Rapport sur 30 jours** en haut de la fenêtre principale pour afficher un résumé de toutes les activités de protection de votre produit Norton au cours des 30 derniers jours.

Vous pouvez utiliser le lien **Paramètres** situé en haut de la fenêtre principale pour accéder à la fenêtre

A propos de la fenêtre principale de Norton Security

Paramètres et configurer les différentes fonctions de votre produit Norton.

Quand vous cliquez sur l'option **Support technique** dans le menu déroulant **Aide**, la fonction Norton Autofix effectue une analyse de votre ordinateur et résout les problèmes automatiquement. Si vous avez besoin de plus d'informations, cliquez sur **Ouvrir le site Web du support technique**, dans la fenêtre **Norton Autofix**, pour accéder au site Web du support technique.

Quand l'état de votre système est **Vulnérable** ou **Attention requise**, cette section affiche automatiquement l'option **Corriger** pour remédier à tous les problèmes en même temps.

A propos de la fenêtre principale de Norton Security

Les options disponibles lorsque vous cliquez deux fois sur **Plus de Norton** vous aident à effectuer les opérations suivantes :

Ajouter des appareils

Permet d'installer la dernière version du produit Norton sur d'autres appareils.

Votre ordinateur et vos autres appareils sont ainsi protégés par Norton.

Vous pouvez utiliser l'option **Ouvrir Norton** pour vous connecter au compte Norton. Pour vous connecter, utilisez les informations d'authentification de votre compte Norton.

Une fois connecté, vous pouvez utiliser les options suivantes :

- **Télécharger Norton** : vous pouvez télécharger le produit Norton sur l'appareil actuel ou sur un autre appareil.

🔑 L'accès au compte Norton peut ne pas être disponible sur certaines versions de Norton Security.

A propos de la fenêtre principale de Norton Security

Family

Permet de surveiller les activités de votre enfant sur Internet.

Norton Family fournit des contrôles avancés permettant de surveiller les activités en ligne de vos enfants.

🔒 Norton Family peut ne pas être disponible sur certaines versions de Norton Security. Dans ce cas, vous ne pouvez pas accéder aux options de Norton Family.

Lorsque vous cliquez sur l'icône **Family**, la fenêtre principale de Norton Security affiche un résumé des fonctions que vous pouvez utiliser pour la sécurité en ligne de votre famille.

Cliquez sur l'option **Inscrivez-vous gratuitement dès maintenant** pour accéder au site Web de Norton Family.

Vous pouvez utiliser les informations de connexion de votre compte Norton pour vous connecter à Norton Family.

Si vous enregistrez votre produit avec votre compte Norton, votre produit vous connecte directement au site Web de Norton Family.

A propos de la fenêtre principale de Norton Security

Studio

Permet d'accéder à Norton Studio.

Norton Studio est une application Windows 8 qui permet de gérer l'ensemble de vos produits et clés de produit Norton à partir d'un seul endroit. Vous pouvez afficher l'état de sécurité de chacun de vos appareils et résoudre les problèmes de sécurité en utilisant Norton Studio où que vous soyez dans le monde. Vous pouvez accéder à l'App Store de Windows 8 pour télécharger et installer Norton Studio.

 Cette option apparaît uniquement dans Windows 8. Cette option peut ne pas être disponible dans certaines versions de Norton Security.

L'état d'activation ou de votre abonnement s'affiche au bas de la fenêtre principale. Vous pouvez utiliser l'option **Activer maintenant** pour activer votre produit Norton ou vous y abonner.

Contrôle de l'état de protection d'une fonction

La fenêtre principale de Norton Security fait office d'interface de gestion de la sécurité. Vous pouvez accéder aux fonctionnalités principales et surveiller les performances de votre ordinateur depuis la fenêtre principale.

Vous pouvez vouloir désactiver des options pour une quelconque raison. Dans ce cas, l'état du système est remplacé par **Attention** ou **Vulnérable**. Vous pouvez ignorer alors l'état de protection d'une fonction pour

A propos de la fenêtre principale de Norton Security

maintenir l'intégrité de l'état de l'ensemble du système. Supposons que vous voulez désactiver la **protection du navigateur** pendant une période limitée en maintenant la **sécurité** du système. Dans ce cas, vous pouvez ignorer l'état **Protection du navigateur** et désactiver l'option. Lorsque vous ignorez l'état de protection d'une fonction, vous n'affectez pas l' **état système** général.

Vous pouvez également contrôler l'état de protection d'une fonction ignorée à tout moment.

Vous pouvez ignorer ou contrôler l'état de protection des fonctions sélectionnées disponibles dans la fenêtre Avancé uniquement.

Ces fonctions sont :

- Antivirus
- Antispyware
- Protection SONAR
- Pare-feu intelligent
- Prévention d'intrusion
- Protection du courrier
- Protection du navigateur
- Navigation sécurisée

Pour contrôler l'état de protection d'une fonction

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Avancé**.
- 2 Dans la fenêtre qui apparaît, placez le pointeur de la souris sur le nom de la fonction.
- 3 Dans la fenêtre contextuelle qui s'affiche, effectuez l'une des opérations suivantes :
 - Pour ignorer l'état de protection de la fonction qui affecte l'évaluation de l'état d'intégrité de votre ordinateur, cliquez sur **Ignorer**.
 - Pour contrôler l'état de protection de la fonction ignorée, cliquez sur **Contrôler**.

Connexion à votre compte Norton

Un compte Norton vous permet d'accéder à diverses offres Norton telles que Norton Security, Norton Family, etc. Vous devrez peut-être vous connecter à votre compte Norton pour effectuer les opérations suivantes sur votre produit Norton :

- Activer votre produit
- Renouveler votre abonnement
- Vérifier l'état de votre abonnement
- Accéder ou créer votre centre de sauvegarde dans le cloud

Le compte Norton vous offre de nombreux avantages, dont :

- la gestion aisée de tous vos produits Norton à partir d'un seul emplacement ;
- la réinstallation facile de vos produits Norton en utilisant les clés de produit stockées dans votre compte ;

Comment puis-je me connecter à mon compte Norton ?

Pour vous connecter, saisissez l'adresse électronique et le mot de passe utilisés lors de l'enregistrement de votre compte Norton. Saisissez l'adresse électronique et le mot de passe dans les champs correspondants, puis cliquez sur **Connexion**.

Si vous restez connecté à votre compte Norton, il n'est pas nécessaire de saisir vos informations d'authentification Norton chaque fois que vous voulez accéder à certaines fonctions.



Si vous avez opté pour la vérification en deux étapes pour accéder à votre compte Norton, vous devez utiliser le code de vérification en plus de votre mot de passe. Pour plus d'informations, reportez-vous à l'article Vérification en deux étapes pour le compte Norton.

J'ai oublié le mot de passe de mon compte Norton

Assurez-vous d'abord d'être connecté à Internet. Vous devez être connecté à Internet pour vous connecter à votre compte Norton. Vérifiez ensuite l'adresse électronique et le mot de passe que vous avez fournis.

Si vous ne pouvez toujours pas vous connecter, procédez aux opérations suivantes :

- 1 Cliquez sur **Mot de passe oublié ?**.
- 2 Saisissez l'adresse électronique utilisée lors de l'enregistrement de votre compte Norton. Norton vous envoie un message électronique à cette adresse pour vous permettre de réinitialiser votre mot de passe.
- 3 Ouvrez le message et cliquez sur le lien **Réinitialiser le mot de passe** pour créer un nouveau mot de passe.

Je ne sais pas si je dispose d'un compte Norton

Si vous avez installé ou activé Norton Security, il est fort probable que vous disposiez d'un compte Norton. Un compte Norton est requis pour installer ou activer Norton Security.

Si vous avez acheté Norton Security depuis la boutique Norton, votre compte Norton a été créé automatiquement.

Si vous vous êtes inscrit à d'autres produits Norton, il est également probable que vous disposiez d'un compte Norton. Assurez-vous toutefois d'utiliser le compte auquel est associée votre licence Norton Security.

Je souhaite créer un compte Norton

Si vous êtes sûr de ne pas avoir de compte Norton, vous pouvez en créer un gratuitement. Vous devez disposer d'une adresse électronique valide. Symantec envoie les mises à jour de produit et d'autres informations liées à votre compte à cette adresse électronique.

Création d'un compte Norton

- 1 Cliquez sur **Inscrivez-vous maintenant !**.
- 2 Saisissez une adresse électronique et un mot de passe valides à associer au compte. Ces informations d'authentification seront nécessaires pour vous connecter à votre compte Norton.
- 3 Choisissez votre région.
- 4 Lisez la politique de confidentialité et acceptez-la.
- 5 Cliquez sur **Procédure d'abonnement**.

A propos de Norton Bootable Recovery Tool

Norton Bootable Recovery Tool analyse et supprime les virus, logiciels espions et autres risques portant sur la sécurité de votre ordinateur. Votre ordinateur est peut-être infecté si vous vous trouvez dans l'une des situations suivantes.

- Vous ne pouvez pas installer Norton Security.
- Vous ne pouvez pas démarrer l'ordinateur.
- L'ordinateur est très lent.

Norton Bootable Recovery Tool est intégré à l'environnement de préinstallation Windows (WinPE). Par conséquent, vous pouvez exécuter Norton Bootable Recovery Tool uniquement à partir d'un DVD ou d'un lecteur USB. Vous devez utiliser l'assistant Norton Bootable Recovery Tool pour créer le DVD ou le lecteur USB Norton Bootable Recovery Tool.



Vous ne pouvez pas exécuter l'outil Norton Bootable Recovery Tool dans WinPE pendant plus de 72 heures. Si vous exécutez l'outil Norton Bootable Recovery pendant plus de 72 heures, votre ordinateur redémarre sans notification.

Vous pouvez utiliser le DVD ou le lecteur USB Norton Bootable Recovery Tool pour récupérer un ordinateur infecté par un virus et d'autres menaces de sécurité. Ce programme de sécurité ne remplace pas la protection continue et en temps réel contre les virus et les risques

de sécurité. Pour protéger votre ordinateur contre les infections futures, veuillez installer ou continuez à utiliser la version de Norton Security que vous avez achetée.

Norton Bootable Recovery Tool détecte et résout les menaces de sécurité suivantes portant sur la sécurité :

Virus	Programmes qui infectent d'autres programmes, les zones de démarrage, les secteurs de partition ou les documents ou s'insérant dans ces éléments ou en s'y attachant. La plupart des virus ne font que se répliquer, mais bon nombre d'entre eux occasionnent des dégâts.
Chevaux de Troie	Programmes contenant des codes malicieux qui sont déguisés ou cachés dans un élément bénin, tel qu'un jeu ou un utilitaire.
Outils de piratage	Outils utilisés par un pirate pour obtenir un accès non autorisé à votre ordinateur. Parmi les différents outils de piratage existants, les enregistreurs de frappe enregistrent automatiquement les frappes individuelles et renvoient ces informations au pirate.
Logiciels espions	Programmes qui analysent les systèmes ou surveillent les activités et relayent ces informations vers un autre ordinateur.

Logiciels publicitaires	Programmes facilitant la diffusion de contenu publicitaire dans leur propre fenêtre ou en utilisant l'interface d'un autre programme.
Logiciels de suivi	Programmes qui analysent les activités des systèmes, collectent des informations ou observent les habitudes de l'utilisateur puis relayent ces informations vers d'autres organisations. Les informations collectées par ces programmes ne sont ni personnelles ni confidentielles. Les programmes de suivi sont installés avec l'accord de l'utilisateur et peuvent également accompagner d'autres logiciels installés par l'utilisateur.

Télécharger l'assistant Norton Bootable Recovery Tool

Si votre tentative d'installation d'un produit Norton ne réussit pas, téléchargez l'assistant Norton Bootable Recovery Tool. Cet assistant simple d'utilisation vous aide à créer l'outil Norton Bootable Recovery Tool sur un DVD ou lecteur USB. Utilisez l'outil de récupération au démarrage Norton pour analyser votre ordinateur et supprimer les menaces de sécurité qui empêchent la réussite de l'installation.

Il est recommandé de télécharger et installer l'assistant de l'outil de récupération au démarrage Norton sur un ordinateur ne comportant aucune menace de sécurité et de créer l'outil de récupération au démarrage Norton. Si vous créez l'outil Norton Bootable Recovery Tool sur

un ordinateur infecté, le DVD ou lecteur USB de récupération risque d'être également infecté.

Vous pouvez désinstaller l'assistant Norton Bootable Recovery Tool de votre ordinateur de l'une des manières suivantes :

- A partir du menu **Démarrer**.
- A partir du site Web du support Norton.

Téléchargement de l'assistant Norton Bootable Recovery Tool à partir du menu Démarrer

- 1 Effectuez l'une des opérations suivantes :
 - Sous Windows XP, cliquez sur **Démarrer > Programmes > Norton Security > Norton Recovery Tools**.
 - Sous Windows Vista ou Windows 7, cliquez sur **Démarrer > Tous les programmes > Norton Security > Norton Recovery Tools**.
 - Sous Windows 8, vous pouvez télécharger l'assistant Norton Bootable Recovery Tool à partir du site Web du support Norton.
- 2 Suivez les instructions à l'écran.

Téléchargement de l'assistant Norton Bootable Recovery Tool à partir d'Internet

- 1 Ouvrez votre navigateur et accédez à l'URL suivante :
<http://www.norton.com/recoverytool>
- 2 Suivez les instructions à l'écran.

Création du Norton Bootable Recovery Tool sur un DVD

Norton Bootable Recovery Tool est intégré à l'environnement de préinstallation Windows (WinPE). Par conséquent, vous pouvez exécuter Norton Bootable Recovery Tool uniquement à partir d'un DVD ou d'un lecteur USB. Pour l'utiliser, vous devez d'abord le graver sur un DVD.



Si vous choisissez de créer Norton Bootable Recovery Tool sur un DVD réinscriptible, toutes les données stockées sur le DVD seront définitivement supprimées. Veillez à effectuer la sauvegarde de toutes les données avant la création de Norton Bootable Recovery Tool sur un DVD réinscriptible.

Création d'un DVD Norton Bootable Recovery Tool

- 1 Ouvrez votre lecteur DVD et insérez un DVD vierge.
- 2 Dans la fenêtre principale **Norton Bootable Recovery Tool**, cliquez sur **DVD**.
- 3 Dans la fenêtre **Créer sur un média DVD**, effectuez l'une des opérations suivantes :
 - Sélectionnez le lecteur DVD dans la liste déroulante **Spécifier le lecteur**.
 - Si vous souhaitez ajouter des pilotes, cliquez sur **Ajouter** à côté de **Ajouter des pilotes**.
 - Si vous souhaitez modifier la langue par défaut, cliquez sur **Modifier** à côté de **Spécifier la langue**. Vous pouvez modifier la langue dans la fenêtre **Sélectionnez une langue**. Par défaut, Norton Bootable Recovery Tool est créé en anglais.
- 4 Cliquez sur **Suivant**.
- 5 Si vous souhaitez créer l'outil Norton Bootable Recovery Tool sur un DVD réinscriptible, cliquez sur **Oui** pour confirmer.
- 6 Passez les résultats en revue et effectuez l'une des opérations suivantes :
 - Cliquez sur **Terminé** pour fermer Norton Bootable Recovery Tool.
 - Cliquez sur **Retour au menu principal** pour créer ou mettre à jour Norton Bootable Recovery Tool sur un autre média.

Création du fichier ISO Norton Bootable Recovery Tool

Vous pouvez créer un fichier ISO Norton Bootable Recovery Tool sur votre ordinateur. Vous pouvez graver

ce fichier ISO sur un DVD et l'utiliser en tant que DVD de récupération sur votre ordinateur. Vous pouvez également utiliser ce fichier ISO pour renvoyer vers un ordinateur virtuel en tant que DVD-ROM virtuel.

Création d'un fichier ISO Norton Bootable Recovery Tool

- 1 Dans la fenêtre principale **Assistant Norton Bootable Recovery Tool**, cliquez sur **Fichier ISO**.
- 2 Dans la fenêtre **Créer un fichier ISO**, procédez comme suit :
 - Si vous souhaitez enregistrer le fichier ISO à un emplacement spécifique, cliquez sur **Modifier** à côté de **Sélectionner l'emplacement**.
Vous pouvez parcourir et sélectionner l'emplacement du dossier.
 - Si vous souhaitez ajouter des pilotes, cliquez sur **Ajouter** à côté de **Ajouter des pilotes**.
 - Si vous souhaitez modifier la langue par défaut, cliquez sur **Modifier** à côté de **Spécifier la langue**.
Vous pouvez modifier la langue dans la fenêtre **Sélectionnez une langue**. Par défaut, Norton Bootable Recovery Tool est créé en anglais.
- 3 Cliquez sur **Suivant**.
- 4 Passez les résultats en revue et effectuez l'une des opérations suivantes :
 - Cliquez sur **Terminé** pour fermer Norton Bootable Recovery Tool.
 - Cliquez sur **Retour au menu principal** pour créer ou mettre à jour Norton Bootable Recovery Tool sur un autre média.

Création de Norton Bootable Recovery Tool sur un lecteur USB

Vous pouvez créer Norton Bootable Recovery Tool sur un lecteur USB et utiliser ce dernier pour exécuter Norton Bootable Recovery Tool sur votre ordinateur.

Lorsque vous créez Norton Bootable Recovery Tool sur un lecteur USB, toutes les données stockées sur ce lecteur sont définitivement supprimées et le lecteur USB est formaté. Veillez à effectuer la sauvegarde de toutes les données avant la création de Norton Bootable Recovery Tool sur un lecteur USB.

Création de Norton Bootable Recovery Tool sur un lecteur USB

- 1 Insérez le lecteur USB dans le port USB de votre ordinateur.
- 2 Dans la fenêtre principale **Assistant Norton Bootable Recovery Tool**, cliquez sur **Clé USB**.
- 3 Dans la fenêtre **Créer sur une clé USB**, procédez comme suit :
 - Sélectionnez le lecteur USB à partir de la liste déroulante **Spécifier le lecteur**.
 - Si vous souhaitez ajouter des pilotes, cliquez sur **Ajouter** à côté de **Ajouter des pilotes**.
 - Si vous souhaitez modifier la langue par défaut, cliquez sur **Modifier** à côté de **Spécifier la langue**.

Vous pouvez modifier la langue dans la fenêtre **Sélectionnez une langue**. Par défaut, Norton Bootable Recovery Tool est créé en anglais.
- 4 Cliquez sur **Suivant**.
- 5 Dans le message de confirmation, cliquez sur **Oui** pour que Norton Bootable Recovery Tool formate le lecteur USB avant de créer Norton Bootable Recovery Tool.
- 6 Passez les résultats en revue et effectuez l'une des opérations suivantes :
 - Cliquez sur **Terminé** pour fermer Norton Bootable Recovery Tool.
 - Cliquez sur **Retour au menu principal** pour créer ou mettre à jour Norton Bootable Recovery Tool sur un autre média.

Accès à l'assistant Norton Bootable Recovery Tool

Norton Bootable Recovery Tool est intégré à l'environnement de préinstallation Windows (WinPE). Par conséquent, vous pouvez exécuter Norton Bootable Recovery Tool uniquement à partir d'un DVD ou d'un lecteur USB.

L'assistant Norton Bootable Recovery Tool vous permet de créer l'outil Norton Bootable Recovery Tool. Vous pouvez créer l'outil Norton Bootable Recovery Tool sur un DVD ou un lecteur USB. Vous pouvez utiliser ce média pour exécuter l'outil Norton Bootable Recovery Tool sur votre ordinateur.

Vous pouvez vous connecter à votre compte Norton et accéder au lien de téléchargement de l'outil Norton Bootable Recovery Tool.

Pour accéder à votre compte Norton, rendez-vous à l'adresse suivante :

<https://account.norton.com>

Accès à l'assistant Norton Bootable Recovery Tool

- 1 Effectuez l'une des opérations suivantes :
 - Cliquez deux fois sur l'icône de l'assistant Norton Bootable Recovery Tool sur le Bureau.
 - Sous Windows XP, Windows Vista et Windows 7, dans la barre des tâches Windows, cliquez sur **Démarrer > Tous les programmes > Assistant Norton Bootable Recovery Tool > Assistant Norton Bootable Recovery Tool**.
 - Sous Windows 8, vous pouvez accéder à l'assistant Norton Bootable Recovery Tool à partir du site Web du support Norton.
- 2 Suivez les instructions à l'écran pour télécharger l'assistant Norton Bootable Recovery Tool.

Utilisation de l'outil Norton Bootable Recovery Tool

Si l'installation de votre produit Norton échoue, utilisez l'Outil de récupération au démarrage Norton pour

A propos de Norton Bootable Recovery Tool

analyser et supprimer les menaces de sécurité qui empêchent la réussite de l'installation. Si votre ordinateur est infecté et vous n'êtes pas en mesure de démarrer le système d'exploitation Windows, l'Outil de récupération au démarrage Norton vous permet de supprimer les menaces et de rétablir ainsi votre ordinateur.

L'outil de récupération au démarrage Norton est disponible sur le CD du produit que vous avez acheté. Utilisez ce CD de produit comme média de récupération.

Si vous avez acheté ce produit sous format téléchargeable, accédez à l'URL suivante pour télécharger l'assistant Norton Bootable Recovery Tool :

http://www.norton.com/fr/recoverytool_n360

Norton Bootable Recovery Tool télécharge automatiquement les définitions de virus les plus récentes à partir des serveurs Symantec et les utilise pour protéger votre ordinateur contre tous les types de virus et les dernières menaces de sécurité. Si Dynamic Host Configuration Protocol (DHCP) est activé, des définitions de virus sont automatiquement mises à jour lorsque votre ordinateur est connecté à Internet. Vous devez donc utiliser une connexion Ethernet pour mettre à jour les définitions de virus dans Norton Bootable Recovery Tool. Vous ne pouvez pas mettre à jour les définitions de virus de Norton Bootable Recovery Tool en utilisant une connexion réseau sans fil.

Si les définitions de virus sont périmées, Norton Bootable Recovery Tool peut ne pas être en mesure de détecter et de supprimer toutes les menaces de sécurité les plus récentes présentes sur votre ordinateur.

Utilisation de l'outil Norton Bootable Recovery Tool

- 1 Insérez le média de récupération Norton Bootable Recovery Tool.

- 2 Démarrez ou redémarrez votre ordinateur en mode BIOS.
Vous pouvez accéder au mode BIOS en appuyant sur la touche indiquée à l'écran immédiatement après le redémarrage de l'ordinateur.
- 3 Sélectionnez le média de récupération sur lequel vous avez créé l'outil Norton Bootable Recovery Tool, puis appuyez sur **Entrée**.
Si votre ordinateur est compatible UEFI, sélectionnez le média de récupération via l'option **Legacy Boot** plutôt que l'option **UEFI Boot**.
Le média de récupération peut être le DVD ou le lecteur USB Norton Bootable Recovery Tool.
- 4 Lisez le **contrat de licence Norton**, puis cliquez sur **J'accepte**.
- 5 Dans la fenêtre **Norton Bootable Recovery Tool**, cliquez sur **Norton Advanced Recovery Scan**.
- 6 Dans la section **Analyse**, cliquez sur **Lancer l'analyse**.
A la fin de l'analyse, la fenêtre des résultats répertorie les éléments suivants.
 - Le nombre total de fichiers analysés
 - Le nombre total de menaces détectées
 - Le nombre total de menaces corrigées
 - Le nombre total de menaces non traitées
 - Les détails de chaque menace détectée
- 7 Dans la fenêtre des résultats de l'analyse, effectuez l'une des opérations suivantes :
 - Pour réparer toutes les menaces détectées sur votre ordinateur, sélectionnez **Définir toutes les actions à Réparer**.
 - Pour effectuer des actions appropriées pour chacune des menaces, sélectionnez **Réparer** ou **Ignorer**.
- 8 Cliquez sur **Continuer**.
- 9 Cliquez sur **OK** si une boîte de dialogue de confirmation s'affiche.

Démarrage de Norton Security à partir de l'invite de commande

10 Dans la fenêtre **Résumé de l'analyse**, affichez le résumé de l'analyse et effectuez l'une des opérations suivantes :

- Cliquez sur **Terminé**.
- Pour exécuter une autre analyse, cliquez sur **Nouvelle analyse**.

Mise à jour des définitions de virus sur un lecteur USB

Les définitions de virus Symantec sont utilisées dans l'outil Norton Bootable Recovery Tool pour analyser votre ordinateur et rechercher les risques de sécurité les plus récents. Lorsque vous créez Norton Bootable Recovery Tool sur un lecteur USB, les dernières définitions de virus sont automatiquement téléchargées et incluses dans le lecteur USB. Vous pouvez mettre à jour les définitions de virus dans Norton Bootable Recovery Tool sur un lecteur USB créé précédemment.

Mise à jour des définitions de virus de Norton Bootable Recovery Tool sur un lecteur USB

- 1 Insérez votre lecteur USB Norton Bootable Recovery Tool dans le port USB de votre ordinateur.
- 2 Dans la fenêtre principale **Assistant Norton Bootable Recovery Tool**, cliquez sur **Mettre à jour les définitions de clé USB**.
- 3 Dans la fenêtre **Mettre à jour les définitions sur la clé USB**, à partir de la liste déroulante **Spécifier le lecteur**, sélectionnez le **lecteur USB**.
- 4 Cliquez sur **Suivant**.
- 5 Consultez les résultats et cliquez sur **Terminé**.

Démarrage de Norton Security à partir de l'invite de commande

Si vous travaillez à partir de la ligne de commande (par exemple, si vous écrivez un script ou un code), vous pouvez démarrer Norton Security sans quitter le DOS.

Pour démarrer Norton Security à partir de l'invite de commande

- 1 A l'invite de la ligne de commande, saisissez le répertoire d'installation de Norton Security et le fichier exécutable.
 - Dans la version 32 bits de Windows, Norton Security et l'exécutable figurent dans le chemin d'accès suivant :


```
\Program Files\Norton Security\Engine\version\Uistub.exe
```

 Où *version* représente le numéro de version de Norton Security installé.
 - Dans la version 64 bits de Windows, Norton Security et l'exécutable figurent dans le chemin d'accès suivant :


```
\Program Files (x86)\Norton Security\Engine64\version\Uistub.exe
```

 Où *version* représente le numéro de version de Norton Security installé.
- 2 Appuyez sur la touche **Entrée**.

Réaction face aux indicateurs d'état de sécurité

Le produit Norton affiche l'état de sécurité de votre ordinateur dans la section **Sécurité** de la fenêtre principale. Selon l'état de sécurité de votre ordinateur, le produit Norton affiche l'état **Protégé**, **Attention** ou **Vulnérable**.

L'indicateur d'état du système affiche un des états suivants :

Protégé	Indique que votre ordinateur est protégé contre les menaces, les risques et les dommages.
----------------	---

Réaction face aux indicateurs d'état de sécurité

<p>Attention</p>	<p>Indique que votre ordinateur nécessite de l'attention.</p> <p>Au bas de la fenêtre principale du produit Norton, cliquez sur Corriger pour résoudre les menaces portant sur la sécurité de votre ordinateur.</p>
<p>Vulnérable</p>	<p>Indique que votre ordinateur est vulnérable.</p> <p>Au bas de la fenêtre principale du produit Norton, cliquez sur Corriger pour résoudre les menaces portant sur la sécurité de votre ordinateur.</p>

Le produit Norton affiche l'état de sécurité individuel de chaque catégorie de protection, telle que Sécurité, Identité et Performances. Selon l'état de sécurité des différents composants de votre ordinateur, les zones d'état des trois catégories de protection sont marquées comme **Protégé**, **Attention** ou **Vulnérable**.

Si l'état du système ou les états des catégories sont sur **Vulnérable** ou **Attention**, cliquez sur **Corriger** au bas de la fenêtre du produit Norton pour résoudre toutes les menaces portant sur la sécurité de votre ordinateur.

Si l'état du système ou les états des catégories sont sur **Vulnérable** ou **Attention**, vous pouvez résoudre les problèmes liés à la sécurité directement dans la fenêtre principale.

Réponse aux indicateurs d'état de sécurité

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Corriger**.
- 2 Suivez les instructions à l'écran.

A propos de l'icône du produit Norton

Lorsque vous installez le produit Norton, une icône est placée dans la zone de notification, sur la droite de la barre des tâches. Cette icône indique l'état de sécurité actuel de votre ordinateur. Le produit Norton affiche une icône animée lorsqu'il corrige activement des problèmes ou souhaite vous informer d'avertissements ou de problèmes urgents.

Vous pouvez voir les icônes du produit Norton suivantes dans la zone de notification :

Icône sous forme de badge vert avec une marque de pointage	Indique que votre ordinateur est parfaitement protégé.
Icône sous forme de badge orange avec un point d'exclamation	Indique que des problèmes de protection de votre ordinateur existent et nécessitent votre attention.
Icône sous forme de badge rouge avec une croix	Indique que des problèmes urgents de protection de votre ordinateur existent et nécessitent une correction immédiate.
Icône dotée d'un cercle gris	Indique que la fonction Mode silencieux est activée. Cette icône affiche également le badge de l'état de protection actuelle.

Vous pouvez cliquer avec le bouton droit sur l'icône afin d'afficher un menu de raccourci pour les activités du produit Norton. Vous pouvez choisir des options dans le menu de raccourci permettant d'ouvrir la fenêtre du produit Norton, de corriger les problèmes détectés par le produit Norton ou d'obtenir une aide supplémentaire.

A propos du menu de raccourcis du produit Norton

Le produit Norton fonctionne en arrière-plan afin d'assurer la sécurité de votre PC. L'icône du produit Norton est disponible dans la zone de notification, sur la droite de la barre des tâches. L'icône vous confirme que votre protection est à jour. Elle change de couleur en cas de changement de l'état de la protection.

Des messages s'affichent dans la zone de notification et peuvent nécessiter une intervention de votre part, pour ouvrir une fenêtre par exemple. Généralement, les messages vous informent des activités en cours d'exécution et disparaissent après quelques secondes.

Vous pouvez effectuer un clic droit sur l'icône de **Norton Security** afin d'accéder à des activités spécifiques. Selon les activités en cours, les options disponibles peuvent être les suivantes :

Ouvrir Norton Security.	Cette option permet d'ouvrir la fenêtre principale du produit Norton afin d'effectuer des tâches, d'afficher l'état en cours ou d'accéder à d'autres fonctionnalités.
Exécuter l'analyse rapide	Cette option permet d'exécuter une analyse rapide afin de protéger des zones de votre ordinateur susceptibles d'être infectées par un virus.
Exécuter LiveUpdate	Cette option permet d'exécuter LiveUpdate pour rechercher les mises à jour des définitions et du programme.

Afficher l'historique récent	Cette option permet de passer en revue les informations sur les événements de sécurité de toutes les catégories.
Support technique	Cette option vous permet de résoudre votre problème facilement avec Norton Autofix.
Activer/Désactiver le mode silencieux	Cette option permet d'activer ou de désactiver le mode silencieux.
Activer/Désactiver le pare-feu intelligent	Cette option permet d'activer ou de désactiver le pare-feu.
Activer/Désactiver Antivirus Auto-Protect	Cette option permet d'activer ou de désactiver Antivirus Auto-Protect.

A propos de Norton LiveUpdate

Les produits Symantec téléchargent les mises à jour de protection les plus récentes à partir du serveur Symantec. Les mises à jour de protection protègent votre ordinateur contre les derniers virus et menaces de sécurité inconnues. Avec la technologie LiveUpdate, les produits Symantec vous aident à obtenir et installer ces mises à jour.

Lorsque LiveUpdate s'exécute, il détermine si votre produit Norton est à jour en termes de protection. Si le produit ne possède pas les dernières mises à jour, LiveUpdate télécharge les mises à jour de protection nécessaires à votre appareil, traite les mises à jour, puis supprime les fichiers et les définitions plus anciens du dossier temporaire.

LiveUpdate permet de télécharger et de traiter les mises à jour de protection rapidement. Vous pouvez toutefois annuler la session LiveUpdate à tout moment.

Votre appareil doit être connecté à Internet pour obtenir ces mises à jour. Si votre réseau utilise des serveurs proxy pour se connecter à Internet, LiveUpdate utilise les paramètres proxy de votre produit pour télécharger les dernières mises à jour. Vous pouvez utiliser l'option **Paramètres proxy de réseau** de la fenêtre **Paramètres administratifs** pour configurer les paramètres proxy de votre réseau.

Un problème de connexion peut se produire si un logiciel de contrôle parental est utilisé. Si vous pensez que ce logiciel de contrôle parental pourrait bloquer la connexion, configurez-le pour qu'il ne bloque pas la procédure d'activation. Vous devez vous connecter à votre logiciel de contrôle parental ou à Internet par le biais de votre FAI en tant qu'administrateur pour modifier votre configuration.



LiveUpdate ne peut pas fonctionner si l'option **Limitation de l'utilisation réseau** de la fenêtre **Pare-feu** sous **Paramètres** est définie sur **Aucun trafic** ou **Economie**. L'option Limitation de l'utilisation réseau permet d'établir la quantité de bande passante réseau que Norton Security peut utiliser. Par conséquent, vous devez vous assurer que l'option **Limitation de l'utilisation réseau** est activée et définie sur **Aucune limite** pour que LiveUpdate s'exécute.

La fenêtre **Limitation de l'utilisation réseau** s'affiche lorsque vous exécutez LiveUpdate et que la politique est définie sur **Aucun trafic** ou **Economie**. Vous pouvez toutefois remplacer la politique et mener à bien la tâche LiveUpdate.

A propos des mises à jour de la protection

Les mises à jour de la protection sont des fichiers qui maintiennent votre produit Norton à jour avec les technologies de protection contre les menaces les plus récentes. De nouveaux virus et de nouvelles menaces

peuvent apparaître chaque jour, c'est pourquoi le fait de maintenir votre produit Norton à jour permet de protéger votre appareil contre les dernières menaces. Votre produit Norton utilise la technologie LiveUpdate pour obtenir les mises à jour de protection pour votre appareil en contactant le serveur Symantec. LiveUpdate automatise le téléchargement et l'installation des mises à jour de la protection. Pour plus d'informations, Se reporter à "[A propos de Norton LiveUpdate](#)" à la page 36..

Pour assurer votre sécurité, Symantec vous recommande d'installer la version la plus récente de votre produit Norton et de télécharger les fichiers de protection les plus récents. Pour plus d'informations, Se reporter à "[A propos de la mise à niveau de votre produit](#)" à la page 388..

Pour obtenir des mises à jour de la protection, votre abonnement à Norton Security doit être actif. Si votre abonnement arrive à expiration, votre produit ne peut obtenir aucune mise à jour de la protection.

Les mises à jour de la protection comprennent des mises à jour des définitions et du programme. Les mises à jour de programme sont des améliorations mineures apportées à votre produit Norton déjà installé. Elles diffèrent des mises à niveau de produit, qui installent une nouvelle version d'un produit entier. Les mises à jour de programme sont généralement destinées à étendre les possibilités du système d'exploitation ou la compatibilité du matériel, à résoudre un problème de performances ou à corriger une erreur. Les mises à jour de programme sont publiées en fonction des besoins.



Certaines mises à jour de la protection peuvent nécessiter un redémarrage de votre ordinateur afin de terminer la mise à jour.

Les mises à jour des définitions sont des fichiers qui assurent votre protection contre les virus et les menaces émergentes. Les mises à jour des définitions comprennent les éléments suivants :

- Définitions de virus – Identifie les virus qui attaquent votre appareil.
- Règles de pare-feu prédéfinies – Contrôle le trafic et l'accès réseau des programmes sur votre appareil.
- Signatures de prévention d'intrusion – Identifie les tentatives d'accès non autorisé à votre appareil.
- Fichiers de définitions de spam Symantec – Identifie les spams parmi les messages électroniques que vous recevez.

Désactivation et activation de LiveUpdate automatique

LiveUpdate peut vérifier automatiquement la disponibilité de nouvelles mises à jour de protection si vous activez l'option **LiveUpdate automatique**. Ainsi, votre produit Norton se maintient à jour sans que vous deviez intervenir. Si cette option est désactivée, vous devez exécuter LiveUpdate à intervalles réguliers pour obtenir les dernières mises à jour de la protection.

Vous disposez des options suivantes :

- [Configuration de LiveUpdate automatique via Commandes rapides](#)
- [Configuration de LiveUpdate automatique à partir des Paramètres](#)



Si vous êtes connecté à Internet, LiveUpdate automatique télécharge les mises à jour des définitions et du produit toutes les heures. Si vous avez un routeur RNIS configuré pour se connecter automatiquement à votre fournisseur d'accès Internet (FAI), chacune de ses connexions pourra occasionner des frais téléphoniques. Si vous ne voulez pas de cette configuration, vous pouvez désactiver la connexion automatique de votre routeur RNIS ou désactiver l'option **LiveUpdate automatique**. Vous pouvez définir la quantité de bande passante utilisée par Norton Security à l'aide de l'option **Limitation de l'utilisation réseau**.

Configuration de LiveUpdate automatique via Commandes rapides

- 1 Dans la fenêtre principale Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Commandes rapides**, effectuez l'une des opérations suivantes :
 - Pour désactiver LiveUpdate automatique, désélectionnez la case **LiveUpdate automatique**, et dans la liste déroulante **Sélectionner la durée**, sélectionnez la durée pour laquelle vous voulez désactiver la fonction LiveUpdate automatique, puis cliquez sur **OK**.
 - Pour activer LiveUpdate automatique, sélectionnez l'option **LiveUpdate automatique**.

Configuration de LiveUpdate automatique à partir des Paramètres

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antivirus**.
- 3 Dans l'onglet **Antispyware et mises à jour**, sous **Mises à jour**, à la ligne **LiveUpdate automatique**, effectuez l'une des opérations suivantes :
 - Pour désactiver LiveUpdate automatique, déplacez le curseur **Ac./Désac.** vers la droite sur la position **Désactivé**.
Dans la liste déroulante **Sélectionner la durée**, sélectionnez la durée pour laquelle vous voulez désactiver la fonction LiveUpdate automatique, puis cliquez sur **OK**.
 - Pour activer LiveUpdate automatique, déplacez le curseur **Ac./Désac.** vers la gauche sur la position **Activé**.

Exécution manuelle de Norton LiveUpdate

Il est recommandé d'exécuter régulièrement LiveUpdate dans les cas suivants :

- Si l'option **LiveUpdate automatique** est désactivée
- Si l'ordinateur est resté longtemps sans connexion à Internet



Pour exécuter LiveUpdate, vous devez disposer d'un abonnement valide et d'une connexion Internet.

Exécution manuelle de LiveUpdate

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **LiveUpdate**.
- 2 Dans la fenêtre **Norton LiveUpdate**, une fois la mise à jour LiveUpdate effectuée, cliquez sur **OK**.

Recherche de la date des dernières mises à jour de la protection

Les mises à jour de la protection contiennent des informations permettant à votre produit Norton de détecter la présence d'un virus ou d'une menace de sécurité spécifique, et de vous en alerter. Elles peuvent également mettre à niveau votre produit pour que ce dernier inclue une nouvelle fonction et puisse améliorer ses performances. Norton Security affiche la dernière date à laquelle vous avez téléchargé et installé les dernières mises à jour de la protection.

Recherche de la date de la dernière mise à jour de la protection

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Sécurité**.
- 2 Sous l'indicateur de l'état de la sécurité, recherchez la date en regard de **Mises à jour de la protection**.
- 3 Si la date est antérieure à un ou deux jours, exécutez LiveUpdate immédiatement.

Activation ou désactivation de la fonction Appliquer les mises à jour uniquement au redémarrage

Certaines des mises à jour de protection qui sont téléchargées pendant une session LiveUpdate nécessitent un redémarrage système pour être

correctement appliquées. Sous Windows 7 ou version ultérieure, toutes les mises à jour téléchargées peuvent être appliquées immédiatement sans redémarrage système. Toutefois, l'option **Appliquer les mises à jour uniquement au redémarrage** permet de choisir la méthode d'application de ces mises à jour.



Cette option n'est disponible que sous Windows 7 ou version ultérieure.

Si vous désactivez cette option, les mises à jour téléchargées peuvent être appliquées immédiatement sans redémarrage système. Cette option est désactivée par défaut. Vous trouverez les options suivantes dans la fenêtre **Norton LiveUpdate** :

■ **Appliquer maintenant**

Si vous choisissez cette option, les mises à jour téléchargées sont appliquées immédiatement sans redémarrage système.

■ **Appliquer plus tard**

Si vous choisissez cette option, les mises à jour téléchargées sont appliquées lors du prochain redémarrage de votre ordinateur.

Si cette option est activée, les mises à jour téléchargées sont appliquées après un redémarrage système uniquement. Vous trouverez les options suivantes dans la fenêtre **Norton LiveUpdate** :

■ **Redémarrer maintenant**

Si vous choisissez cette option, votre ordinateur redémarre une fois les mises à jour appliquées.

■ **Redémarrer plus tard**

Si vous choisissez cette option, les mises à jour téléchargées sont appliquées lors du prochain redémarrage de votre ordinateur.

Activation ou désactivation de l'option Appliquer les mises à jour uniquement au redémarrage

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.

- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antivirus**.
- 3 Dans la fenêtre de paramètres **Antivirus**, cliquez sur l'onglet **Antispyware et mises à jour**.
- 4 A la ligne **Appliquer les mises à jour uniquement au redémarrage**, effectuez l'une des opérations suivantes :
 - Pour désactiver **Appliquer les mises à jour uniquement au redémarrage**, déplacez le curseur **Ac./Désac.** vers la droite sur la position **Désactivé**.
 - Pour activer **Appliquer les mises à jour uniquement au redémarrage**, déplacez le curseur **Ac./Désac.** vers la gauche sur la position **Activé**.
- 5 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**.
- 6 Cliquez sur **Fermer**.

Configuration des paramètres de proxy réseau

Lorsque vous passez par un serveur proxy pour vous connecter à Internet, vous devez indiquer les détails du serveur proxy. La fenêtre **des paramètres de proxy réseau** vous permet de saisir des paramètres de configuration automatique, des paramètres de proxy et des paramètres d'authentification du serveur proxy. Les paramètres de Proxy réseau vous permettent de vous connecter à Internet pendant que vous exécutez des tâches comme l'activation du produit ou l'accès des options de support.

Configuration des paramètres proxy de réseau

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.

- 3 A la ligne **Paramètres de proxy réseau**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Paramètres proxy réseau**, vous pouvez:
 - Si vous souhaitez que votre navigateur détecte automatiquement des paramètres de connexion réseau, sous **Configuration automatique**, vérifier **Détecter automatiquement les paramètres**.
 - Si le serveur proxy exige un URL automatique de configuration, sous **Configuration automatique**, vérifier **Utiliser script de configuration automatique**. Saisissez l'URL du fichier PAC dans le champ **URL**.
 - Si votre réseau utilise un serveur proxy, sous **Paramètres proxy**, cochez **Utiliser un serveur proxy pour les connexions HTTP**. Dans la case **Adresse**, saisissez l'URL ou l'adresse IP du serveur proxy et dans la case **Port**, saisissez le numéro de port du serveur proxy. Indiquez une valeur comprise entre 1 et 65535.
 - Si votre serveur proxy requiert un nom d'utilisateur et un mot de passe, sous **Authentification**, cochez la case **J'ai besoin d'une authentification pour me connecter via mon pare-feu ou mon serveur proxy**. Saisissez le nom d'utilisateur dans la zone de texte **Nom d'utilisateur** et le mot de passe dans la zone de texte **Mot de passe**.
- 5 Dans la fenêtre **Paramètres de proxy réseau**, cliquez sur **Appliquer**.

Contrôle des performances de votre système

2

Ce chapitre traite des sujets suivants :

- [A propos de Diagnostic du système](#)
- [Rapport sur 30 jours](#)

A propos de Diagnostic du système

Votre produit Norton surveille constamment votre ordinateur afin de le protéger contre les problèmes et qu'il fonctionne de manière optimale. Le produit Norton analyse constamment les zones essentielles de votre ordinateur, y compris la mémoire, les clés de registre et les processus actifs. Il contrôle les activités importantes, telles que l'exécution générale des fichiers, le trafic réseau et la navigation sur Internet. De plus, votre produit Norton s'assure que les activités qu'il exécute sur votre ordinateur ne dégradent pas les performances globales de votre ordinateur.

La fenêtre Diagnostic du système fournit un emplacement centralisé dans lequel vous pouvez voir et surveiller les activités que vous réalisez sur votre système. Le diagnostic du système présente ces informations dans la fenêtre **Graphiques**.

Vous pouvez utiliser la fenêtre **Graphiques** pour les opérations suivantes :

- Consultation de l'historique mensuel des activités importantes du système que vous avez effectuées

ou qui se sont produites au cours des trois derniers mois.

Le graphique des événements, visible en haut de la fenêtre, fournit une représentation en image des activités importantes du système. Les activités comprennent les installations et téléchargements d'applications, les optimisations de disque, les détections de menaces, les alertes de performances et les analyses rapides.

Le graphique affiche les activités sous forme d'icône ou de bande et la description de chaque icône ou bande est fournie en dessous du graphique. La fenêtre contextuelle qui s'affiche lorsque vous placez le pointeur de la souris sur une icône fournit des détails sur l'activité concernée. Le lien **Affichage des détails** dans la fenêtre contextuelle permet d'afficher des informations supplémentaires sur l'activité dans la fenêtre **Historique de la sécurité**. Vous pouvez utiliser les onglets en haut du graphique pour obtenir des détails pour le mois en cours et les deux derniers mois.

- Réorganisation des fichiers de votre ordinateur
L'optimisation de votre système permet d'optimiser l'espace libre utilisable d'un disque en regroupant les fichiers selon leur accessibilité. L'option **Optimiser** en haut du graphique des événements permet de défragmenter votre système.

- Pour voir et analyser l'impact du produit Norton sur les performances de votre ordinateur.

Le graphique d'utilisation de l'UC, visible sur la gauche de la fenêtre, fournit une représentation graphique de l'utilisation de l'UC. Le graphique présente le pourcentage d'utilisation globale de l'UC du système et l'utilisation de l'UC spécifique à Norton.

Vous pouvez utiliser l'option **Suivi de performance** pour suivre les performances de votre ordinateur. Pour accéder à l'option **Suivi de performance**, ouvrez la fenêtre principale du produit Norton, puis cliquez sur

Paramètres > Paramètres administratifs > Suivi de performance.

Accès à la fenêtre Graphiques

Le diagnostic du système fournit un emplacement centralisé dans lequel vous pouvez voir et surveiller les activités de votre système. Le diagnostic du système présente ces informations dans la fenêtre **Graphiques**. Vous pouvez accéder à la fenêtre **Graphiques** pour afficher des détails sur les activités importantes du système et l'utilisation de l'UC. Vous pouvez également défragmenter votre volume de démarrage.

Accès à la fenêtre Graphiques

- ❖ Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Performances**, puis sur **Graphiques**.

A propos de la surveillance des activités du système

Le diagnostic du système fournit des informations sur les activités importantes du système que vous avez exécutées ou qui se sont produites au cours des trois derniers mois. Vous pouvez utiliser les onglets situés en haut du graphique pour obtenir des détails concernant le mois en cours et les deux derniers mois. Le diagnostic du système présente les informations dans la fenêtre **Graphiques**. La fenêtre **Graphiques** affiche chaque activité sous la forme d'une icône ou d'une bande. La description de chaque icône ou bande s'affiche en bas du graphique. Vous pouvez utiliser les onglets situés en haut du graphique pour obtenir des

détails concernant le mois en cours et les deux derniers mois. Les activités incluent :

Les installations	<p>Fournit des détails sur les opérations d'installation que vous avez effectuées sur votre système au cours des trois derniers mois.</p> <p>Les détails incluent l'application que vous avez installée, la date à laquelle vous avez installé l'application et le nombre total d'installations à cette date.</p>
Les téléchargements	<p>Fournit des détails sur les opérations de téléchargement d'applications que vous avez effectuées sur votre système au cours des trois derniers mois.</p> <p>Les détails incluent la date à laquelle vous avez téléchargé un fichier et le nombre total de téléchargements à cette date. Vous pouvez cliquer sur le nom du fichier pour afficher des informations supplémentaires sur le fichier téléchargé, telles que le rapport de Diagnostic des téléchargements, le nom du fichier, le niveau de réputation et l'action recommandée.</p>
Optimisé	<p>Indique les opérations d'optimisation que vous avez effectuées sur votre système au cours des trois derniers mois.</p>

Détections	<p>Fournit des détails sur les activités de détection des menaces que le produit Norton a effectuées sur votre système au cours des trois derniers mois.</p> <p>Les détails incluent la date à laquelle votre produit Norton a détecté une menace et le nombre total de menaces que votre produit Norton a identifiées à cette date. Le lien Afficher les détails fournit des détails supplémentaires sur le risque, tels que son impact et son origine. Les détails incluent également l'action qu'une menace a effectuée sur votre système et l'action que Symantec recommande afin d'éliminer la menace.</p>
Les alertes	<p>Fournit des informations sur les alertes de performances que le produit Norton a affichées sur les trois derniers mois.</p> <p>Les détails comprennent la date de surveillance et le nombre d'alertes de performance générées. Le lien Afficher les détails fournit des informations supplémentaires sur les activités associées aux performances, le nom du programme, l'emplacement du programme et l'utilisation des ressources du système.</p>

Analyses rapides	<p>Fournit des détails sur les analyses rapides que votre produit Norton a effectuées sur votre système au cours des trois derniers mois.</p> <p>Les détails incluent la date à laquelle une analyse rapide a été effectuée et le nombre d'analyses rapides effectuées à cette date. Le lien Afficher les détails fournit des détails supplémentaires, tels que l'heure de l'analyse, le nombre total d'éléments analysés, de risques détectés et de risques éliminés, ainsi que les actions recommandées.</p>
-------------------------	---

Affichage des détails des activités du système

Le diagnostic du système permet d'afficher les détails des opérations système que vous avez effectuées ou qui se sont produites au cours des trois derniers mois dans la fenêtre **Graphiques**. Ces activités comprennent les installations et téléchargements d'applications, les optimisations de disque, les détections de menaces, les alertes de performances et les analyses rapides.

Vous pouvez utiliser les onglets situés en haut du graphique des événements pour obtenir des détails pour le mois en cours et les deux derniers mois. La fenêtre **Graphiques** affiche chaque activité sous la forme d'une icône ou d'une bande. La description de chaque icône ou bande s'affiche en bas du graphique. La fenêtre contextuelle qui s'affiche lorsque vous placez le pointeur de la souris sur une icône fournit des détails sur l'activité concernée. Les détails incluent la date à laquelle une activité a été effectuée et le nombre d'activités effectuées à cette date. Le lien **Afficher les détails** fournit des détails supplémentaires sur l'activité dans la fenêtre **Historique de la sécurité**.

Affichage des détails des activités de votre système

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Performances**, puis sur **Graphiques**.
- 2 Dans la fenêtre **Graphiques**, cliquez sur l'onglet d'un mois pour afficher les détails.
- 3 Dans le graphique des événements, déplacez le pointeur de la souris sur l'icône ou sur la bande d'une activité.
- 4 Dans la fenêtre contextuelle qui s'affiche, consultez les détails de l'activité.
- 5 Si l'option **Afficher les détails** s'affiche dans la fenêtre contextuelle, cliquez sur **Afficher les détails** pour consulter des détails supplémentaires dans la fenêtre **Historique de la sécurité**.

A propos des alertes de performances

Votre produit Norton surveille les performances de votre système. S'il détecte une utilisation en hausse des ressources système par un programme ou un processus quelconque, il vous en avertit à l'aide d'alertes de performances. Les alertes de performances fonctionnent uniquement lorsque l'option **Suivi de performance** et l'option **Alertes de performances** sont activées.

Les alertes de performances vous avertissent à l'aide d'informations relatives au nom du programme et aux ressources que le programme utilise excessivement. Le lien **Détails et paramètres** dans les alertes de notification des performances vous permet d'afficher des informations supplémentaires sur la consommation des ressources par le programme. La fenêtre **Diagnostic des fichiers** s'ouvre et affiche les détails de réputation du fichier, son origine, l'ID du processus et la liste complète d'utilisation des ressources par le programme. Dans la fenêtre **Diagnostic des fichiers**, vous pouvez choisir d'exclure le programme du suivi. L'option **Paramètres** de la fenêtre **Diagnostic des fichiers** permet de désactiver l'option **Alertes de performances**.



Les alertes de performances ne s'affichent pas quand l'ordinateur est inactif ou en mode silencieux.

Pour chaque ressource système comme l'UC, la mémoire et le disque dur, un seuil de consommation de ressources est défini. Quand la consommation des ressources d'un programme dépasse la limite de seuil définie, votre produit Norton vous avertit avec une alerte de performances.

Vous pouvez utiliser l'option **Profil de seuil de ressource pour les alertes** afin de configurer le seuil admissible. Pour accéder à l'option **Profil de seuil de ressource pour les alertes**, ouvrez la fenêtre principale du produit Norton, puis cliquez sur **Paramètres > Paramètres administratifs > Suivi de performance > Profil de seuil de ressource pour les alertes**.

Vous pouvez utiliser l'option **Utiliser le profil de ressource faible avec l'alimentation sur batterie** pour permettre à votre produit Norton de définir automatiquement le profil du seuil de ressources sur Faible lorsque l'ordinateur est alimenté par batterie.

Vous pouvez utiliser l'option **Alerte pour une utilisation élevée de** afin de configurer votre produit Norton de manière à ce qu'il vous alerte en cas d'utilisation élevée de l'UC, de la mémoire, du disque et des poignées.

En outre, vous pouvez ajouter des programmes à la liste **Exclusions de programme** à l'aide de l'option **Exclusions de programme**. Lorsque vous ajoutez un programme à la liste **Exclusions de programme**, votre produit Norton ne vous avertit pas lorsque le programme dépasse le seuil admissible de consommation des ressources défini.

Vous pouvez afficher les journaux relatifs aux performances sous la catégorie **Alertes de performances** dans la fenêtre **Historique de la sécurité**.

Configuration des alertes de performances

Vous pouvez utiliser l'option **Alertes de performances** pour recevoir des alertes de performances quand un programme ou un processus augmente son utilisation des ressources système.

Vous pouvez utiliser les options suivantes pour configurer les alertes de performances :

Désactivé

Désactive les alertes de performances.

Sélectionnez cette option si vous ne voulez pas que votre produit Norton vous envoie des alertes de performances.

Activé

Active les alertes de performances.

Sélectionnez cette option si vous voulez que votre produit Norton vous envoie des alertes de performances lorsqu'un programme ou un processus dépasse le seuil admissible d'utilisation des ressources système.

Consigner uniquement

Surveille et enregistre l'utilisation des ressources système.

Sélectionnez cette option si vous voulez que votre produit Norton surveille uniquement l'utilisation des ressources système par chaque programme ou processus s'exécutant sur l'ordinateur.

L'option **Alertes de performances** est définie sur **Consigner uniquement** par défaut.

Lorsqu'un programme ou un processus dépasse le seuil admissible d'utilisation des ressources système, votre produit Norton enregistre ces informations dans la fenêtre **Historique de la sécurité**. Vous pouvez afficher les informations relatives aux alertes de performances sous la catégorie **Alertes de performances** de la fenêtre **Historique de la sécurité**.

Pour configurer des alertes de performance

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.

- 3 Sous **Suivi de performance**, sur la ligne **Alertes de performance**, effectuez l'une des opérations suivantes :
 - Pour désactiver les alertes de performance, déplacez le commutateur **Alertes de performances** à la position **Arrêt**.
 - Pour activer les alertes de performance, déplacez le commutateur **Alertes de performances** à la position **Marche**.
 - Pour supprimer les alertes de performance, déplacez le commutateur **Alertes de performances** à la position **Consigner uniquement**.
- 4 Sous **Alerte pour une utilisation élevée de**, effectuez l'une des opérations suivantes :
 - Si vous voulez que votre produit Norton surveille l'utilisation de l'UC, déplacez le curseur **UC** vers la gauche, sur la position **Activé**.
 - Si vous voulez que votre produit Norton surveille l'utilisation de la mémoire, déplacez le curseur **Mémoire** vers la gauche, sur la position **Activé**.
 - Si vous voulez que votre produit Norton surveille l'utilisation du disque, déplacez le curseur **Disque** vers la gauche, sur la position **Activé**.
 - Si vous voulez que votre produit Norton surveille le nombre de handles, déplacez le curseur **Handles** vers la gauche, sur la position **Activé**. Cette option est désactivée par défaut.
- 5 Cliquez sur **Appliquer**, puis sur **Fermer**.

Configuration du profil de seuil de ressources

Le seuil admissible pour les ressources système détermine à quel niveau votre produit Norton doit vous avertir par des alertes de performances. Lorsqu'un programme spécifique dépasse le seuil limite d'utilisation des ressources système, votre produit Norton vous envoie une alerte de performances.

Configuration du profil de seuil de ressources

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Suivi de performance**, sur la ligne **Profil de seuil de ressources pour les alertes**, sélectionnez l'une des options suivantes :

Faible

Configure un seuil admissible faible pour les alertes.

Symantec recommande de sélectionner cette option quand l'ordinateur est alimenté par batterie.

Moyen

Configure un seuil admissible moyen pour les alertes.

Par défaut, le seuil admissible est défini sur Moyen.

Maximum

Configure un seuil admissible maximal pour les alertes.

Symantec vous recommande de sélectionner cette option lorsque l'ordinateur exécute des tâches nécessitant de nombreuses ressources.

- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Désactivation et activation de l'option Utiliser le profil de ressource faible avec l'alimentation sur batterie

Lorsque l'ordinateur est alimenté par batterie, il est important que tous les programmes logiciels actifs consomment des ressources minimales. En diminuant l'utilisation des ressources, la durée de vie de la batterie de l'ordinateur s'allonge et l'ordinateur devient plus efficace en terme d'énergie.

Vous pouvez configurer un profil de seuil faible, et vous assurer que tous les programmes consomment le minimum de ressource. Quand l'utilisation des ressources d'un programme ou d'un processus dépasse le seuil admissible faible, le produit Norton vous en avertit au moyen d'une alerte de performances. Vous pouvez choisir de fermer le programme ou le processus manuellement et de libérer les ressources.

Si l'option **Utiliser le profil de ressource faible avec l'alimentation sur batterie** est activée, le produit Norton règle automatiquement le profil du seuil de ressource sur Faible quand l'ordinateur est alimenté par batterie. Par défaut, cette option est activée.



Symantec vous recommande de laisser l'option **Utiliser le profil de ressource faible avec l'alimentation sur batterie** activée.

Désactivation de l'option Utiliser le profil de ressource faible avec l'alimentation sur batterie

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Suivi de performance**, sur la ligne **Utiliser le profil de ressource faible avec l'alimentation sur batterie**, déplacez le curseur **Ac./Désac.** vers la droite sur la position **Désactivé**.
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Activation de l'option Utiliser le profil de ressource faible avec l'alimentation sur batterie

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Suivi de performance**, sur la ligne **Utiliser le profil de ressource faible avec l'alimentation sur batterie**, déplacez le curseur **Ac./Désac.** vers la gauche sur la position **Activé**.
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Exclusion de programmes des alertes de performances

Votre produit Norton vous permet d'exclure des programmes des alertes de performances. Vous pouvez ajouter des programmes qui utilisent fortement l'UC, la mémoire ou le disque à la liste **Exclusions de programme**. Lorsque vous ajoutez un programme à la liste **Exclusions de programme**, votre produit Norton ne vous avertit pas lorsque le programme dépasse le seuil admissible de consommation des ressources.

Exclusion d'un programme des alertes de performances

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Suivi de performance**, à la ligne **Exclusions de programme**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Exclusion de programme**, cliquez sur **Ajouter**.
- 5 Dans la boîte de dialogue **Sélectionner un programme**, accédez au fichier exécutable du programme à ajouter.
- 6 Cliquez sur **Ouvrir**.
- 7 Dans la fenêtre **Exclusions de programme**, cliquez sur **Appliquer**.
- 8 Cliquez sur **OK**.

9 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Suppression des programmes des Exclusions de programmes

La fenêtre **Exclusions de programme** répertorie tous les programmes exclus des alertes de performances. Vous pouvez supprimer les programmes que vous avez déjà ajoutés à la fenêtre **Exclusions de programme**. Lorsque vous supprimez un programme, il apparaît dans l'alerte de performances lorsqu'il dépasse le seuil admissible de consommation des ressources défini.

Suppression d'un programme des exclusions de programme

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Suivi de performance**, à la ligne **Exclusions de programmes**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Exclusions de programmes**, sélectionnez le programme que vous souhaitez supprimer, et cliquez sur **Supprimer**.
Pour supprimer tous les programmes de la fenêtre **Exclusions de programme**, cliquez sur **Tout supprimer**.
- 5 Dans la fenêtre **Exclusions de programme**, cliquez sur **Appliquer**.
- 6 Cliquez sur **OK**.
- 7 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

A propos de l'indicateur d'utilisation de l'UC

Votre produit Norton surveille l'utilisation globale de l'UC par le système, ainsi que son utilisation par Norton. Il affiche l'indicateur d'utilisation de l'UC dans la fenêtre **Graphiques**. L'indicateur d'utilisation de l'UC est un graphique en temps réel représentant l'utilisation de l'UC.

Le graphique affiche un temps de performances pour les dernières 90 minutes ou pour la durée pour laquelle vous avez démarré votre ordinateur. Le motif bleu dans le graphique dépeint l'utilisation globale du système et le motif jaune dépeint l'utilisation par Norton. Les blocs gris étiquetés **Inactif** indiquent la période d'inactivité de votre ordinateur. Les blocs gris incluent la période d'arrêt, de veille ou de déconnexion de votre ordinateur.

Affichage du graphique d'UC ou du graphique de mémoire

Votre produit Norton contrôle l'utilisation globale de l'UC et de la mémoire par le système, ainsi que leur utilisation par Norton. Le graphique sur la gauche de la fenêtre **Graphiques** affiche l'indicateur d'utilisation de l'UC.

Affichage du graphique de l'UC ou du graphique de mémoire

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Performances**, puis sur **Graphiques**.
- 2 Dans la fenêtre **Graphiques** sur le volet de gauche, cliquez sur **Utilis. de l'UC et de la mémoire**.
- 3 Effectuez l'une des opérations suivantes :
 - Pour afficher le graphique de l'UC, cliquez sur l'onglet **UC**.
 - Pour afficher le graphique de la mémoire, cliquez sur l'onglet **Mémoire**.
 - Pour agrandir ou réduire le graphique, cliquez sur **10 mn**, **30 mn**, **1 j**, **1 s**, **1 m** en regard de l'option **Zoom**.

Obtention de données historiques sur l'utilisation de l'UC et de la mémoire

Les options **Agrandissement** fournissent également les données historiques du graphique de l'UC et de la mémoire. Par exemple, si vous sélectionnez l'option **1 j**, Norton Security affiche les données du graphique de l'UC ou de la mémoire des dernières 24 heures.

Affichage de l'historique des données d'utilisation de l'UC ou de la mémoire

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Performances**, puis sur **Graphiques**.
- 2 Dans la fenêtre **Graphiques**, cliquez sur **Utilis. de l'UC et de la mémoire** sur le volet de gauche.
- 3 Effectuez l'une des opérations suivantes :
 - Pour afficher le graphique de l'UC, cliquez sur l'onglet **UC**.
 - Pour afficher le graphique de la mémoire, cliquez sur l'onglet **Mémoire**.
- 4 Effectuez l'une des opérations suivantes :
 - Pour obtenir l'historique des données des dernières 24 heures, cliquez sur **1 j**.
 - Pour obtenir l'historique des données des sept derniers jours, cliquez sur **1 s**.
 - Pour obtenir l'historique des données des quatre dernières semaines, cliquez sur **1 m**.

Identification des processus consommant des ressources

Vous pouvez cliquer à tout moment sur le graphique de l'UC ou de la mémoire pour obtenir la liste des trois processus qui consomment le plus de ressources sur votre ordinateur à ce moment précis. Vous pouvez cliquer sur un processus dans la liste pour d'obtenir des informations supplémentaire sur le processus dans la fenêtre **Diagnostic des fichiers**.

Pour identifier les processus consommant des ressources

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Performances**, puis sur **Graphiques**.
- 2 Dans la fenêtre **Graphiques**, cliquez sur **Utilis. de l'UC et de la mémoire** dans le volet de gauche.

- 3 Effectuez l'une des opérations suivantes :
 - Pour afficher le graphique de l'UC, cliquez sur l'onglet **UC**.
 - Pour afficher le graphique de la mémoire, cliquez sur l'onglet **Mémoire**.
- 4 Cliquez sur un point du graphique de l'UC pour obtenir la liste des processus qui consomment des ressources.
- 5 Cliquez sur le nom d'un processus pour obtenir des informations supplémentaires sur le processus dans la fenêtre **Diagnostic des fichiers**.

A propos de l'optimisation

L'espace de stockage des données d'un lecteur est divisé en petites unités. Ces unités sont appelées des clusters. Quand des fichiers sont écrits sur le disque, ils sont fragmentés en morceaux de la taille d'un cluster. Lorsque toutes les pièces d'un fichier sont situées dans des groupes proches ou contigus, vous pouvez rapidement accéder au fichier.

Le disque dur de votre ordinateur stocke tous vos fichiers, toutes vos applications et le système d'exploitation Windows. Les éléments d'information composant vos fichiers sont progressivement répartis sur tout le disque. Ce processus est appelé fragmentation. Plus vous utilisez votre ordinateur, plus le disque est fragmenté.

Lorsque vous accédez à un fichier fragmenté, les performances du disque diminuent. Ceci s'explique par le fait que la tête du disque recherche, charge, enregistre et assure le suivi de tous les fragments d'un fichier. Si l'espace libre est également fragmenté, la tête du disque doit rechercher l'espace libre adéquat pour stocker les fichiers temporaires ou les fichiers ajoutés.

L'optimisation réorganise les fragments de fichiers dans des clusters contigus. Lorsque la tête du disque accède à toutes les données d'un fichier dans un même endroit, la lecture du fichier en mémoire est plus rapide.

L'optimisation augmente également l'espace libre utilisable d'un disque en regroupant les fichiers les plus utilisés et les fichiers rarement utilisés. L'optimisation regroupe l'espace libre afin d'éviter la fragmentation des fichiers ajoutés. Elle ajoute un espace supplémentaire après les structures de données principales pour qu'elles puissent augmenter sans se refragmenter immédiatement.

Vous pouvez optimiser manuellement le volume de démarrage à l'aide de l'option **Optimiser** qui se trouve dans la fenêtre **Graphiques**.

Vous pouvez également configurer votre produit Norton pour que le volume de démarrage ou le disque local contenant le volume de démarrage soit défragmenté lorsque l'ordinateur est inactif. Le produit Norton planifie automatiquement l'optimisation quand il détecte l'installation d'une application sur l'ordinateur. Le processus d'optimisation démarre dès que votre ordinateur est inactif.

Vous pouvez utiliser l'option **Optimiseur du temps d'inactivité** dans la fenêtre **Paramètres administratifs** pour optimiser le volume de démarrage en période d'inactivité.

Optimisation de votre volume de démarrage

L'option **Optimiser** permet d'optimiser votre volume de démarrage afin d'améliorer le temps de démarrage de votre ordinateur. L'optimisation de votre volume de démarrage optimise l'espace libre utilisable en réorganisant les fragments de fichiers dans des clusters contigus. Lorsque la tête du disque accède à toutes les données d'un fichier dans un même emplacement, la lecture du fichier est plus rapide.

Toutefois, lorsque vous utilisez l'option **Optimiser**, votre produit Norton optimise le lecteur contenant le volume de démarrage. Il lui faut donc plus de temps pour effectuer l'optimisation.

Vous pouvez accéder à l'option **Optimiser** en haut du graphique de l'état de la sécurité dans la fenêtre **Graphiques**. Vous pouvez également optimiser le volume de démarrage à l'aide de l'option **Optimiseur Insight** qui se trouve dans la fenêtre **Tâches en arrière-plan**. La ligne **Optimiseur Insight** de la liste des travaux en arrière-plan de la fenêtre **Tâches en arrière-plan** affiche les détails du processus d'optimisation du volume de démarrage. Elle vous fournit des détails comme l'horodatage, la durée et l'état des travaux en arrière-plan.

Optimisation de votre volume de démarrage depuis la fenêtre Graphiques

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Performances**, puis sur **Graphiques**.
- 2 Dans la fenêtre **Graphiques**, en haut du graphique de l'état de la sécurité, cliquez sur **Optimiser**.

Optimisation de votre volume de démarrage depuis la fenêtre Tâches en arrière-plan

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Dans la ligne **Tâches en arrière-plan**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Tâches en arrière-plan**, sous la colonne **Tâches Norton**, cliquez sur l'icône de lecture qui apparaît devant l' **Optimiseur Insight**.

A propos de l'optimiseur du temps d'inactivité

L'Optimiseur du temps d'inactivité permet de configurer votre produit Norton afin qu'il défragmente votre volume de démarrage ou votre disque local contenant le volume de démarrage quand l'ordinateur est inactif. Le produit Norton planifie automatiquement l'optimisation quand il détecte l'installation d'une application sur l'ordinateur ou quand ce dernier est inactif. Si vous recommencez à utiliser votre ordinateur, le produit Norton arrête la

tâche d'optimisation et la redémarrage à la période d'inactivité suivante. De cette manière, le travail d'optimisation en arrière-plan n'affecte pas les performances de votre ordinateur.

L'optimisation réorganise les fragments de fichiers dans des groupes proches ou contigus sur le disque dur. Elle améliore les performances de l'ordinateur en lisant plus rapidement les fichiers dans la mémoire. L'optimisation maximise également l'espace libre utilisable d'un disque en regroupant les fichiers les plus utilisés et les fichiers rarement utilisés. De plus, elle consolide l'espace libre afin d'éviter la fragmentation des fichiers récemment ajoutés.

Vous devez activer l'option **Optimiseur du temps d'inactivité** sous **Paramètres administratifs** dans la fenêtre **Paramètres** pour optimiser le volume d'amorçage pendant la période d'inactivité. Par défaut, cette option est activée.

Activation ou désactivation de l'optimiseur du temps d'activité

Le produit Norton planifie automatiquement l'optimisation lorsqu'il détecte l'installation d'une application sur votre ordinateur. Le produit Norton exécute cette optimisation uniquement lorsque votre ordinateur est inactif.

Vous pouvez utiliser l'option **Optimiseur du temps d'inactivité** pour optimiser le volume de démarrage en période d'inactivité. Par défaut, cette option est activée.

Désactivation de l'Optimiseur du temps d'activité

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sur la ligne **Optimiseur du temps d'inactivité**, déplacez le commutateur **Marche/Arrêt** vers la droite sur la position **Arrêt**.
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Activation de l'optimiseur du temps d'inactivité

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 A la ligne **Optimiseur du temps d'inactivité**, déplacez le commutateur **Marche/Arrêt** vers la gauche sur la position **Marche**.
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Surveillance des travaux en arrière-plan de votre produit Norton

La fenêtre **Tâches en arrière-plan** fournit les détails des tâches en arrière-plan que le produit Norton exécute et permet d'afficher et de surveiller les tâches en arrière-plan. Votre produit Norton exécute la plupart des tâches en arrière-plan lorsque votre ordinateur est inactif. L'exécution de toutes les tâches en arrière-plan lorsque votre ordinateur est inactif aide votre ordinateur à fonctionner de manière optimale lorsque vous l'utilisez. Cependant, vous pouvez démarrer ou arrêter une tâche manuellement à tout moment. Vous pouvez également préciser la durée du **délai d'inactivité**. A l'échéance du **délai d'inactivité**, votre produit Norton identifie l'ordinateur comme étant inactif et exécute les tâches en arrière-plan.

Surveillance des travaux en arrière-plan

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Dans la ligne **Tâches en arrière-plan**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Tâches en arrière-plan**, consultez les détails des travaux en arrière-plan.

- 5 Effectuez l'une des opérations suivantes :
 - Pour exécuter un travail en arrière-plan, cliquez sur l'icône de lecture qui s'affiche avant le nom du travail d'arrière-plan.
 - Pour arrêter un travail en arrière-plan en cours d'exécution, cliquez sur l'icône d'arrêt qui s'affiche avant le nom du travail en arrière-plan.
- 6 Cliquez sur **Fermer**.

Configuration de la source d'alimentation

Vous pouvez déterminer la source d'alimentation pour que votre produit Norton effectue des tâches en arrière-plan. Les tâches en arrière-plan sont des tâches spécifiques que votre produit Norton effectue lorsque l'ordinateur est inactif.

Les tâches en arrière-plan incluent Analyse rapide, LiveUpdate automatique, Communauté de veille Norton, Norton Insight, Analyse complète du système et Optimiseur Insight. Votre produit Norton consomme davantage d'énergie lorsqu'il exécute les tâches en arrière-plan. Par défaut, votre produit Norton effectue ces tâches seulement quand votre ordinateur est relié à une source d'alimentation externe. Si votre ordinateur fonctionne sur batterie, votre produit Norton n'exécute pas les tâches en arrière-plan. Cela permet de prolonger l'utilisation de votre ordinateur sur batterie.

Vous pouvez déterminer la source d'alimentation pour effectuer des tâches en arrière-plan. Vous pouvez configurer la source d'alimentation pour chacune des tâches en arrière-plan.

Configuration de la source d'alimentation

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Dans la ligne **Tâches en arrière-plan**, cliquez sur **Configurer**.

- 4 Dans la fenêtre **Tâches en arrière-plan**, sous la colonne **Source d'alimentation**, cliquez sur le lien **Configurer** pour la tâche en arrière-plan pour laquelle vous souhaitez configurer la source d'alimentation.
- 5 Dans la fenêtre **Source d'alimentation**, sélectionnez parmi ce qui suit :
 - **Externe**
Permet aux tâches en arrière-plan de ne s'exécuter que lorsque l'ordinateur utilise une source d'alimentation externe.
 - **Externe et batterie**
Autorise l'exécution des tâches en arrière-plan lorsque l'ordinateur utilise une source d'alimentation externe ou la batterie.
Si vous sélectionnez cette option, Norton Security exécute les tâches en arrière-plan lorsque l'ordinateur est inactif. Il ne prend pas en compte le type de source d'alimentation utilisé par l'ordinateur.
- 6 Cliquez sur **OK**.
- 7 Dans la fenêtre **Tâches en arrière-plan**, cliquez sur **Fermer**.

A propos de Norton Insight

Norton Insight permet une analyse intelligente des fichiers sur votre ordinateur. Il optimise les performances des analyses effectuées par votre produit Norton en analysant moins de fichiers sans compromettre la sécurité de l'ordinateur.

Une analyse Norton peut identifier les menaces sur votre ordinateur comme suit :

<p>La technique de liste noire</p>	<p>A intervalles réguliers, votre produit Norton obtient des mises à jour des définitions de la part de Symantec. Ces mises à jour contiennent des signatures de menaces connues. Chaque fois que le produit Norton obtient les mises à jour des définitions, il effectue une analyse de tous les fichiers disponibles sur votre ordinateur. Il compare la signature des fichiers avec celles des menaces connues pour identifier les menaces sur votre ordinateur.</p>
------------------------------------	---

La technique de la Liste blanche

Le produit Norton obtient des informations spécifiques sur les fichiers d'intérêt et soumet les informations à Symantec pendant la période d'inactivité. Ces informations incluent le nom du fichier, sa taille et sa clé de hachage. Symantec analyse les informations de chaque fichier et son total mêlé unique et applique au fichier un niveau de confiance. Le serveur Symantec enregistre le total mêlé et le niveau de confiance dans les fichiers d'intérêts. Le serveur fournit les détails dès l'ouverture de la fenêtre **Norton Insight**. La plus légère modification du fichier provoque même un changement dans le total mêlé et le niveau de confiance du fichier. La plupart des fichiers appartenant habituellement au système d'exploitation ou aux applications connues ne changent jamais. Ces fichiers ne demandent pas d'analyses ou de surveillances répétées. Excel.exe est un fichier par exemple, qui n'est jamais modifié mais vous l'analysez toujours pendant une normale analyse de sécurité.

Symantec assigne les niveaux de confiance suivants aux Fichiers d'intérêts :

Approuvé	<p>Symantec analyse le fichier et le classe comme approuvé en fonction de l'évaluation statistique des fichiers qui sont disponibles au sein de la communauté Norton.</p> <p>Si le fichier compte trois barres vertes, Symantec classe le fichier comme Approuvé par Norton.</p> <p>Les fichiers qui comptent trois barres vertes affichent une fenêtre contextuelle "Approuvé par Norton" lorsque vous placez le pointeur de la souris sur les barres vertes.</p>
Fiable	<p>Symantec analyse le fichier et le classe comme fiable en fonction de l'évaluation statistique des fichiers qui sont disponibles au sein de la communauté Norton.</p> <p>Symantec classe les fichiers approuvés comme suit :</p> <ul style="list-style-type: none">■ Si le fichier compte deux barres vertes, Symantec classe le fichier comme Fiable.■ Si le fichier compte une barre verte, Symantec classe le fichier comme Favorable.

Non testé	Symantec ne dispose pas de suffisamment d'informations sur le fichier pour lui attribuer un niveau d'approbation.
Faible	Symantec dispose de peu d'indications quant au manque de fiabilité du fichier.

La technique de la Liste blanche que Norton Insight utilise facilite également la détection heuristique des applications suspectes. Le comportement d'exécution normalement des applications bien connues semble identique au comportement d'exécution des applications inconnues. Un tel comportement a comme conséquence l'identification fautive des bonnes applications comme suspectes, et donc, nécessite des applications de sécurité pour maintenir un seuil de détection heuristique faible. Le maintien cependant d'un faible seuil de détection ne fournit pas une protection heuristique complète contre les applications malveillantes. Le produit Norton utilise la technique de liste blanche, qui aide à maintenir un seuil de détection heuristique élevé. Il exclut les applications connues de la détection heuristique pour empêcher la détection erronée des applications connues et pour assurer un taux élevé de détection des applications malveillantes.

Affichage des fichiers à l'aide de Norton Insight

Norton Insight fournit des informations de réputation sur les fichiers d'intérêts disponibles sur votre ordinateur. Votre produit Norton vous permet d'afficher des catégories de fichiers spécifiques en fonction de l'option que vous avez sélectionnée dans la fenêtre **Norton Insight**.

La liste déroulante disponible dans la fenêtre **Norton Insight** fournit les options suivantes :

Tous les processus actifs	Répertorie les processus exécutés sur votre ordinateur.
Tous les fichiers	Répertorie tous les fichiers d'intérêt.
Éléments de démarrage	Répertorie les programmes exécutés lorsque vous démarrez votre ordinateur.
Tous les modules chargés	Affiche la liste des fichiers et programmes actuellement chargés dans l'espace mémoire de programme.
Impact le plus élevé sur les performances	Répertorie les programmes qui consomment le plus de ressources sur votre ordinateur. Votre produit Norton affiche une liste des dix premières ressources qui ont un impact élevé sur les performances de votre ordinateur.
Utilisation la plus élevée par la communauté	Répertorie les fichiers les plus utilisés par la communauté.

Fichiers autorisés utilisateur	<p>Répertorie les fichiers d'intérêt que vous avez manuellement autorisés dans la fenêtre Diagnostic des fichiers.</p> <p>Cette catégorie ne répertorie pas les fichiers qui n'appartiennent pas à la liste des fichiers d'intérêt même si vous approuvez manuellement les fichiers.</p> <p>Vous pouvez également supprimer l'approbation utilisateur de tous les fichiers d'intérêts que vous avez approuvés manuellement. Vous pouvez utiliser l'option Effacer toutes les approbations d'utilisateur située en regard de la liste déroulante afin de supprimer l'approbation utilisateur.</p>
Fichiers non approuvés	<p>Répertorie les fichiers qui ne sont pas approuvés par Norton.</p> <p>Vous pouvez approuver manuellement tous les fichiers qui ne sont pas autorisés en cliquant sur l'option Approuver tous les fichiers en regard de la liste déroulante.</p>

Vous pouvez également afficher les détails de fichier comme le nom de fichier, le niveau d'approbation, l'utilisation par la communauté et l'utilisation des ressources. Il arrive que le niveau d'approbation d'un fichier ait changé ou qu'un processus actif se soit arrêté. Vous pouvez actualiser la fenêtre **Norton Insight** pour

mettre à jour la liste de fichiers et les détails des fichiers. La mesure de la couverture fournit une représentation graphique du pourcentage de fichiers approuvés par Norton par rapport au nombre total de fichiers d'intérêt. Plus le pourcentage est élevé, moins l'analyse prend de temps.

Affichage des fichiers à l'aide de Norton Insight

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sélectionnez **Norton Insight**, puis cliquez sur **OK**.
- 3 Dans la fenêtre **Norton Insight**, sélectionnez une option dans la liste déroulante **Afficher** pour afficher une catégorie de fichiers.
Vous devez peut-être faire défiler la fenêtre pour afficher tous les fichiers associés.
- 4 Cliquez sur **Fermer**.

Actualisation de la liste des fichiers

- ❖ Dans la fenêtre **Norton Insight**, cliquez sur l'icône d'actualisation située au-dessus de l'icône du fichier.

Vérification du niveau d'approbation d'un fichier

Norton Insight vous permet de vérifier les détails de réputation des fichiers d'intérêts disponibles sur votre ordinateur. Vous pouvez voir des détails comme la signature d'un fichier et sa date d'installation. Vous pouvez également afficher des détails comme le niveau d'approbation, l'utilisation par la communauté, l'utilisation des ressources, et la source du fichier. Vous pouvez utiliser l'option **Localiser** pour localiser le fichier sur votre ordinateur. Lorsque vous cliquez avec le bouton droit de la souris sur un fichier qui est disponible sur votre ordinateur, le menu de raccourcis affiche l'option **Norton Security**, puis l'option **Diagnostic Norton des fichiers**. Vous pouvez utiliser les options pour vérifier les détails d'un fichier.



Votre produit Norton affiche l'option **Diagnostic Norton des fichiers** uniquement lorsque vous effectuez un clic droit sur un fichier d'intérêt. Dans le mode sans échec de Windows, vous ne pouvez accéder à cette option pour aucun fichier. Votre produit Norton classe également les fichiers que vous affichez dans la fenêtre **Diagnostic des fichiers** pour afficher leurs détails en tant que fichiers d'intérêt.

Le serveur Symantec enregistre la valeur de hachage et le niveau d'approbation du fichier d'intérêt. Le serveur fournit les détails du fichier dès l'ouverture de la fenêtre **Norton Insight**. Cependant, vous pouvez utiliser l'option **Vérifier la fiabilité maintenant** dans la fenêtre **Diagnostic des fichiers** pour mettre à jour la valeur d'approbation d'un fichier. Vous pouvez également approuver manuellement tous les fichiers connus. Vous pouvez définir le niveau d'approbation de tout fichier sur **Approuvé par l'utilisateur**, à l'exception des fichiers qui sont approuvés par Norton.

Vous pouvez également déterminer l'impact d'un fichier sur l'utilisation des ressources de votre ordinateur. La fenêtre **Diagnostic des fichiers** affiche le graphique d'UC et les détails d'utilisation des ressources système pour les processus en cours d'exécution. Le graphique affiche l'analyse de l'utilisation globale de l'UC par le système et de l'utilisation de l'UC par le processus.

Vérification du niveau d'approbation d'un fichier

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sélectionnez **Norton Insight**, puis cliquez sur **OK**.
- 3 Dans la fenêtre **Norton Insight**, cliquez sur un fichier dont vous souhaitez vérifier les informations.
- 4 Dans la fenêtre **Diagnostic des fichiers**, affichez les détails du fichier.
- 5 Cliquez sur **Fermer**.

Vérification du niveau d'approbation d'un fichier

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sélectionnez **Norton Insight**, puis cliquez sur **OK**.
- 3 Dans la fenêtre **Norton Insight**, cliquez sur **Vérifier un fichier spécifique**.
- 4 Allez sur l'emplacement du fichier dont vous voulez vérifier les détails.
- 5 Sélectionnez le fichier, puis cliquez sur **Ouvrir**.
- 6 Dans la fenêtre **Diagnostic des fichiers**, affichez les détails du fichier.
- 7 Cliquez sur **Fermer**.

Recherche de l'emplacement du fichier

- ❖ Dans la fenêtre de **Diagnostic des fichiers**, cliquez sur **Rechercher**.

Actualisation du niveau d'approbation du fichier

- ❖ Dans l'onglet **Détails** de la fenêtre **Diagnostic des fichiers**, cliquez sur **Vérifier la fiabilité maintenant**.

Approbation manuelle du fichier

- ❖ Dans l'onglet **Détails** de la fenêtre **Diagnostic des fichiers**, cliquez sur **Approuver maintenant**.
Vous pouvez approuver manuellement les fichiers qui sont faibles, non testés ou pas approuvés par Norton.

Utilisation des ressources d'un processus en cours d'exécution

- 1 Dans la fenêtre de **Diagnostic des fichiers**, cliquez sur **Activité**.

- 2 Dans la liste déroulante **Afficher**, effectuez l'une des opérations suivantes :
 - Sélectionnez **Performances** pour afficher le graphique de performances du processus.
 - Sélectionnez **Alertes de performances** pour afficher les détails liés aux alertes de performances du processus.
 - Sélectionnez **Réseau** pour afficher les activités réseau du processus.
 - Sélectionnez **Modification de la clé Run** pour inclure les modifications du registre.

Rapport sur 30 jours

Le **rapport sur 30 jours** est un résumé de toutes les activités de protection de votre produit Norton au cours des 30 derniers jours. Le **rapport sur 30 jours** est automatiquement affiché tous les 30 jours à compter de l'installation de votre produit Norton.

Le produit Norton effectue diverses activités pour vous protéger contre les virus, les téléchargements infectés, l'usurpation d'identité et autres menaces en ligne. Le produit Norton exécute également diverses tâches en arrière-plan pour effacer les fichiers indésirables et optimiser votre ordinateur.

Le produit Norton effectue notamment les activités suivantes :

- Analyse de vos fichiers
- Exécution de LiveUpdate automatique
- Analyse de vos téléchargements
- Blocage des intrusions
- Sécurisation de votre réseau
- Réparation des fichiers infectés
- Enregistrement de vos identifiants sur différents sites Web à l'aide de la fonction Identity Safe

- Gestion du niveau d'approbation des fichiers de votre ordinateur
- Suppression des fichiers inutiles et optimisation de votre ordinateur

La fenêtre **Rapport sur 30 jours** affiche les détails suivants :

- Les quatre activités principales que votre produit Norton a effectuées pour vous au cours des 30 derniers jours
- Etat de LiveUpdate

L'option **Détails** de la fenêtre **Rapport sur 30 jours** permet de visualiser une liste complète de toutes les activités de votre produit Norton.

Puis-je empêcher le produit Norton d'afficher le rapport sur 30 jours ?

Oui, si vous ne souhaitez pas que votre produit Norton affiche automatiquement le **rapport sur 30 jours** tous les 30 jours, vous pouvez désactiver l'option **Rapport sur 30 jours** dans la fenêtre **Paramètres administratifs**.

Désactivation du rapport sur 30 jours

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Dans la ligne **Rapport sur 30 jours**, faites glisser le curseur **Ac./Désac.** vers la droite pour l'amener sur la position **Désactivé**.

Comment consulter manuellement le rapport sur 30 jours ?

Le **rapport sur 30 jours** est automatiquement affiché tous les 30 jours à compter de l'installation de votre produit Norton. Cependant, vous pouvez également l'afficher manuellement à l'aide de l'option **Rapport sur 30 jours** de la fenêtre principale de Norton Security.

L'option **Rapport sur 30 jours** est disponible lorsque le produit Norton a effectué des activités sur votre ordinateur uniquement.



Ce chapitre traite des sujets suivants :

- [A propos de la protection permanente](#)
- [A propos des analyses de Norton Security](#)

A propos de la protection permanente

Après avoir installé le produit Norton et exécuté LiveUpdate, vous êtes complètement protégé contre les virus et autres risques portant sur la sécurité. Les nouveaux risques pour la sécurité demeurent toutefois une menace constante. Les risques de sécurité peuvent se propager au démarrage de l'ordinateur à partir d'un disque infecté ou lors de l'exécution d'un programme infecté. Vous disposez de plusieurs solutions pour éviter les risques de sécurité.

Vous pouvez mieux protéger votre ordinateur en effectuant régulièrement l'entretien des fichiers et en maintenant à jour votre protection de sécurité.

Pour éviter les risques de sécurité :

- Restez informé des derniers virus et autres risques de sécurité en vous connectant au site Web Symantec Security Response à l'adresse suivante : <http://securityresponse.symantec.com>
Ce site Web fournit des informations complètes et fréquemment actualisées sur les virus et la protection antivirus automatique.

- Maintenez **LiveUpdate automatique** activé en permanence pour mettre à jour vos définitions en permanence.
- Exécutez régulièrement LiveUpdate pour recevoir les nouvelles mises à jour de programme.
- Laissez **Auto-Protect** activé en permanence pour empêcher les virus d'infecter l'ordinateur.
- Méfiez-vous des messages électroniques provenant d'expéditeurs inconnus. N'ouvrez pas de pièces jointes anonymes.
- Maintenez **Protection du courrier électronique** activée pour éviter d'envoyer ou de recevoir des pièces jointes infectées.
- Maintenez activés tous les paramètres recommandés pour une protection maximale.
- Conservez les paramètres par défaut activés en permanence.

Vous devez toujours être prêt à faire face à l'infection de l'ordinateur par un virus.

A propos des analyses de Norton Security

Votre produit Norton analyse votre ordinateur pour rechercher tous les types de virus et les menaces inconnues en utilisant les dernières définitions de virus. Il analyse également toutes les activités Internet exécutées sur l'ordinateur pour le protéger contre les menaces Internet qui exploitent les failles logicielles.

Votre produit Norton effectue automatiquement différents types d'analyse pour protéger votre ordinateur des menaces les plus récentes. Il permet également d'exécuter différents types d'analyse manuellement pour protéger l'ordinateur.

A l'aide du produit Norton, vous pouvez effectuer les types d'analyse suivants :

Analyses et tâches	<p>Le produit Norton utilise les dernières définitions de virus disponibles sur l'ordinateur.</p> <p>Si vous suspectez qu'un virus infecte l'ordinateur, vous pouvez exécuter manuellement trois types d'analyses d'ordinateur pour éviter les infections virales sur l'ordinateur. Les trois types d'analyse disponibles sous Analyses et tâches sont Analyse rapide, Analyse complète du système et Analyse personnalisée.</p> <p>Vous pouvez également améliorer les performances de votre ordinateur en exécutant des tâches personnalisées.</p>
Norton Power Eraser	<p>Norton Power Eraser est un outil de suppression des malwares performant qui vous aide à supprimer les risques de sécurité récalcitrants. Norton Power Eraser utilise des techniques plus agressives que celle du processus d'analyse normal ; il peut donc arriver que Norton Power Eraser marque un programme légitime pour suppression. Examinez soigneusement les résultats d'analyse avant de supprimer des fichiers à l'aide de Norton Power Eraser.</p>

Analyse du mur Facebook	<p>L' analyse du mur Facebook permet d'analyser les liens et les URL disponibles dans votre profil Facebook.</p> <p>Lorsque vous cliquez sur l'option Analyse du mur Facebook, le produit Norton affiche la page de connexion à Facebook. Quand vous êtes connecté à votre profil Facebook, Norton Safe Web vous demande l'autorisation d'accéder à votre mur Facebook. Après avoir autorisé Norton Safe Web à accéder à vos informations de profil Facebook, Norton Safe Web analyse votre fil d'actualités Facebook.</p>
Norton Insight	<p>Norton Insight permet une analyse intelligente des fichiers sur votre ordinateur. Il optimise les performances de votre produit Norton en analysant moins de fichiers sans compromettre la sécurité de l'ordinateur. Lorsque vous exécutez Norton Insight, votre produit Norton vous redirige vers la fenêtre Norton Insight où vous pouvez afficher le niveau d'approbation de tous les processus, fichiers et éléments de démarrage en cours d'exécution.</p>

Rapport de diagnostic	Le rapport de diagnostic collecte des informations sur votre ordinateur, y compris le système d'exploitation, les programmes installés et le matériel. Si vous pensez que votre ordinateur rencontre des problèmes logiciels ou matériels, vous pouvez utiliser ce rapport pour les résoudre.
------------------------------	--

Votre produit Norton protège votre ordinateur contre les menaces les plus récentes en exécutant automatiquement une analyse complète du système lorsque votre ordinateur est inactif.

Accès aux analyses de Norton Security

Vous pouvez recourir aux analyses Norton Security pour protéger votre ordinateur contre tous types de virus et menaces inconnus.

Vous pouvez accéder à l'analyse rapide depuis l'icône Norton de la barre des tâches.

Vous pouvez également analyser un dossier en utilisant la fonction Analyse personnalisée. L'analyse personnalisée est disponible lorsque vous effectuez un clic droit sur le fichier ou dossier que vous voulez analyser.

Accès à l'analyse depuis la fenêtre principale du produit Norton

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.

- 2 Dans la fenêtre qui s'affiche, effectuez l'une des opérations suivantes :
 - Dans le volet **Analyses et tâches**, cliquez sur l'analyse à exécuter.
 - Exécutez **Norton Power Eraser** pour qu'il analyse votre ordinateur.
 - Exécutez une **analyse du mur Facebook** pour analyser les liens présents sur votre mur Facebook.

Accès à l'analyse depuis la zone de notification

- ❖ Dans la zone de notification de la barre des tâches, cliquez avec le bouton droit de la souris sur l'icône de **Norton Security**, puis sur **Effectuer une analyse rapide**.

Analyse d'un fichier ou dossier particulier

- ❖ Cliquez avec le bouton droit de la souris sur le fichier ou dossier, sélectionnez **Norton Security** puis cliquez sur **Analyser maintenant**.

A propos de l'Analyse de l'ordinateur

Votre produit Norton télécharge automatiquement et régulièrement les définitions de virus les plus récentes et protège votre ordinateur contre tous les types de virus et de menaces inconnues. Quand le produit Norton effectue une analyse de l'ordinateur, il utilise les dernières définitions de virus fournies par Symantec.

Les détections de menaces basées sur la définition locale sont spécifiées avec un nom précis. Par exemple, si un cheval de Troie est détecté, les résultats de l'analyse de l'option Analyse de l'ordinateur affiche la menace en tant que Trojan.Foo. Vous pouvez cliquer sur l'option **Exécuter des analyses** disponible dans l'onglet **Sécurité** pour accéder aux différents types d'analyses d'ordinateur.

Si vous suspectez qu'un virus infecte l'ordinateur, vous pouvez exécuter manuellement trois types d'analyses

d'ordinateur pour éviter les infections virales sur l'ordinateur.

Vous pouvez exécuter les types suivants d'analyses d'ordinateur :

Analyse rapide	<p>Analyse les emplacements importants de l'ordinateur que les virus et autres menaces de sécurité ciblent généralement.</p> <p>L' Analyse rapide prend moins de temps qu'une Analyse complète du système, car elle n'effectue pas l'analyse complète de l'ordinateur.</p>
Analyse complète du système	<p>Recherche tous les types de virus et de menaces de sécurité sur l'ordinateur.</p> <p>L' Analyse complète du système effectue une analyse approfondie de l'ordinateur pour supprimer les virus et les autres menaces portant sur la sécurité. Elle vérifie l'ensemble des zones de démarrage, des fichiers et des processus en cours d'exécution auxquels l'utilisateur a accès. Par conséquent, une analyse complète du système effectuée avec des privilèges administrateur analyse plus de fichiers qu'une analyse exécutée sans privilèges administrateur.</p>
Analyse personnalisée	<p>Analyse un fichier, dossier, une unité ou unité amovible sélectionné(e).</p>

Tâche personnalisée	Exécute LiveUpdate, libère de l'espace disque et optimise le volume de votre disque.
---------------------	--

L'analyse de l'ordinateur fournit des informations sur les éléments analysés. Vous pouvez afficher les détails tels que le nombre de fichiers analysés, de risques détectés, de risques résolus et le nombre d'éléments nécessitant votre attention. Elle fournit également les différentes façons de résoudre des éléments qui n'ont pas été automatiquement résolus lors de l'analyse. Vous pouvez également afficher la gravité du risque, le nom du risque et l'état du risque concernant les éléments analysés.

Exécution d'une analyse complète du système

L'**analyse complète du système** exécute une analyse approfondie du système pour supprimer les virus et autres menaces de sécurité. Elle vérifie l'ensemble des zones de démarrage, des fichiers et des processus en cours d'exécution auxquels l'utilisateur a accès. Par conséquent, une **analyse complète du système** effectuée avec les privilèges d'administrateur, analyse plus de fichiers qu'une analyse exécutée sans les privilèges d'administrateur.

Pour exécuter une analyse complète du système

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse complète du système**.
- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Résumé des résultats**, effectuez l'une des opérations suivantes :
 - Si aucun élément ne nécessite votre intervention, cliquez sur **Terminé**.
 - Si un élément nécessite de l'attention, consultez les risques dans la fenêtre **Menaces détectées**.

Exécution d'une analyse rapide

L' **Analyse rapide** examine les zones de l'ordinateur qui sont les plus susceptibles d'être attaquées par des virus et d'autres risques de sécurité. Cette analyse prend moins de temps qu'une **analyse complète du système** car elle n'analyse pas l'intégralité de votre ordinateur.

Exécution d'une analyse rapide

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse rapide**.
- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Résumé des résultats**, effectuez l'une des opérations suivantes :
 - Si aucun élément ne nécessite votre intervention, cliquez sur **Terminé**.
 - Si un élément nécessite de l'attention, consultez les risques dans la fenêtre **Menaces détectées**.

Analyse des lecteurs, des dossiers et des fichiers sélectionnés

Occasionnellement, vous pouvez choisir d'analyser un fichier particulier, des lecteurs amovibles, l'un des lecteurs ou certains dossiers ou fichiers de votre ordinateur. Par exemple, lorsque vous travaillez avec un média amovible et suspectez un virus, vous pouvez analyser ce disque particulier. Egalement, si vous avez reçu un fichier compressé par courrier électronique et que vous suspectez un virus, vous pouvez analyser cet élément individuel.

Analyse des éléments individuels

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse personnalisée**.

- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Analyses**, effectuez l'une des opérations suivantes :
 - Pour analyser des lecteurs particuliers, cliquez sur **Exécuter** en regard de **Analyse du lecteur**, sélectionnez les lecteurs à analyser, puis cliquez sur **Analyse**.
 - Pour analyser des dossiers particuliers, cliquez sur **Exécuter** en regard de **Analyse du dossier**, sélectionnez les dossiers à analyser, puis cliquez sur **Analyse**.
 - Pour analyser des fichiers particuliers, cliquez sur **Exécuter** en regard de **Analyse du fichier**, sélectionnez les fichiers à analyser, puis cliquez sur **Analyse**.

Vous pouvez également appuyer sur **Ctrl** et sélectionner plusieurs fichiers à analyser.

Vous pouvez utiliser les options suivantes pour suspendre une analyse :

Suspendre	Suspend l'analyse personnalisée. Cliquez sur Reprendre pour poursuivre l'analyse.
Arrêter	Termine l'analyse.

- 5 Dans la fenêtre **Résumé des résultats**, effectuez l'une des opérations suivantes :
 - Si aucun élément ne nécessite votre intervention, cliquez sur **Terminé**.
 - Si un élément nécessite de l'attention, consultez-le dans la fenêtre **Menaces détectées**.

A propos de la fenêtre Résumé des résultats

Le produit Norton affiche la fenêtre **Résumé des résultats** lorsque vous exécutez une analyse manuelle.

A la fin d'une analyse, la fenêtre **Résumé des résultats** fournit le résumé des résultats de l'analyse.

Si votre analyse la plus récente était une Analyse rapide, cette fenêtre affiche les résultats de l'analyse rapide des zones de votre ordinateur, qui sont les plus susceptibles d'être attaquées par des virus, des spywares et d'autres risques.

Si vous avez effectué une analyse complète du système, la fenêtre affiche les résultats de l'analyse complète de votre ordinateur dans son intégralité.

La fenêtre **Résumé des résultats** fournit les informations suivantes :

- Nombre total d'éléments analysés
- Nombre total de risques de sécurité détectés
- Nb. total de risques de sécurité détectés :
- Nombre total d'éléments nécessitant votre attention :

Configuration des options d'analyse

Le produit Norton vous permet de configurer les options d'analyse de chaque analyse que vous personnalisez. Par défaut, les options d'analyse reflètent les paramètres courants des **Analyses d'ordinateur** de la fenêtre **Paramètres**. Les modifications que vous apportez s'appliquent uniquement à l'analyse en cours.

Outre les analyses personnalisées que vous créez, vous pouvez configurer les options d'analyse pour les analyses par défaut. Vous pouvez configurer les options d'analyse pour l'Analyse complète du système, l'Analyse rapide, l'Analyse du lecteur, l'Analyse du dossier et l'Analyse du fichier.

Configuration des options d'analyse

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse personnalisée**.

- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Analyses**, dans la colonne **Modifier l'analyse**, cliquez sur l'icône "Modifier" en regard de l'analyse à planifier.
- 5 Dans la fenêtre **Modifier l'analyse**, sur l'onglet **Options d'analyse**, modifiez les options au besoin.
- 6 Cliquez sur **Enregistrer**.

A propos de la fenêtre Menaces détectées

Votre produit Norton affiche la fenêtre **Menaces détectées** lorsqu'il détecte des menaces. À la fin d'une analyse, la fenêtre **Menaces détectées** vous présente différentes manières de résoudre les éléments n'ayant pas été automatiquement résolus pendant l'analyse.

La fenêtre **Menaces détectées** fournit des informations comme la gravité, le nom et l'état du risque. Il fournit également une solution possible pour remédier à ce risque. La fenêtre **Menaces détectées** vous offre différentes options afin de résoudre l'élément : **Corriger**, **Réparation manuelle**, **Exclure**, **Aide** et **Réanalyser**.

Il fournit également l'option **Ignorer** uniquement à la première détection d'éléments présentant un risque faible.

L'option **Ignorer** est disponible tant que les paramètres par défaut ne sont pas remplacés par l'option **Risques faibles**. Pour accéder à l'option **Risques faibles**, ouvrez la fenêtre principale du produit Norton, puis cliquez sur **Paramètres > Antivirus > Analyses et risques > Exclusions/risques faibles**.

Les options dans la fenêtre **Menaces détectées** varient en fonction des types de fichiers que le produit Norton a identifiés comme infectés au cours de l'analyse.

Sélectionner les éléments de l'analyse

Lorsque vous configurez une analyse personnalisée, vous devez sélectionner les éléments que vous souhaitez inclure dans l'analyse. Vous pouvez inclure

des fichiers, dossier ou lecteurs individuellement. Vous pouvez inclure plusieurs lecteurs, dossiers et fichiers à ajouter à l'analyse. Vous pouvez également exclure des éléments de l'analyse.



Lorsque vous sélectionnez un lecteur, tous les éléments du lecteur, notamment les fichiers et dossiers, sont automatiquement ajoutés à l'analyse. Lorsque vous sélectionnez un dossier, tous ses fichiers sont ajoutés à l'analyse.

Sélection des éléments de l'analyse

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse personnalisée**.
- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Analyses**, effectuez l'une des opérations suivantes :
 - Pour ajouter des éléments à la nouvelle analyse, cliquez sur **Créer une analyse**.
Vous devez donner un nom à l'analyse dans le champ **Nom de l'analyse**.
 - Pour ajouter des éléments à une analyse existantes, dans le colonne **Modifier l'analyse**, cliquez sur l'icône de modification pour l'analyse à modifier.

- 5 Dans la fenêtre qui apparaît, sur l'onglet **Éléments de l'analyse**, effectuez ce qui suit :
 - Pour ajouter des lecteurs, cliquez sur **Ajouter des lecteurs**, dans la boîte de dialogue **Analyse des lecteurs**, sélectionnez les lecteurs à analyser et cliquez sur **Ajouter**.
 - Pour ajouter des dossiers, cliquez sur **Ajouter des dossiers**, dans la boîte de dialogue **Analyse des dossiers**, sélectionnez les dossiers à analyser et cliquez sur **Ajouter**.
 - Pour ajouter des fichiers, cliquez sur **Ajouter des fichiers**, dans la boîte de dialogue **Analyse des fichiers**, sélectionnez les fichiers à analyser et cliquez sur **Ajouter**.

Pour supprimer un élément de la liste, sélectionnez-le et cliquez sur **Supprimer**.
- 6 Cliquez sur **Suivant**.
- 7 Dans l'onglet **Calendrier d'analyse**, sélectionnez le calendrier d'analyse souhaité et cliquez sur **Suivant**.
- 8 Dans l'onglet **Options d'analyse**, cliquez sur **Enregistrer**.

Création d'une analyse personnalisée

Vous pouvez créer une analyse personnalisée si vous analysez régulièrement une section particulière de l'ordinateur et si vous souhaitez éviter d'indiquer chaque fois la section à analyser. Vous pouvez également planifier une analyse personnalisée qui s'exécute automatiquement à des dates et heures précises ou à intervalles réguliers. Vous pouvez planifier une analyse selon vos préférences. Si l'analyse planifiée commence alors que vous utilisez l'ordinateur, vous pouvez exécuter l'analyse en arrière-plan au lieu d'interrompre votre travail.

Vous pouvez supprimer l'analyse lorsqu'elle n'est plus nécessaire. Par exemple si vous travaillez sur un projet pour lequel vous devez fréquemment échanger des fichiers avec d'autres utilisateurs. Dans ce cas, vous

pouvez créer un dossier dans lequel ces fichiers seront copiés et analysés avant toute utilisation. Lorsque le projet est terminé, vous pouvez supprimer l'analyse personnalisée correspondant à ce dossier.

Création d'une analyse personnalisée

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse personnalisée**.
- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Analyses**, cliquez sur **Créer une analyse**.
- 5 Dans la fenêtre **Nouvelle analyse**, dans la zone de texte **Nom de l'analyse**, donnez un nom à l'analyse. Vous ne pouvez pas indiquer un nom d'analyse déjà utilisé.
- 6 Dans l'onglet **Éléments de l'analyse**, ajoutez les éléments à analyser. Se reporter à "[Sélectionner les éléments de l'analyse](#)" à la page 92.
- 7 Sur l'onglet **Planification d'analyse**, réglez la fréquence et l'heure à laquelle vous voulez effectuer l'analyse. Se reporter à "[Planification d'une analyse](#)" à la page 98.
- 8 Sur l'onglet **Options d'analyse**, configurez les options d'analyse requises. Se reporter à "[Configuration des options d'analyse](#)" à la page 91.
- 9 Cliquez sur **Enregistrer**.

Modification d'une analyse personnalisée

Vous pouvez modifier une analyse personnalisée que vous avez créée. Vous pouvez inclure des fichiers ou des dossiers supplémentaires à l'analyse ou supprimer des fichiers ou dossiers que vous ne souhaitez pas analyser. Vous pouvez également changer le nom de l'analyse.

Vous pouvez modifier une analyse personnalisée dans la fenêtre **Analyses**.

Modification d'une analyse personnalisée

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse personnalisée**.
- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Analyses**, dans la colonne **Modifier l'analyse**, cliquez sur l'icône "Modifier" en regard de l'analyse personnalisée que vous voulez modifier.
- 5 Dans la fenêtre **Modifier l'analyse**, sur l'onglet **Éléments d'analyse**, sélectionnez les éléments à analyser. Se reporter à "[Sélectionner les éléments de l'analyse](#)" à la page 92.
- 6 Sur l'onglet **Planification d'analyse**, réglez la fréquence et l'heure à laquelle vous voulez effectuer l'analyse. Se reporter à "[Planification d'une analyse](#)" à la page 98.
- 7 Sur l'onglet **Options d'analyse**, configurez les options d'analyse requises. Se reporter à "[Configuration des options d'analyse](#)" à la page 91.
- 8 Cliquez sur **Enregistrer**.

Exécution d'une analyse personnalisée

Lors de l'exécution d'une analyse personnalisée, il est inutile de redéfinir les éléments à analyser.

Vous pouvez exécuter une analyse personnalisée depuis la fenêtre **Analyses**.

Exécution d'une analyse personnalisée

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse personnalisée**.

- 3 Cliquez sur **OK**.
- 4 Dans la boîte de dialogue **Analyses**, cliquez sur **Exécuter** en regard de l'analyse personnalisée à exécuter.
 Vous pouvez utiliser les options suivantes pour suspendre une analyse personnalisée :

Suspendre	Suspend l'analyse personnalisée. Cliquez sur Reprendre pour poursuivre l'analyse.
Arrêter	Arrête l'analyse personnalisée. Cliquez sur Oui pour confirmer.

- 5 Dans la fenêtre **Résumé des résultats**, effectuez l'une des opérations suivantes :
 - Si aucun élément ne nécessite votre intervention, cliquez sur **Terminé**.
 - Si un élément nécessite de l'attention, consultez les risques dans la fenêtre **Menaces détectées**.

Suppression d'une analyse personnalisée

Vous pouvez supprimer vos analyses personnalisées dès qu'elles ne sont plus nécessaires.

Suppression d'une analyse personnalisée

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse personnalisée**.
- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Analyses**, dans la colonne **Supprimer**, cliquez sur l'icône "Supprimer" en regard de l'analyse personnalisée à supprimer.

- 5 Cliquez sur **Oui** pour confirmer la suppression de l'analyse.

Planification d'une analyse

Votre produit Norton détecte automatiquement l'inactivité de votre ordinateur et exécute une analyse complète du système. Vous pouvez cependant planifier une analyse complète du système en fonction de vos préférences. Vous pouvez également planifier une analyse rapide et des analyses personnalisées.

Vous pouvez planifier les analyses personnalisées comme bon vous semble. Lorsque vous sélectionnez la fréquence d'exécution d'une analyse (quotidienne, hebdomadaire ou mensuelle), des options supplémentaires s'affichent. Par exemple, vous pouvez demander une analyse mensuelle, puis la planifier pour qu'elle survienne plutôt sur plusieurs jours.

Outre les analyses personnalisées que vous créez, votre produit Norton vous permet de planifier l'analyse complète du système et l'analyse rapide.

Vous pouvez également planifier l'exécution de l'analyse à intervalles spécifiques (heures ou jours).



Votre produit Norton vous permet de sélectionner plusieurs dates si vous planifiez une analyse mensuelle.

Planification d'une analyse personnalisée

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse personnalisée**.
- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Analyses**, dans la colonne **Modifier l'analyse**, cliquez sur l'icône "Modifier" en regard de l'analyse personnalisée à planifier.

- 5 Dans la fenêtre **Modifier l'analyse**, sur l'onglet **Planification de l'analyse**, effectuez l'une des opérations suivantes :
- Si vous ne voulez pas exécuter l'analyse à une date et une heure particulières mais souhaitez conserver les options de l'analyse et les éléments de l'analyse enregistrés, sélectionnez **Ne pas planifier cette analyse**.
 - Pour exécuter une analyse à intervalles spécifiques, sélectionnez **Exécuter à un intervalle de temps donné**.
 - Pour exécuter l'analyse à une heure spécifique tous les jours, sélectionnez **Quotidienne**.
 - Pour exécuter l'analyse un jour spécifique de la semaine, sélectionnez **Hebdomadaire**.
 - Pour exécuter l'analyse un jour spécifique dans le mois, sélectionnez **Mensuelle**.

La plupart des options de fréquence incluent des options supplémentaires que vous pouvez utiliser pour affiner la planification. Définissez les options supplémentaires en fonction de vos besoins.

- 6 Sous **Exécuter l'analyse**, effectuez ce qui suit :
- Pour exécuter l'analyse uniquement en période d'inactivité, cochez **Uniquement en période d'inactivité**.
 - Pour exécuter l'analyse uniquement lorsque votre ordinateur est relié à une source d'alimentation externe, cochez **Uniquement sur secteur**.
 - Pour empêcher votre ordinateur de passer en mode Veille, cochez **Empêcher la mise en veille**.

- 7 Sous **Après l'analyse** :, sélectionnez l'état dans lequel votre ordinateur doit se trouver après l'analyse. Vous disposez des options suivantes :
 - **Rester allumé**
 - **S'éteindre**
 - **Se mettre en veille**

Cette option fonctionne uniquement si vous avez configuré les options d'alimentation de l'ordinateur à l'aide du Panneau de configuration de Windows.
 - **Se mettre en veille prolongée**

Cette option fonctionne uniquement si vous avez configuré les options d'alimentation de l'ordinateur à l'aide du Panneau de configuration de Windows.
- 8 Cliquez sur **Suivant**.
- 9 Dans l'onglet **Options d'analyse**, cliquez sur **Enregistrer**.

Planification d'une analyse complète du système

Votre produit Norton détecte automatiquement l'inactivité de votre ordinateur et exécute une analyse complète du système. L'analyse complète du système protège votre ordinateur contre les infections, sans mettre en péril son niveau de performance. Vous pouvez planifier une analyse complète du système à des dates et heures spécifiques ou à intervalles réguliers.

Vous pouvez planifier une analyse complète du système dans la fenêtre **Analyses**.

Planification d'une Analyse complète du système

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse personnalisée**.
- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Analyses**, dans la colonne **Modifier l'analyse**, cliquez sur l'icône "Modifier" en regard de **Analyse complète du système**.

- 5 Dans la fenêtre **Modifier l'analyse**, sous **Quand voulez-vous exécuter l'analyse ?**, définissez la fréquence et l'heure d'exécution de l'analyse. La plupart des options de fréquence incluent des options supplémentaires que vous pouvez utiliser pour affiner la planification. Définissez les options supplémentaires en fonction de vos besoins.
- 6 Cliquez sur **Suivant**.
- 7 Dans l'onglet **Options d'analyse**, cliquez sur **Enregistrer**.

Planifier une Analyse rapide

L'analyse rapide analyse les emplacements importants de votre ordinateur souvent ciblés par les virus et autres menaces de sécurité. Lorsque vous effectuez une analyse rapide, le produit Norton analyse uniquement les processus en cours d'exécution et les programmes chargés. L'analyse rapide est moins longue que l'analyse complète du système, car elle n'analyse pas l'intégralité de l'ordinateur.

Votre produit Norton vous permet de planifier une analyse rapide. Vous pouvez planifier une Analyse rapide dans la fenêtre **Analyses**.

Planification d'une analyse rapide

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse personnalisée**.
- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Analyses**, dans la colonne **Modifier l'analyse**, cliquez sur l'icône "Modifier" en regard de **Analyse rapide**.

- 5 Dans la fenêtre **Modifier l'analyse**, sous **Quand voulez-vous exécuter l'analyse ?**, définissez la fréquence et l'heure d'exécution de l'analyse. La plupart des options de fréquence incluent des options supplémentaires que vous pouvez utiliser pour affiner la planification. Définissez les options supplémentaires en fonction de vos besoins.
- 6 Cliquez sur **Suivant**.
- 7 Dans l'onglet **Options d'analyse**, cliquez sur **Enregistrer**.

Modification d'une analyse planifiée

Vous pouvez modifier la planification de toute analyse personnalisée planifiée, d'une **analyse rapide** ou d'une **analyse complète du système** à partir de la fenêtre **Analyses**.

Modification d'une analyse planifiée

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Analyse personnalisée**.
- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Analyses**, dans la colonne **Modifier l'analyse**, cliquez sur l'icône "Modifier" en regard de l'analyse personnalisée à modifier.
- 5 Dans la fenêtre **Modifier l'analyse**, sur l'onglet **Planification de l'analyse**, modifiez la planification au besoin. La plupart des options de fréquence incluent des options supplémentaires que vous pouvez utiliser pour affiner la planification. Définissez les options supplémentaires en fonction de vos besoins.
- 6 Cliquez sur **Suivant**.
- 7 Dans l'onglet **Options d'analyse**, cliquez sur **Enregistrer**.

Exécution d'une analyse à l'invite de commande

Vous pouvez démarrer une analyse à l'aide de votre produit Norton à partir de l'invite de commande, sans ouvrir la fenêtre principale du produit Norton. Il vous suffit de saisir le chemin d'accès et le nom du fichier à analyser ou de personnaliser l'analyse en ajoutant une commande spécifique. Les commandes suivantes sont les plus fréquentes :

/?	NAVW32 lance l'aide et termine.
/A	Analyse tous les disques
/L	Analyse les lecteurs locaux
/S[+ -]	Active (+) ou désactive (-) analyse des sous-dossiers
/B[+ -]	Active (+) ou désactive (-) l'analyse de l'enregistrement de démarrage et enregistrement de démarrage principal (par-exemple, NAVW32 C: /B+ ou NAVW32 C: /B-)
/BOOT	Analyse uniquement les zones amorce
/QUICK	Exécute une Analyse rapide

/SE[+ -]	Active (+) ou désactive (-) une Analyse rapide
/ST[+ -]	Active (+) ou désactive (-) l'analyse d'éléments furtifs
[folder_path]*[?]	Analyse les fichiers qui correspondent au caractère générique spécifié
[drive]folder[file]	Analyse le lecteur, dossier ou fichier indiqué
/SESCAN	Exécute une analyse rapide à l'arrière-plan.  Votre produit Norton n'affiche la fenêtre Analyses que si une menace est détectée.

Exécution d'une analyse depuis l'invite de commande

- 1 A l'invite de commande, tapez le chemin d'accès dans lequel se trouve Norton Security, et le nom du fichier exécutable.

Les exemples suivants indiquent la syntaxe d'une commande d'analyse :

```
❏ "\Program Files\Norton  
Security\Engine\version\NAVW32"  
/nom_commande
```

où *version* représente le numéro de version de Norton Security et *nom_commande* représente la commande.

```
❏ "\Program Files\Norton  
Security\Engine\version\NAVW32"  
[chemin]nom_fichier
```

où *version* représente le numéro de version de Norton Security et *[chemin] nom_fichier* représente l'emplacement, le nom et l'extension du fichier.

- 2 Appuyez sur la touche **Entrée**.

Analyse de l'ordinateur à l'aide de Norton Power Eraser

Norton Power Eraser est un outil de suppression des malwares performant qui vous aide à supprimer les risques de sécurité récalcitrants. Si un programme a piraté votre ordinateur et que vous n'arrivez pas à le détecter ou à le supprimer, Norton Power Eraser peut supprimer ce risque de sécurité de votre ordinateur. Il s'attaque aux logiciels criminels difficiles à détecter ("scareware" ou "rogueware") qu'utilisent les cybercriminels pour vous amener à télécharger des menaces sur votre ordinateur à votre insu.

Norton Power Eraser détecte et supprime les risques de sécurité détournant vos applications légitimes, tels que les faux logiciels antivirus connus sous le nom de scareware, rogueware ou scamware. Cet outil utilise des techniques plus agressives que Norton Security. Il

existe donc un risque qu'il vous demande de supprimer des programmes légitimes. Consultez attentivement les résultats de l'analyse avant de supprimer des fichiers.

Quand vous analysez des menaces et que vous y remédiez, Norton Power Eraser crée un point de restauration du système. Si vous supprimez des fichiers essentiels, Norton Power Eraser vous permet de les restaurer à l'aide de l'option **Annuler la correction précédente**. Norton Power Eraser répertorie les dernières sessions de réparation dans lesquelles vous pouvez afficher les fichiers importants et les restaurer.

Pour plus d'informations sur Norton Power Eraser, consultez Didacticiels Norton Power Eraser.

Exécution d'une analyse à l'aide de Norton Power Eraser

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Norton Power Eraser**, cliquez sur **Norton Power Eraser**.
- 3 Cliquez sur **OK**.
- 4 Dans la fenêtre **Norton Power Eraser**, cliquez sur **OK**.
- 5 Dans la fenêtre **Norton Power Eraser**, cliquez sur **Options avancées**.
- 6 Sous **Analyse du système**, cliquez sur **Analyser maintenant**.
- 7 Examinez les résultats de l'analyse et suivez les instructions à l'écran pour résoudre les risques de sécurité détectés.

Analyse de votre mur Facebook

Norton Safe Web protège votre ordinateur contre les URL malveillantes lorsque vous utilisez Facebook. Cet outil analyse chaque URL présente sur votre mur Facebook et affiche les icônes d'évaluation Norton pour les URL analysées.

Vous pouvez également vérifier la sécurité de l'URL. Norton Safe Web analyse votre fil d'actualités sur Facebook et vous indique un état de sécurité pour chaque URL. De cette manière, vous êtes non seulement protégé des sites non sécurisés, mais vous pouvez également informer d'autres utilisateurs de Facebook sur l'état de sécurité d'un site Web.

Toutefois, Norton Safe Web nécessite votre autorisation pour analyser les URL présentes sur votre mur Facebook. Lorsque vous installez l'application Facebook Norton Safe Web, elle vous demande l'autorisation d'accéder à votre mur Facebook. Vous pouvez autoriser ou non l'accès à votre mur Facebook par Norton Safe Web.

La fonction d'analyse automatique de l'application Norton Safe Web permet de protéger votre mur Facebook lorsque vous n'êtes pas connecté. Norton Safe Web analyse quotidiennement le fil d'actualité de votre mur Facebook et vous protège contre les liens malveillants. Lorsque Norton Safe Web détecte un lien malveillant, il publie une notification sur votre mur Facebook. Pour activer l' **analyse automatique Norton**, déplacez le curseur **Analyse automatique activée/Analyse automatique désactivée** vers la gauche sur la position **Analyse automatique activée**. L'application demande une autre autorisation pour afficher automatiquement une publication sur votre mur lorsque des liens malveillants sont identifiés.

Pour supprimer le lien malveillant de votre mur Facebook, accédez à votre mur Facebook et supprimez le lien. Vous pouvez aussi cliquer sur **Afficher le rapport de Norton Safe Web** pour voir les évaluations Norton et d'autres détails concernant ce lien malveillant. Si aucune activité malveillante n'est détectée sur votre mur Facebook, Norton Safe Web publie un message pour vous avertir que votre mur Facebook est sécurisé. Norton Safe Web publie ce message sur votre mur Facebook une fois tous les 30 jours.

Si vous décidez par la suite de supprimer la fonction Norton Safe Web de votre profil Facebook, vous pouvez utiliser l'option **Paramètres de compte** de Facebook.

Norton Safe Web indique les états de sécurité suivants après avoir analysé les liens de votre mur Facebook :

Norton Secured	<p>Indique que le site présente les meilleures pratiques en matière de sécurité.</p> <p>Les sites ayant ce type d'évaluation n'exposent votre ordinateur à aucun danger, et vous pouvez les visiter en toute confiance.</p>
Sécurisé	<p>Indique que le site est fiable et approuvé par Norton.</p> <p>Les sites ayant ce type d'évaluation n'exposent votre ordinateur à aucun danger, et vous pouvez les visiter.</p>
Attention	<p>Indique que le site présente des menaces de sécurité. Symantec vous recommande d'être très prudent lorsque vous visitez ce type de site Web.</p>
Warning (Avertissement)	<p>Indique que le site présente des risques de sécurité.</p> <p>Ces sites ayant ce type d'évaluation peuvent tenter d'installer des logiciels malveillants sur votre ordinateur. Symantec vous recommande de ne pas les visiter.</p>

<p>Non testé</p>	<p>Indique que Norton Safe Web n'a pas encore testé ce site et ne possède pas assez d'informations à son sujet.</p>
-------------------------	---

Activation de l'analyse de votre mur Facebook

La fonction Norton Safe Web analyse votre mur Facebook et détermine les niveaux de sécurité de tous les liens publiés sur votre mur durant les dernières 24 heures. Il affiche ensuite l'état de sécurité des URL analysées. Toutefois, Norton Safe Web nécessite votre autorisation pour analyser votre mur Facebook.

Activation de l'analyse de votre mur Facebook

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyser le mur Facebook**, cliquez sur **Analyser le mur Facebook**.
- 3 Cliquez sur **OK**.
- 4 A partir de la page Web de connexion à Facebook, connectez-vous à votre profil Facebook.
- 5 Autorisez l'application à accéder à votre profil public, votre liste d'amis et votre fil d'actualités.
- 6 Cliquez sur **Analyse automatique activée** afin que l'analyse automatique Norton protège votre compte Facebook.
- 7 Autorisez l'application à publier des notifications de votre part.

Désactivation ou activation de la fonction Protection SONAR

SONAR détecte les codes malveillants et vous protège même avant que les définitions des virus ne soient disponibles par LiveUpdate. En outre, vous pouvez activer la Protection SONAR pour détecter de manière

proactive les risques de sécurité inconnus sur votre ordinateur.

Lorsque vous désactivez la Protection SONAR, vous êtes invité par une alerte de protection. Cette alerte de protection permet de préciser la durée de désactivation de la protection SONAR.



Lorsqu'Auto-Protect est arrêté, l'option Protection SONAR est également désactivée. Dans ce cas, votre ordinateur n'est pas protégé contre les menaces naissantes.

Activation ou désactivation de la fonction Protection SONAR

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antivirus**.
- 3 Dans l'onglet **Protection automatique**, sous **Protection en temps réel**, à la ligne **Protection SONAR**, effectuez l'une des opérations suivantes :
 - Pour désactiver la Protection SONAR, déplacez le curseur **Marche/Arrêt** vers la droite sur la position Arrêt.
 - Pour activer la Protection SONAR, déplacez le curseur **Marche/Arrêt** vers la gauche sur la position Marche.
- 4 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**.

Exclure des menaces de sécurité de l'analyse

Vous pouvez utiliser la fenêtre **Exclusions d'analyse** et la fenêtre **Exclusions en temps réel** pour exclure de l'analyse les virus et autres menaces élevées de sécurité.

Exclusion des menaces élevées de sécurité de l'analyse

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.

- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antivirus**.
- 3 Dans la fenêtre de paramètres **Antivirus**, cliquez sur l'onglet **Analyses et risques**.
- 4 Sous **Exclusions/risques faibles**, procédez de l'une des manières suivantes :
 - A la ligne **Éléments à exclure des analyses**, cliquez sur **Configurer**.
 - A la ligne **Éléments à exclure de la détection des fonctions Auto-Protect, SONAR et Diagnostic des téléchargements**, cliquez sur **Configurer**.
- 5 Dans la fenêtre qui s'affiche, cliquez sur **Ajouter des dossiers** ou **Ajouter des fichiers**.
- 6 Dans la boîte de dialogue **Ajouter des éléments**, cliquez sur l'icône parcourir.
- 7 Dans la boîte de dialogue qui s'affiche, sélectionnez l'élément à exclure de l'analyse.
- 8 Cliquez sur **OK**.
- 9 Dans la boîte de dialogue **Ajouter des éléments**, cliquez sur **OK**.
- 10 Dans la fenêtre qui s'affiche, cliquez sur **Appliquer**, puis sur **OK**.

Ajouter des éléments aux Exclusions de signatures

Pour exclure un risque de sécurité des analyses, vous devez ajouter le risque de sécurité en question à la fenêtre **Exclusions de signatures**. Vous pouvez sélectionner un risque connu par son nom et l'ajouter à la liste.



Lorsque vous excluez un risque de sécurité connu des analyses Norton Security, le niveau de protection de votre ordinateur est amoindri. Vous ne devez exclure des éléments que si vous êtes sûr qu'ils ne sont pas infectés.

Ajout d'une signature aux Exclusions de signatures

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antivirus**.
- 3 Dans la fenêtre de paramètres **Antivirus**, cliquez sur l'onglet **Analyses et risques**.
- 4 Dans la section **Exclusions/risques faibles**, à la ligne **Signatures à exclure de toutes les détections**, cliquez sur **Configurer**.
- 5 Dans la fenêtre **Exclusions de signatures**, cliquez sur **Ajouter**.
- 6 Dans la fenêtre **Risques de sécurité**, cliquez sur un risque de sécurité à exclure, puis cliquez sur **Ajouter**.
- 7 Dans la fenêtre **Exclusions de signatures**, cliquez sur **Appliquer**, puis sur **OK**.

Effacement des ID de fichiers exclus lors des analyses

Votre produit Norton attribue les niveaux d'approbation **Approuvé** et **Bon** à tous les fichiers approuvés. Si un fichier est marqué comme **Approuvé** ou **Bon**, le produit Norton ne le réanalyse pas. Cela permet d'améliorer les performances de l'analyse du produit Norton sur votre ordinateur.

Si vous souhaitez toutefois que le produit Norton analyse tous les fichiers de votre ordinateur, vous devez effacer toutes les informations de réputation des fichiers exclus.



Si vous effacez les ID des fichiers exclus lors des analyses, l'analyse prendra plus de temps.

Votre produit Norton exclut des analyses les fichiers dont le niveau d'approbation est **Approuvé** et **Bon**. Si vous souhaitez toutefois que le produit Norton analyse tous les fichiers de votre ordinateur, vous devez effacer toutes les informations de réputation des fichiers exclus.

Effacement des ID de fichiers exclus lors des analyses

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.

- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antivirus**.
- 3 Dans la fenêtre **Paramètres de l'antivirus**, cliquez sur l'onglet **Analyses et risques**.
- 4 Sous **Exclusions/risques faibles**, à la ligne **Effacer tous les ID de fichiers exclus lors des analyses**, cliquez sur **Tout effacer**.
- 5 Dans la fenêtre **Avertissement**, cliquez sur **Oui**.

A propos du Mode silencieux activé manuellement

Votre produit Norton permet d'activer manuellement le mode silencieux pendant une durée déterminée. Lorsque le mode silencieux est activé, votre produit Norton supprime toutes les alertes et suspend les activités en arrière-plan pendant la durée déterminée. Vous pouvez vérifier que le mode silencieux est activé dans la zone de notification, à droite de la barre des tâches. L'icône de Norton Security, en forme de cercle et placée dans la zone de notification, passe du jaune au gris pour indiquer que le mode silencieux est activé. L'activation manuelle du mode silencieux avant l'exécution de vos tâches permet d'éviter que des alertes, des notifications ou des activités d'arrière-plan vous interrompent, et ce, pendant une durée déterminée.

Vous pouvez activer le mode silencieux pour une, deux, quatre ou six heures, ou pour une journée entière. Au terme de la durée indiquée, le produit Norton désactive le mode silencieux. Vous pouvez également désactiver manuellement le mode silencieux à tout instant. Votre produit Norton vous informe après la désactivation du mode silencieux. Les activités suspendues lors de l'activation du Mode silencieux reprennent après la désactivation de ce mode.

Activation ou désactivation manuelle du mode silencieux

Vous pouvez activer manuellement le mode silencieux pour une durée précise avant d'effectuer des tâches importantes sur votre ordinateur. Vous pouvez activer

le mode silencieux pour une, deux, quatre ou six heures, ou pour une journée entière. L'icône Norton Security affiche l'état d'activation du Mode silencieux dans la zone de notification, dans la partie droite de la barre des tâches. Votre produit Norton vous informe après la désactivation du mode silencieux. Après la désactivation du mode silencieux, votre produit Norton affiche également des alertes si des activités de sécurité qui se sont produites pendant la session du mode silencieux sont détectées.

Vous pouvez activer ou désactiver le mode silencieux depuis la section **Paramètres de mode silencieux** de la fenêtre **Paramètres**. Vous pouvez également activer ou désactiver le Mode silencieux à l'aide de l'icône Norton Security dans la zone de notification.

Activation du mode silencieux dans la fenêtre Paramètres administratifs

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Paramètres du mode silencieux**, à la ligne **Mode silencieux**, déplacez le curseur **Marche/Arrêt** vers la gauche sur la position **Marche**.
- 4 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**.
- 5 Dans la boîte de dialogue **Activer le mode silencieux**, dans la liste déroulante **Sélectionner la durée**, sélectionnez la durée pendant laquelle le Mode silencieux doit être activé, puis cliquez sur **OK**.
- 6 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Activation du mode silencieux dans la fenêtre Paramètres administratifs

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.

- 3 Sous **Paramètres du mode silencieux**, à la ligne **Mode silencieux**, déplacez le curseur **Marche/Arrêt** vers la droite sur la position **Arrêt**.
- 4 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**, puis sur **Fermer**.

Activation du mode silencieux depuis la zone de notification

- 1 Dans la zone de notification de la barre des tâches, cliquez avec le bouton droit sur l'icône de Norton Security, puis cliquez sur **Activer le mode silencieux**.
- 2 Dans la boîte de dialogue **Activer le mode silencieux**, dans la liste déroulante **Sélectionner la durée**, sélectionnez la durée pendant laquelle le Mode silencieux doit être activé, puis cliquez sur **OK**.

Désactivation du mode silencieux depuis la zone de notification

- ❖ Dans la zone de notification de la barre des tâches Windows, cliquez avec le bouton droit sur l'icône de Norton Security, puis cliquez sur **Désactiver le mode silencieux**.

Activation ou désactivation du mode silencieux dans les commandes rapides

- 1 Dans la fenêtre principale Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Commandes rapides**, effectuez l'une des opérations suivantes :
 - Pour désactiver le mode silencieux, désélectionnez **Mode silencieux**.
 - Pour activer le mode silencieux, sélectionnez **Mode silencieux** et la durée pendant laquelle le mode silencieux doit être activé dans la boîte de dialogue Activer le mode silencieux, puis cliquez sur **OK**.

A propos de l'activation automatique du Mode silencieux

Lorsque vous regardez un film, jouez à un jeu ou animez une présentation, vous exécutez l'application en mode plein écran. Votre produit Norton détecte l'application en mode plein écran et active automatiquement le mode silencieux. Lorsque le mode silencieux est activé, votre produit Norton supprime la plupart des alertes et suspend les activités en arrière-plan. Seules les activités chargées de la protection de l'ordinateur contre les virus et autres menaces de sécurité sont exécutées. Un minimum d'activités d'arrière-plan assure également à votre ordinateur une meilleure performance. Les activités suspendues reprennent leur exécution après que vous ayez terminé d'utiliser une application en mode plein écran.

Le Mode silencieux vous aide également à maintenir une session Media Center Extender ininterrompue. Une session Media Center Extender est une session du Media Center étendue à un appareil de divertissement comme un téléviseur. Les alertes et notifications qui s'affichent pendant une session Media Center Extender déconnectent la session entre l'ordinateur hôte et l'appareil de divertissement. Votre produit Norton identifie une session Media Center Extender comme une application plein écran active et déclenche le mode silencieux. Lorsque le mode silencieux est activé, votre produit Norton supprime les alertes et les notifications et suspend les activités en arrière-plan pour prévenir toute interruption des options du mode silencieux, telles que la détection plein écran ou les applications Media Center.

Activation ou désactivation de la fonction Détection plein écran

Vous pouvez utiliser l'option **Détection plein écran** de la fenêtre **Paramètres** pour activer ou désactiver automatiquement le mode silencieux lorsque le produit Norton détecte une application plein écran. Par défaut,

l'option **Détection plein écran** reste activée après l'installation de Norton Security.

Désactivation de la détection plein écran

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Paramètres du mode silencieux**, sur la ligne **Détection plein écran**, déplacez le curseur **Marche/Arrêt** vers la droite sur la position **Arrêt**.
- 4 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**, puis sur **Fermer**.

Activation de la détection plein écran

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Paramètres du Mode silencieux**, sur la ligne **Détection plein écran**, déplacez le curseur **Marche/Arrêt** vers la gauche sur la position **Marche**.
- 4 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**, puis sur **Fermer**.

A propos du Mode discret

Votre produit Norton active automatiquement le Mode discret lorsque vous exécutez des tâches nécessitant une utilisation plus large des ressources de votre système. Lorsque le Mode discret est activé, votre produit Norton suspend les activités d'arrière-plan et laisse la tâche utiliser le maximum des ressources pour de meilleures performances.

Vous avez la possibilité de configurer votre produit Norton afin qu'il active le Mode discret automatiquement lorsque vous effectuez les tâches suivantes :

- Gravure de disque IMAPI 2.0
- Programmes spécifiés par l'utilisateur

Le tableau ci-dessous fournit des explications concernant les différentes options :

Gravure de disque IMAPI 2.0	
--	--

Lorsque vous utilisez une application Media Center pour graver un CD ou un DVD, votre produit Norton active automatiquement le Mode discret si l'option **Gravure de disque IMAPI 2.0** est activée. L'option **Gravure de disque IMAPI 2.0** est activée par défaut. Lorsque le Mode discret est activé, votre produit Norton suspend les activités d'arrière-plan pour améliorer les performances de votre session de gravure de disque. Cependant, votre produit Norton continue d'afficher des alertes et des notifications pendant la session.

Votre produit Norton prend en charge les applications du graveur de disques du Media Center pour activer le Mode discret :

- IMAPI 2.0
- J. River MEDIA CENTER (version 13.0.125 et suivante)

Votre produit Norton active le mode discret dès que vous commencez à graver un CD ou un DVD à l'aide d'une application Media Center. Votre produit Norton désactive le mode discret à la fin de la session de gravure de disque. Vous ne pouvez pas désactiver le Mode discret pendant la session de gravure en désactivant l'option **Gravure de disque IMAPI 2.0** dans la

<p>Programmes spécifiés par l'utilisateur</p>	<p>fenêtre Paramètres.</p> <p>Votre produit Norton active automatiquement le mode discret lorsqu'il détecte une session de gravure de disque. De plus, vous pouvez ajouter manuellement les programmes pour lesquels vous souhaitez que le produit Norton active le mode discret à la liste Programmes du mode discret. Lorsque le produit Norton détecte une instance en cours d'exécution d'un programme ajouté à la liste, il active automatiquement le mode discret. Lorsque le mode discret est activé, votre produit Norton suspend les activités en arrière-plan, mais ne supprime pas les alertes et les notifications.</p> <p>Vous pouvez également ajouter ou supprimer un programme en cours d'exécution à la liste des programmes du mode discret.</p>
--	---

Désactivation ou activation des options du Mode discret

Vous pouvez désactiver ou activer les options du mode discret, comme **Gravure de disque IMAPI 2.0** ou **Programmes spécifiés par l'utilisateur** dans la fenêtre **Paramètres**. L'option Gravure de disque IMAPI 2.0 est activée par défaut. Si vous exécutez une tâche pour l'option Gravure de disque IMAPI 2.0 que vous avez activée, votre produit Norton détecte la tâche et active automatiquement le Mode silencieux. Par exemple, vous activez l'option **Gravure de disque IMAPI 2.0** et commencez à graver un disque en utilisant l'application

Media Center. Dans ce cas, votre produit Norton détecte la session de gravure du disque et active le Mode discret.

Votre produit Norton active le mode discret dès que vous commencez à graver un CD ou un DVD. Dès que le Mode discret est activé, il se désactive uniquement à la fin de la session d'enregistrement du programme TV ou de la gravure du disque. Vous ne pouvez pas désactiver le Mode discret pendant des sessions en utilisant les options de la fenêtre **Paramètres**.

Désactivation ou activation de la fonction Gravure de disque IMAPI 2.0

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Paramètres du mode silencieux**, dans la **ligne Gravure de disque IMAPI 2.0**, effectuez l'une des opérations suivantes :
 - Pour désactiver la détection d'une session de gravure de disque, déplacez le curseur **Ac./Désac.** vers la droite sur la position **Désac..**
 - Pour activer la détection lors d'une session de gravure de disque, déplacez le curseur **Ac./Désac.** vers la gauche sur la position **Ac..**
- 4 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**.
- 5 Cliquez sur **Fermer**.

A propos des programmes spécifiés par l'utilisateur

Le produit Norton active automatiquement le mode discret lorsqu'il détecte une session de gravure de disque. De plus, vous pouvez ajouter manuellement les programmes pour lesquels vous souhaitez que le produit Norton active le mode discret à la liste Programmes du mode discret. Lorsque le produit Norton détecte une instance en cours d'exécution d'un programme ajouté à la liste, il active automatiquement le mode discret. Lorsque le mode discret est activé, votre produit Norton

suspend les activités en arrière-plan, mais ne supprime pas les alertes et les notifications.

Vous pouvez également ajouter un programme en cours d'exécution à la liste Programmes en Mode discret. Cependant, lorsque vous ajoutez un programme en cours d'exécution, le produit Norton ne détecte pas l'instance du programme en cours d'exécution et n'active donc pas le mode discret. Le produit Norton activera le mode discret la prochaine fois que vous exécuterez le programme.

Vous pouvez également supprimer un programme en cours d'exécution de la liste Programmes en Mode discret. Cependant, si le Mode discret est activé, il se désactivera uniquement après que les occurrences de tous les programmes en cours d'exécution de la liste soient terminées. La suppression d'un programme de la liste lorsqu'il fonctionne vous empêche de désactiver le Mode discret.

Vous pouvez afficher les détails des programmes que vous ajoutez ou supprimez dans la liste Programmes en Mode discret dans la fenêtre **Historique de la sécurité**.

Ajout de programmes à la liste Programmes spécifiés par l'utilisateur

Vous pouvez ajouter manuellement les programmes pour lesquels vous souhaitez que le produit Norton active le mode discret à la liste Programmes du mode discret. Lorsque vous exécutez le programme ajouté à la liste, le produit Norton le détecte et active le mode discret.

Vous pouvez également ajouter un programme en cours d'exécution à la liste **Programmes du mode discret**. Cependant, lorsque vous ajoutez un programme en cours d'exécution, le produit Norton ne détecte pas l'instance du programme en cours d'exécution et n'active donc pas le mode discret. Le produit Norton activera le

mode discret la prochaine fois que vous exécuterez le programme.

Vous pouvez uniquement ajouter des programmes portant l'extension de fichier .exe à la liste **Programmes en Mode discret**.

Ajout d'un programme

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Paramètres de mode silencieux**, à la ligne **Programmes spécifiés par l'utilisateur**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Programmes en Mode discret**, cliquez sur **Ajouter**.
- 5 Dans la boîte de dialogue **Ajouter un programme**, naviguez jusqu'à l'emplacement du fichier à ajouter dans la liste Programmes en mode discret.
- 6 Sélectionnez le fichier, puis cliquez sur **Ouvrir**.
- 7 Dans la fenêtre **Programmes en Mode discret**, cliquez sur **OK**.

Suppression des programmes de la liste Programmes spécifiés par l'utilisateur

Vous pouvez également supprimer un programme de la liste **Programmes du mode discret**. Après avoir supprimé un programme, votre produit Norton n'activera pas le Mode discret la prochaine fois qu'il détectera une occurrence de programme en cours d'exécution.

Vous pouvez également supprimer un programme en cours d'exécution de la liste **Programmes en Mode discret**. Cependant, si le Mode discret est activé, il se désactivera uniquement après que les occurrences de tous les programmes en cours d'exécution de la liste soient terminées. La suppression d'un programme de la liste lorsqu'il fonctionne vous empêche de désactiver le Mode discret.

Suppression d'un programme

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Paramètres du Mode silencieux**, à la ligne **Programmes spécifiés par l'utilisateur**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Programmes en Mode discret**, sélectionnez le programme que vous souhaitez supprimer, et cliquez sur **Supprimer**.
- 5 Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.
- 6 Dans la fenêtre **Programmes du mode discret**, cliquez **Appliquer**, puis sur **OK**.

Configuration de la protection au démarrage

La fonction Protection au démarrage assure un niveau de sécurité amélioré dès le moment où vous démarrez votre ordinateur. Dès que vous démarrez l'ordinateur, votre produit Norton lance Auto-Protect et tous les pilotes et plug-ins requis se mettent en marche. Cette fonction garantit un niveau de sécurité supérieur dès que vous mettez l'ordinateur sous tension.

Configuration de la protection au démarrage

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antivirus**.
- 3 Dans l'onglet **Protection automatique**, dans la ligne **Protection au démarrage**, cliquez sur l'un des paramètres. Vos options sont :
 - **Agressif**
 - **Normal**
 - **Désactivé**
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Activation ou désactivation de la protection antimalware au démarrage

La fonction **Protection antimalware au démarrage** assure un niveau de sécurité renforcé au démarrage de l'ordinateur. Cette option améliore la protection en exécutant tous les composants du produit Norton nécessaires pour bloquer l'exécution de tout malware au démarrage de l'ordinateur.



Cette option n'est disponible que sous Windows 8 ou version ultérieure.

Activation ou désactivation d'antimalware au démarrage

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antivirus**.
- 3 Dans la fenêtre de paramètres **Antivirus**, cliquez sur l'onglet **Protection automatique**.
- 4 A la ligne **Protection antimalware au démarrage**, effectuez l'une des actions suivantes :
 - Pour activer l'option **Protection antimalware au démarrage**, déplacez le curseur **Ac./Désac.** vers la gauche sur la position **Activé**.
 - Pour désactiver l'option **Protection antimalware au démarrage**, déplacez le curseur **Ac./Désac.** vers la droite sur la position **Désactivé**.
- 5 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**, puis sur **Fermer**.

Ce chapitre traite des sujets suivants :

- [Maintenir votre ordinateur sécurisé](#)
- [A propos de la résolution des problèmes de connexion](#)
- [A propos de la réaction aux urgences](#)
- [Mesures à prendre en cas de détection d'un virus](#)

Maintenir votre ordinateur sécurisé

L'installation de la dernière version du produit Norton est la meilleure façon d'assurer la protection de votre PC contre les logiciels malveillants et les virus. Nous vous recommandons de maintenir à jour les définitions de virus. Si vous disposez d'une connexion Internet active, les définitions sont mises à jour automatiquement.

De plus, il existe plusieurs règles de sécurité que vous devriez respecter pour éviter les menaces et protéger votre PC et vos données contre les virus et les logiciels malveillants :

Pour éviter les menaces portant sur la messagerie, procédez comme suit :

- N'ouvrez une pièce jointe de courrier électronique que si elle provient d'une source de confiance et que vous vous attendiez à recevoir cette pièce jointe.

- Supprimez tous les messages indésirables sans les ouvrir.
- Si vous suspectez qu'un message électronique est du spam, n'y répondez pas. Supprimez-le.
- Méfiez-vous particulièrement des messages vous demandant des informations confidentielles et vérifiez l'authenticité de la requête avant d'y répondre.

Pour vous protéger des tentatives de phishing, procédez comme suit :

- Lorsque vous visitez un site Web, entrez directement l'adresse dans votre navigateur plutôt que de cliquer sur un lien.
- Ne fournissez d'informations personnelles qu'à des sites approuvés. Il s'agit par exemple des sites dont l'adresse Web commence par "https" ou pour lesquels une icône en forme de verrou apparaît en bas de la fenêtre du navigateur.
- Ne communiquez jamais d'informations confidentielles en réponse à une demande d'informations non sollicitée.

Pour éviter les virus, les vers et les chevaux de Troie, procédez comme suit :

- Ne transférez des fichiers vers votre ordinateur qu'à partir d'une source connue et de confiance.
- Ne transmettez pas de fichiers (envoi ou réception) par l'intermédiaire de connexions de messagerie instantanée.
- Mettez fin à une connexion de messagerie instantanée si une personne faisant partie de votre liste d'amis vous envoie des messages, des fichiers ou des liens Web inopportuns.

Pour éviter les spywares, procédez comme suit :

- Ne cliquez pas sur OK dans les boîtes de dialogue d'erreur suspectes qui s'affichent dans votre navigateur.
- Méfiez-vous des "offres gratuites" : les spywares se propagent souvent de cette manière.

- Lisez soigneusement le contrat de licence d'utilisateur des programmes que vous installez. N'installez pas non plus de programme dont l'installation implique celle d'autres programmes.

A propos de la résolution des problèmes de connexion

Votre produit Norton utilise une connexion à Internet pour plusieurs de ses fonctions de protection. Si vous passez par un serveur proxy pour vous connecter à Internet, vous devez configurer les paramètres proxy du produit Norton. Vous pouvez configurer les paramètres proxy de réseau dans la fenêtre **Paramètres administratifs**.

Si vous ne parvenez pas à vous connecter à Internet après l'installation du produit Norton, vous pouvez utiliser les fonctions de support pour résoudre votre problème de connexion.

A propos de la réaction aux urgences

Votre produit Norton télécharge automatiquement et régulièrement les mises à jour des définitions et protège votre ordinateur contre les nouveaux virus et les nouvelles menaces inconnues. En outre, le produit Norton surveille également vos activités sur Internet pour protéger votre ordinateur contre les menaces en provenance d'Internet qui pourraient exploiter les vulnérabilités de logiciels légitimes.

Cependant, il se peut que dans certains cas vous deviez décider des mesures à prendre à propos des problèmes de sécurité.

Si vous pensez que votre ordinateur est infecté par un virus ou un logiciel malveillant, vous pouvez effectuer les opérations suivantes :

Analyse rapide	<p>L'Analyse rapide vous permet d'analyser les zones de l'ordinateur qui sont le plus souvent la cible de virus et d'autres risques de sécurité.</p> <p>L'Analyse rapide prend moins de temps qu'une Analyse complète du système, car elle n'effectue pas l'analyse complète de l'ordinateur.</p>
Analyse complète du système	<p>Vérifie tous les enregistrements d'amorçage, fichiers et programmes en cours d'exécution pour protéger votre ordinateur contre les virus et les logiciels espions.</p> <p>Ainsi, une analyse complète du système avec des privilèges administrateur analyse plus de fichiers qu'une analyse exécutée sans privilèges administrateur. Cette analyse peut durer plus longtemps que les autres types d'analyse.</p>
Analyse personnalisée	<p>Analyse le fichier, dossier, lecteur ou lecteur amovible sélectionné. Vous pouvez également créer votre propre analyse et planifier son exécution à une date et une heure précises.</p>

Tâche personnalisée	Cette analyse recherche les vulnérabilités et les risques et protège votre ordinateur en effectuant les contrôles suivants : <ul style="list-style-type: none">■ LiveUpdate■ Fichiers Internet Explorer temporaires■ Fichiers temporaires Windows■ Historique Internet Explorer■ Optimisation du disque
----------------------------	---

Lorsque vous cliquez avec le bouton droit de la souris sur un dossier, le menu contextuel affiche Norton Security et l'option **Analyser maintenant**. Vous pouvez utiliser cette option pour analyser un fichier ou un dossier spécifique. L'analyse de Norton Insight est exécutée en même temps que cette analyse. Cette option analyse ainsi un fichier à l'aide des définitions locales et de celles hébergées dans le cloud.

Mesures à prendre en cas de détection d'un virus

Votre produit fournit un grand nombre de solutions et de fonctions pour gérer les virus et les autres menaces de sécurité qu'il détecte.

Lorsque votre produit Norton détecte un risque de sécurité sur l'ordinateur, vous devez appliquer l'action appropriée pour ce risque. Votre produit Norton vous avertit lorsqu'il détecte un risque sécurité. Vous pouvez consulter différentes informations sur le risque dans la fenêtre qui s'affiche et sélectionner l'action que votre produit Norton doit réaliser.

Par défaut, le produit Norton supprime le risque de sécurité de votre ordinateur et le met en quarantaine. Toutefois, vous pouvez restaurer le fichier depuis la

Quarantaine vers son emplacement initial et l'exclure des analyses futures.



Excluez un programme des analyses Norton Security uniquement si vous avez la certitude que le programme est sûr. Par exemple, si un programme fait appel à un autre programme présentant des risques de sécurité pour fonctionner, vous pouvez décider de le conserver sur l'ordinateur.

Dans certains cas, le produit Norton requiert votre attention afin de résoudre manuellement le risque de sécurité détecté. Vous pouvez accéder au site Web de Symantec Security Response et consulter les instructions de suppression manuelle.

Dans certains cas, vous pouvez suspecter l'infection d'un élément, même si le produit Norton ne l'a pas identifié comme une menace de sécurité. En de tels cas, vous pouvez transmettre l'élément à Symantec à des fins d'analyse approfondie.

En outre, il fournit des solutions pour les risques de sécurité, tels que les logiciels espions et publicitaires.

A propos de la détection de virus, spywares et autres risques

Les virus et d'autres menaces de sécurité peuvent être détectés pendant une analyse manuelle ou personnalisée. Auto-Protect détecte ces menaces lorsque vous effectuez une action avec un fichier infecté. Les menaces peuvent également apparaître lors de l'envoi d'un message électronique ou lors d'une analyse manuelle ou personnalisée.

Les risques de sécurité, tels que les spywares et les logiciels publicitaires, peuvent également être détectés lors de l'exécution de ces activités.

Les fichiers susceptibles d'infecter votre système au démarrage de l'ordinateur sont analysés en premier.

Les fichiers suivants sont compris dans l'analyse :

- Fichiers associés aux processus en cours d'exécution dans la mémoire
- Fichiers avec des entrées dans le dossier de démarrage
- Fichiers avec des entrées dans le fichier INI de démarrage du système
- Fichiers avec des entrées dans le fichier batch de démarrage du système
- Fichiers auxquels font référence les clés de registre au démarrage du système

Si un fichier infecté est détecté à ce stade de l'analyse manuelle, il est réparé ou supprimé. Toute référence inutile est également supprimée de l'ordinateur. Avant de tenter la réparation, la mise en quarantaine ou la suppression d'un fichier infecté en cours d'exécution dans la mémoire, votre produit tente de mettre fin au processus. Vous êtes alors alerté et invité à fermer tous les programmes superflus avant l'arrêt du processus.

Vous pouvez afficher des informations sur les virus détectés et les autres menaces de sécurité dans l'historique de sécurité.

Vérification des notifications d'Auto-Protect

Auto-Protect est conçu pour analyser les fichiers pour détecter des virus, des vers et des chevaux de Troie lorsque vous exécutez certaines opérations, comme le déplacement, la copie ou l'ouverture de ces fichiers. Il recherche également les spywares, les logiciels publicitaires et d'autres risques de sécurité.

Si Auto-Protect détecte une activité suspecte, il consigne une notification dans l'Historique de la sécurité vous indiquant qu'un risque a été rencontré et neutralisé.

Si Auto-Protect détecte un ou plusieurs virus, il répare ou supprime les virus et vous avertit. La notification donne des informations relatives au fichier qui a été réparé ou supprimé et au virus, cheval de Troie, ou ver qui a infecté le fichier. Aucune autre mesure n'est nécessaire.

Vérification des notifications d'Auto-Protect

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Historique**.

- 2 Dans la liste déroulante **Afficher** de la fenêtre **Historique de la sécurité**, sélectionnez la catégorie pour laquelle vous souhaitez modifier les alertes Auto-Protect.

Les options Auto-Protect sont les suivantes :

Historique récent	Affiche les notifications d'Auto-Protect reçues au cours des sept derniers jours.
Historique complet	Affiche toutes les notifications reçues d'Auto-Protect.
Risques de sécurité résolus	<p>Examinez toutes les menaces de sécurité résolues.</p> <p>La catégorie Risques de sécurité résolus comprend les fichiers infectés que le produit Norton répare, supprime ou met en quarantaine.</p>
Risques de sécurité non résolus	<p>Examinez la liste des risques de sécurité non résolus.</p> <p>La catégorie Risques de sécurité non résolus comprend les fichiers infectés pour lesquels le produit Norton n'était pas capable d'intervenir. Cette catégorie comprend la plupart des risques faibles qui nécessitent votre attention et une intervention adéquate.</p>

- 3 Dans le volet de droite, sous **Action recommandée**, cliquez sur le lien **Options**.
Le nom de l'option s'affiche comme **Restauration et options** pour quelques éléments.
Si un ou plusieurs risques de sécurité tels que des spywares sont détectés, vous pouvez prendre des mesures pour les corriger.



- 4 Dans la fenêtre **Menace détectée**, sélectionnez l'action adéquate pour le risque.
Les options suivantes sont disponibles dans la fenêtre **Menace détectée** :

Restaurer et exclure ce fichier	<p>Restaure l'élément mis en quarantaine sélectionné à son emplacement d'origine et empêche l'élément d'être détecté par les analyses futures.</p> <p>Cette option n'est disponible que pour les menaces virales et non virales détectées.</p>
Exclure ce programme	<p>Exclut ce risque de sécurité des analyses futures.</p> <p>Le produit Norton ajoute le risque de sécurité à la liste d'exclusions appropriée.</p>
Correction manuelle (recommandé)	<p>Vous permet de résoudre le risque à l'aide d'un outil de correction manuelle.</p> <p>Si vous résolvez une menace manuellement, vous devez supprimer les informations de la menace de la fenêtre Historique de la sécurité.</p>

Supprimer ce fichier (peut entraîner la fermeture du navigateur) (recommandée)

Supprime le risque de sécurité de votre ordinateur et le met en quarantaine.

Cette option n'est disponible que pour les risques de sécurité qui requièrent votre attention.

Supprimer ce fichier (peut entraîner la fermeture du navigateur)

Supprime le risque de sécurité sélectionné de votre ordinateur et le met en quarantaine.

Cette option n'est disponible que pour les risques de sécurité qui requièrent votre attention pour une suppression manuelle.

Cette option n'est disponible que pour les risques de sécurité qui ont été mis en quarantaine manuellement.

Supprimer de l'historique

Supprime l'élément mis en quarantaine sélectionné du journal de l'Historique de la sécurité.

Obtenir de l'aide (recommandé)	<p>Renvoie au site Web Symantec Security Response.</p> <p>Cette option est disponible uniquement pour les risques de sécurité qui requièrent votre attention pour une suppression manuelle. Vous pouvez consulter le site Web Symantec Security Response pour obtenir des instructions de suppression manuelle ou d'autres informations sur le risque.</p>
Transmettre à Symantec	<p>Envoie l'élément sélectionné à Symantec.</p> <p>Dans certains cas, vous pouvez suspecter l'infection d'un élément, même si le produit Norton ne l'a pas identifié comme une menace de sécurité. En de tels cas, vous pouvez utiliser cette option pour transmettre l'élément à Symantec à des fins d'analyse approfondie.</p>

Réponse aux alertes du blocage des vers

Si un programme essaie de se propager par courrier électronique ou d'expédier par courrier une copie de son code, il peut s'agir d'un ver cherchant à se répandre par la messagerie électronique. Un ver est en mesure

de s'envoyer lui-même dans un message sans aucune intervention de votre part.

Le Blocage des vers analyse en permanence les pièces jointes aux messages sortants pour y détecter la plupart des vers. S'il détecte un ver, une alerte vous signale sa présence.

L'alerte de blocage des vers s'affiche uniquement lorsque vous activez l'option **Me demander** sous **Comment renforcer la protection** dans la fenêtre **Analyse antivirus du courrier**. Si l'option **Me demander** est désactivée, le produit Norton met automatiquement en quarantaine le ver détecté et vous en informe.

L'alerte vous présente les options et vous demande quoi faire. Si vous n'envoyez pas de courrier électronique à ce moment là, il s'agit probablement un ver et vous devriez mettre le fichier en quarantaine.



Pour répondre aux alertes du Blocage de vers :

- ❖ Dans la fenêtre d'alerte, sélectionnez l'action que vous voulez effectuer. Vos options sont :

Quarantaine	Arrête définitivement le ver en le plaçant dans l'historique de la sécurité. Aussi longtemps qu'il sera dans l'historique de la sécurité, le ver sera incapable de se propager. Cette Quarantaine est l'action la plus sécurisée.
Autoriser	Envoie le message électronique pour lequel vous avez reçu une alerte de blocage des vers. Si vous autorisez l'envoi du message électronique, celui-ci risque d'infecter l'ordinateur du destinataire. Sélectionnez cette option si vous êtes sûr que le message n'est pas infecté par un ver.
Ignorer	Ignore ce risque.

Si un ver malveillant est détecté, il doit être placé en quarantaine.

Pour mettre un fichier infecté par un ver en quarantaine :

- 1 Dans la liste déroulante de l'alerte, cliquez sur **Quarantaine**.

- 2 Une fois le ver placé en quarantaine, effectuez les tâches suivantes :
 - Exécutez LiveUpdate pour vérifier que vous disposez des dernières mises à jour des définitions.
Se reporter à "[A propos des mises à jour de la protection](#)" à la page 37.
 - Analysez votre ordinateur.
Se reporter à "[Exécution d'une analyse complète du système](#)" à la page 88.
- Si rien n'est détecté, transmettez le fichier infecté à Symantec Security Response. Indiquez également que le fichier a été détecté et que vous l'avez analysé avec les mises à jour des définitions les plus récentes. Symantec Security Response vous répondra sous 48 heures.

A propos de la réponse aux risques détectés au cours d'une analyse

A la fin d'une analyse, la fenêtre **Résumé des résultats** fournit le résumé des résultats de l'analyse. Vous pouvez utiliser la fenêtre **Menaces détectées** pour résoudre les éléments qui n'ont pas été automatiquement résolus lors de l'analyse.

Vous pouvez utiliser la liste déroulante **Afficher** qui se trouve dans la fenêtre **Historique de la sécurité** pour résoudre les éléments qui n'ont pas été automatiquement résolus lors de l'analyse. La section **Action recommandée** de la fenêtre **Historique de la sécurité** affiche l'action que vous devez effectuer pour résoudre la menace de sécurité.

A propos des actions possibles lorsque le produit Norton ne parvient pas à réparer un fichier

En règle générale, si le produit Norton ne peut pas réparer ou supprimer automatiquement un fichier infecté, c'est que vous ne disposez pas des dernières mises à

jour des définitions. Exécutez LiveUpdate et lancez de nouveau l'analyse.

Si cela ne fonctionne pas, veuillez lire les informations dans la fenêtre **Historique de la sécurité - Détails avancés** pour identifier les types de fichiers ne pouvant pas être réparés. Vous pouvez effectuer l'une des actions suivantes, selon le type de fichier :

<p>Fichiers infectés</p>	<p>Vous pouvez voir le type de fichier du risque détecté. Cette information vous aide à décider de la mesure pouvant être prise selon le type de fichier.</p> <p>Par exemple, vous pouvez afficher les fichiers infectés avec l'une des extensions suivantes (tout fichier peut être infecté) :</p> <ul style="list-style-type: none"> ■ .exe ■ .doc ■ .dot ■ .xls <p>Utilisez la fenêtre Menaces détectées pour résoudre le problème.</p>
<p>Enregistrement de démarrage principal du disque dur, zones amorce ou fichiers système (comme IO.SYS ou MSDOS.SYS), zone amorce et fichiers système sur disquette</p>	<p>Effectuez un remplacement à l'aide des disques du système d'exploitation.</p>

Exécution de tâches de routine

5

Ce chapitre traite des sujets suivants :

- [Activation ou désactivation des tâches automatiques](#)
- [Exécution de tâches personnalisées](#)
- [Planification des analyses de sécurité et de performances](#)
- [Indication de la durée du délai d'inactivité](#)

Activation ou désactivation des tâches automatiques

Votre produit Norton exécute un certain nombre de tâches automatiques pour assurer la protection de votre ordinateur, sans nécessiter d'intervention de votre part. Il s'agit notamment de la recherche de virus, de la surveillance de votre connexion à Internet et du téléchargement des mises à jour de la protection. Ces activités s'exécutent en arrière-plan lorsque votre ordinateur est allumé.

Si des éléments nécessitent votre attention, votre produit Norton affiche un message pour vous indiquer l'état actuel de votre protection ou pour vous inviter à agir. Si aucun message ne s'affiche, cela signifie que votre ordinateur est protégé.

Vous pouvez ouvrir votre produit Norton à tout moment pour consulter l'état de l'ordinateur d'un simple coup

d'œil ou pour afficher des informations détaillées concernant la protection.

Quand une activité en arrière-plan est en cours, votre produit Norton vous avertit avec un message dans la zone de notification située à l'extrême droite de la barre des tâches. Vous pouvez consulter les résultats de ces activités la prochaine fois que vous ouvrez la fenêtre principale de votre produit Norton.

Activation ou désactivation des tâches automatiques

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Planification des tâches**.
- 3 Dans la fenêtre **Planification des tâches**, sur l'onglet **Tâches automatiques**, procédez comme suit :
 - Sélectionnez la fonction que vous voulez exécuter automatiquement.
Vous pouvez sélectionner **Tâches** pour sélectionner toutes les fonctions.
 - Désélectionnez la fonction que vous ne voulez pas exécuter automatiquement.
Vous pouvez sélectionner **Tâches** pour désélectionner toutes les fonctions.
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Exécution de tâches personnalisées

Votre produit Norton analyse automatiquement votre système et choisit les paramètres appropriés pour optimiser sa sécurité. Cependant, vous pouvez exécuter certaines tâches spécifiques. Vous pouvez choisir les tâches spécifiques à exécuter à l'aide des options de la fenêtre **Tâches personnalisées**.

Votre produit Norton vous permet de choisir une combinaison personnalisée de tâches à effectuer pour une analyse ponctuelle. Vous pouvez également exécuter LiveUpdate, sauvegarder vos données, effacer

l'historique de navigation, libérer de l'espace sur le disque dur en supprimant les fichiers inutiles et optimiser vos disques.

Exécution de tâches personnalisées

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, sous **Analyses et tâches**, cliquez sur **Tâches personnalisées**, puis cliquez sur **OK**.
- 3 Dans la fenêtre **Tâches personnalisées**, sélectionnez les tâches à exécuter.
Pour sélectionner toutes les tâches, cochez **Tâches**.
- 4 Cliquez sur **OK**.

Planification des analyses de sécurité et de performances

Les paramètres de planification des tâches permettent de configurer le produit Norton de sorte qu'il examine automatiquement votre système pour rechercher les problèmes de sécurité et de performances. Vous pouvez spécifier à quel moment et à quelle fréquence le produit Norton doit effectuer ces analyses.

Les options disponibles pour la planification des analyses de la sécurité et des performances sont les suivantes :

Automatique (Recommandé)	<p>Votre ordinateur est examiné pour rechercher les problèmes de sécurité et de performances pendant toute période d'inactivité.</p> <p>Ce paramètre offre une protection optimale.</p>
--------------------------	---

Planification des analyses de sécurité et de performances

<p>Hebdomadaire</p>	<p>Votre ordinateur est examiné pour rechercher les problèmes de sécurité et de performances une ou plusieurs fois par semaine.</p> <p>Vous pouvez choisir le jour de la semaine et l'heure de l'analyse.</p>
<p>Mensuelle</p>	<p>Votre ordinateur est examiné pour rechercher les problèmes de sécurité et de performances une fois par mois.</p> <p>Vous pouvez choisir le jour du mois et l'heure de l'analyse.</p>
<p>Planification manuelle</p>	<p>Aucune analyse de la sécurité et des performances planifiée n'est effectuée sur votre ordinateur.</p> <p>Si vous choisissez cette option, effectuez régulièrement des analyses de la sécurité et des performances sur votre ordinateur pour maintenir sa protection.</p>

Les performances de votre ordinateur sont maximisées si vous planifiez vos opérations critiques pour qu'elles s'exécutent pendant que votre ordinateur est en veille. Si vous attribuez une fréquence hebdomadaire ou mensuelle à vos analyses et que vous cochez la case **Exécuter uniquement en période d'inactivité**, le produit Norton analyse votre ordinateur quand il est en veille. Symantec vous conseille de sélectionner l'option

Exécuter uniquement en période d'inactivité pour obtenir de meilleures performances de votre ordinateur.

Planification des analyses de la sécurité et des performances

- 1 Dans la fenêtre principale Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Planification des tâches**.
- 3 Dans l'onglet **Planification**, sous **Planifier**, sélectionnez une option.
Si vous sélectionnez l'option **Hebdomadaire** ou **Mensuelle**, vous devez sélectionner l'heure et le jour d'exécution des tâches automatiques. Vous pouvez aussi indiquer que les tâches automatiques ne doivent être effectuées que lorsque l'ordinateur est en veille.
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Indication de la durée du délai d'inactivité

Vous pouvez définir la durée après laquelle votre produit Norton devrait identifier votre ordinateur comme étant inactif. Vous pouvez sélectionner une valeur (en minutes) entre 1 minute et 30 minutes. Si vous n'utilisez pas votre ordinateur pendant la durée spécifiée, votre produit Norton identifie votre ordinateur comme étant inactif. Le produit Norton exécute alors les activités planifiées pour la période d'inactivité.

Indication de la durée du délai d'inactivité

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Dans la ligne **Délai d'inactivité**, dans la liste déroulante, sélectionnez la durée que vous voulez spécifier.
Vous devez peut-être faire défiler la fenêtre pour afficher cette option.

- 4 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**.



Protection des activités sur Internet

6

Ce chapitre traite des sujets suivants :

- A propos du pare-feu intelligent
- Désactivation et activation de la protection du navigateur
- Désactivation ou activation du diagnostic des téléchargements
- Configuration de l'option Notifications sur le Diagnostic des téléchargements
- Configurer l'option Afficher le rapport au lancement des fichiers
- Désactivation ou activation des notifications de la prévention d'intrusion
- Exclusion ou inclusion des signatures d'attaque dans la surveillance
- Activation ou désactivation d'AutoBlock
- Déblocage d'ordinateurs bloqués par AutoBlock
- Blocage permanent d'un ordinateur qui a été bloqué par AutoBlock
- A propos de la liste d'exclusions de la prévention d'intrusion
- Retrait de tous les périphériques de la liste d'exclusion de la Prévention d'intrusion

- Ajout d'un périphérique à l'approbation du périphérique
- Modification du niveau d'approbation de votre réseau et de vos périphériques
- A propos des types de risques de sécurité
- A propos de Norton AntiSpam
- Ajout de ports POP3 et SMTP aux Ports protégés
- Suppression d'un port de messagerie électronique des Ports protégés
- Désactivation ou activation de la limitation de l'utilisation réseau
- Définir l'utilisation de bande passante de Norton Security

A propos du pare-feu intelligent

Le Pare-feu intelligent surveille les communications entre votre ordinateur et les autres ordinateurs sur Internet. Il protège également votre ordinateur contre les problèmes de sécurité courants, tels que :

Tentatives de connexion anormales	Vous signale les tentatives de connexion d'autres ordinateurs et les tentatives de connexion des programmes de votre ordinateur à d'autres ordinateurs.
Analyses de port	Masque les ports inactifs de votre ordinateur en vue d'assurer une protection contre des attaques au moyen de techniques de piratage, telles que l'analyse de ports

Intrusions	Surveille le trafic réseau depuis et vers votre ordinateur à la recherche d'un comportement douteux et anticipe l'attaque avant qu'elle ne menace votre système
------------	---

Un pare-feu bloque les pirates et tout autre trafic non autorisé, mais laisse passer le trafic autorisé. La fonction de pare-feu Windows contrôle toutes les communications entrantes sur votre ordinateur. En revanche, elle ne contrôle pas les communications sortantes envoyées par votre ordinateur vers Internet.

Symantec vous recommande de laisser la fonction **Pare-feu intelligent** activée afin de permettre à votre produit Norton de gérer toutes les communications entrantes et sortantes de votre ordinateur. La fonction Pare-feu intelligent crée automatiquement des règles de programme pour chaque programme exécuté. Lorsque la fonction **Pare-feu intelligent** est activée, le produit Norton conserve les paramètres **Contrôle automatique des programmes** pour tous les programmes.

La désactivation du Pare-feu intelligent réduit la protection de votre système. Vérifiez toujours que le Pare-feu intelligent est activé.

Désactivation ou activation du pare-feu intelligent

Le pare-feu intelligent surveille les communications entre votre ordinateur et les autres ordinateurs sur Internet. Il protège également votre ordinateur contre les problèmes de sécurité communs.

Si vous devez désactiver le pare-feu intelligent, désactivez-le temporairement pour qu'il soit réactivé automatiquement. Pour être sûr que votre ordinateur reste protégé, vous pouvez activer le Pare-feu intelligent manuellement avant l'expiration du délai que vous avez spécifié.

Lorsque le pare-feu intelligent est désactivé, votre ordinateur n'est plus protégé contre les menaces Internet et les risques de sécurité.

Désactivation du pare-feu intelligent

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Paramètres généraux**, à la ligne **Pare-feu intelligent**, déplacez le curseur **Marche/Arrêt** vers la droite, sur la position **Arrêt**.
- 4 Cliquez sur **Appliquer**.
- 5 Dans la liste déroulante **Sélectionner la durée** de la fenêtre **Alerte de sécurité**, sélectionnez la durée pendant laquelle vous souhaitez désactiver le pare-feu intelligent.
- 6 Cliquez sur **OK**.
- 7 Cliquez sur **Fermer**.

Activation du pare-feu intelligent

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Paramètres généraux**, à la ligne **Pare-feu intelligent**, déplacez le curseur **Marche/Arrêt** vers la gauche, sur la position **Marche**.
- 4 Cliquez sur **Appliquer**.
- 5 Cliquez sur **Fermer**.

Désactivation du pare-feu intelligent depuis les commandes rapides

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Commandes rapides**, désélectionnez **Pare-feu intelligent**.

Activation du pare-feu intelligent depuis les commandes rapides

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Commandes rapides**, sélectionnez **Pare-feu intelligent**.

Désactivation du pare-feu intelligent depuis la zone de notification

- 1 Depuis la zone de notification de la barre des tâches, cliquez à l'aide du bouton droit sur l'icône de Norton Security, puis cliquez sur **Désactiver le pare-feu intelligent**.
- 2 Dans la liste déroulante **Sélectionner la durée** de la fenêtre **Alerte de sécurité**, sélectionnez la durée pendant laquelle vous souhaitez désactiver le pare-feu intelligent.
- 3 Cliquez sur **OK**.

Activation du pare-feu intelligent depuis la zone de notification

- ❖ Depuis la zone de notification de la barre des tâches, cliquez à l'aide du bouton droit sur l'icône de Norton Security, puis cliquez sur **Activer le pare-feu intelligent**.

A propos des règles de filtrage

Un pare-feu est un système de sécurité qui suit des règles pour bloquer ou autoriser des connexions et la transmission de données entre votre ordinateur et Internet. Les règles de filtrage déterminent la façon dont le Pare-feu intelligent protège votre ordinateur contre les programmes malveillants et les accès non autorisés. Le pare-feu utilise ces règles pour vérifier automatiquement tout le trafic entrant et sortant de votre ordinateur.

Le pare-feu intelligent suit deux types de règles de filtrage :

règles de programme	Contrôlez l'accès réseau des programmes de votre ordinateur.
Règles de trafic	Contrôlent tout le trafic réseau entrant et sortant.

Règles de programme

L'onglet **Contrôle de programme** vous permet d'effectuer les opérations suivantes :

- Renommer la description du programme.
- Modifier les règles d'un programme
- Ajouter une règle pour un programme
- Modifier les paramètres d'accès d'une règle de programme.
- Modifier la priorité d'une règle d'un programme en changeant l'ordre des règles dans la liste.
- Supprimer une règle de programme.
- Afficher le niveau d'approbation d'un programme.

Vous pouvez créer des règles de programme de différentes manières :

En personnalisant automatiquement les paramètres d'accès à Internet

Permet au pare-feu de configurer automatiquement l'accès aux programmes la première fois que l'utilisateur les exécute. Il s'agit de la méthode la plus simple pour créer des règles de pare-feu.

Utiliser les paramètres de pare-feu

Gère la liste des programmes pouvant accéder à Internet.

Répondre aux alertes

Le pare-feu vous prévient lorsqu'un programme tente d'accéder à Internet. Vous pouvez alors décider d'autoriser le programme à accéder à Internet ou de le lui interdire.

Dans certains cas, lorsque vous visionnez un film, par exemple, vous pouvez décider de ne recevoir aucun message d'alerte. En de tels cas, vous pouvez activer le Contrôle automatique des programmes. Dans cet état, votre produit Norton ne vous avertit pas à l'aide d'alertes de pare-feu. Le pare-feu ne vous prévient que si vous avez modifié les options Paramètres généraux du pare-feu intelligent en remplaçant les paramètres par défaut, qui sont les paramètres recommandés.

Règles de trafic

L'onglet **Règles de trafic** contient la liste des règles de trafic prédéfinies. Certaines règles de trafic par défaut sont accessibles en lecture seule et sont verrouillées. Vous ne pouvez pas modifier ces règles.

Les règles sont classées en fonction de leur niveau de priorité. Les règles qui apparaissent en premier dans la liste remplacent celles qui suivent.

Vous pouvez ajouter une nouvelle règle de trafic dans cet onglet. Vous pouvez également effectuer les activités suivantes :

Modifier une règle de trafic	<p>Vous pouvez modifier les paramètres d'une règle de trafic qui ne fonctionne pas de manière appropriée.</p> <p>Toutefois, vous ne pouvez pas modifier certaines règles par défaut qui sont en lecture seule.</p>
Désactiver une règle de trafic	<p>Vous pouvez désactiver une règle de trafic.</p> <p>Toutefois, vous ne pouvez pas désactiver certaines règles par défaut qui sont en lecture seule.</p>
Modifier la priorité d'une règle de trafic	<p>Vous pouvez modifier la priorité d'une règle de trafic en changeant son emplacement dans la liste.</p> <p>🔑 Seuls les utilisateurs avancés ou les utilisateurs qui y sont enjoins par le support technique doivent accomplir cette action.</p>

A propos de l'ordre dans lequel les règles de filtrage sont traitées

Le pare-feu intelligent traite les règles de trafic avant de traiter les règles de programme. Supposons, par exemple, l'existence d'une règle de programme permettant à Internet Explorer d'accéder à Internet via le port 80 et le protocole TCP, et d'une règle de trafic bloquant la communication TCP via le port 80 pour l'ensemble des applications. L'application Internet

Explorer ne peut pas accéder à Internet puisque le produit Norton prend en compte les règles de trafic avant les règles de programme.

Dans la liste des règles de trafic, les règles sont traitées dans l'ordre où elles apparaissent, de haut en bas. Les entrées de **Règles de programme** ne sont pas traitées dans l'ordre. En revanche, les règles de la liste **Règle de programme** sont traitées dans l'ordre où elles apparaissent, de haut en bas.

Par exemple, il peut exister une règle de programme qui empêche l'utilisation de l'application Symantec pcAnywhere avec tout autre ordinateur. Vous ajoutez une autre règle permettant d'utiliser cette même application avec un ordinateur particulier. Vous déplacez ensuite la nouvelle règle avant la règle initiale dans la liste des règles de programme. Le produit Norton traite d'abord la nouvelle règle et vous permet d'utiliser Symantec pcAnywhere avec cet ordinateur particulier. Il traite ensuite la règle initiale et bloque son utilisation sur les autres ordinateurs.

Désactivation du contrôle automatique des programmes

Le contrôle automatique des programmes configure automatiquement les paramètres d'accès à Internet des programmes compatibles Web lors de leur première exécution. Lorsqu'un programme tente d'accéder à Internet pour la première fois, le contrôle automatique des programmes crée des règles.

Il ne configure l'accès à Internet que pour les versions des programmes que Symantec juge sans risque. Une alerte se déclenche lorsqu'un programme infecté essaie d'accéder à votre ordinateur.

Si vous voulez définir vous-même les paramètres d'accès à Internet de vos programmes, désactivez le contrôle automatique des programmes. Lorsqu'un programme tente d'accéder à Internet pour la première

fois, une invite vous demande de définir les paramètres d'accès.

Symantec recommande de configurer le contrôle automatique des programmes sur **Activé**. En le désactivant, vous pourriez prendre des décisions incorrectes pouvant autoriser l'exécution de programmes malveillants ou le blocage de programmes et fonctions importants sur Internet.

Pour désactiver le contrôle automatique des programmes

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans la fenêtre **Pare-feu**, cliquez sur **Contrôle avancé des programmes**.
- 4 A la ligne **Contrôle automatique des programmes**, faites glisser le curseur **Ac./Désac.** vers la droite sur la position **Désactivé**.
- 5 Cliquez sur **Appliquer**.

Ajout d'un programme au contrôle des programmes

Vous pouvez ajouter un programme au contrôle des programmes pour contrôler leur accès à Internet. Lorsque vous ajoutez le programme, vous pouvez configurer ses paramètres d'accès dans les règles de programme. Vous pouvez autoriser, bloquer ou créer des règles personnalisées propres au programme que vous ajoutez.

Les paramètres de pare-feu définis manuellement pour les programmes remplacent les paramètres définis par le contrôle automatique des programmes. Cependant, Symantec recommande de conserver les paramètres que définit le contrôle automatique des programmes lorsque vous exécutez vos programmes.

Ajout d'un programme au contrôle des programmes

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Contrôle de programme**, cliquez sur **Ajouter**.
- 4 Dans la boîte de dialogue **Sélectionner un programme**, accédez au fichier exécutable du programme à ajouter.
- 5 Cliquez sur **Ouvrir**.
- 6 Dans la fenêtre **Alerte de sécurité**, effectuez une analyse des informations de réputation du programme.
Votre produit Norton récupère et affiche les informations sur la réputation et le paramètre d'accès recommandé.

- 7 Dans la liste déroulante **Options**, sélectionnez le niveau d'accès souhaité pour le programme. Vos options sont :

<p>Toujours autoriser</p>	<p>Autorise toutes les tentatives d'accès du programme.</p>
<p>Toujours bloquer</p>	<p>Bloque toutes les tentatives d'accès du programme.</p>
<p>Configurer manuellement</p>	<p>Permet de créer manuellement des règles contrôlant l'accès à Internet de ce programme.</p> <p>Vous pouvez définir les critères suivants pour une règle :</p> <ul style="list-style-type: none"> ■ Action ■ Connexions ■ Ordinateurs ■ Communications ■ Avancé ■ Description <p>Si vous sélectionnez cette option, vous devez suivre les instructions qui s'affichent dans l'assistant et configurer la règle.</p>

- 8 Cliquez sur **OK**.

Suppression d'un programme du contrôle des programmes

Si nécessaire, vous pouvez supprimer des programmes du contrôle des programmes. Dans ce cas, votre produit Norton supprime l'ensemble des règles associées à l'application que vous supprimez.

Suppression d'un programme du contrôle des programmes

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Contrôle de programme**, dans la colonne **Programme**, sélectionnez le programme à supprimer.
- 4 Cliquez sur **Supprimer**.
- 5 Dans la boîte de dialogue **Confirmation**, cliquez sur **Oui**.
La boîte de dialogue de confirmation s'ouvre uniquement si l'option **Contrôle automatique des programmes** est désactivée.
- 6 Cliquez sur **Appliquer**.

Personnalisation des règles de programme

Après avoir utilisé le produit Norton pendant un certain temps, il se peut que vous deviez changer les paramètres d'accès de certains programmes.

Personnalisation des règles de programme

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Contrôle de programme**, dans la colonne **Programme**, sélectionnez le programme à modifier.

- 4 Dans la liste déroulante en regard du programme à modifier, sélectionnez le niveau d'accès à accorder au programme. Vos options sont :

Autoriser	Autorise toutes les tentatives d'accès du programme.
Bloquer	Bloque toutes les tentatives d'accès du programme.
Personnalisé	Créez des règles qui contrôlent l'accès à Internet du programme.

- 5 Cliquez sur **Appliquer**.

Ajout de règles de trafic et de règles de programme

Le Contrôle des programmes crée automatiquement la plupart des règles de filtrage nécessaires. Le cas échéant, vous pouvez ajouter des règles personnalisées.



Ne créez vos propres règles de filtrage que si vous êtes un utilisateur expérimenté.

Vous pouvez ajouter les types de règles de filtrage suivants :

- Règles de trafic
- Règles de programme

Ajout d'une règle de trafic

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Règles de trafic**, cliquez sur **Ajouter**.
- 4 Suivez les instructions de l'Assistant **Ajouter une règle**

5 Dans la fenêtre **Règles de trafic**, cliquez sur **OK**.

Ajout d'une règle de programme

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Contrôle de programme**, dans la colonne **Programme**, sélectionnez le programme auquel vous voulez ajouter une règle.
- 4 Cliquez sur **Modifier**.
Vous pouvez également utiliser la liste déroulante **Accès** située en regard du programme pour modifier son niveau d'accès. Le pare-feu intelligent modifie ou crée, en conséquence, la règle appropriée pour le programme.
- 5 Dans la fenêtre **Règles**, cliquez sur **Ajouter**.
- 6 Suivez les instructions de l'Assistant **Ajouter une règle**.
- 7 Dans la fenêtre **Règles**, cliquez sur **OK**.

Utilisation de l'assistant Ajouter une règle

L'assistant **Ajouter une règle** vous aide à créer des règles de filtrage.

Utilisation de l'assistant Ajouter une règle

- 1 Ouvrez l' **Assistant Ajouter une règle** en créant une règle de trafic ou une règle de programme.

- 2 Dans le premier écran de l' **Assistant Ajouter une règle**, sélectionnez l'action souhaitée pour cette règle. Les options sont les suivantes :

<p>Autoriser</p>	<p>Autoriser les communications de ce type.</p> <p>Supposons l'existence d'une règle de trafic avec le critère suivant : toutes les connexions entrantes provenant de l'adresse Internet 192.168.1.1 doivent passer par le port 8080. Lorsque vous sélectionnez Autoriser, le pare-feu intelligent autorise toutes les connexions répondant au critère de cette règle de trafic.</p>
<p>Bloquer</p>	<p>Interdire les communications de ce type.</p> <p>Supposons l'existence d'une règle de trafic avec le critère suivant : toutes les connexions entrantes provenant de l'adresse Internet 192.168.1.1 doivent passer par le port 8080. Lorsque vous sélectionnez Bloquer, le pare-feu intelligent bloque toutes les connexions répondant au critère de cette règle de trafic.</p>

Surveiller	
-------------------	--



Met à jour la catégorie **Pare-feu - Activités** dans le journal des événements chaque fois qu'une communication de ce type a lieu. Cette option vous permet de surveiller la fréquence d'utilisation de cette règle de pare-feu. Votre produit Norton vous notifie chaque fois que du trafic répondant aux critères de la règle de surveillance est transmis à votre ordinateur. Vous pouvez utiliser les liens présents dans ces notifications pour afficher les journaux. Vous pouvez afficher le journal des événements sous la catégorie **Pare-feu - Activités** dans la fenêtre **Historique de la sécurité**.

Votre produit Norton crée des règles d'action distinctes pour autoriser ou bloquer les programmes associés à une seule règle de **surveillance**. La règle de **surveillance** doit être prioritaire sur la règle d'action pour que l'entrée de l'événement réseau associé au programme soit consignée dans le journal.

La règle de surveillance consigne uniquement les

	<p>événements de trafic dans la fenêtre Historique de la sécurité. Vous devez créer une autre règle Autoriser ou Bloquer pour gérer le trafic réseau.</p> <p>Vous pouvez surveiller et autoriser ou bloquer le trafic en activant l'option Créer une entrée de journal d'Historique de la sécurité dans l' Assistant Ajouter une règle ou l' Assistant Modifier une règle.</p>
--	--

3 Cliquez sur **Suivant**.

4 Sélectionnez le type de connexion de la règle. Les options sont les suivantes :

Connexions à d'autres ordinateurs	La règle s'applique aux connexions qu'établit votre ordinateur à un autre ordinateur.
Connexions depuis d'autres ordinateurs	La règle s'applique aux connexions entrantes qu'établit un autre ordinateur à votre ordinateur.
Connexions à destination et en provenance d'autres ordinateurs	La règle s'applique aux connexions entrantes et sortantes.

- 5 Cliquez sur **Suivant**, puis sélectionnez les ordinateurs auxquels la règle doit s'appliquer. Les options sont les suivantes :

Tout ordinateur	La règle s'applique à tous les ordinateurs.
Tous les ordinateurs du sous-réseau local	Cette règle ne s'applique qu'aux ordinateurs du sous-réseau local. Le réseau d'une organisation est divisé en sous-réseaux pour améliorer l'efficacité des communications Internet. Un sous-réseau représente tous les ordinateurs d'un réseau local.

Uniquement les ordinateurs et sites ci-dessous

La règle ne s'applique qu'aux ordinateurs, sites et domaines que vous indiquez.

Vous pouvez indiquer les noms et adresses des ordinateurs auxquels s'applique la règle. Les détails des ordinateurs indiqués s'affichent dans la liste. Vous pouvez également supprimer des ordinateurs de la liste.

Dans ce cas, l'option **Ajouter** est disponible. Quand vous cliquez sur **Ajouter**, votre produit Norton affiche la boîte de dialogue **Mise en réseau** dans laquelle vous pouvez indiquer différents ordinateurs, une plage d'ordinateurs ou tous les ordinateurs d'un sous-réseau ou d'un réseau.

Vous pouvez utiliser l'option **Ajouter** ou **Supprimer** pour ajouter ou supprimer un ordinateur.

- 6 Cliquez sur **Suivant**, puis sélectionnez les protocoles de la règle. Les options sont les suivantes :

TCP	La règle s'applique aux communications TCP (Transport Control Protocol).
UDP	La règle s'applique aux communications UDP (User Datagram Protocol).
TCP et UDP	La règle s'applique aux communications TCP et UDP.
ICMP	<p>La règle s'applique aux communications ICMP (Internet Control Message Protocol).</p> <p>Cette option n'est disponible que lorsque vous ajoutez ou modifiez une règle de trafic.</p>
ICMPv6	<p>La règle s'applique aux communications ICMPv6 (Internet Control Message Protocol for Internet Protocol version 6).</p> <p>Cette option n'est disponible que lorsque vous ajoutez ou modifiez une règle de trafic.</p>

Tous	<p>La règle s'applique à tous les protocoles pris en charge.</p> <p>Lorsque vous sélectionnez cette option, vous ne pouvez pas indiquer les types de communications ni les ports auxquels s'applique cette règle.</p>
-------------	---

7 Sélectionnez les ports de la règle. Les options sont les suivantes :

<p>Tous les types de communications (tous les ports, locaux et distants)</p>	<p>La règle s'applique à toutes les communications, quel que soit le port utilisé.</p>
<p>Cette règle s'applique uniquement si elle correspond à tous les ports répertoriés ci-dessous</p>	<p>La règle s'applique à tous les ports indiqués. Vous pouvez indiquer les ports en sélectionnant les ports répertoriés ou en ajoutant des ports ou des séries de ports.</p> <p>🔌 Si vous sélectionnez le protocole ICMP ou ICMPv6, vous pouvez spécifier les commandes. Pour ce faire, sélectionnez une commande dans la liste des commandes connues ou ajoutez des commandes spécifiques ou une série de commandes.</p> <p>Lorsque vous sélectionnez cette option l'option Ajouter devient disponible. Vous pouvez utiliser l'option Ajouter ou Supprimer. pour définir ou supprimer un port ou une commande.</p>

8 Cliquez sur **Suivant**.

- 9 Sélectionnez **Créer une entrée de journal de l'historique de la sécurité** si vous souhaitez que le produit Norton crée une entrée dans le journal des événements du pare-feu.
Votre produit Norton crée une entrée lorsqu'une communication réseau correspond à cette règle. Vous pouvez afficher le journal des événements dans la fenêtre **Historique de la sécurité**, sous **Pare-feu - Activités**. Si vous avez sélectionné l'option **Surveiller** dans la fenêtre **Action**, l'option **Créer une entrée dans le journal historique de la sécurité** est cochée par défaut. Vous ne pouvez pas la désélectionner pour désactiver l'option, car il s'agit de la valeur par défaut.
- 10 Sous **Appliquer la règle pour le trafic transversal NAT IPv6**, sélectionnez une option. Les options disponibles sont les suivantes :
 - **Activé**
 - **Si explicitement requis**
 - **Désactivé**
- 11 Cliquez sur **Suivant**, puis, dans la zone de texte, entre le nom de la règle.
- 12 Cliquez sur **Suivant**, puis vérifiez les paramètres de la nouvelle règle.
- 13 Cliquez sur **Terminer**.
- 14 Quand vous avez fini d'ajouter des règles, cliquez sur **Fermer**.

Modification des règles de trafic et des règles de programme

Vous pouvez modifier une règle de pare-feu existante qui ne fonctionne pas de manière appropriée. Vous pouvez utiliser l'option **Modifier** pour changer les paramètres d'une règle de pare-feu existante. Lorsque vous changez une règle, le pare-feu utilise les nouveaux critères de la règle modifiée pour contrôler le trafic réseau.

Vous ne pouvez pas modifier certaines règles par défaut qui sont en lecture seule. Cependant, vous pouvez

afficher les paramètres de ces règles en utilisant l'option **Afficher**.

Modification d'une règle de trafic

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Règles de trafic**, sélectionnez la règle que vous souhaitez modifier.
- 4 Cliquez sur **Modifier**.
- 5 Dans la fenêtre **Modifier une règle**, modifiez les éléments appropriés de la règle.
- 6 Une fois les modifications effectuées, cliquez sur **OK**.

Modification d'une règle de programme

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Contrôle de programme**, sélectionnez le programme que vous souhaitez modifier.
- 4 Cliquez sur **Modifier**.
Vous pouvez également utiliser la liste déroulante **Accès** située en regard du programme pour modifier son niveau d'accès. Le pare-feu intelligent modifie ou crée, en conséquence, la règle appropriée pour le programme.
- 5 Dans la fenêtre **Règles**, sélectionnez la règle à modifier.
- 6 Cliquez sur **Modifier**.
- 7 Dans la fenêtre **Modifier une règle**, modifiez les éléments appropriés de la règle.
- 8 Une fois les modifications effectuées, cliquez sur **OK**.

Modification de l'ordre des règles de filtrage

Chaque liste de règles de filtrage est traitée de haut en bas. Vous pouvez définir le traitement des règles de filtrage en modifiant leur ordre.



Ne modifiez l'ordre des règles de trafic par défaut que si vous êtes un utilisateur expérimenté. La modification de l'ordre des règles de trafic par défaut peut affecter le pare-feu et la sécurité de votre ordinateur.

Modification de l'ordre des règles de trafic

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Règles de trafic**, sélectionnez la règle à déplacer.
- 4 Effectuez l'une des opérations suivantes :
 - Pour déplacer cette règle en haut de celle qui la précède, cliquez sur **Vers le haut**.
 - Pour déplacer cette règle en bas de la règle qui la suit, cliquez sur **Vers le bas**.
- 5 Quand vous avez fini de déplacer les règles, cliquez sur **Appliquer**.

Modification de l'ordre des règles de programme

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Contrôle de programme**, sélectionnez le programme qui contient la règle à déplacer.
- 4 Cliquez sur **Modifier**.
- 5 Dans la fenêtre **Règles**, sélectionnez la règle à déplacer.

- 6 Effectuez l'une des opérations suivantes :
 - Pour déplacer cette règle en haut de celle qui la précède, cliquez sur **Vers le haut**.
 - Pour déplacer cette règle en bas de la règle qui la suit, cliquez sur **Vers le bas**.
- 7 Une fois les règles déplacées, cliquez sur **OK**.
- 8 Dans la fenêtre **Pare-feu**, cliquez sur **Appliquer**.

Désactivation temporaire d'une règle de trafic

Vous pouvez désactiver temporairement une règle de trafic si vous souhaitez autoriser un accès spécifique à un ordinateur ou un programme. Veillez à réactiver la règle lorsque vous avez fini d'utiliser le programme ou l'ordinateur ayant nécessité la modification.



Vous ne pouvez pas désactiver certaines règles de filtrage par défaut de la liste. Vous pouvez afficher uniquement les paramètres de ces règles en utilisant l'option **Afficher**.

Désactivation temporaire d'une règle de trafic

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Règles de trafic**, désélectionnez la case en regard de la règle que vous souhaitez désactiver.
- 4 Cliquez sur **Appliquer**.

Suppression d'une règle de pare-feu

Si nécessaire, vous pouvez supprimer certaines règles de filtrage. Cependant, certaines règles de trafic par défaut figurant dans la liste ne peuvent pas être modifiées. Vous pouvez afficher uniquement les paramètres de ces règles en utilisant l'option **Afficher**.



Ne supprimez des règles générales que si vous êtes un utilisateur expérimenté. La suppression de règles de filtrage par défaut peut affecter le pare-feu et la sécurité de votre ordinateur.

Suppression d'une règle de trafic

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Règles de trafic**, sélectionnez la règle à supprimer.
- 4 Cliquez sur **Supprimer**.
- 5 Dans la boîte de dialogue **Confirmation**, cliquez sur **Oui**.

Suppression d'une règle de programme

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Contrôle de programme**, dans la colonne **Programme**, sélectionnez le programme qui contient la règle à supprimer.
- 4 Cliquez sur **Modifier**.
Cliquez sur **Supprimer** pour supprimer toutes les règles de programme associées au programme en question.
- 5 Dans la fenêtre **Règles**, sélectionnez la règle à supprimer.
- 6 Cliquez sur **Supprimer**.
- 7 Dans la boîte de dialogue **Confirmation**, cliquez sur **Oui**.
- 8 Cliquez sur **OK**.

Activation et désactivation des notifications de blocage du pare-feu

Lorsque le contrôle automatique des programmes est activé, le Pare-feu intelligent bloque automatiquement la connexion à Internet des applications malveillantes et des applications dont la réputation est faible ou les empêche de communiquer avec d'autres ordinateurs sur votre réseau.

Votre produit Norton vous avertit lorsque le Pare-feu intelligent bloque la connexion au réseau d'une application. Vous pouvez désactiver cette option à l'aide du **Contrôle avancé des programmes** si vous ne souhaitez pas afficher la notification.

Désactivation des notifications de blocage du pare-feu

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Contrôle avancé des programmes**, déplacez le curseur en regard de **Afficher les notifications de blocage du pare-feu** sur la position **Désactivé**.

A propos de la fonction Norton Firewall Diagnosis

Il peut arriver que le pare-feu bloque le trafic réseau que vous souhaitez autoriser en fonction de ses paramètres de configuration. Cette situation peut entraîner des problèmes d'accès à Internet, au réseau ou à un autre ordinateur dans le cadre de tâches telles que le partage de ressources.

Lorsque vous rencontrez des problèmes d'accès au réseau, Norton Firewall agit rapidement en identifiant la cause de la panne et donne son diagnostic. Votre produit Norton affiche l' **Assistant de diagnostic du pare-feu** lors de problèmes de connexion réseau.



La fonction Norton Firewall Diagnosis est disponible uniquement sous Windows 7 ou version ultérieure.

L'Assistant contient le rapport du diagnostic du problème spécifique à divers cas de blocages de réseau. Un blocage de réseau peut, par exemple, se produire dans un des cas suivants :

- Le protocole inhabituel gérant le trafic est bloqué
- La règle de pare-feu actuellement activée est conditionnée pour bloquer le trafic que vous souhaitez autoriser
- Le trafic a violé la politique de processus du pare-feu
- Le trafic a violé la politique de trafic du pare-feu
- Le trafic provient de la zone à accès restreint des réseaux ou ordinateurs
- Le trafic correspond à une signature d'attaque de Prévention d'intrusion

Vous pouvez utiliser l' **Assistant de diagnostic du pare-feu** comme guide de dépannage du problème de connexion réseau.

Pour chaque cas de blocage du réseau, l'Assistant propose l'analyse de la cause du pare-feu et les solutions potentielles de résolution du blocage.

Votre produit Norton vous recommande d'utiliser l' **Assistant de diagnostic du pare-feu** pour supprimer tout type de blocage. Les solutions de l'Assistant vous permettent d'analyser le problème et de prendre la mesure adéquate en vue de résoudre le problème.

Utiliser l'Assistant pour résoudre le problème présente les avantages suivants :

- il essaie automatiquement de résoudre lui-même le problème
- Il vous permet de modifier les paramètres relatifs au blocage
- il vous permet d'afficher les informations du journal relatives à l'événement de blocage du réseau
- il vous offre la possibilité de désactiver le pare-feu comme dernier recours afin de résoudre le problème

A propos des informations de réputation dans les alertes de pare-feu

Les alertes de pare-feu vous informent des tentatives de connexion provenant d'autres ordinateurs et des tentatives de connexion à d'autres ordinateurs provenant des programmes installés sur votre ordinateur. Les informations de réputation des alertes de pare-feu vous permettent de décider d'autoriser ou de bloquer les tentatives de communication par des applications de mise en réseau.

Elles peuvent également vous aider à déterminer la fiabilité des programmes et processus exécutés sur votre ordinateur ayant accès au réseau. La technologie de sécurité basée sur la réputation offre des indices de réputation de sécurité pour tous les fichiers Internet basés sur les informations recueillies auprès des clients Norton.

Votre produit Norton obtient des informations spécifiques, telles que le nom de fichier et la clé de hachage du fichier, et les envoie au serveur Symantec. Les serveurs Symantec analysent les informations du fichier et fournissent un niveau d'approbation le concernant. Ces informations de réputation sont renvoyées à votre ordinateur. En fonction des informations de réputation du programme, vous pouvez autoriser ou bloquer le trafic entrant ou sortant. Si l'un des fichiers analysés est suspect ou vulnérable, votre produit Norton lui attribue un niveau d'approbation **Faible** ou **Nul**.



Votre ordinateur doit être connecté à Internet pour accéder aux informations de réputation les plus récentes recueillies par Symantec. Si votre ordinateur n'est pas connecté à Internet, votre produit Norton utilise les informations de réputation disponibles localement.

Vous trouverez les informations de réputation suivantes dans le volet gauche des alertes de pare-feu :

Prévalence

Affiche la prévalence des utilisateurs du fichier. Ces données sont fondées sur les informations partagées par des millions de clients de la Communauté de veille Norton et sur les recherches de Symantec.

Les différentes catégories sont les suivantes :

■ Très peu d'utilisateurs

Indique que la prévalence des utilisateurs du fichier est très faible.

■ Peu d'utilisateurs

Indique que la prévalence des utilisateurs du fichier est moyenne.

■ Beaucoup d'utilisateurs

Indique que la prévalence des utilisateurs du fichier est élevée.

Age

Indique l'ancienneté du fichier fondée sur les données partagées par des millions de clients de la Communauté de veille Norton et les recherches de Symantec.

Niveau d'approbation



Affiche le niveau d'approbation du fichier.

Les niveaux d'approbation assignés par Symantec sont les suivants :

- **Approuvé** : indique que le fichier est approuvé par Norton.
- **Fiable** : Symantec dispose de nombreuses indications quant à la fiabilité du fichier.
- **Non testé** : Symantec ne dispose pas d'informations suffisantes sur le fichier pour lui attribuer un niveau d'approbation.

Le fichier n'est ni sûr ni risqué.

- **Faible** : Symantec dispose de quelques indications attestant du manque de fiabilité du fichier.
- **Nul** : Symantec dispose de nombreuses indications quant au manque de fiabilité du fichier.

Ce fichier est suspect et susceptible d'endommager l'ordinateur.

Si les niveaux d'approbation affichés dans la fenêtre **Alerte de pare-feu** sont **Faible** ou **Nul**, Symantec recommande de sélectionner les options **Terminer** ou

Toujours bloquer dans la liste déroulante **Options**. Cette action termine ou bloque toutes les tentatives d'accès par le programme ou le processus. Ce fichier ou processus est suspect et susceptible d'endommager l'ordinateur.

Désactivation et activation de la protection du navigateur

Vous pouvez choisir de protéger votre navigateur en autorisant votre produit Norton à bloquer l'accès à votre ordinateur par des programmes inconnus.

Par défaut, l'option **Protection du navigateur** est activée. Dans ce cas, votre produit Norton bloque proactivement les programmes malveillants nouveaux ou inconnus, avant qu'ils n'attaquent votre ordinateur. En protégeant votre navigateur, votre produit Norton sécurise vos informations sensibles et empêche les attaquants de contrôler votre système à distance. Cette fonction recherche les vulnérabilités éventuelles des navigateurs Internet Explorer 7.0 ou version ultérieure, Chrome 17.0 ou version ultérieure et Firefox 10.0 ou version ultérieure.



Maintenez toujours le paramètre de protection du navigateur activée, pour protéger votre navigateur contre les attaques menées par des sites Web malveillants.

Désactivation ou activation de la protection du navigateur

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.

- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 4 A la ligne **Protection du navigateur**, effectuez l'une des opérations suivantes :
 - Pour désactiver la protection du navigateur, déplacez le curseur **Marche/Arrêt** vers la droite, sur la position **Arrêt**.
 - Pour activer la protection du navigateur, déplacez le curseur **Marche/Arrêt** vers la gauche, sur la position **Marche**.
- 5 Cliquez sur **Appliquer**.
- 6 Si vous désactivez la protection du navigateur, dans la boîte de dialogue **Alerte de sécurité**, dans la liste déroulante **Sélectionner la durée**, spécifiez pendant combien de temps vous voulez désactiver la protection du navigateur.
- 7 Dans la fenêtre Alerte de sécurité , cliquez sur **OK**.
- 8 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Désactivation ou activation du diagnostic des téléchargements

La fonction Diagnostic des téléchargements protège l'ordinateur contre tout fichier risqué que vous pouvez exécuter ou lancer après l'avoir téléchargé à l'aide d'un navigateur pris en charge. L'option **Diagnostic des téléchargements** est activée par défaut. Dans ce cas, Diagnostic des téléchargements vous informe sur les niveaux de fiabilité des fichiers exécutables que vous téléchargez. Les informations de fiabilité que Diagnostic des téléchargements fournit indiquent si le fichier téléchargé peut être installé en toute sécurité.

Il peut parfois être utile de désactiver Diagnostic des téléchargements. Par exemple, vous voulez télécharger un fichier risqué. Dans ce cas, vous devez désactiver l'option Diagnostic des téléchargements afin que le

produit Norton vous laisse télécharger le fichier et ne le supprime pas de votre ordinateur.

Vous pouvez utiliser l'option **Diagnostic des téléchargements** pour désactiver ou activer le diagnostic des téléchargements.

Désactivation de l'option Diagnostic des téléchargements

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 4 Sur la ligne **Diagnostic des téléchargements**, déplacez le curseur **Ac./Désac.** vers la droite sur la position **Désactivé**.
- 5 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**.
- 6 Dans la boîte de dialogue **Alerte de sécurité** de la liste déroulante **Sélectionner la durée**, sélectionnez pendant combien de temps vous souhaitez désactiver Diagnostic des téléchargements, puis cliquez sur **OK**.
- 7 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Activation de l'option Diagnostic des téléchargements

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 4 Sur la ligne **Diagnostic des téléchargements**, déplacez le curseur **Ac./Désac.** vers la gauche, sur la position **Activé**.
- 5 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**, puis sur **Fermer**.

Configuration de l'option **Notifications sur le Diagnostic des téléchargements**

L'option **Notifications sur le Diagnostic des téléchargements** permet de choisir le moment auquel vous voulez que **Détail des téléchargements** affiche les notifications.

Par défaut, l'option **Notifications sur le Diagnostic des téléchargements** est définie sur **Marche**. En fonction du type d'application que vous utilisez pour télécharger votre fichier, le produit Norton effectue l'une des actions suivantes :

- Il vous avertit à chaque fois que vous téléchargez un fichier exécutable.
- Il vous avertit uniquement quand vous téléchargez un fichier qui est infecté par une identification virale locale. Si le fichier que vous téléchargez est infecté avec une identification virale de nuage, votre produit Norton supprime le fichier de votre ordinateur et vous avertit avec les détails de la menace.

Lorsque l'option **Notifications sur le Diagnostic des téléchargements** est définie sur **Risques seulement**, le diagnostic des téléchargements vous avertit uniquement lorsque vous téléchargez un fichier exécutable infecté ou suspect.

Le fait de définir **Notifications sur le Diagnostic des téléchargements** sur **Risques seulement** ne désactive pas l'analyse de tous les fichiers exécutables que vous téléchargez. Que vous receviez des notifications pour tous les fichiers ou pas, l'historique de la sécurité enregistre un dossier de toutes les activités de la fonction **Diagnostic des téléchargements**. Vous pouvez afficher un résumé des alertes et notifications de la fonction **Diagnostic des téléchargements** dans l'historique de la sécurité.

Configuration de l'option **Notifications sur le Diagnostic des téléchargements**

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 4 Sous **Diagnostic des téléchargements**, à la ligne **Notifications sur le Diagnostic des téléchargements**, effectuez l'une des opérations suivantes :
 - Pour recevoir des notifications de la fonction Diagnostic des téléchargements seulement pour les fichiers exécutables infectés ou suspects que vous téléchargez, déplacez le curseur **Notifications sur le Diagnostic des téléchargements** vers la droite, à la position **Risques seulement**.
 - Pour recevoir des notifications de la fonction Diagnostic des téléchargements pour tous les fichiers que vous téléchargez, déplacez le curseur **Notifications sur le Diagnostic des téléchargements** vers la gauche, sur la position **Activé**.
- 5 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**, puis sur **Fermer**.

Configurer l'option **Afficher le rapport au lancement des fichiers**

L'option **Afficher le rapport au lancement des fichiers** permet de spécifier le moment et le type de fichier pour lequel il vous sera demandé de choisir l'action appropriée. Par exemple, vous pouvez indiquer le type des fichiers téléchargés pour lesquels la fenêtre Diagnostic des téléchargements vous invite à choisir l'action à appliquer aux fichiers et à indiquer la fréquence

Configurer l'option Afficher le rapport au lancement des fichiers

à laquelle ces invites doivent s'afficher pour vous demander d'intervenir de manière adéquate.

Vous pouvez utiliser les options suivantes pour configurer **Afficher le rapport au lancement des fichiers** :

<p>Toujours</p>	<p>Lorsque vous définissez l'option Afficher le rapport concernant le lancement de fichiers sur Toujours, la fenêtre Diagnostic des téléchargements vous demande de choisir l'action appropriée pour les fichiers fiables ou de réputation inconnue. Dans ce cas, la fenêtre Diagnostic des téléchargements s'affiche chaque fois que vous tentez de lancer tout fichier téléchargé ayant un score fiable ou de réputation inconnue. Dans cette fenêtre, vous pouvez voir des informations détaillées sur le fichier et les options vous permettant de sélectionner une intervention adéquate pour le fichier.</p> <p>Dans le cas des fichiers pouvant présenter des risques, le produit Norton les identifie comme étant des menaces et les supprime.</p>
------------------------	--

Non testé uniquement

Lorsque vous définissez l'option **Afficher le rapport concernant le lancement de fichiers sur Non testés uniquement**, la fenêtre Diagnostic des téléchargements vous demande de choisir l'action appropriée pour les fichiers inconnus uniquement. Dans ce cas, la fenêtre **Diagnostic des téléchargements** s'affiche chaque fois que vous tentez de lancer tout fichier téléchargé ayant un score de réputation inconnue. Dans cette fenêtre, vous pouvez voir des informations détaillées sur le fichier et les options vous permettant de sélectionner une intervention adéquate pour le fichier.

Par défaut, l'option **Afficher le rapport concernant le lancement de fichiers** est définie sur **Non testé uniquement**. Dans ce cas, le produit Norton permet l'exécution des fichiers sécurisés sans vous demander de choisir l'action appropriée. Dans le cas des fichiers pouvant présenter des risques, le produit Norton les identifie comme étant des menaces et les supprime.

Jamais	<p>Lorsque vous configurez l'option Afficher le rapport concernant le lancement de fichiers sur Jamais, Diagnostic des téléchargements ne vous invite pas à sélectionner une action appropriée pour tout type de fichier que vous téléchargez. Dans ce cas, la fenêtre Diagnostic des téléchargements s'affiche chaque fois que vous tentez de lancer tout fichier téléchargé.</p> <p>Les messages d'alerte que vous supprimez et les informations sur l'activité peuvent être examinés à tout moment dans l'historique de la sécurité.</p>
---------------	---

Configuration de l'option **Afficher le rapport concernant le lancement de fichiers**

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.

- 4 Sous **Diagnostic des téléchargements**, à la ligne **Afficher le rapport concernant le lancement de fichiers**, effectuez l'une des opérations suivantes :
 - Pour que le Diagnostic des téléchargements vous invite à prendre une mesure appropriée dans le cas des fichiers fiables ou inconnus, déplacez le curseur **Afficher le rapport concernant le lancement de fichiers** vers la position **Toujours**.
 - Pour que le Diagnostic des téléchargements vous invite à prendre une mesure appropriée dans le cas des fichiers inconnus uniquement, déplacez le curseur **Afficher le rapport concernant le lancement de fichiers** sur **Non testés uniquement**.
 - Si vous ne voulez pas que le Diagnostic des téléchargements vous invite à prendre une mesure appropriée pour tout type de fichier, déplacez le curseur **Afficher le rapport concernant le lancement de fichiers** vers la position **Jamais**.
- 5 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**, puis sur **Fermer**.

Désactivation ou activation des notifications de la prévention d'intrusion

Vous pouvez choisir de recevoir ou non des notifications lorsque la Prévention d'intrusion bloque des attaques suspectées. Qu'une notification s'affiche ou pas, les activités de la Prévention d'intrusion sont consignées dans l'Historique de la sécurité. Les entrées de l'Historique de la sécurité contiennent des informations concernant l'ordinateur à l'origine de l'attaque et l'attaque elle-même.

Vous pouvez également choisir de recevoir des notifications lorsque la Prévention d'intrusion bloque des attaques suspectées avec une signature précise.

Désactivation ou activation des notifications de la Prévention d'intrusion

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 4 Sous **Prévention d'intrusion**, sur la ligne **Notifications**, effectuez l'une des opérations suivantes :
 - Déplacez le curseur **Marche/Arrêt** vers la droite sur la position **Arrêt**.
 - Déplacez le curseur **Marche/Arrêt** vers la gauche sur la position **Marche**.
- 5 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**, puis sur **Fermer**.

Désactivation ou activation d'une notification spécifique de la Prévention d'intrusion

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 4 Sous **Prévention d'intrusion**, sur la ligne **Signatures d'intrusion**, cliquez sur **Configurer**.
- 5 Dans la fenêtre **Signatures d'intrusion**, cliquez sur une signature d'attaque, puis sur **Propriétés**.
- 6 Dans la fenêtre, **Propriétés de signature**, sélectionnez ou désélectionnez l'option **Me prévenir quand cette signature est détectée**.
- 7 Cliquez sur **OK**.
- 8 Dans la fenêtre **Signatures d'intrusion**, cliquez sur **OK**.
- 9 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**, puis sur **Fermer**.

Exclusion ou inclusion des signatures d'attaque dans la surveillance

Il arrive que certaines activités de réseau inoffensives ressemblent à une signature d'attaque. Il se peut que vous receviez des notifications répétées faisant allusion à des attaques possibles. Si vous savez que les attaques qui déclenchent ces notifications sont inoffensives, vous pouvez créer une exclusion pour la signature d'attaque correspondante.

Chaque nouvelle exclusion rend l'ordinateur vulnérable aux attaques.

Si vous avez exclu des signatures d'attaque que vous voulez surveiller de nouveau, vous pouvez les inclure dans la liste de signatures actives.

Exclusion des signatures d'attaque de la surveillance

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 4 Sous **Prévention d'intrusion**, sur la ligne **Signatures d'intrusion**, cliquez sur **Configurer**.
- 5 Dans la fenêtre **Signatures d'intrusion**, désélectionnez les signatures d'attaque que vous souhaitez exclure, puis cliquez sur **OK**.
- 6 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Inclusion des signatures d'attaque préalablement exclues

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.

- 4 Sous **Prévention d'intrusion**, sur la ligne **Signatures d'intrusion**, cliquez sur **Configurer**.
- 5 Dans la fenêtre **Signatures d'intrusion**, sélectionnez les signatures d'attaque que vous souhaitez inclure, puis cliquez sur **OK**.
- 6 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Activation ou désactivation d'AutoBlock

Lorsqu'une attaque provenant d'un ordinateur est détectée, elle est automatiquement bloquée pour garantir la sécurité de votre ordinateur. Si une signature d'attaque différente provenant du même ordinateur est détectée, votre produit Norton active AutoBlock. La fonction AutoBlock bloque tout le trafic entre votre ordinateur et l'ordinateur attaquant, pendant une durée spécifique. Au cours de cette période, AutoBlock bloque également le trafic qui ne correspond pas à une signature d'attaque.



Vous pouvez spécifier la durée pendant laquelle votre produit Norton doit bloquer les connexions des ordinateurs attaquants. Par défaut, votre produit Norton bloque tout le trafic entre votre ordinateur et l'ordinateur attaquant pendant 30 minutes.

AutoBlock interrompt tout le trafic entre votre ordinateur et un ordinateur spécifique. Si vous voulez bloquer tout le trafic à destination et en provenance de votre ordinateur, vous pouvez utiliser l'option **Blocage de tout le trafic réseau**.

Si des ordinateurs auxquels vous voulez accéder sont bloqués par AutoBlock, vous pouvez désactiver AutoBlock.

Activation ou désactivation d'AutoBlock

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.

- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 4 Sous **Prévention d'intrusion**, sur la ligne **AutoBlock d'intrusion**, cliquez sur **Configurer**.
- 5 Dans la fenêtre **AutoBlock intrusion**, sous **AutoBlock**, effectuez l'une des opérations suivantes :
 - Pour désactiver AutoBlock d'intrusion, cliquez sur **Arrêt**.
 - Pour activer AutoBlock d'intrusion, cliquez sur **Activé (Recommandé)**, puis dans la liste déroulante **AutoBlock sur les ordinateurs attaquants pendant**, sélectionnez la durée pendant laquelle AutoBlock doit rester activé.
- 6 Dans la fenêtre **AutoBlock d'intrusion**, cliquez sur **OK**.
- 7 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Déblocage d'ordinateurs bloqués par AutoBlock

Il arrive que certaines activités de réseau inoffensives ressemblent à des signatures d'attaque et qu'AutoBlock bloque l'activité de réseau automatiquement pour garantir la sécurité de votre ordinateur. La liste des ordinateurs actuellement bloqués par AutoBlock peut contenir celui avec lequel vous devez pouvoir communiquer.

Si un ordinateur auquel vous voulez accéder apparaît dans la liste des ordinateurs bloqués, débloquez-le. Il est possible que vous souhaitiez réinitialiser la liste AutoBlock si vous avez modifié vos paramètres de protection. Pour réinitialiser la liste AutoBlock, vous pouvez simultanément débloquer tous les ordinateurs de la liste AutoBlock..

Déblocage d'un ordinateur bloqué par AutoBlock

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.

- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 4 Sous **Prévention d'intrusion**, sur la ligne **AutoBlock d'intrusion**, cliquez sur **Configurer**.
- 5 Dans la fenêtre **AutoBlock d'intrusion**, sous **Ordinateurs actuellement bloqués par AutoBlock**, sélectionnez l'adresse IP de l'ordinateur.
- 6 Sous la colonne **Action**, sélectionnez **Débloquer** dans la liste déroulante.
- 7 Dans la fenêtre AutoBlock d'intrusion, cliquez sur **OK**.
- 8 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Blocage permanent d'un ordinateur qui a été bloqué par AutoBlock

Vous pouvez bloquer de manière permanente un ordinateur qui a été bloqué par AutoBlock. L'ordinateur bloqué de manière permanente est supprimé de la liste AutoBlock et ajouté comme ordinateur restreint à la liste Approbation du périphérique.

Blocage permanent d'un ordinateur qui a été bloqué par AutoBlock

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 4 Sous **Prévention d'intrusion**, sur la ligne **AutoBlock d'intrusion**, cliquez sur **Configurer**.
- 5 Dans la fenêtre **AutoBlock d'intrusion**, sous **Ordinateurs actuellement bloqués par AutoBlock**, cliquez sur l'ordinateur que vous voulez bloquer de manière permanente.

A propos de la liste d'exclusions de la prévention d'intrusion

- 6 Dans la colonne **Action**, sélectionnez **Restreindre** dans la liste déroulante.
- 7 Dans la fenêtre AutoBlock d'intrusion, cliquez sur **OK**.
- 8 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

A propos de la liste d'exclusions de la prévention d'intrusion

Le système de prévention d'intrusion de votre produit Norton analyse tout le trafic réseau entrant et sortant de votre ordinateur. Quand un périphérique de votre réseau demande l'accès à votre ordinateur, la prévention d'intrusion analyse cette requête afin de vérifier qu'il ne s'agit pas d'une attaque virale. Si les informations correspondent à une signature d'attaque, la prévention d'intrusion bloque le trafic du périphérique suspect et protège votre ordinateur. Le fait d'analyser chaque requête en provenance de tous les périphériques qui accèdent à l'ordinateur augmente le temps d'analyse, ce qui diminue la vitesse réseau de l'ordinateur.

Si vous avez la certitude qu'un périphérique de votre réseau est sûr, vous pouvez définir son niveau d'approbation sur **Approb. totale**. Vous pouvez configurer le niveau d'approbation d'un périphérique à l'aide de la fonction **Approbation du périphérique** sous **Paramètres réseau**. Vous pouvez exclure ces périphériques approuvés de l'analyse de prévention d'intrusion. L'exclusion des périphériques dont le niveau d'approbation est **Approb. totale** de l'analyse de prévention d'intrusion réduit la durée de l'analyse et améliore les performances réseau de votre ordinateur. Quand vous excluez un périphérique dont le niveau d'approbation est **Approb. totale**, votre produit Norton n'analyse aucune information en provenance de ce périphérique. Les périphériques d'un niveau **Approbation totale** qui sont exclus de l'analyse de la Prévention d'intrusion sont ajoutés à la liste d'exclusions de la Prévention d'intrusion.

Retrait de tous les périphériques de la liste d'exclusion de la Prévention d'intrusion

Quand un périphérique de votre réseau tente d'infecter votre ordinateur, AutoBlock intercepte toutes les demandes d'accès de ce périphérique. Si vous ajoutez ce périphérique à la liste des exclusions de la prévention d'intrusion, votre produit Norton supprime le périphérique de la liste d'exclusions.



Vérifiez que l'adresse IP des périphériques ajoutés à la liste d'exclusions de prévention d'intrusion ne change jamais.

Si vous découvrez que l'un des périphériques exclus de l'analyse de prévention d'intrusion est infecté, vous pouvez purger la liste d'exclusions enregistrée. Quand vous purgez la liste d'exclusions, votre produit Norton supprime de la liste tous les périphériques exclus de l'analyse de prévention d'intrusion.

Retrait de tous les périphériques de la liste d'exclusion de la Prévention d'intrusion

Si vous avez la certitude qu'un périphérique de votre réseau est sûr, vous pouvez définir son niveau d'approbation sur Approb. totale. Vous pouvez ensuite sélectionner l'option **Exclure de l'analyse IPS** afin d'exclure les périphériques approuvés de l'analyse de prévention d'intrusion. L'exclusion de périphériques dont le niveau d'approbation est Approb. totale de l'analyse de prévention d'intrusion raccourcit le temps d'analyse et améliore la vitesse du réseau de l'ordinateur. Lorsque vous excluez un périphérique dont le niveau d'approbation est Approb. totale de l'analyse de prévention d'intrusion, votre produit Norton n'analyse pas les informations reçues à partir de ce périphérique. Les périphériques d'un niveau Approbation totale qui sont exclus de l'analyse de la Prévention d'intrusion sont ajoutés à la liste d'exclusions de la Prévention d'intrusion.

Si vous découvrez que l'un des périphériques que vous avez exclus de l'analyse de la Prévention d'intrusion est

Retrait de tous les périphériques de la liste d'exclusion de la Prévention d'intrusion

infecté, vous pouvez purger la liste d'exclusions enregistrée et supprimer tous les périphériques.

Vous pouvez purger la liste d'exclusions enregistrée dans les circonstances suivantes :

- L'un des périphériques que vous avez exclus de l'analyse de la Prévention d'intrusion est infecté.
- L'un des périphériques que vous avez exclus de l'analyse de la Prévention d'intrusion tente d'infecter l'ordinateur.
- Votre réseau domestique est infecté.

Lorsqu'un périphérique sur votre réseau tente d'infecter l'ordinateur, AutoBlock arrête toutes les demandes d'accès en provenance de ce périphérique. Si vous ajoutez ce périphérique à la liste des exclusions de la prévention d'intrusion, votre produit Norton supprime le périphérique de la liste d'exclusions.

Lorsque vous retirez tous les périphériques de la liste d'exclusions enregistrée, la Prévention d'intrusion analyse chaque demande provenant de tous les périphériques qui accèdent à l'ordinateur.

Suppression de tous les périphériques de la liste d'exclusion de la Prévention d'intrusion

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 4 Sous **Prévention d'intrusion**, sur la ligne **Liste d'exclusions**, cliquez sur **Purger**.
- 5 Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.
- 6 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Ajout d'un périphérique à l'approbation du périphérique

Par défaut, le produit Norton détecte tous les périphériques connectés à votre réseau. Cependant, vous pouvez ajouter manuellement des ordinateurs et des périphériques non connectés à l'approbation du périphérique.

Vous pouvez ajouter les détails suivants lors de l'ajout d'un périphérique :

- Un nom ou une description.
- L'adresse IP ou l'adresse physique.



Si vous approuvez un périphérique qui n'est pas sur votre réseau, vous pouvez exposer votre ordinateur à des risques de sécurité potentiels.

Ajout d'un périphérique à l'approbation du périphérique

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Sur l'onglet **Paramètres généraux**, à la ligne **Approbation du périphérique**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Approbation du périphérique**, cliquez sur **Ajouter**.
- 5 Dans la fenêtre **Ajouter un périphérique**, saisissez le nom du périphérique à ajouter au réseau dans la zone de texte **Nom**.
Le nom d'un périphérique peut contenir 15 caractères maximum.

- 6 Dans la case **Adresse IP ou physique**, saisissez l'adresse IP ou l'adresse physique du périphérique à ajouter à l'approbation du périphérique. Vous pouvez utiliser les formats suivants dans la zone **Adresse IP ou adresse physique** :

Adresse IPv4	172.16.0.0
Adresse IPv6	fe80::12ac:fe44:192a:14cc
Adresse physique	11-22-c3-5a-fe-a4
Hôte résoluble	ftp.myfiles.com

L'adresse donnée est vérifiée une fois que le périphérique a été détecté physiquement sur le réseau.

- 7 Sélectionnez une option dans le menu déroulant **Niveau d'approbation**. Les options sont les suivantes :

Approb. totale

Ajoute un périphérique à la liste Approb. totale.

Les périphériques qui ont ce niveau d'approbation sont surveillés uniquement par rapport aux attaques et aux infections connues. Sélectionnez ce paramètre uniquement lorsque vous êtes sûr que le périphérique est complètement sécurisé.

Restreint

Ajoute un périphérique à la liste Restreint.

Les périphériques restreints n'ont pas accès à votre ordinateur.

- 8 Si vous souhaitez exclure le périphérique des analyses de la fonction Prévention d'intrusion, sélectionnez **Exclure de l'analyse IPS**.
- 9 Cliquez sur **Ajouter un périphérique**.

Modification du niveau d'approbation de votre réseau et de vos périphériques

Le niveau d'approbation détermine le niveau d'accès par défaut à votre ordinateur que les périphériques de votre réseau possèdent. Tout périphérique de votre réseau qui n'est pas explicitement approuvé ou restreint utilise le niveau d'approbation du réseau. Le niveau d'approbation réseau initial est fonction de la configuration de l'ordinateur.



Attribuez le niveau d'approbation Approb. totale à un périphérique uniquement s'il est connu et connecté à votre réseau.

Pour qu'un périphérique ait le niveau d'approbation Privé, les conditions suivantes doivent exister :

- L'ordinateur ne doit pas avoir d'adresse IP publique. Votre ordinateur n'a pas d'adresse IP publique s'il n'est pas connecté directement à Internet.
- L'ordinateur doit être connecté à un réseau local via une connexion sécurisée.
- La catégorie réseau doit être privée dans Windows Vista.



Si vous utilisez un réseau sans fil non sécurisé, le niveau d'approbation par défaut de tous les périphériques du réseau est **Public**.

Le niveau d'approbation d'un périphérique dépend également du niveau d'approbation de son réseau. Lorsque vous modifiez le niveau d'approbation d'un réseau, le produit Norton attribue le même niveau d'approbation à tous les appareils connectés au réseau. Cependant, le produit Norton ne modifie pas le niveau

Modification du niveau d'approbation de votre réseau et de vos périphériques

d'approbation des périphériques que vous approuvez ou restreignez individuellement.

Vous pouvez modifier ces paramètres pour changer le niveau d'approbation :

- de votre réseau
- Périphériques connectés au réseau

Modification du niveau d'approbation du réseau

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Sur l'onglet **Paramètres généraux**, à la ligne **Approbation du réseau**, cliquez sur **Configurer**.

- 4 Dans la fenêtre **Approbation du réseau**, sous **Niveau d'approbation**, choisissez l'une des options suivantes :

Approb. totale	<p>Ajoute le réseau à la liste Approb. totale.</p> <p>L'ensemble du trafic réseau que reçoit votre ordinateur depuis un réseau approuvé est filtré et autorisé à passer par le pare-feu. Cependant, les attaques et les infections connues sont encore contrôlées. Sélectionnez ce paramètre uniquement lorsque vous êtes sûr que le réseau est totalement fiable.</p>
Privé	<p>Ajoute le réseau à la liste Privé.</p> <p>Ce paramètre vous permet de partager des fichiers, des dossiers, des médias et des imprimantes sur votre ordinateur avec d'autres périphériques sur votre réseau. Vous pouvez paramétrer des connexions distantes du bureau avec d'autres appareils sur votre réseau.</p> <p>Votre ordinateur est protégé contre les attaques connues et tout le trafic inattendu.</p>

<p>Public</p>	<p>Ajoute le réseau à la liste Public.</p> <p>Par défaut, votre produit Norton bloque les fichiers, dossiers, médias, partages d'imprimantes et connexions distantes de bureau à d'autres périphériques du réseau.</p> <p>Pour partager les fichiers, dossiers, médias et imprimantes et paramétrer la connexion distante du bureau avec des appareils sur le réseau, vous pouvez configurer le paramètre Exceptions au blocage du trafic.</p> <p>Vous êtes protégé contre les attaques connues et tout le trafic inattendu.</p>
<p>Restreint</p>	<p>Ajoute le réseau à la liste Restreint.</p> <p>Les périphériques d'un réseau restreint ne peuvent pas communiquer avec votre ordinateur. Toutefois, vous pouvez toujours utiliser le réseau pour naviguer sur le Web, envoyer des messages électroniques ou utiliser d'autres modes de communication.</p>

5 Cliquez sur **Appliquer**, puis sur **OK**.

Modification du niveau d'approbation d'un périphérique

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Paramètres généraux**, à la ligne **Approbation du périphérique**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Approbation du périphérique**, sous **Niveau d'approbation**, choisissez l'une des options suivantes pour la configurer :

Approb. totale	Ajoute un périphérique à la liste Approb. totale. Les périphériques qui ont ce niveau d'approbation sont surveillés uniquement par rapport aux attaques et aux infections connues. Sélectionnez ce paramètre uniquement lorsque vous êtes sûr que le périphérique est complètement sécurisé.
Restreint	Ajoute un périphérique à la liste Restreint. Les périphériques restreints n'ont pas accès à votre ordinateur.

- 5 Cliquez sur **Appliquer**, puis sur **OK**.
Votre produit Norton affiche l'état du niveau d'approbation du périphérique restreint sur son icône.

A propos des types de risques de sécurité

Les risques de sécurité, tels que les programmes espions et publicitaire, peuvent affecter vos informations

personnelles et la confidentialité. Les programmes espions et publicitaire sont étroitement apparentés. Dans certains cas, leurs fonctionnalités peuvent se recouper, mais bien qu'ils collectent des informations sur vous, les types d'informations qu'ils recueillent sont différents.

Les programmes espions peuvent vous exposer au vol de votre identité ou à des fraudes. Ces programmes peuvent enregistrer automatiquement les frappes et capturer le trafic de votre messagerie et de votre messagerie instantanée ou dérober vos informations personnelles sensibles, telles que les mots de passe, ID de connexion ou numéros de cartes bancaires. Les données compromises sont ensuite envoyées à d'autres personnes.

Les logiciels publicitaires affichent des publicités sur votre ordinateur et recueillent des informations sur vos habitudes de navigation sur le Web. Ils fournissent ensuite ces données à des entreprises qui peuvent vous envoyer des publicités en fonction de ces préférences.

Les cookies de suivi sont de petits fichiers enregistrés que les programmes peuvent placer sur votre ordinateur pour suivre vos activités. Ces cookies peuvent ensuite envoyer ces informations à un tiers.

Certains programmes utilisent d'autres programmes considérés comme étant des risques de sécurité pour fonctionner. Par exemple, un logiciel gratuit que vous téléchargez peut utiliser des logiciels publicitaires pour maintenir son coût bas. Dans ce cas, il se peut que vous souhaitiez conserver le risque de sécurité sur votre ordinateur. Vous pouvez également souhaiter restaurer ce programme à risque si la protection contre les spywares l'a supprimé.

Par défaut, Norton Security autorise l'installation sur votre ordinateur des programmes blagues et des autres éléments présentant un risque faible. Vous pouvez modifier vos paramètres dans la fenêtre **Paramètres** pour que Norton Security détecte ces risques de sécurité.

A propos de Norton AntiSpam

Norton AntiSpam permet de classer les messages électroniques reçus dans vos programmes de messagerie dans les catégories Spam et Courrier légitime. Le courrier électronique est filtré et classé dans le dossier Boîte de réception s'il est légitime et dans le dossier Courrier indésirable ou Norton AntiSpam s'il ne l'est pas.

Norton AntiSpam utilise la technologie Symantec de filtrage de spam d'entreprise pour distinguer les messages électroniques indésirables des messages légitimes. Norton AntiSpam utilise un mécanisme de distribution avec filtrage en temps réel qui filtre les messages électroniques en utilisant divers filtres locaux à différents niveaux. Les filtres locaux classent les messages électroniques sous forme de spams ou de courriers légitimes. Si les filtres locaux classent le courrier électronique comme légitime, Norton AntiSpam récupère les informations du courrier électronique, telles que la signature et les hachages de l'URL. Norton AntiSpam envoie ensuite ces informations au serveur Web de Symantec afin d'effectuer une analyse supplémentaire.

Si un message électronique est classé comme spam, Norton AntiSpam change son objet, puis l'envoie à votre client de messagerie. Le client de messagerie identifie les modifications apportées à l'objet du message électronique et déplace ce dernier dans le dossier Courrier indésirable ou Norton AntiSpam.

Les filtres locaux Norton AntiSpam utilisent la technique de la Liste blanche, de la Liste noire et la technologie de filtrage brevetée pour classer les messages électroniques comme légitimes ou spam. Pour que ces filtres fonctionnent efficacement, Norton AntiSpam nécessite de mettre à jour les définitions antis spam régulièrement par l'intermédiaire de LiveUpdate. Ces mises à jour contiennent des informations sur les signatures des spams et des messages électroniques légitimes. Les mises à jour contiennent également toutes

les nouvelles règles créées par Symantec pour filtrer les spams.

Norton AntiSpam utilise des règles de messagerie prédéfinies et les listes Autorisés et Bloqués définies par l'utilisateur pour analyser le courrier électronique. Il accepte les messages des expéditeurs de la liste Autorisés et bloque ceux des expéditeurs de la liste Bloqués.

Norton AntiSpam importe automatiquement les listes d'adresses des programmes de messagerie pris en charge lors de l'intégration initiale. Cela permet de synchroniser la liste des expéditeurs autorisés et bloqués avec vos carnets d'adresses. Lorsque Norton AntiSpam importe les adresses de votre Carnet d'adresses Outlook ou votre carnet d'adresses de messagerie Windows, il importe également les adresses disponibles dans les listes Expéditeurs autorisés et Expéditeurs bloqués.



La désactivation de Norton AntiSpam augmente l'exposition aux messages électroniques indésirables. Vérifiez toujours que Norton AntiSpam est activé. Il protège votre client de messagerie contre le contenu indésirable en ligne.

Vous pouvez passer en revue les statistiques antis spam sous la catégorie **Antispam** de la fenêtre **Historique de la sécurité**.

Configuration de l'intégration client

L'onglet **Intégration client** répertorie les programmes de messagerie compatibles, ou clients, installés sur votre ordinateur et leurs carnets d'adresses. Lorsque vous sélectionnez un programme de messagerie électronique, votre produit Norton ajoute une liste déroulante **Norton AntiSpam** ou quelques options à la barre d'outils du logiciel de messagerie électronique utilisé. Vous pouvez utiliser la liste déroulante de **Norton AntiSpam** ou les options pour classer les messages électroniques comme du spam ou du courrier légitime. Vous pouvez également utiliser ces options pour vider

le dossier de spam et ouvrir la fenêtre **Paramètres** pour configurer les paramètres Norton AntiSpam. Si votre programme de messagerie électronique ne dispose pas d'un dossier Courrier indésirable, il ajoute également un dossier Norton AntiSpam dans la zone des dossiers. Vous pouvez utiliser le dossier Norton AntiSpam pour trier et stocker les spams. Toutefois, si votre client de messagerie dispose d'un dossier Norton AntiSpam provenant d'une version précédente de votre produit Norton, Norton AntiSpam utilise le dossier Norton AntiSpam à la place du dossier Courrier indésirable.



Les clients de messagerie électronique suivants ne prennent pas en charge l'intégration client :

- Thunderbird
- Windows Mail/Windows Live Mail
- Outlook Express

Lorsque vous classez un message électronique comme du spam ou du courrier légitime, Norton AntiSpam vous permet d'envoyer le message mal classé à Symantec sous la forme d'un commentaire. Vous pouvez utiliser l'option **Commentaire** pour envoyer à Symantec le message mal classé pour analyse.

Vous pouvez également importer une liste d'adresses figurant dans le programme de messagerie électronique pris en charge dans les listes Autorisés et Bloqués de Norton AntiSpam. Une fois par jour, lorsque l'ordinateur est en veille, Norton AntiSpam ajoute automatiquement les nouvelles adresses électroniques provenant du carnet d'adresses de votre programme de messagerie électronique pris en charge. Si toutefois, vous voulez importer manuellement des adresses, utilisez l'option **Importer** des adresses dans la fenêtre **Liste Autorisés**.

L'écran d'accueil apparaît lors de l'ouverture de votre client de messagerie. Si vous ne voulez pas l'apparition de l'écran d'accueil à l'avenir, vérifiez l'option **Ne pas afficher cela à nouveau** avant de cliquer sur **Fermer**. Votre produit Norton vous signale la réussite de

l'intégration de Norton AntiSpam à votre client de messagerie.

Norton AntiSpam importe également automatiquement les listes d'adresses issues des programmes de messagerie électronique pris en charge pendant l'intégration client initiale. Cela permet de conserver une liste des expéditeurs autorisés et bloqués à jour par rapport à vos carnets d'adresses actuels. Lorsque Norton AntiSpam importe les adresses de votre Carnet d'adresses Outlook ou votre carnet d'adresses de messagerie Windows, il importe également les adresses disponibles dans les listes Expéditeurs autorisés et Expéditeurs bloqués.

Votre produit Norton prend en charge l'intégration de Norton AntiSpam avec Microsoft Outlook 2002/2003/2007/2010/2013.

Configuration de l'intégration client

- 1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Dans l'onglet **Intégration client**, activez ou désactivez les programmes auxquels Norton AntiSpam doit s'intégrer.
- 4 Sélectionnez les carnets d'adresses à importer automatiquement dans votre liste Autorisés.
- 5 Cliquez sur **Appliquer**, puis sur **Fermer**.

Définition des exclusions du carnet d'adresses

Lorsque vous ajoutez une adresse électronique à la liste des exclusions de carnet d'adresses, Norton AntiSpam n'importe pas l'adresse dans la liste Autorisés ou Bloqués. Si vous supprimez une adresse électronique de la liste Autorisés ou Bloqués, Norton AntiSpam ajoute automatiquement l'adresse à la liste des exclusions du carnet d'adresses. Cependant, lorsque vous supprimez une adresse électronique que vous avez manuellement ajoutée à la liste Autorisés ou Bloqués, Norton AntiSpam

n'ajoute pas l'adresse à la liste des exclusions du carnet d'adresses.

Vous ne pouvez pas ajouter un nom de domaine à la liste des exclusions du carnet d'adresses. Lorsque vous supprimez un nom de domaine de la liste Autorisés ou Bloqués, Norton AntiSpam n'ajoute pas le nom de domaine à la liste des exclusions du carnet d'adresses.



Vous pouvez indiquer les exclusions du carnet d'adresses avant d'importer le carnet d'adresses. Ajoutez à la liste des exclusions du carnet d'adresses toutes les adresses électroniques à ne pas importer depuis le carnet d'adresses du programme de messagerie.

Ajout d'entrées à la liste des exclusions du carnet d'adresses

- 1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Dans l'onglet **Filtre**, dans la ligne **Exclusions du carnet d'adresses**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Exclusions du carnet d'adresses**, cliquez sur **Ajouter**.
- 5 Dans la boîte de dialogue **Ajouter une adresse de messagerie électronique**, entrez l'adresse électronique.
Si vous le désirez, vous pouvez entrer le nom correspondant à l'adresse électronique pour identifier aisément l'adresse.
- 6 Cliquez sur **OK** pour fermer la boîte de dialogue **Ajouter une adresse électronique**.
- 7 Cliquez sur **OK** pour enregistrer et fermer la fenêtre **Exclusions du carnet d'adresses**.

Modification ou suppression des entrées dans la liste des exclusions du carnet d'adresses

- 1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.

- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Dans l'onglet **Filtre**, dans la ligne **Exclusions du carnet d'adresses**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Exclusions du carnet d'adresses**, sélectionnez l'élément à utiliser.
- 5 Effectuez l'une des opérations suivantes :
 - Pour modifier une entrée, cliquez sur **Modifier** pour ouvrir la fenêtre **Modifier l'adresse électronique**, modifiez les informations, puis cliquez sur **OK**.
 - Pour supprimer une entrée, cliquez sur **Supprimer**.
- 6 Cliquez sur **OK** pour enregistrer et fermer la fenêtre **Exclusions du carnet d'adresses**.

Identification des expéditeurs autorisés

Si vous êtes certain qu'une adresse électronique ou un domaine ne présente aucun danger et ne voulez pas que Norton AntiSpam les bloque, vous pouvez les ajouter à la **liste Autorisés**.

Lorsque votre ordinateur est inactif, Norton AntiSpam importe automatiquement les entrées du carnet d'adresses et de la liste d'expéditeurs autorisés une fois par jour.

Si vous ajoutez un nouveau programme de messagerie électronique, vous pouvez importer son carnet d'adresses dans votre **liste Autorisés** à tout moment. Vous pouvez également ajouter individuellement des noms et des domaines à la **liste Autorisés**.



Avant d'importer le carnet d'adresses, vous pouvez spécifier vos exclusions de carnet d'adresses. Norton AntiSpam n'importe pas les adresses électroniques que vous ajoutez à la liste **Exclusions du carnet d'adresses**.

Importation d'un carnet d'adresses

- 1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Dans l'onglet **Filtre**, dans la ligne **Liste Autorisés**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Liste Autorisés**, cliquez sur **Importer**.
- 5 Dans la fenêtre **Liste Autorisés**, cliquez sur **Appliquer**.
- 6 Cliquez sur **OK**.

Ajout d'entrées à la liste Autorisés

- 1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Dans l'onglet **Filtre**, dans la ligne **Liste Autorisés**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Liste Autorisés**, cliquez sur **Ajouter**.
- 5 Dans la boîte de dialogue **Ajouter une adresse électronique**, sélectionnez le type d'adresse dans la liste déroulante **Type d'adresse**.
Vous pouvez sélectionner une des options suivantes.
 - **Adresse électronique**
 - **Domaine**
- 6 Effectuez l'une des opérations suivantes :
 - Si vous ajoutez une adresse électronique, saisissez l'adresse à autoriser et, éventuellement, le nom de l'expéditeur.
 - Si vous ajoutez un nom de domaine, tapez l'adresse du domaine (par exemple, @symantec.com) et éventuellement le nom du domaine.
- 7 Cliquez sur **OK**.

8 Dans la fenêtre **Liste Autorisés**, cliquez sur **Appliquer**.

9 Cliquez sur **OK**.

Modification ou suppression d'entrées de la liste Autorisés

1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.

2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.

3 Dans l'onglet **Filtre**, dans la ligne **Liste Autorisés**, cliquez sur **Configurer**.

4 Dans la fenêtre **Liste Autorisés**, sélectionnez l'élément à modifier ou supprimer.

5 Effectuez l'une des opérations suivantes :

- Pour modifier une entrée, cliquez sur **Modifier** pour ouvrir la boîte de dialogue **Modifier une adresse électronique**, modifiez les informations, puis cliquez sur **OK**.

- Pour supprimer une entrée, cliquez sur **Supprimer**.

Lorsque vous supprimez une entrée importée, Norton AntiSpam l'ajoute automatiquement à la liste Exclusions du carnet d'adresses.

6 Dans la fenêtre **Liste Autorisés**, cliquez sur **Appliquer**.

7 Cliquez sur **OK**.

Identification des expéditeurs de spam

Si vous ne souhaitez pas recevoir des messages d'une adresse ou d'un domaine, ajoutez l'adresse ou le domaine à la liste Bloqués. Norton AntiSpam traitera les messages électroniques en provenance de cette adresse ou domaine comme du spam.



Norton AntiSpam importe également automatiquement les listes d'adresses des listes d'expéditeurs bloqués de vos programmes de messagerie électronique vers la liste Bloqués au cours de l'intégration initiale au client ou de l'importation d'un carnet d'adresses.

Norton AntiSpam permet de saisir les adresses électroniques non valides dans la liste Bloqués.



Ajoutez toujours les adresses électroniques et domaines suspects à liste Bloqués afin de ne pas recevoir de messages électroniques indésirables de ces adresses ou domaines.

Ajout d'entrées à la liste Bloqués

- 1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Dans l'onglet **Filtre**, dans la ligne **Liste Bloqués**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Liste Bloqués**, cliquez sur **Ajouter**.
- 5 Dans la boîte de dialogue **Ajouter une adresse électronique**, sélectionnez le type d'adresse dans la liste déroulante **Type d'adresse**.
Vous pouvez sélectionner l'une des options suivantes :
 - **Adresse électronique**
 - **Domaine**
- 6 Effectuez l'une des opérations suivantes :
 - Si vous ajoutez une adresse électronique, entrez l'adresse à bloquer et le nom de l'expéditeur.
 - Si vous ajoutez un domaine, entrez l'adresse du domaine (par exemple, symantec.com) et le nom du domaine.
- 7 Cliquez sur **OK**.
- 8 Dans la fenêtre **Liste Bloqués**, cliquez sur **Appliquer**.
- 9 Cliquez sur **OK**.

Modification ou suppression d'entrées de la liste Bloqués

- 1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Dans l'onglet **Filtre**, dans la ligne **Liste Bloqués**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Liste Bloqués** sélectionnez l'élément qui vous intéresse.
- 5 Effectuez l'une des opérations suivantes :
 - Pour modifier une entrée, cliquez sur **Modifier** pour ouvrir la boîte de dialogue **Modifier une adresse électronique**, modifiez les détails, puis cliquez sur **OK**.
 - Pour supprimer une entrée, cliquez sur **Supprimer**.
Lorsque vous supprimez une entrée importée, Norton AntiSpam l'ajoute automatiquement à la liste **Exclusions de carnet d'adresses**.
- 6 Dans la fenêtre **Liste Bloqués**, cliquez sur **Appliquer**.
- 7 Cliquez sur **OK**.

Configuration de l'option Commentaires

Les messages électroniques du client de messagerie électronique risquent parfois d'être mal classifiés soit comme spams soit comme légitimes. L'option **Commentaires** vous permet d'envoyer le courrier électronique mal classé sous forme de rapport à Symantec pour analyse.



L'option **Commentaires** n'est disponible que si Microsoft Outlook est installé sur votre ordinateur.

Configuration de l'option Commentaires

- 1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.

- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Dans l'onglet **Intégration client**, à la ligne **Commentaires**, sélectionnez l'une des trois options suivantes :

Activé	Envoie automatiquement le message électronique mal classé à Symantec lorsque vous classez un message électronique comme du spam ou du courrier légitime.
Me demander	Vous avertit avant que Norton AntiSpam n'envoie automatiquement le message électronique mal classé à Symantec lorsque vous classez un message électronique comme du spam ou du courrier légitime.
Désactivé	N'envoie pas le message électronique mal classé à Symantec.

- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

A propos de la Requête Web

Avec l'utilisation accrue du courrier électronique, de nombreux utilisateurs reçoivent un grand nombre de messages électroniques commerciaux non sollicités ou indésirables connus comme spam. Le spam rend difficile l'identification des messages utiles et peut contenir des textes ou des images choquants. La Requête Web est une fonction de Norton AntiSpam que votre produit Norton utilise pour classer les messages électroniques plus efficacement.

Pour que le filtrage des spams soit efficace, chaque message électronique reçu doit être analysé par différents filtres. Avec seulement un ou deux niveaux de filtres de messages électroniques, un haut pourcentage de messages électroniques légitimes est classé comme spam ou un spam est mal classé comme légitime. Pour éviter ce classement incorrect, Norton AntiSpam utilise différents filtres. Chaque filtre de courrier électronique utilise une approche unique pour filtrer les spam des messages électroniques légitimes.

Les messages électroniques que vous recevez dans votre programme de courrier électronique sont analysés à l'aide de différents filtres locaux de Norton AntiSpam. Les filtres locaux utilisent la technique de la Liste blanche, de la Liste noire et la technologie de filtrage brevetée pour classer les messages électroniques comme courrier légitime ou spam. Si les filtres locaux classent un message électronique comme étant du spam, Norton AntiSpam modifie le sujet du message électronique. Norton AntiSpam envoie ensuite le courrier électronique à votre client de messagerie électronique. Si les filtres locaux ne parviennent pas à classer le courrier électronique comme spam, Norton AntiSpam récupère les informations du courrier électronique, telles que la signature et les hachages de l'URL. Norton AntiSpam envoie ensuite ces informations au filtre Requête Web afin d'effectuer une analyse approfondie.

Ce filtre analyse la signature et les hachages de l'URL du courrier électronique, puis envoie son rapport d'analyse à Norton AntiSpam. Si le message électronique est identifié comme un spam, alors Norton AntiSpam altère le sujet du courrier électronique, puis l'envoie à votre programme de messagerie électronique. Selon des règles de courrier électronique prédéfinies, le programme de messagerie électronique déplace ensuite le courrier électronique dans votre dossier Courrier indésirable ou dans le dossier Norton AntiSpam.



Symantec vous recommande de garder l'option **Requête Web** activée. La désactivation de l'option **Requête Web** augmente votre exposition aux spams contenant des URL de phishing ou de spam.

Désactivation ou activation de la Requête Web

Norton AntiSpam utilise des filtres locaux pour identifier des spam. Les messages électroniques que les filtres locaux n'identifient pas comme des spam sont ensuite analysés à nouveau par le filtre Requête Web. Le filtre Requête Web analyse la signature et les hachages de l'URL des messages électroniques afin de les classer comme du courrier légitime ou spam.

Si le message électronique est identifié comme un spam, alors Norton AntiSpam altère le sujet du message électronique. Norton AntiSpam envoie ensuite le message électronique à votre programme de messagerie électronique. Selon des règles de courrier électronique prédéfinies, le programme de messagerie électronique déplace ensuite le courrier électronique dans votre dossier Courrier indésirable ou dans le dossier Norton AntiSpam.



Symantec vous recommande de garder l'option **Requête Web** activée. La désactivation de l'option **Requête Web** augmente votre exposition aux spam contenant des URL de phishing ou de spam.

Désactivation du filtre Requête Web

- 1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Sous **Filtre**, à la ligne **Requête Web**, déplacez le curseur **Marche/Arrêt** vers la droite, sur la position **Arrêt**.
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Activation du filtre Requête Web

- 1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Dans l'onglet **Filtre**, à la ligne **Requête Web**, déplacez le curseur **Marche/Arrêt** vers la gauche, sur la position **Marche**.
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Ajout de ports POP3 et SMTP aux Ports protégés

Le produit Norton protège automatiquement les ports POP3 et SMTP par défaut pour préserver votre programme de messagerie électronique des virus et autres menaces de sécurité.

Le produit Norton prend en charge tous les comptes de messagerie électronique qui utilisent les protocoles de communication POP3 ou SMTP non SSL et ne prend pas en charge les ports de messagerie électronique. Le produit Norton analyse également tous les messages électroniques entrants et sortants.

Pour assurer la protection du courrier électronique, Symantec vous recommande de vérifier les numéros de ports POP3 et SMTP de votre programme de messagerie électronique. Si votre programme de messagerie électronique n'utilise pas les numéros de ports par défaut, vous devez ajouter les numéros de port manuellement dans la fenêtre **Ports protégés**. Cela vous aidera à préserver votre programme de messagerie électronique des virus et autres menaces de sécurité.

Si les numéros de port de votre programme de messagerie électronique ne sont pas ajoutés à la fenêtre **Ports protégés**, votre programme n'est pas protégé. Votre fournisseur d'accès Internet (FAI) vous fournit les

numéros de ports de votre programme de messagerie électronique.

Vous pouvez uniquement ajouter les numéros de port qui ne sont assignés à aucun autre protocole par l'IANA (Internet Assigned Numbers Authority). Les ports standard qui sont assignés à d'autres protocoles par l'IANA sont bloqués. Pour plus d'informations, consultez le site Web de l'IANA.

Ajout des ports POP3 et SMTP aux Ports protégés

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Dans l'onglet **Filtre**, dans la ligne **Ports protégés**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Ports protégés**, cliquez sur **Ajouter**.
- 5 Dans la fenêtre **Ajouter le port à protéger**, dans la liste déroulante **Type de port**, effectuez l'une des opérations suivantes :
 - Pour ajouter le port de courrier entrant, cliquez sur **POP3**.
 - Pour ajouter le port de courrier sortant, cliquez sur **SMTP**.
- 6 Dans le champ **Port**, tapez le numéro de port. Le numéro de port doit être compris entre 1 et 65535.
- 7 Cliquez sur **OK**.
- 8 Dans la fenêtre **Ports protégés**, cliquez sur **Appliquer**, puis sur **OK**.
- 9 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Suppression d'un port de messagerie électronique des Ports protégés

Si vous ne voulez pas que le produit Norton protège un port, vous pouvez supprimer le port de la fenêtre **Ports protégés**.



Le produit Norton protège automatiquement le port SMTP par défaut (25) et le port POP3 par défaut (110). Vous ne pouvez pas supprimer les ports par défaut.

Suppression d'un port de messagerie électronique des Ports protégés

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Dans l'onglet **Filtre**, dans la ligne **Ports protégés**, cliquez sur **Configurer**.
- 4 Dans la fenêtre **Ports protégés**, cliquez sur le port à supprimer, puis sur **Supprimer**.
- 5 Cliquez sur **Appliquer**, puis sur **OK**.
- 6 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Désactivation ou activation de la limitation de l'utilisation réseau

Vous pouvez définir des politiques pour restreindre l'utilisation d'Internet de Norton Security. Si vous ne souhaitez pas restreindre l'utilisation de bande passante de Norton Security, vous pouvez désactiver la **Limitation de l'utilisation réseau**.

Si vous estimez que Norton Security utilise trop de bande passante réseau, vous pouvez activer la **Limitation de l'utilisation réseau**. Vous pouvez ensuite définir des politiques pour restreindre l'utilisation d'Internet de Norton Security. La connexion de votre produit Norton à Internet dépend de la politique définie dans la fenêtre des paramètres **Limitation de l'utilisation réseau**. Par défaut, l'option **Limitation de l'utilisation réseau** est activée.

Désactivation de la limitation de l'utilisation réseau

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.

- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans la ligne **Limitation de l'utilisation réseau** de l'onglet **Paramètres généraux**, faites glisser le curseur **Ac. / Désac.** vers la droite pour l'amener sur la position **Désactivé**.
- 4 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**, puis sur **Fermer**.

Activation de la limitation de l'utilisation réseau

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans la ligne **Limitation de l'utilisation réseau** de l'onglet **Paramètres généraux**, faites glisser le curseur **Ac. / Désac.** vers la gauche pour l'amener sur la position **Activé**.
- 4 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**, puis sur **Fermer**.

Définir l'utilisation de bande passante de Norton Security

Si vous estimez que Norton Security utilise une trop grande quantité de votre bande passante réseau, vous pouvez restreindre l'utilisation d'Internet de Norton Security. Vous pouvez définir une politique pour chaque connexion réseau que Norton Security utilise pour se connecter à Internet.

La fenêtre de paramètres **Limitation de l'utilisation réseau** répertorie toutes les connexions réseau que l'ordinateur utilise pour se connecter à Internet. Vous pouvez afficher l'état des connexions réseau utilisées actuellement. La politique réseau que vous avez configurée définit la quantité de bande passante réseau qu'utilise Norton Security.

Définition de l'utilisation de bande passante de Norton Security

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Dans l'onglet **Paramètres généraux**, à la ligne **Limitation de l'utilisation réseau**, cliquez sur **Configurer**.
Si l'option **Configurer** est désactivée, déplacez le curseur **Ac. / Désac.** vers la gauche sur **Activé**.
- 4 Sous la colonne **Politique** de la fenêtre de paramètres **Limitation de l'utilisation réseau**, cliquez dans la liste déroulante en regard de la connexion réseau pour laquelle vous souhaitez configurer une politique.

5 Sélectionnez l'une des options suivantes :

■ **Automatique**

Permet à Norton Security de recevoir toutes les mises à jour de produits et de définition de virus selon la politique de limitation de l'utilisation de Windows 8. Par défaut, la politique **Automatique** propose une connexion illimitée à Internet par LAN ou Wi-Fi.



L'option **Automatique** n'est disponible que sous Windows 8.

■ **Aucune limite**

Permet à Norton Security d'utiliser toute la bande passante réseau nécessaire pour recevoir toutes les mises à jour de produits et des définitions de virus. Si vous n'utilisez pas Windows 8, la politique par défaut est **Aucune limite**.

■ **Economie**

Permet à Norton Security d'accéder à Internet uniquement pour recevoir les mises à jour de produits et les définitions de virus critiques.

Si vous disposez d'une connexion Internet limitée, vous pouvez sélectionner l'option **Economie** pour garantir la protection contre les menaces de sécurité critiques.

■ **Aucun trafic**

Bloque les connexions de Norton Security à Internet. Si vous choisissez cette politique, Norton Security ne peut pas recevoir les définitions de virus ni les mises à jour de programmes critiques, ce qui peut entraîner d'éventuels dangers et attaques virales.

6 Cliquez sur **Appliquer**, puis sur **OK**.

7 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Sécuriser vos données sensibles

7

Ce chapitre traite des sujets suivants :

- [A propos de Norton Safe Web](#)
- [A propos de l'antiphishing](#)
- [A propos d'Identity Safe](#)
- [A propos de la barre d'outils Norton](#)
- [Norton Identity Safe](#)

A propos de Norton Safe Web

Norton Safe Web vous aide à naviguer, faire des recherches et effectuer des achats sur Internet en toute sécurité. Avec Norton Safe Web, vous pouvez vérifier si un site Web est malveillant ou non avant de le visiter. Norton Safe Web analyse les sites Web que vous visitez et détecte s'ils contiennent des virus, spyware, malwares ou d'autres menaces de sécurité. En fonction de l'analyse, Norton Safe Web fournit des évaluations de sécurité pour tous les sites Web.

De plus, Norton Safe Web vous permet d'afficher l'évaluation de la communauté et les commentaires des utilisateurs sur les sites Web que vous visitez.



Norton Safe Web prend en charge les navigateurs Internet Explorer, Firefox ou Chrome.

Vous pouvez afficher l'état de sécurité des sites Web avec l'option **Rapport Safe Web complet** de la fenêtre contextuelle **Norton Safe Web**.

Pour chaque site Web dont vous voulez connaître l'état de sécurité, Norton Safe Web vous permet d'effectuer ce qui suit :

- Consulter l'évaluation Norton.
- Consulter l'évaluation de la communauté.
- Ajouter vos commentaires.
- Consulter les commentaires des utilisateurs.
- Consulter la liste des mots-clés associés au site Web.
- Consulter des informations sur les menaces et des informations générales concernant le site Web.

Si vous passez par un serveur proxy pour vous connecter à Internet, vous devez configurer les paramètres de proxy réseau du produit Norton.

Lorsque vous effectuez une recherche sur Internet via les moteurs de recherche Google, Yahoo ou Bing, Norton Safe Web affiche les icônes d'évaluation de site en regard des résultats de la recherche. Lorsque vous déplacez le pointeur de la souris sur une icône Norton, une fenêtre contextuelle s'affiche répertoriant les informations de sécurité du site et des achats. La fenêtre contextuelle affiche de brèves informations sur la sécurité du site. Norton Safe Web fournit également des rapports détaillés sur la sécurité des sites Web que vous visitez.

Vous pouvez cliquer sur l'icône en regard des résultats de la recherche ou sur l'option **Rapport Safe Web complet** de la fenêtre contextuelle **Norton Safe Web** pour afficher le rapport détaillé. Le rapport est affiché sur le site Web de Norton Safe.

Norton Safe Web fournit les états de sécurité de site Web suivants lorsque vous naviguez sur Internet :

SECURISE(E)	<p>L'icône Norton Secured apparaît en regard des résultats de recherche.</p> <p>Symantec a analysé cette page et établi que le site Web est approuvé par Symantec et peut être visité en toute sécurité.</p>
SUR(E)	<p>Une icône OK verte apparaît en regard des résultats de recherche.</p> <p>Lorsque vous consultez un site Web avec cet état, vous pouvez voir une icône d'état similaire dans la barre d'outils Norton. Norton Safe Web a analysé ce site Web et identifié qu'il pouvait être visité en toute sécurité.</p>
NON TESTE(E)	<p>Un point d'interrogation gris apparaît en regard des résultats de recherche.</p> <p>Lorsque vous consultez ce site Web, la barre d'outils Norton affiche une icône OK verte. Norton Safe Web n'a pas analysé ce site Web et ne possède pas assez d'informations à son sujet. Etant donné que Symantec n'a pas testé le site Web, il est recommandé de ne pas consulter ce site.</p>

RISQUE(E)	<p>Une croix rouge (x) apparaît en regard des résultats de recherche.</p> <p>Lorsque vous consultez un site Web avec cet état, vous pouvez voir une icône d'état similaire dans la barre d'outils Norton. Norton Safe Web a analysé ce site Web et a établi qu'il est risqué de le visiter. Ce site Web peut tenter d'installer des logiciels malveillants sur votre ordinateur.</p>
ATTENTION	<p>Une icône de point d'exclamation orange apparaît en regard des résultats de recherche.</p> <p>Lorsque vous consultez un site Web avec cet état, vous pouvez voir une icône d'état similaire dans la barre d'outils Norton. Norton Safe Web a analysé ce site Web et établi qu'il comportait des menaces classées comme Facteurs de nuisance. Ces facteurs de nuisance ne sont pas dangereux mais des applications indésirables peuvent être installées sur votre ordinateur sans votre autorisation.</p>

Outre les informations de sécurité du site, Norton Safe Web fournit des informations de sécurité d'achat en ligne dans la session **Informations de sécurité d'e-commerce**.

Lorsque vous visitez un site Web non sécurisé, Norton Safe Web bloque cette page Web. Si vous souhaitez néanmoins visiter le site Web, utilisez l'option **Continuer tout de même sur le site** qui s'affiche sur la page bloquée.

Vous pouvez bloquer les pages malveillantes à l'aide de l'option **Bloquer les pages malveillantes** de la section **Navigation sécurisée** de la fenêtre **Paramètres de protection de l'identité**.

Si vous désactivez cette option, Norton Safe Web ne bloque pas les sites non sécurisés. Cependant, la **barre d'outils Norton** affiche ces sites comme étant risqués même si l'option est désactivée.

En outre, Norton Safe Web protège votre ordinateur lorsque vous utilisez Facebook. Cet outil analyse chaque URL présente sur votre mur Facebook et affiche les icônes d'évaluation Norton pour les URL analysées. Vous pouvez également informer d'autres utilisateurs de Facebook de l'état de la sécurité d'un site Web donné.

Pour analyser votre mur Facebook à l'aide de Norton Safe Web, utilisez l'option **Analyse du mur Facebook** dans la fenêtre **Analyses**. L'option s'affiche lorsque vous cliquez sur l'option **Exécuter des analyses** dans la fenêtre **Tâches et analyses**.

Désactivation et activation de Norton Safe Web

Norton Safe Web protège votre ordinateur pendant que vous naviguez sur Internet avec les navigateurs Web Internet Explorer, Firefox ou Chrome. Il analyse les niveaux de sécurité des sites Web que vous visitez et vous indique si ces sites sont sûrs. Il fournit un environnement sécurisé sur le Web en affichant les icônes d'évaluation de site en regard de chaque résultat de recherche. Les icônes d'évaluation de site permettent de savoir si un site Web est malveillant avant même de vous y rendre.

Vous pouvez activer ou désactiver Norton Safe Web dans la section **Navigation sécurisée** de la fenêtre des paramètres **Protection de l'identité**.

Désactivation ou activation de Norton Safe Web

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Paramètres d'ID**.

- 2 Sous **Navigation sécurisée**, à la ligne **Norton Safe Web**, effectuez l'une des opérations suivantes :
 - Pour désactiver Norton Safe Web, déplacez le curseur **Activé / Désactivé** vers la droite sur **Désactivé**.
 - Pour activer Norton Safe Web, déplacez le curseur **Activé / Désactivé** vers la gauche sur **Activé**.
- 3 Cliquez sur **Appliquer**, puis sur **Fermer**.

Recherche sur le Web à l'aide de Norton Safe Search

Norton Safe Search améliore vos recherches sur le Web. Lorsque vous effectuez une recherche sur l'Internet, Norton Safe Search utilise Ask.com pour générer les résultats de la recherche. Norton Safe Search fournit un état de sécurité du site et une évaluation Norton pour chaque résultat généré.

Lors de son installation, Norton Security ajoute le champ **Norton Safe Search** aux navigateurs. Les navigateurs pris en charge sont les suivants : Internet Explorer, Firefox et Chrome.

Norton Safe Search fournit la fonction intelligente de recherche intuitive qui affiche des suggestions de recherche lorsque vous tapez quelques lettres de l'expression à rechercher.



La fonction Norton Safe Search est disponible uniquement dans certains pays, dont l'Australie, la Belgique, le Brésil, le Canada, le Danemark, la Finlande, la France, l'Allemagne, l'Italie, le Japon, les Pays-Bas, la Norvège, l'Espagne, la Suède, la Suisse, les Etats-Unis et le Royaume-Uni. La fonction Privacy Safeguard est disponible uniquement aux Etats-Unis, au Royaume Uni et au Canada.

Vous pouvez utiliser Norton Safe Search même si vous désactivez les fonctions Identity Safe.



Norton Safe Search est uniquement pris en charge par les navigateurs Internet Explorer, Firefox ou Chrome.

Recherche sur le Web à l'aide de Norton Safe Search

- 1 Démarrez votre navigateur.
- 2 Dans la **barre d'outils Norton**, dans le champ **Norton Safe Search**, tapez la chaîne à rechercher.
- 3 Effectuez l'une des opérations suivantes :
 - Cliquez sur **Safe Search**.
 - Dans la fenêtre contextuelle qui apparaît, sélectionnez une suggestion de recherche qui correspond à votre chaîne de recherche.

Désactivation ou activation de la fonction Diagnostic des fraudes

La fonction Diagnostic des fraudes vous empêche de divulguer des informations sensibles, telles que vos numéros de sécurité sociale ou de carte bancaire, à des sites Web frauduleux. Elle vous permet de détecter les sites Web suspects ou vulnérables à l'aide de la détection des menaces par réputation. Elle s'intéresse principalement aux sites Web vous demandant d'indiquer vos informations personnelles.

Pour activer/désactiver la fonction Diagnostic Norton des fraudes, utilisez l'option **Diagnostic des fraudes** de la fenêtre **Paramètres de protection de l'identité**.

La fenêtre contextuelle **Norton Safe Web** vous aide à déterminer si le site Web visité est sûr ou non.

Désactivation ou activation de la fonction Diagnostic des fraudes

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis cliquez sur **Paramètres d'ID**.

- 2 Sous **Navigation sécurisée**, dans la ligne **Diagnostic des fraudes**, effectuez l'une des actions suivantes :
 - Pour désactiver la fonction Diagnostic des fraudes, déplacez le curseur **Ac./Désac** vers la droite, sur la position **Désactivé**.
 - Pour activer la fonction Diagnostic des fraudes, déplacez le curseur **Ac./Désac** vers la gauche, sur la position **Activé**.
- 3 Cliquez sur **Appliquer**, puis sur **Fermer**.

A propos de l'antiphishing

La fonction Antiphishing vous protège contre les sites Web non sécurisés. Lorsque la fonction Antiphishing est activée, le composant Antiphishing analyse le niveau de sécurité des sites Web que vous visitez. Les résultats sont ensuite affichés dans la fenêtre contextuelle **Norton Safe Web**. La fonction Antiphishing bloque aussi la navigation vers des sites Web confirmés comme frauduleux ou suspects.

La fonction Antiphishing vous fournit les informations suivantes sur les sites Web que vous visitez :

- Si la saisie d'informations confidentielles est sécurisée sur ce site Web
- Si le site Web est frauduleux
- Si le site Web est suspect
- Si le site Web est classé comme produisant des résultats gênants

La fenêtre contextuelle **Norton Safe Web** disponible dans les navigateurs Internet Explorer, Firefox ou Chrome vous permet d'afficher davantage de détails sur l'état de sécurité des sites Web que vous visitez.

La fenêtre contextuelle **Norton Safe Web** inclut également des informations sur les sites Web Norton Secured. Les pirates informatiques créent souvent des sites frauduleux qui sont des miroirs de sites Web

d'entreprise légitimes. La fonction Antiphishing identifie les sites Web frauduleux.

Symantec analyse les pages de ces sites et vérifie qu'elles appartiennent à l'entreprise qu'elles sont censées représenter. Ainsi, vous savez que les informations que vous fournissez sont transmises à l'entreprise avec laquelle vous entrez en relation.

Même si vous désactivez l'option **Antiphishing**, votre ordinateur est protégé contre les menaces Internet via la fonction Norton Safe Web. Cependant, vous ne pouvez pas utiliser l'option **Signaler ce site** pour envoyer l'évaluation du site Web à Symantec.

La fenêtre contextuelle **Norton Safe Web** affiche les messages suivants :

Icône	Message
SECURISE(E)	L'icône Norton Secured apparaît en regard des résultats de recherche. Symantec a analysé cette page et établi que le site Web est approuvé par Symantec et peut être visité en toute sécurité.
SUR(E)	Une icône OK verte apparaît en regard des résultats de recherche. Lorsque vous consultez un site Web avec cet état, vous pouvez voir une icône d'état similaire dans la barre d'outils Norton. Norton Safe Web a analysé ce site et a identifié qu'il pouvait être visité en toute sécurité.

Icône	Message
NON TESTE(E)	<p>Un point d'interrogation gris apparaît en regard des résultats de recherche.</p> <p>Quand vous visitez ce site Web, la barre d'outils Norton affiche une icône OK verte. Norton Safe Web n'a pas analysé ce site et ne possède pas assez d'informations à son sujet. Etant donné que Symantec n'a pas testé le site, il vous est recommandé de ne pas consulter ce site.</p>
RISQUE(E)	<p>Une croix rouge (x) apparaît en regard des résultats de recherche.</p> <p>Lorsque vous consultez un site Web avec cet état, vous pouvez voir une icône d'état similaire dans la barre d'outils Norton. Norton Safe Web a analysé cette page et établi qu'il est risqué de la visiter. Ce site Web peut tenter d'installer des logiciels malveillants sur votre ordinateur.</p>

Icône	Message
ATTENTION	<p data-bbox="637 263 942 375">Une icône de point d'exclamation orange apparaît en regard des résultats de recherche.</p> <p data-bbox="637 399 942 874">Lorsque vous consultez un site Web avec cet état, vous pouvez voir une icône d'état similaire dans la barre d'outils Norton. Norton Safe Web a analysé ce site et a établi que ce site comportait des menaces classées comme facteurs de nuisance. Ces facteurs de nuisance ne sont pas dangereux mais des applications indésirables peuvent être installées sur votre ordinateur sans votre autorisation.</p>

Désactivation ou activation de l'antiphishing

La fonction Antiphishing vous protège contre les sites Web non sécurisés. Elle analyse le niveau de sécurité de tous les sites Web que vous visitez et affiche les résultats dans la fenêtre contextuelle **Norton Safe Web**. La fonction Antiphishing bloque aussi les sites Web confirmés comme étant frauduleux.

La fenêtre contextuelle **Norton Safe Web** vous aide à comprendre si le site Web visité est sûr ou non.

Vous pouvez activer ou désactiver l'antiphishing dans la section **Navigation sécurisée** de la fenêtre de paramètres de **Protection de l'identité**.

Désactivation ou activation de l'antiphishing

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Paramètres d'ID**.
- 2 Sous **Navigation sécurisée**, à la ligne **Antiphishing**, effectuez l'une des opérations suivantes :
 - Pour désactiver l'antiphishing, déplacez le curseur **Ac. / Désac.** vers la droite sur la position **Désactivé**.
 - Pour activer l'antiphishing, déplacez le curseur **Ac. / Désac.** vers la gauche sur la position **Activé**.
- 3 Cliquez sur **Appliquer**.
- 4 Si vous y êtes invité, sélectionnez le laps de temps pendant lequel la fonctionnalité d'antiphishing sera désactivée, puis cliquez sur **OK**.

Signalement de l'évaluation incorrecte d'un site Web

Il arrive très exceptionnellement que la fonction Antiphishing signale un site Web de manière erronée. Par exemple, vous visitez un site sur lequel vous faites régulièrement des achats et la fonction Antiphishing indique que la page est frauduleuse. Inversement, vous pouvez visiter un site Web que vous soupçonnez de phishing, mais la fonction Antiphishing signale qu'aucune fraude n'a été détectée. Dans ce cas, vous pouvez signaler la page à Symantec pour évaluation.

Signalement de l'évaluation incorrecte d'un site Web

- 1 Ouvrez votre navigateur et accédez au site Web dont vous pensez que l'évaluation est incorrecte.
- 2 Dans la barre d'outils Norton, cliquez sur l'**indicateur Norton Safe Web**.
- 3 Dans la fenêtre qui s'affiche, cliquez sur **Signaler ce site**.
- 4 Dans la boîte de dialogue de confirmation, cliquez sur **Transmettre**.

A propos d'Identity Safe

Identity Safe permet de gérer les identités et renforce la sécurité au cours des transactions en ligne.

Les fonctions suivantes dans Identity Safe vous donnent la possibilité de protéger les informations sensibles que vous stockez :

Identifiants	Enregistre les informations de connexion, telles que vos informations d'authentification pour votre compte bancaire en ligne, vos identifiant et mot de passe de messagerie électronique.
Adresses	Stocke vos informations personnelles, telles que votre nom, votre date de naissance, vos adresses postale et électronique et vos numéros de téléphone.
Portefeuille	Enregistre vos informations financières, telles que vos informations de carte, de compte bancaire et de paiements.
Notes	Enregistre les informations saisies pour référence future.

Identity Safe fait office de référentiel d'informations sensibles et fournit également les fonctions suivantes :

- Protection contre l'usurpation d'identité lors des transactions en ligne.
- Il vous permet de gérer facilement plusieurs informations concernant vos cartes de crédit.

- Il vous permet de récupérer et d'utiliser vos données Identity Safe facilement lors de vos déplacements. En enregistrant vos données à l'aide d'un centre de sauvegarde dans le cloud, vous pouvez accéder à vos données sensibles Identity Safe depuis un ordinateur sur lequel Norton Security est installé ou via le site Web Identity Safe.

Norton Security ajoute la **barre d'outils Norton** aux navigateurs Internet Explorer, Firefox ou Chrome. La **barre d'outils Norton** contient les éléments suivants :

- **Norton Safe Search**
- Indicateur **Safe Web**
- Menu **LE CENTRE EST OUVERT/Centre de sauvegarde fermé**
- **PARTAGER SUR**
- Paramètres de la barre d'outils Norton

Lorsqu'Identity Safe contient des identifiants, le menu **LE CENTRE EST OUVERT** affiche la liste complète des identifiants stockés dans Identity Safe. Plutôt que de devoir accéder à un site Web et saisir vos informations de connexion, vous pouvez cliquer directement sur un identifiant dans la liste enregistrée pour accéder au site Web.

Si vous désactivez Identity Safe, vous ne pouvez pas accéder aux fonctionnalités d'identifiants et d'Identity Safe à partir de la barre d'outils Norton.

Vous pouvez accéder à Identity Safe même lorsque le produit a expiré. Cependant, le produit risque de ne pas détecter les dernières attaques, étant donné que la définition de virus ne sera plus mise à jour après l'expiration du produit. Ainsi, il est déconseillé d'utiliser Internet après l'expiration de Norton Security, car vous vous exposez à des risques de vol et d'usurpation d'identité.

A propos de la configuration d'un compte Norton Identity Safe

Identity Safe vous aide à gérer vos informations sensibles et offre une sécurité supplémentaire lorsque vous réalisez des transactions en ligne. Identity Safe fournit un stockage sûr de vos informations personnelles telles que votre adresse, vos informations de connexion, vos mots de passe et vos détails de carte de crédit.

Identity Safe vous permet de stocker les informations suivantes :

- Les informations de connexion telles que les identifiants et mots de passe de vos comptes de messagerie.
- Les informations personnelles telles que vos adresse, date de naissance, numéro de passeport et numéro de sécurité sociale.
- Les détails de carte de crédit, notamment le numéro et la date d'expiration de la carte.

Vous pouvez stocker vos informations sensibles uniquement après avoir configuré Identity Safe et créé votre centre de sauvegarde.

Identity Safe vous permet de créer un centre de sauvegarde dans le cloud et d'enregistrer vos données Identity Safe. Vous ne pouvez créer qu'un seul centre de sauvegarde dans le cloud par compte Norton. Vous ne pouvez pas créer de nouveau centre de sauvegarde local. En revanche, vous pouvez déplacer les données de votre centre de sauvegarde local vers un centre de sauvegarde dans le cloud lors de la mise à niveau vers Norton Security. Lorsque vous déplacez vos données Identity Safe depuis un centre de sauvegarde local vers un centre de sauvegarde dans le cloud, les données de votre centre de sauvegarde local sont supprimées de manière définitive.

Vous pouvez accéder à votre centre de sauvegarde Identity Safe dans le cloud depuis tout ordinateur connecté à Internet.

Les données Identity Safe sont stockées en ligne avec votre compte Norton. Vous ne pouvez créer qu'un seul centre de sauvegarde dans le cloud par compte Norton.

Désactivation et activation d'Identity Safe

Identity Safe vous aide à gérer votre identité et offre une sécurité supplémentaire pendant que vous réalisez des transactions en ligne. Vous pouvez utiliser les différentes fonctions d'Identity Safe pour gérer vos données personnelles, notamment les adresses, la date de naissance et les informations relatives aux cartes de crédit.

Vous pouvez également activer ou désactiver la fonction Identity Safe dans **Commandes rapides** de la fenêtre **Paramètres** ou dans la fenêtre **Paramètres** de la fonction **Protection de l'identité**.



Après avoir activé Identity Safe, vous devez vous connecter à Identity Safe pour accéder aux diverses fonctions.

Activation ou désactivation d'Identity Safe dans les commandes rapides

- 1 Dans la fenêtre principale Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Commandes rapides**, effectuez l'une des opérations suivantes :
 - Pour désactiver Identity Safe, décochez **Identity Safe**.
 - Pour activer Identity Safe, cochez **Identity Safe**.

Activation ou désactivation d'Identity Safe dans la fenêtre des paramètres

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Paramètres d'ID**.

- 2 Dans la fenêtre des paramètres **Protection de l'identité**, à la ligne **Identity Safe**, effectuez l'une des opérations suivantes :
 - Pour désactiver Identity Safe, déplacez le curseur **Ac./Désac.** vers la droite sur la position **Désactivé**.
 - Pour activer Identity Safe, déplacez le curseur **Ac./Désac.** vers la gauche sur la position **Activé**.
- 3 Cliquez sur **Appliquer**, puis sur **Fermer**.

A propos des centres de sauvegarde Identity Safe

Identity Safe vous permet de créer un centre de sauvegarde dans le cloud et d'enregistrer vos données sensibles. Vous ne pouvez créer qu'un seul centre de sauvegarde dans le cloud par compte Norton. Vous ne pouvez pas créer de nouveau centre de sauvegarde local. En revanche, vous pouvez déplacer les données de votre centre de sauvegarde local vers un centre de sauvegarde dans le cloud lors de la mise à niveau vers Norton Security. Lorsque vous déplacez vos données Identity Safe depuis un centre de sauvegarde local vers un centre de sauvegarde dans le cloud, vous n'avez plus accès aux données de votre centre de sauvegarde local. Un centre de sauvegarde dans le cloud permet de récupérer et d'utiliser vos données Identity Safe facilement lors de vos déplacements.

Lors de la configuration d'un centre de sauvegarde dans le cloud, Identity Safe importe automatiquement les identifiants que vous avez enregistrés dans Internet Explorer. Les identifiants importés apparaissent dans le menu **LE CENTRE EST OUVERT** de la barre d'outils Norton et de la fenêtre **Identifiants**.



La version 10 d'Internet Explorer n'autorise pas l'importation des informations de connexion par Identity Safe.

Vous pouvez accéder à votre centre de sauvegarde Identity Safe dans le cloud depuis tout ordinateur connecté à Internet.

création d'un centre de sauvegarde dans le cloud

Identity Safe vous permet de créer un centre de sauvegarde dans le cloud et d'enregistrer vos données Identity Safe. Vous ne pouvez créer qu'un seul centre de sauvegarde dans le cloud par compte Norton. Vous ne pouvez pas créer de nouveau centre de sauvegarde local. En revanche, vous pouvez déplacer les données de votre centre de sauvegarde local vers un centre de sauvegarde dans le cloud lors de la mise à niveau vers Norton Security. Lorsque vous déplacez vos données Identity Safe depuis un centre de sauvegarde local vers un centre de sauvegarde dans le cloud, vous n'avez plus accès aux données de votre centre de sauvegarde local. Un centre de sauvegarde dans le cloud permet de récupérer et d'utiliser vos données Identity Safe facilement lors de vos déplacements.

Vous pouvez accéder à votre centre de sauvegarde Identity Safe dans le cloud depuis tout ordinateur connecté à Internet.

Création d'un centre de sauvegarde dans le cloud

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Dans la fenêtre **Mise en route**, cliquez sur **Connexion**.
Si ce n'est pas le cas, cliquez sur le lien **Inscrivez-vous maintenant !** pour créer un compte Norton.
- 3 Dans la fenêtre **Nouveau centre de sauvegarde** : **Mot de passe du centre**, dans la zone de texte **Mot de passe du centre**, saisissez votre mot de passe, puis cliquez sur **Suivant**.
- 4 Dans la fenêtre **Nouveau centre de sauvegarde** : **Confirmer le mot de passe**, saisissez à nouveau le mot de passe pour le confirmer et cliquez sur **Suivant**.

- 5 Dans la fenêtre **Nouveau centre de sauvegarde** : **indice pour le mot de passe**, saisissez un indice pour le mot de passe et cliquez sur **Suivant**.
Si vous disposez déjà d'une sauvegarde pour vos données Identity Safe, cliquez sur **Importer** et sélectionnez le fichier sauvegardé pour fusionner le nouveau compte.
- 6 Cliquez sur **Terminer**.

Connexion au centre de sauvegarde dans le cloud

Identity Safe vous permet de créer un centre de sauvegarde dans le cloud pour enregistrer vos données Identity Safe. Vous devez vous connecter à votre compte Norton pour créer un centre de sauvegarde dans le cloud. Les données Identity Safe sont stockées en ligne avec votre compte Norton.

Vous pouvez accéder à votre centre de sauvegarde Identity Safe dans le cloud depuis tout ordinateur connecté à Internet.



Vous pouvez créer un seul centre de sauvegarde dans le cloud par compte Norton. Si vous possédez déjà un compte Norton, vous pouvez vous connecter avec vos informations d'authentification ou créer un nouveau compte.

A l'aide de votre produit Norton, vous pouvez accéder à plusieurs centres de sauvegarde créés à l'aide de différents comptes Norton. Vous pouvez utiliser le **Menu Compte** situé en bas de la fenêtre **Norton Identity Safe** pour accéder aux centres de sauvegarde associés à plusieurs comptes Norton.

En cas d'oubli du mot de passe de votre centre de sauvegarde dans le cloud, cliquez sur le lien **Afficher l'indice pour le mot de passe** pour afficher l'indice que vous avez fourni pour vous souvenir de votre mot de passe. Si cela ne vous permet pas de vous souvenir de votre mot de passe, pour des raisons de sécurité, Norton vous fait supprimer le centre de sauvegarde actuel afin d'en créer un nouveau.

Si vous saisissez un mot de passe incorrect trois fois, le lien **Vous devez supprimer votre centre de sauvegarde ? cliquez ici** apparaît. Vous pouvez utiliser ce lien pour supprimer le centre de sauvegarde. Pour supprimer votre centre de sauvegarde, vous devez fournir les informations d'authentification de votre compte Norton.

Connexion au centre de sauvegarde dans le cloud depuis la fenêtre Paramètres

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis cliquez sur **Paramètres d'ID**.
- 2 A la ligne **Identity Safe**, cliquez sur **Configurer**.
- 3 Dans la fenêtre **Mise en route**, cliquez sur **Connexion**.
- 4 Fournissez vos informations d'authentification de compte Norton et cliquez sur **Connexion**.
- 5 Dans la fenêtre **Centre de sauvegarde fermé**, saisissez le mot de passe de votre centre de sauvegarde dans le cloud.
- 6 Cliquez sur **Ouvrir**.

Connexion au centre de sauvegarde dans le cloud depuis la barre d'outils Norton

- 1 Démarrez votre navigateur.
- 2 Dans la barre d'outils Norton, cliquez sur **LE CENTRE EST FERME**.
- 3 Dans la fenêtre **Mise en route**, cliquez sur **Connexion**.
- 4 Fournissez vos informations de compte Norton et cliquez sur **Connexion**.
- 5 Dans la fenêtre **Centre de sauvegarde fermé**, saisissez le mot de passe de votre centre de sauvegarde dans le cloud.
- 6 Cliquez sur **Ouvrir**.

Connexion à un autre compte Norton

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis cliquez sur **Identity Safe**.

- 2 Dans la fenêtre **Centre de sauvegarde fermé**, cliquez sur l'option **Menu Compte** située au bas de la fenêtre.
- 3 Sélectionnez **Se connecter avec un autre compte**.
- 4 Dans la fenêtre **Mise en route**, cliquez sur **Connexion**.
- 5 Fournissez les informations d'authentification d'un compte Norton différent et cliquez sur **Connexion**.
- 6 Dans la fenêtre **Centre de sauvegarde fermé**, saisissez le mot de passe de votre centre de sauvegarde dans le cloud.
- 7 Cliquez sur **Ouvrir**.

Synchronisation d'un centre de sauvegarde local avec un centre de sauvegarde dans le cloud

Vous pouvez synchroniser les données Identity Safe de votre centre de sauvegarde local vers le centre de sauvegarde dans le cloud. Lorsque vous déplacez vos données depuis un centre de sauvegarde local vers un centre de sauvegarde dans le cloud, les données de votre centre de sauvegarde local sont supprimées de manière définitive.

Les versions les plus récentes de Norton Security ne prennent en charge que la fonction de centre de sauvegarde dans le cloud. Si vous avez créé votre centre de sauvegarde à l'aide d'une version antérieure, vous devez le déplacer vers le cloud. Vous ne pouvez plus utiliser votre centre de sauvegarde local. Vous pouvez utiliser l'option **Fusionner** de la fenêtre **Vous passez au cloud ?** pour déplacer votre centre de sauvegarde local vers le cloud.



La fenêtre **Vous passez au cloud ?** est activée uniquement lorsqu'un centre de sauvegarde local a été créé.

Voici les avantages liés au déplacement de vos données Identity Safe en ligne :

- Vous permet d'accéder à vos données Identity Safe à partir de n'importe quel ordinateur.
-  Votre ordinateur doit disposer de Norton Security et être connecté à Internet.
- Vous permet d'accéder à vos données Identity Safe sur un appareil via le site Web Norton Identity Safe.
 - Fournit un moyen pratique pour synchroniser automatiquement vos données Identity Safe sur différents ordinateurs au moyen de votre compte Norton.

-  Vous devez vous connecter à votre compte Norton pour déplacer les données Identity Safe du centre de sauvegarde local vers le centre de sauvegarde dans le cloud.

Synchronisation d'un centre de sauvegarde local avec un centre de sauvegarde dans le cloud

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Dans la fenêtre **Norton Identity Safe**, sous **Se connecter ou créer un compte**, saisissez l'adresse électronique de votre compte Norton, puis cliquez sur **Suivant**.
- 3 Dans la boîte de dialogue **Vous passez au cloud ?**, cliquez sur **Oui, convertir** pour configurer votre centre de sauvegarde dans le cloud.
Vous pouvez également choisir de sélectionner **Non, rester local** dans un premier temps et utiliser l'option **Convertir en centre de sauvegarde dans le cloud** dans l'onglet **Général** de la fenêtre des paramètres d'Identity Safe pour déplacer les données de votre centre de sauvegarde local vers un centre de sauvegarde dans le cloud.
- 4 Dans la fenêtre **Centre de sauvegarde dans le cloud : Compte Norton**, saisissez vos détails et cliquez sur **Accepter et se connecter**.
- 5 Lorsque le message de configuration terminée apparaît, cliquez sur **Terminer**.

- 6 Dans la boîte de dialogue **Centre de sauvegarde dans le cloud configuré**, effectuez l'une des opérations suivantes :
 - Cliquez sur **Fusionner** pour synchroniser votre centre de sauvegarde local avec le centre de sauvegarde dans le cloud et le supprimer.
 - Cliquez sur **Conserver les deux** pour conserver votre centre de sauvegarde local en plus de votre centre de sauvegarde dans le cloud.
- 7 Si vous disposez de mots de passe différents pour le centre de sauvegarde local et le centre de sauvegarde dans le cloud, Norton Security affiche un message de confirmation. Sélectionnez l'une des options suivantes :
 - Cliquez sur **Conserver le mot de passe existant** pour conserver le mot de passe enregistré sur le centre de sauvegarde dans le cloud.
 - Cliquez sur **Conserver le mot de passe importé** pour remplacer le mot de passe enregistré sur le centre de sauvegarde dans le cloud par le mot de passe enregistré dans le centre de sauvegarde local.
- 8 Dans la boîte de dialogue de confirmation, cliquez sur **OK**.

Réinitialisation d'Identity Safe

Vous pouvez devoir réinitialiser Identity Safe dans les cas suivants :

- Votre ordinateur connaît une défaillance.
- Vous avez oublié votre mot de passe Identity Safe.



Si vous oubliez votre mot de passe Identity Safe, vous ne pouvez pas le récupérer. Vous pouvez seulement réinitialiser Identity Safe en supprimant votre centre de sauvegarde Identity Safe et réenregistrer toutes vos données à nouveau.

Si vous saisissez un mot de passe incorrect trois fois, Identity Safe vous offre la possibilité de supprimer votre

centre de sauvegarde. Si vous supprimez le centre de sauvegarde, vous perdez toutes les données Identity Safe que vous avez enregistrées, telles que vos informations de connexion, vos adresses, cartes et notes.

Suppression de votre centre de sauvegarde et réinitialisation d'Identity Safe

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis cliquez sur **Identity Safe**.
- 2 Dans la boîte de dialogue **Centre de sauvegarde fermé**, tapez votre mot de passe Identity Safe. Si vous entrez un mot de passe incorrect trois fois, l'option **Vous devez supprimer votre centre de sauvegarde ? cliquez ici** s'affiche.
- 3 Cliquez sur **cliquez ici** en regard de **Vous devez supprimer votre centre de sauvegarde ?** option.
- 4 Dans la fenêtre **Supprimer le centre de sauvegarde**, cliquez sur **Oui, supprimer mon centre de sauvegarde**.
- 5 Dans la boîte de dialogue Avertissement, cliquez sur **Oui**.
- 6 Saisissez le mot de passe de votre compte Norton et cliquez sur **Connexion**.
- 7 Dans la boîte de dialogue de confirmation, cliquez sur **OK**.
- 8 Dans la fenêtre **Nouveau centre de sauvegarde : Mot de passe du centre**, dans la zone de texte **Mot de passe du centre**, saisissez votre mot de passe, puis cliquez sur **Suivant**.
- 9 Dans la fenêtre **Nouveau centre de sauvegarde : Confirmer le mot de passe**, saisissez à nouveau le mot de passe pour le confirmer et cliquez sur **Suivant**.
- 10 Dans la fenêtre **Nouveau centre de sauvegarde : indice pour le mot de passe**, saisissez un indice pour le mot de passe et cliquez sur **Suivant**.
- 11 Cliquez sur **Terminer**.

Accès à Identity Safe

Vous pouvez accéder aux paramètres d'Identity Safe depuis les zones suivantes :

- Section **Identité** de la fenêtre principale du produit
- Barre d'outils Norton

Vous pouvez accéder à l'ensemble des données d'Identity Safe même lorsque le produit a expiré. Vous pouvez accéder aux fonctions suivantes ou les afficher lorsque le produit a expiré :

Identifiants	Vous pouvez afficher les informations de connexion enregistrées, telles que vos informations d'authentification pour votre compte bancaire en ligne, vos identifiant et mot de passe d'utilisateur de messagerie électronique.
Adresses	Vous pouvez afficher vos informations personnelles enregistrées, telles que votre nom, votre date de naissance, vos adresses postale et électronique et vos numéros de téléphone.
Portefeuille	Vous pouvez afficher vos informations financières enregistrées, telles que vos informations de carte de crédit, de compte bancaire et de paiements.
Notes	Vous pouvez afficher les informations que vous saisissez pour référence future.



Vous devez vous connecter à Identity Safe pour accéder à ses diverses fonctions. Les fonctions d'Identity Safe sont prises en charge uniquement par les navigateurs Internet Explorer, Firefox et Chrome.

Ouverture et fermeture de session Identity Safe

Vous pouvez vous connecter à Identity Safe et vous en déconnecter depuis les emplacements suivants :

- La section **Identité** de la fenêtre principale de Norton Security
- La section **Identity Safe** de la fenêtre **Paramètres** de la Protection de l'identité
- L'option **Menu Compte** située au bas de la fenêtre **Norton Identity Safe**
- La barre d'outils Norton

Pour sécuriser vos données Identity Safe, fermez votre session Identity Safe avant de quitter votre ordinateur.

Pour afficher ou modifier vos données confidentielles, vous devez vous connecter à Identity Safe.

Connexion à Identity Safe

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Dans la fenêtre **Centre de sauvegarde fermé**, saisissez le mot de passe de votre centre de sauvegarde au niveau de la zone de texte **Entrez votre mot de passe**.
- 3 Cliquez sur **Ouvrir**.

Déconnexion d'Identity Safe :

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Dans la fenêtre **Norton Identity Safe**, cliquez sur le curseur situé au bas de la fenêtre à gauche.

Ouverture d'une session d'Identity Safe depuis la barre d'outils Norton

- 1 Démarrez votre navigateur.

- 2 Dans la **barre d'outils Norton**, cliquez sur **LE CENTRE EST FERME**.
- 3 Dans la fenêtre **Centre de sauvegarde fermé**, saisissez le mot de passe de votre centre de sauvegarde.
- 4 Cliquez sur **Ouvrir**.

Fermeture de la session d'Identity Safe depuis la barre d'outils Norton

- 1 Démarrez votre navigateur.
- 2 Dans la barre d'outils Norton, cliquez sur le menu **LE CENTRE EST OUVERT** situé en bas, puis sur **Fermer le centre de sauvegarde**.

Configuration des paramètres d'Identity Safe

Vous pouvez utiliser les fonctions Identity Safe pour gérer vos informations personnelles sensibles. Vous pouvez configurer Identity Safe de manière à pouvoir y accéder depuis divers appareils et améliorer ses capacités et son efficacité.

Configuration des paramètres Identity Safe

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.

- 2 Dans la fenêtre **Norton Identity Safe**, cliquez sur l'icône **Paramètres** située au bas de la fenêtre. Vos options sont :

Général	<p>Permet de configurer les paramètres de la barre d'outils Norton.</p> <p>Options de la barre d'outils : vous pouvez activer ou désactiver l'option Norton Safe Web.</p> <p>L'option est activée par défaut.</p> <p>Extensions de navigateur : vous pouvez afficher l'état de la barre d'outils Norton installée sur les navigateurs suivants :</p> <ul style="list-style-type: none">■ Internet Explorer■ Google Chrome■ Mozilla Firefox <p>L'état indique si la barre d'outils Norton est activée dans le navigateur ou si vous devez l'activer manuellement. Vous pouvez utiliser le lien des paramètres de navigateur pour activer la barre d'outils.</p> <p>🔗 Vous pouvez configurer les paramètres Général sans même vous connecter au centre de sauvegarde.</p>
----------------	--

Importer/Exporter

Permet d'importer et d'exporter les données Identity Safe stockées dans le centre de sauvegarde.

Importer le centre de sauvegarde :

Vous pouvez importer des données à partir du fichier sauvegardé ou exporté.

Lorsque vous importez des données Identity Safe, vous disposez des options suivantes :

- Fusionner les données importées avec les données existantes
- Remplacer les données existantes par les données importées

Exporter le centre de sauvegarde :

Vous pouvez sauvegarder les données d'Identity Safe au format .DAT ou .CSV.

Vous pouvez sélectionner l'une des options suivantes :

- Format de sauvegarde Identity Safe - Fichier DAT
- Texte simple - Fichier CSV (identifiants et notes uniquement)

🔒 Il est conseillé de sauvegarder régulièrement toutes vos données Identity Safe. Lors de l'exportation des données, fournissez un mot de passe afin d'éviter toute utilisation frauduleuse de vos données Identity Safe.

Sauvegarde automatique :

Votre centre de sauvegarde est automatiquement sauvegardé et stocké localement sur votre appareil. Pour désactiver la sauvegarde automatique, désélectionnez la case **Activez les sauvegardes automatiques**. Cette option est activée par défaut.

Les fichiers sauvegardés dans le centre de sauvegarde sont stockés dans le dossier du système suivant : **Users\<Nom d'utilisateur>\Mes documents\Norton Identity Safe Backups\<Nom de compte Norton>**. Pour accéder aux fichiers enregistrés dans le centre de sauvegarde, cliquez sur le lien ici.

Sécurité

Permet de modifier le mot de passe Identity Safe et d'en définir le niveau de sécurité. Vos options sont :

Accès au centre de sauvegarde : Vous pouvez configurer les paramètres de sécurité suivants pour l'ouverture et la fermeture de votre centre de sauvegarde. Vos options sont :

- **Demander le mot de passe au début de chaque session** : vous invite à entrer le mot de passe de votre centre de sauvegarde lors de chaque accès à Identity Safe. Symantec conseille d'utiliser cette option pour renforcer la sécurité de vos informations d'identification.
- **Demander le mot de passe avant de fournir un identifiant ou de remplir un formulaire** : Vous demande de saisir votre mot de passe Identity Safe pour chaque formulaire en ligne avant de renseigner automatiquement des identifiants. Vous pouvez spécifier que chaque identifiant nécessite la saisie du mot de passe Identity Safe avant le remplissage automatique.
- **Fermer le centre de sauvegarde après *minutes* minutes d'inactivité** : vous déconnecte automatiquement d'Identity Safe lorsqu'il reste inutilisé pendant une période donnée. Vous pouvez définir le délai d'inactivité sur 15, 30 ou 45 minutes. Cette option est utile si vous vous trouvez fréquemment dans une zone où d'autres personnes ont accès à votre ordinateur.
- **Fermer le centre de sauvegarde en mode veille** : vous déconnecte automatiquement d'Identity Safe lorsque votre ordinateur est en veille.

Mot de passe du centre : permet de modifier le mot de passe du centre de sauvegarde. Vous pouvez modifier le mot de passe de votre centre de sauvegarde Identity Safe et définir un nouvel indice de mot de passe à l'aide de l'option **Modifier le mot de passe du centre de sauvegarde**.

Navigation



Enregistrement de l'identifiant : Permet de configurer Norton Identity Safe pour enregistrer et fournir vos informations de connexion. Vos options sont :

- **Enregistrer mes informations d'authentification quand je me connecte à un site Web** : permet d'enregistrer vos informations de connexion pour les sites Web que vous consultez. Les options disponibles sont les suivantes : Toujours, Non ou Demander.
- **Désactiver le gestionnaire de mots de passe du navigateur** : permet de spécifier comment le gestionnaire de mots de passe du navigateur doit fonctionner. Les options disponibles sont les suivantes : Oui, Non ou Demander.

Barre d'informations : Permet de configurer Norton Identity Safe pour afficher la liste des identités dans la barre d'informations. Vos options sont :

- **Afficher mes identifiants lorsque je dispose de plusieurs identifiants pour un même site** : Affiche vos identifiants à chaque fois que vous visitez un site Web doté de plusieurs identifiants.
- **Afficher mes options de remplissage chaque fois que je visite une page comportant un formulaire** : Affiche les adresses chaque fois que vous visitez une page Web comportant des formulaires à remplir avec vos détails personnels.
- **M'inviter à ouvrir mon centre de sauvegarde** : vous invite à ouvrir votre centre de sauvegarde à chaque fois que vous consultez un site Web contenant des champs à remplir.

Remplissage : Permet de configurer Norton Identity Safe pour fournir vos identités automatiquement lorsque vous accédez à un site Web. Vos options sont :

- **Remplir automatiquement mes identifiants quand je visite des sites Web** : Vous pouvez activer l'option de remplissage automatique de vos informations de connexion lorsque vous accédez à un site Web.

Remplissage automatique pour les sites contenant

- **des menaces de sécurité** : permet de spécifier comment Identity Safe doit répondre aux sites Web présentant des menaces de sécurité. Les options disponibles sont les suivantes : **Oui**, **Non** ou **Demander**.

A propos des identifiants

La fonction **Identifiants** d'Identity Safe vous permet d'afficher tous les identifiants que vous avez stockés dans Identity Safe. Les informations de connexion comprennent les informations d'authentification de votre messagerie électronique, de vos services bancaires en ligne, de vos réseaux sociaux et de vos achats en ligne.

Identity Safe permet d'enregistrer vos identifiants lorsque vous entrez vos informations de connexion dans la page de connexion d'un site Web. Vous pouvez enregistrer instantanément vos informations de connexion dans Identity Safe.



Pour pouvoir gérer vos identifiants, vous devez être connecté à Identity Safe.

Identity Safe propose les fonctions suivantes :

- Enregistrer en toute sécurité les informations de connexion au site Web
- Enregistrer plusieurs identifiants ou comptes et mots de passe pour un site Web
- Effectuer des recherches avancées pour trouver un identifiant précis
- Enregistrer un nom de site Web autre que celui par défaut
- Afficher l'identifiant de connexion et d'afficher ou de masquer le mot de passe
- Afficher la fiabilité du mot de passe de votre identifiant
- Lancer rapidement la page de connexion d'un site Web

- Entrer automatiquement votre identifiant lorsque vous visitez à nouveau des sites Web
- Ajouter manuellement des identifiants
- Changer l'URL de vos identifiants enregistrés.
- Accéder aux fonctions de connexion que vous avez enregistrées pour un site Web, même lorsque Norton Security a expiré.

Les fonctions d'Identity Safe sont prises en charge par les navigateurs Internet Explorer, Firefox et Chrome.

Si votre centre de sauvegarde est fermé lorsque vous vous rendez sur un site Web pour lequel vous devez spécifier des informations de connexion, Norton Identity Safe ouvre automatiquement la barre d'informations. Depuis cette barre, vous pouvez saisir le mot de passe de votre centre de sauvegarde, puis choisir l'identifiant à utiliser sur le site Web.



La barre d'informations s'affiche uniquement si vous cliquez sur un champ dans un site Web pour lequel vos informations de connexion sont nécessaires.

Vous pouvez utiliser le menu **LE CENTRE EST OUVERT** disponible dans la **barre d'outils Norton** pour afficher et insérer automatiquement les détails des identifiants enregistrés. Si vous avez enregistré plusieurs identifiants pour le même site Web, vous pouvez choisir un identifiant dans la liste déroulante.



Vous devez valider le mot de passe de votre centre de sauvegarde pour gérer les informations de connexion si vous avez sélectionné l'option **Mot de passe du centre de sauvegarde requis** dans la fenêtre **Identifiants**.

Enregistrement des identifiants

Norton Identity Safe enregistre automatiquement vos identifiants lorsque vous les entrez pour la première fois. Après qu'Identity Safe a enregistré un identifiant, il remplit automatiquement les détails de connexion à votre prochaine visite du site Web.

Vous devez être connecté à Identity Safe pour enregistrer et insérer automatiquement des mots de passe. Si le champ du mot de passe ou du nom d'utilisateur est vierge, Identity Safe ne vous invite pas à enregistrer l'identifiant.

Si vous ne souhaitez pas que vos identifiants soient enregistrés automatiquement, vous pouvez configurer l'option **Enregistrer mes informations d'authentification quand je me connecte à des sites Web** dans la fenêtre de navigation. Vous pouvez la configurer sur **Toujours**, **Non** ou **Demander**. Par défaut, cette option est définie sur **Toujours**.

Après qu'Identity Safe a enregistré un identifiant, il remplit automatiquement les détails de connexion à votre prochaine visite du site Web.

Enregistrement d'identifiants supplémentaires pour un site Web

- 1 Rendez-vous sur la page Web pour laquelle vous souhaitez enregistrer un autre identifiant. Vos données d'identification apparaissent automatiquement sur la page Web.
- 2 Effacez les données d'identification qui apparaissent sur la page Web.
- 3 Saisissez le nouvel identifiant et cliquez sur l'option ou sur le lien permettant de demander la connexion.
- 4 A l'invite **Voulez-vous remplacer votre identifiant enregistré pour ce site ?**, cliquez sur **Enregistrer nouveau**.



Cette invite s'affiche uniquement la première fois que vous tentez d'enregistrer un identifiant supplémentaire pour un site Web.

- 5 Au niveau de la barre d'informations, dans le message de confirmation **Voulez-vous remplacer votre identifiant enregistré pour ce site ?** qui apparaît, cliquez sur **Enregistrer** pour ajouter les nouvelles informations de connexion.

- 6 Entrez un nom de référence pour le nouvel identifiant dans la zone de texte **Enregistrer sous**, puis cliquez sur **Enregistrer**.

Gestion des identifiants

Identity Safe vous permet d'ajouter un nouvel identifiant ou de modifier le titre, l'URL, le nom d'utilisateur et le mot de passe des identifiants enregistrés dans la fenêtre **Identifiants**. Les identifiants mis à jour sont automatiquement renseignés lors de votre prochaine consultation de la page Web.

Vous pouvez utiliser la flèche disponible à côté de l'URL pour lancer rapidement une page Web de connexion.

Ajout manuel d'une connexion

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis cliquez sur **Identity Safe**.
- 2 Cliquez sur le menu déroulant dans la partie supérieure de la fenêtre et sélectionnez **Nouvel identifiant**.
- 3 Dans la fenêtre **CREER IDENTIFIANT**, dans la zone de texte **Titre**, donnez un nom à l'identifiant.
- 4 Dans la zone de texte **Mots-clés**, indiquez la catégorie de l'identifiant.
- 5 Dans le champ **URL de connexion**, saisissez l'URL du site Web. Assurez-vous d'inclure le préfixe HTTP ou HTTPS à l'URL.
- 6 Dans la boîte de dialogue **Nom d'utilisateur**, saisissez le nom d'utilisateur de connexion.
- 7 Dans le champ **Mot de passe**, saisissez votre mot de passe de connexion.

8 Utilisez les options suivantes pour configurer la sécurité de l'identifiant :

Mot de passe du centre requis	<p>Vous demande de saisir votre mot de passe Identity Safe avant de renseigner des identifiants automatiquement.</p> <p>Sélectionnez cette option pour renforcer la sécurité de vos informations de connexion. Par exemple, vous pouvez utiliser cette option pour votre site de banque en ligne.</p>
Remplissage automatique	<p>Remplit automatiquement vos identifiants à chaque visite du site Web concerné.</p> <p>Symantec conseille d'utiliser cette option pour remplir les informations de connexion de la page Web.</p>
Transmission automatique	<p>Vous connecte automatiquement au site Web.</p>

9 Cliquez sur **Enregistrer**.

Modification d'un identifiant

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis cliquez sur **Identity Safe**.
- 2 Dans le volet gauche, cliquez sur **Identifiants**.
- 3 Cliquez sur l'identifiant que vous voulez modifier. Vous pouvez utiliser l'option **Trier par** située en haut du volet **Identifiants** pour localiser un identifiant plus rapidement. Vous pouvez également rechercher des identifiants directement dans la zone **Rechercher**.

4 Dans la fenêtre qui s'affiche, cliquez sur **Modifier** et apportez les modifications requises.

5 Cliquez sur **Enregistrer**.

Suppression d'un identifiant

1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis cliquez sur **Identity Safe**.

2 Dans le volet gauche, cliquez sur **Identifiants**.

3 Cliquez sur l'identifiant à supprimer.

Vous pouvez utiliser l'option **Trier par** située en haut du volet **Identifiants** pour localiser un identifiant plus rapidement. Vous pouvez également rechercher des identifiants directement dans la zone **Rechercher**.

4 Dans la fenêtre qui s'affiche, cliquez sur **Supprimer**.

5 Dans la boîte de dialogue Avertissement, cliquez sur **Oui**.

A propos des adresses

La fonction Adresses permet de visualiser l'ensemble des informations personnelles que doit gérer Identity Safe. Les informations personnelles incluent votre nom, votre date de naissance, vos adresses postale et électronique et vos numéros de téléphone.

Identity Safe permet d'enregistrer vos identités lorsque vous entrez vos informations personnelles dans le formulaire d'un site Web.



Pour pouvoir gérer vos adresses, vous devez être connecté à Identity Safe.

Vous pouvez utiliser les informations enregistrées dans les adresses pour :

- Remplir des formulaires automatiquement
- Communiquer des informations sensibles sans avoir à les taper lorsque vous êtes en ligne

Identity Safe protège ainsi vos données sensibles de tout vol ou utilisation frauduleuse.

Lorsque vous cliquez sur un champ dans un formulaire en ligne, Norton Identity Safe ouvre une barre

d'informations qui vous demande l'autorisation de remplir automatiquement le formulaire. Dans la barre d'informations, vous pouvez choisir l'adresse à utiliser, puis cliquer sur **Remplir**. Si vous souhaitez que la barre d'informations ne s'affiche plus dans le formulaire en ligne, cliquez sur **Ne plus afficher**. Vous pouvez ouvrir la barre d'informations à tout moment à l'aide de l'option **LE CENTRE EST OUVERT > OPTIONS > Afficher la barre d'informations pour ce site**.

Gestion des adresses

Identity Safe permet d'ajouter une nouvelle adresse ou de modifier les détails enregistrés.

Toutes les adresses enregistrées sont répertoriées dans la fenêtre **Adresses**. Vous pouvez également modifier les détails des adresses enregistrées. Vous pouvez également supprimer une adresse lorsqu'elle n'est plus nécessaire.

Ajout d'une adresse

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Cliquez sur le menu déroulant dans la partie supérieure de la fenêtre et sélectionnez **Nouvelle adresse**.
- 3 Dans la fenêtre **CREER UNE ADRESSE**, indiquez votre région et saisissez vos informations personnelles, telles que votre nom, votre sexe, votre date de naissance et vos coordonnées.
- 4 Sélectionnez l'option **Mot de passe du centre requis** pour requérir le mot de passe Identity Safe avant le remplissage automatique de votre adresse sur le site Web.
- 5 Cliquez sur **Enregistrer**.

Modification d'une adresse

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Dans le volet gauche, cliquez sur **Adresses**.

- 3 Dans la fenêtre **Adresses**, cliquez sur l'adresse à modifier.
Vous pouvez utiliser l'option **Trier par** située en haut du volet **Adresses** pour localiser une adresse plus rapidement. Vous pouvez également rechercher une adresse directement dans la zone **Rechercher**.
- 4 Si un message vous y invite, saisissez le mot de passe de votre centre de sauvegarde, puis cliquez sur **OK**.
- 5 Cliquez sur **Modifier** et modifiez les détails nécessaires.
- 6 Cliquez sur **Enregistrer**.

Suppression d'une adresse

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Dans le volet gauche, cliquez sur **Adresses**.
- 3 Dans la fenêtre **Adresses**, cliquez sur l'adresse à supprimer.
Vous pouvez utiliser l'option **Trier par** située en haut du volet **Adresses** pour localiser une adresse plus rapidement. Vous pouvez également rechercher une adresse directement dans la zone **Rechercher**.
- 4 Si un message vous y invite, saisissez le mot de passe de votre centre de sauvegarde, puis cliquez sur **OK**.
- 5 Cliquez sur **Supprimer**.
- 6 Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
Vous devez valider le mot de passe de votre centre de sauvegarde pour supprimer l'adresse si vous avez sélectionné l'option **Mot de passe du centre requis** lorsque vous avez créé l'adresse.

A propos du portefeuille

L'option **Portefeuille** d'Identity Safe vous permet de gérer vos informations financières, telles que vos informations de carte bancaire, de compte bancaire et de paiement.

Vous pouvez utiliser cette fonction pour effectuer les opérations suivantes :

- renseigner automatiquement les champs contenant les informations de carte ou de compte bancaire lorsque vous effectuez des transactions en ligne ;
- sélectionner les informations d'une carte en particulier pour remplir le formulaire d'un site Web ;
- protéger vos informations financières quand vous naviguez en ligne.

Identity Safe vous protège ainsi contre les enregistreurs de frappes qui usurent votre identité à des fins délictueuses. Les sites Web d'opérations bancaires et d'e-commerce contiennent des formulaires avec des champs destinés aux cartes de crédit ou autres informations financières. Lorsque vous cliquez sur un champ d'un site Web de ce type, Norton Identity Safe ouvre une barre d'informations qui vous demande l'autorisation de remplir automatiquement le formulaire. Dans la barre d'informations, vous pouvez choisir la méthode de paiement, puis cliquer sur **Remplir**.

Vous pouvez utiliser l'icône Ouvrir l'assistant de remplissage du menu **LE CENTRE EST OUVERT** pour afficher une liste des paiements que vous avez enregistrés. Sélectionnez ensuite un paiement et glissez-déplacez les informations de ce paiement dans le formulaire.

Vous pouvez utiliser l'option de tri pour organiser les paiements par nom, date de modification ou date d'utilisation. Vous pouvez également rechercher un paiement parmi ceux enregistrés dans votre centre de sauvegarde.

Le portefeuille offre également les fonctions suivantes :

- Il protège les informations financières en ajoutant un niveau de sécurité supplémentaire.
- Il identifie les pages Web qui contiennent des formulaires et affiche immédiatement une fenêtre contextuelle proposant les cartes disponibles.

- Il affiche un aperçu des cartes et comptes bancaires non protégés par un mot de passe. Identity Safe applique un niveau de sécurité renforcé pour le portefeuille protégé par mot de passe en n'affichant pas de résumé.

Ajout d'un portefeuille

Vous pouvez créer un portefeuille pour ajouter vos détails de carte, de compte bancaire ou de paiement. Les informations financières contenues dans le portefeuille étant particulièrement sensibles, il est recommandé de toujours le protéger par mot de passe. Pendant les procédures de paiement en ligne, selon le mode de paiement sélectionné (carte de crédit, opérations bancaires en ligne), Identity Safe remplit automatiquement les détails dans les champs concernés.

Si vous disposez de plusieurs cartes de crédit, vous pouvez créer plusieurs portefeuilles contenant des informations différentes. Lorsque vous visitez un site Web impliquant des transactions, vous pouvez donner les informations de carte de crédit présentes dans l'un des portefeuilles créés.

Vous pouvez également créer des cartes anonymes à utiliser sur des sites Web peu familiers auxquels vous hésitez à donner vos coordonnées personnelles. Vous pouvez remplir automatiquement les formulaires en ligne lorsque vous visitez un site Web.

Ajout de détails de paiement par carte

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Cliquez sur le menu déroulant dans la partie supérieure de la fenêtre et sélectionnez **Nouveau paiement**.
- 3 Dans la fenêtre **CREER PAIEMENT** de la zone de texte **Titre**, donnez un nom au paiement.
- 4 Dans le champ **Mots-clés**, saisissez la catégorie de paiement, par exemple Maison ou Personnel.

- 5 Sélectionnez **Carte de crédit** dans la liste déroulante **Type**.
- 6 Dans la liste déroulante **Carte**, sélectionnez le type de carte (Visa, Master, etc.).
- 7 Dans le champ **Numéro**, saisissez le numéro de la carte.
- 8 Dans le champ **Date d'expiration**, sélectionnez la date de fin de validité de la carte.
- 9 Dans le champ **Nom sur la carte**, saisissez le nom du propriétaire de la carte, tel qu'imprimé sur la carte.
- 10 Dans la liste déroulante **Adresse de facturation**, sélectionnez l'adresse à associer au paiement, enregistrée dans l'onglet **Adresses**.
- 11 Dans la case **Infos sur la carte**, saisissez les informations à retenir sur la carte.
- 12 Sélectionnez l'option **Mot de passe du centre requis** pour requérir le mot de passe Identity Safe avant le remplissage automatique des informations sur le site Web.
- 13 Cliquez sur **Enregistrer**.

Ajout de détails de compte bancaire pour un paiement

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Cliquez sur le menu déroulant en haut de la fenêtre et sélectionnez **Nouveau paiement**.
- 3 Dans la fenêtre **CREER PAIEMENT** de la zone de texte Titre, donnez un nom au paiement.
- 4 Dans le champ **Mots-clés**, saisissez la catégorie de paiement, par exemple Maison ou Personnel.
- 5 Sélectionnez **Compte bancaire** dans la liste déroulante **Type**.
- 6 Dans le champ **Banque**, saisissez le nom de la banque.
- 7 Dans le champ **Propriétaire du compte**, saisissez le nom du propriétaire du compte bancaire.
- 8 Dans le champ **Code bancaire/code guichet**, saisissez le code guichet.

- 9 Dans le champ **Numéro de compte**, saisissez le numéro du compte bancaire.
- 10 Sélectionnez l'option **Mot de passe du centre requis** pour requérir le mot de passe Identity Safe avant le remplissage automatique des informations sur le site Web.
- 11 Cliquez sur **Enregistrer**.

Gestion des portefeuilles

Tous les portefeuilles enregistrés sont répertoriés dans la fenêtre **Portefeuille**. Vous pouvez afficher et modifier le résumé du portefeuille créé. Vous pouvez également supprimer un portefeuille lorsqu'il n'est plus nécessaire.



Lorsque vous verrouillez votre portefeuille avec un mot de passe, Identity Safe renforce sa sécurité. Vous ne pouvez pas afficher le récapitulatif du portefeuille verrouillé. Vous ne pouvez pas modifier ou supprimer un portefeuille à moins d'en fournir le mot de passe.

Si vous disposez de plusieurs cartes, utilisez les flèches de défilement pour parcourir la liste.

Modification des détails de paiement dans un portefeuille

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Cliquez sur l'onglet **Portefeuille**.
- 3 Dans la fenêtre **Portefeuille**, cliquez sur le paiement à modifier.
Vous pouvez utiliser l'option **Trier par** située en haut du volet **Portefeuille** pour localiser un portefeuille plus rapidement. Vous pouvez également rechercher des portefeuilles directement dans la zone **Rechercher**.
- 4 Si un message vous y invite, saisissez le mot de passe de votre centre de sauvegarde, puis cliquez sur **OK**.
- 5 Cliquez sur **Modifier**.
- 6 Modifiez les détails souhaités.

7 Cliquez sur **Enregistrer**.

Suppression des détails de paiement d'un portefeuille

1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.

2 Cliquez sur l'onglet **Portefeuille**.

3 Dans la fenêtre **Portefeuille**, cliquez sur le paiement à supprimer.

Vous pouvez utiliser l'option **Trier par** située en haut du volet **Portefeuille** pour localiser un portefeuille plus rapidement. Vous pouvez également rechercher des portefeuilles directement dans la zone **Rechercher**.

4 Si un message vous y invite, saisissez le mot de passe de votre centre de sauvegarde, puis cliquez sur **OK**.

5 Cliquez sur **Supprimer**.

6 Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.

Vous devez valider le mot de passe de votre centre de sauvegarde pour supprimer le portefeuille si vous avez sélectionné l'option **Mot de passe du centre requis** lorsque vous avez créé le portefeuille.

Gestion des notes

Identity Safe enregistre et gère vos informations sensibles. La fonction Notes d'Identity Safe enregistre les informations ou indices que vous souhaitez consulter ultérieurement. Vous pouvez utiliser cette fonction pour enregistrer des informations, comme vos rendez-vous, vos tâches quotidiennes ou vos citations préférées.

Vous pouvez également afficher, modifier et supprimer les notes que vous avez sauvegardées.

Création d'une note

1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.

- 2 Cliquez sur le menu déroulant dans la partie supérieure de la fenêtre et sélectionnez **Nouvelle note**.
- 3 Dans la fenêtre **Nouvelle note**, saisissez le nom de la note dans la zone de texte **Titre**.
- 4 Dans la zone de texte **Mots-clés**, définissez une catégorie pour la note, par exemple, Privé, Personnel ou Officiel.
- 5 Dans le champ **Texte**, saisissez vos données de référence.
- 6 Sélectionnez **Mot de passe du centre requis** pour que le mot de passe de votre centre de sauvegarde soit demandé avant de modifier la note.
- 7 Cliquez sur **Enregistrer**.

Modification d'une note

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis cliquez sur **Identity Safe**.
- 2 Dans le volet gauche, cliquez sur **Notes**.
- 3 Dans la fenêtre **Notes**, cliquez sur la note que vous souhaitez modifier.
Vous pouvez utiliser l'option **Trier par** située en haut du volet **Notes** pour localiser une note plus rapidement. Vous pouvez également rechercher des notes directement dans la zone **Rechercher**.
Vous devez valider le mot de passe de votre centre de sauvegarde pour modifier la note si vous avez sélectionné l'option **Mot de passe du centre requis** lorsque vous avez créé la note.
- 4 Cliquez sur **Modifier**.
- 5 Modifiez les détails souhaités.
- 6 Cliquez sur **Enregistrer**.

Suppression d'une note

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis cliquez sur **Identity Safe**.
- 2 Dans le volet gauche, cliquez sur **Notes**.

- 3 Dans la fenêtre **Notes**, cliquez sur la note que vous souhaitez supprimer.
Vous pouvez utiliser l'option **Trier par** située en haut du volet **Notes** pour localiser une note plus rapidement. Vous pouvez également rechercher des notes directement dans la zone **Rechercher**.
Vous devez valider le mot de passe de votre centre de sauvegarde pour supprimer la note si vous avez sélectionné l'option **Mot de passe du centre requis** lorsque vous avez créé la note.
- 4 Cliquez sur **Supprimer**.
- 5 Dans la boîte de dialogue Avertissement, cliquez sur **Oui**.

A propos de l'assistant de remplissage

La fonction Assistant de remplissage vous aide à compléter les formulaires en ligne si Identity Safe ne remplit pas certains champs. Identity Safe utilise les adresses et les portefeuilles que vous avez enregistrés pour remplir automatiquement les formulaires et les informations bancaires sur les sites Web. Ainsi, vous n'avez pas besoin de remplir de longs formulaires qui vous demandent vos informations personnelles comme le nom, la date de naissance et le numéro de téléphone. Vous avez également besoin de saisir des informations de compte bancaire ou de carte de crédit chaque fois que vous faites des achats sur Internet. Si les champs d'un formulaire en ligne ne sont pas remplis, Identity Safe affiche la barre d'informations **Ouvrir l'assistant de remplissage**. Vous pouvez cliquer sur l'option **Ouvrir l'assistant de remplissage** pour ouvrir le volet de l'**assistant de remplissage**. Vous pouvez l'utiliser pour compléter les champs en question. Il suffit de choisir une adresse ou un portefeuille de l'assistant de remplissage, puis de faire glisser les informations requises sur les pages Web.

Il est possible qu'Identity Safe ne remplisse pas un champ d'un formulaire en ligne correctement si :

- Les noms de champ du formulaire en ligne ne correspondent pas à ceux stockés dans vos adresses ou votre portefeuille. Par exemple, le champ de pays ou de région peut être désigné sous un autre nom qu'Identity Safe ne reconnaît pas ;
- aucun nom n'est associé au champ ;
- le type de données qu'un champ peut recevoir est différent de celui enregistré dans vos adresses ou votre portefeuille. Par exemple, la date de naissance est enregistrée sous forme numérique mais le formulaire en ligne accepte uniquement les dates en toutes lettres.

Certains sites Web nécessitent quelques informations personnelles comme votre adresse électronique ou votre numéro de téléphone. Dans ces sites Web, vous pouvez utiliser l'assistant de remplissage pour entrer rapidement les données requises. Il suffit de faire glisser les informations depuis la fonction Adresses ou Portefeuille vers le champ de texte du formulaire en ligne. Par exemple, si vous souhaitez renseigner le champ de numéro de téléphone dans un formulaire en ligne, faites glisser le numéro de téléphone depuis la fonction Adresses vers la zone de texte du formulaire en ligne. Ainsi, l'assistant de remplissage évite le remplissage incorrect des champs tout en vous préservant des pirates et des enregistreurs de frappe qui cherchent à accéder à vos informations personnelles. Pour l'utiliser, il faut que la barre d'outils Norton soit activée dans vos navigateurs. Pour ouvrir l'assistant de remplissage, dans la barre d'outils Norton, cliquez sur **LE CENTRE EST OUVERT**, puis cliquez sur l'icône **Ouvrir l'assistant de remplissage** en bas de la fenêtre contextuelle.

La fonction Assistant de remplissage propose les options suivantes :

Adresses

Permet d'afficher et de choisir toutes les adresses enregistrées dans votre centre de sauvegarde.

Portefeuille

Permet d'afficher et de choisir tous les portefeuilles enregistrés dans votre centre de sauvegarde.

Vous pouvez utiliser l'icône **Déplacer de l'autre côté** pour déplacer la fenêtre de l'assistant de remplissage de droite à gauche et vice versa.

Ajout de mots-clés

La fonction Mots-clés vous permet d'ajouter des mots-clés aux **identifiants**, aux **adresses**, au **portefeuille** et aux **notes**. Lorsque vous ajoutez des mots-clés, les informations de votre centre de sauvegarde sont catégorisées et rassemblées pour vous permettre de les identifier et d'y accéder plus facilement, par exemple, si vous ajoutez le mot-clé Social à tous les identifiants de réseaux sociaux dans votre centre de sauvegarde. Vous pouvez utiliser le mot-clé Social dans le volet **Mots-clés** pour afficher tous vos réseaux sociaux et y accéder facilement.

Ajout d'un mot-clé aux données Identity Safe existantes

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Sélectionnez les données auxquelles attribuer un mot-clé.
Par exemple, si vous souhaitez attribuer un mot-clé à un identifiant, cliquez sur **Identifiants**, puis cliquez sur l'identifiant dans la liste.
- 3 Dans la fenêtre qui s'affiche, cliquez sur **Modifier**.
- 4 Dans la zone de texte **Mots-clés**, indiquez la catégorie de l'identifiant.



Pour attribuer plusieurs mots-clés aux données, séparez les mots-clés par des virgules.

Suppression définitive de votre centre de sauvegarde dans le cloud

Votre centre de sauvegarde dans le cloud est chiffré et accessible uniquement à l'aide de votre compte Norton et des mots de passe de centre de sauvegarde. Vous ne pouvez supprimer votre centre de sauvegarde dans le cloud que manuellement. Même si vous désinstallez Norton Security de votre appareil, vous pouvez continuer d'utiliser votre centre de sauvegarde à partir d'autres appareils. S'il reste une possibilité que vous utilisiez à nouveau les données de votre centre de sauvegarde, ne le supprimez pas.



Si vous le supprimez, toutes les données Identity Safe qu'il contenait seront définitivement supprimées.

Suppression de votre centre de sauvegarde dans le cloud

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Dans la fenêtre **Centre de sauvegarde fermé**, entrez un mot de passe incorrect à trois reprises.
- 3 Cliquez sur le lien **Cliquez ici** en regard de l'option **Vous devez supprimer votre centre de sauvegarde ?**.
- 4 Dans la fenêtre **Supprimer le centre de sauvegarde**, cliquez sur **Oui, supprimer mon centre de sauvegarde**.
- 5 Dans la boîte de dialogue Avertissement, cliquez sur **Oui**.
- 6 Saisissez le mot de passe de votre compte Norton pour valider l'opération et cliquez sur **Connexion**.
- 7 Dans la fenêtre de confirmation, cliquez sur **OK**.

A propos des paramètres généraux de Norton Identity Safe

Lors de son installation sur le système, Norton Security ajoute automatiquement la barre d'outils Norton à vos navigateurs. Certains navigateurs requièrent votre

autorisation pour ajouter la barre d'outils. Si tel est le cas, il est recommandé d'autoriser la barre d'outils Norton. La barre d'outils Norton vous informe des niveaux de sécurité des sites Web que vous visitez. Vous pouvez prévenir l'usurpation de vos identités et informations d'authentification en étant informé du caractère frauduleux d'un site Web avant même d'y accéder.

La fenêtre **Paramètres généraux** vous permet de configurer les fonctions de la barre d'outils Norton. Vous pouvez activer ou désactiver la fonction Norton Safe Web. La fonction est activée par défaut.

Vous pouvez afficher l'état de la barre d'outils Norton dans les navigateurs suivants :

- **Internet Explorer**
- **Google Chrome**
- **Mozilla Firefox**

A propos des paramètres d'importation/exportation de Norton Identity Safe

Vous pouvez exporter vos données Identity Safe pour plus de sécurité, pour la récupération des données ou si vous transférez vos données Identity Safe vers un autre ordinateur. Les fichiers de sauvegarde sont enregistrés au format de fichier .DAT.

Vous pouvez protéger les fichiers sauvegardés à l'aide d'un mot de passe. Nous vous conseillons d'utiliser un mot de passe pour optimiser la protection de vos données Identity Safe. Le mot de passe de sauvegarde ne doit pas forcément être le même que votre mot de passe Identity Safe. Vous devez fournir le mot de passe lorsque vous restaurez les données Identity Safe que vous avez sauvegardées.

Vous pouvez importer vos données Identity Safe à partir du fichier sauvegardé précédemment. Le mot de passe de votre centre de sauvegarde ne peut être réinitialisé. Symantec vous recommande donc de sauvegarder

régulièrement les données de votre centre de sauvegarde. Lorsque vous activez la fonction de sauvegarde automatique, des sauvegardes de votre centre sont créées automatiquement et enregistrées localement sur votre appareil. Vous pouvez accéder aux sauvegardes de votre centre au chemin suivant : **Users\<Nom d'utilisateur>\Mes documents\Sauvegardes Norton Identity Safe\<Nom du compte Norton>**.

Lorsque vous importez les données Identity Safe, vous pouvez effectuer les actions suivantes :

- Fusionner les données importées dans le centre de sauvegarde auquel vous êtes actuellement connecté.
- Remplacer les données Identity Safe existantes stockées dans le centre de sauvegarde auquel vous êtes connecté par les données importées.

Exportation de vos données Identity Safe

Vous pouvez exporter vos données Identity Safe pour plus de sécurité, pour la récupération des données ou si vous transférez vos données Identity Safe vers un autre ordinateur. Le mot de passe de votre centre de sauvegarde ne peut être réinitialisé. Symantec vous recommande donc de sauvegarder régulièrement les données de votre centre de sauvegarde. Lorsque vous activez la fonction de sauvegarde automatique, des sauvegardes de votre centre sont créées automatiquement et enregistrées localement sur votre appareil. Vous pouvez accéder aux sauvegardes de votre centre en suivant le chemin suivant : **Users\<Nom d'utilisateur>\Mes documents\Norton Identity Safe Backups\<Nom du compte Norton>**.

Vous pouvez extraire les données Identity Safe lorsque votre produit a expiré.

Exportation de vos données Identity Safe

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.

- 2 Dans la fenêtre **Norton Identity Safe**, cliquez sur l'icône **Paramètres** située au bas de la fenêtre.
- 3 Cliquez sur l'onglet **Importer/Exporter**.
- 4 Dans le volet **Exporter**, sélectionnez le format de fichier.
Vous pouvez sélectionner l'une des options suivantes :
 - **Format de sauvegarde Identity Safe - Fichier DAT**
Si vous voulez sauvegarder vos données avec un mot de passe pour renforcer la sécurité, saisissez et confirmez le mot de passe.
 - **Texte simple - Fichier CSV (identifiants et notes uniquement)**
- 5 Cliquez sur **Exporter**.
- 6 Dans la fenêtre **Valider le mot de passe pour Identity Safe**, saisissez le mot de passe de votre centre de sauvegarde afin d'exporter vos données Identity Safe.
- 7 Dans la boîte de dialogue de confirmation, cliquez sur **OK**.

Importer vos données Identity Safe

Vous pouvez importer vos données Identity Safe à partir du fichier sauvegardé précédemment. Vous pouvez également importer les données Identity Safe depuis le profil portable que vous avez enregistré dans l'ancienne version de votre produit Norton.

Les options Fusionner les données importées avec les données existantes et Remplacer les données existantes par les données importées s'affichent lorsque vous importez les données Identity Safe depuis un fichier sauvegardé. Vous pouvez fusionner les données importées dans le centre de sauvegarde auquel vous êtes connecté actuellement ou remplacer les données Identity Safe que vous avez enregistrées dans le centre de sauvegarde.



Lors de l'importation, la taille du fichier ne doit pas dépasser 15 Mo pour les fichiers CSV et 35 Mo pour les fichiers NPM.

Importation de vos données

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Dans la fenêtre **Norton Identity Safe**, cliquez sur l'icône **Paramètres** située au bas de la fenêtre.
- 3 Cliquez sur l'onglet **Importer/Exporter**.
- 4 A la ligne **Importer**, cliquez sur **Importer**.
- 5 Dans la fenêtre **Importation de centre de sauvegarde**, effectuez l'une des opérations suivantes :
 - **Fusionner les données importées avec les données existantes**
 - **Remplacer les données existantes par les données importées**
- 6 Cliquez sur **Importer**.
- 7 Allez à l'emplacement du fichier à importer.
- 8 Sélectionnez le fichier, puis cliquez sur **Ouvrir**.
- 9 Si vous disposez de mots de passe différents pour les identifiants enregistrés dans le centre de sauvegarde en cours d'utilisation et dans celui dans lequel vous importez, Norton Security affiche un message de confirmation. Sélectionnez l'une des options suivantes :
 - Cliquez sur **Conserver le mot de passe existant** pour conserver le mot de passe enregistré dans le centre de sauvegarde cloud.
 - Cliquez sur **Conserver le mot de passe importé** pour remplacer le mot de passe enregistré dans le centre de sauvegarde cloud par le mot de passe enregistré dans le centre de sauvegarde que vous importez.
- 10 Dans la boîte de dialogue de confirmation, cliquez sur **OK**.

A propos des paramètres de navigation de Norton Identity Safe

L'onglet **Navigation** de la fenêtre **Paramètres** vous permet de configurer la manière dont Identity Safe devra collecter, stocker et afficher les informations relatives aux identifiants pour les pages Web visitées. Vous pouvez configurer Identity Safe de manière à ce qu'il affiche les cartes que vous avez créées pour les sites Web contenant des formulaires. Vous pouvez également configurer les paramètres de remplissage automatique pour les sites Web contenant des menaces de sécurité.



Symantec recommande de maintenir les configurations par défaut pour les identifiants.

Vous pouvez configurer les options suivantes dans la fenêtre **Navigation** :

Enregistrement de l'identifiant

Permet de configurer Norton Identity Safe pour enregistrer et fournir vos informations de connexion. Vos options sont :

Enregistrer mes informations d'authentification quand je me connecte à un site Web : permet d'enregistrer vos informations de connexion pour les sites Web que vous consultez. Les options disponibles sont les suivantes : **Toujours, Non** ou **Demander**.

Désactiver le gestionnaire de mots de passe du navigateur : permet de spécifier comment le gestionnaire de mots de passe du navigateur doit fonctionner. Les options disponibles sont les suivantes : **Oui, Non** ou **Demander**.

Barre d'informations

Permet de configurer Norton Identity Safe pour afficher la liste des identités dans la barre d'informations. Vos options sont :

- **Afficher mes identifiants lorsque je dispose de plusieurs identifiants pour un même site** : Affiche vos identifiants à chaque fois que vous visitez un site Web doté de plusieurs identifiants.
- **Afficher mes options de remplissage chaque fois que je visite une page comportant un formulaire** : Affiche les adresses chaque fois que vous visitez une page Web comportant des formulaires à remplir avec vos détails personnels.
- **M'inviter à ouvrir mon centre de sauvegarde** : vous invite à ouvrir votre centre de sauvegarde à chaque fois que vous consultez un site Web contenant des champs à remplir.

Remplissage

Permet de configurer Norton Identity Safe pour fournir vos identités automatiquement lorsque vous accédez à un site Web. Vos options sont :

Remplir automatiquement mes identifiants quand je visite des sites Web : Vous pouvez activer l'option de remplissage automatique de vos informations de connexion lorsque vous accédez à un site Web.

Remplissage automatique pour les sites contenant des menaces de sécurité : permet de spécifier comment Identity Safe doit répondre aux sites Web présentant des menaces de sécurité. Les options disponibles sont les suivantes : **Oui**, **Non** ou **Demander**.

A propos des paramètres de sécurité de Norton Identity Safe

Vous pouvez modifier votre mot de passe Identity Safe dans l'onglet **Sécurité** de la fenêtre **Paramètres**. Vous pouvez également utiliser cette option pour définir le niveau de sécurité associé à l'utilisation du mot de passe Identity Safe.

Les sections suivantes permettent de modifier le mot de passe Identity Safe et de définir le niveau de sécurité du mot de passe

Accès au centre de sauvegarde



Vous pouvez configurer les paramètres de sécurité suivants pour l'ouverture et la fermeture de votre centre de sauvegarde.

Vos options sont :

■ **Demander le mot de passe au début de chaque session**

Vous invite à entrer le mot de passe de votre centre de sauvegarde lors de chaque accès à Identity Safe.

■ **Demander le mot de passe avant de fournir un identifiant ou de remplir un formulaire**

Vous demande de saisir votre mot de passe Identity Safe pour chaque formulaire en ligne avant de renseigner automatiquement des identifiants. Vous pouvez spécifier que chaque identifiant nécessite la saisie du mot de passe Identity Safe avant le remplissage automatique.

■ **Fermer le centre de sauvegarde après <minutes> minutes d'inactivité**

Vous déconnecte automatiquement d'Identity Safe quand vous n'utilisez pas votre Identity Safe pendant une période donnée. Vous pouvez définir le délai d'inactivité sur 15, 30 ou 45 minutes. Cette option est utile si vous vous trouvez fréquemment dans une zone où d'autres personnes ont accès à votre ordinateur.

■ **Fermer le centre de sauvegarde en mode veille**

Vous déconnecte automatiquement d'Identity Safe lorsque votre ordinateur est en veille.

Mot de passe de centre de sauvegarde Permet de modifier le mot de passe du centre de sauvegarde.

Vous pouvez utiliser l'option **Modifier le mot de passe du centre de sauvegarde** pour modifier le mot de passe de votre centre de sauvegarde et définir un nouvel indice de mot de passe.

Modification de votre mot de passe Identity Safe

Il est conseillé de changer régulièrement le mot de passe Identity Safe pour éviter tout accès non autorisé à vos informations personnelles enregistrées dans Identity Safe. Vous pouvez modifier votre mot de passe depuis l'onglet **Sécurité** de la fenêtre **Paramètres** de Norton Identity Safe.

Si vous souhaitez modifier le mot de passe Identity Safe de votre centre de sauvegarde dans le cloud, il doit comporter les caractéristiques suivantes :

- Il doit comporter au moins huit caractères.
- Il doit comporter au moins une lettre majuscule.
- Il doit comporter au moins un chiffre (compris entre 0 et 9).
- Il doit comporter au moins un symbole (par exemple * > & \$ %)
- Le mot de passe doit être différent du nom d'utilisateur que vous utilisez pour votre compte Norton.



Vous pouvez définir l'indice de votre mot de passe si vous ne l'avez pas fait lorsque vous avez configuré Identity Safe.

Changement du mot de passe de centre de sauvegarde Identity Safe

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Identité**, puis sur **Identity Safe**.
- 2 Dans la fenêtre **Norton Identity Safe**, cliquez sur l'icône **Paramètres** située au bas de la fenêtre.

- 3 Cliquez sur l'onglet **Sécurité**.
- 4 A la ligne **Mot de passe du centre**, cliquez sur **Modifier le mot de passe du centre de sauvegarde**.
- 5 Dans la fenêtre **Modifier le mot de passe du centre de sauvegarde**, saisissez le mot de passe actuel et le nouveau mot de passe, puis confirmez ce dernier.
- 6 Cliquez sur **OK**.
- 7 Dans la boîte de dialogue de confirmation, cliquez sur **OK**.

A propos de la barre d'outils Norton

Lors de son installation, Norton Security ajoute automatiquement la barre d'outils Norton aux navigateurs Internet Explorer (barre d'outils), Firefox (Extensions) et Chrome (Extensions).

Vous pouvez utiliser les options suivantes dans la barre d'outils Norton :

Norton Safe Search	Vous pouvez utiliser l'option Norton Safe Search pour améliorer vos recherches sur le Web. Norton Safe Search utilise Ask.com pour générer les résultats de la recherche. Norton Safe Search génère des résultats de recherche qui indiquent l'état Sécurité du site et l'évaluation Norton pour chaque résultat.
--------------------	---

Indicateur Safe Web

Permet de savoir si le site Web que vous visitez est fiable ou risqué.

Les options Antiphishing et Norton Safe Web analysent le niveau de sécurité des sites Web que vous visitez. Les résultats sont ensuite affichés dans la fenêtre contextuelle **Norton Safe Web**.

Vous pouvez cliquer sur l'indicateur Safe Web pour afficher les détails des menaces dans la fenêtre contextuelle **Norton Safe Web**. Si vous pensez que ce résultat n'est pas correct, vous pouvez utiliser l'option **Signaler ce site** pour en informer Symantec afin d'effectuer une évaluation approfondie.

Menu LE CENTRE EST OUVERT/LE CENTRE EST FERME	
---	--



Permet d'afficher les identifiants que vous avez enregistrés dans Identity Safe.

Certains sites Web requièrent des informations de connexion. Vous pouvez utiliser le menu **LE CENTRE EST OUVERT** pour remplir ces informations. Le menu **LE CENTRE EST OUVERT** affiche la liste de tous les identifiants enregistrés. Vous pouvez sélectionner un identifiant dans la liste et l'utiliser pour vous connecter au site Web.

Vous pouvez utiliser les icônes suivantes, disponibles au bas du menu **LE CENTRE EST OUVERT** :

- Ouvrir l'assistant de remplissage :
Permet d'afficher le volet de l'assistant de remplissage qui s'ouvre à droite de votre navigateur. Vous pouvez glisser-déplacer les identités depuis le volet de l'assistant de remplissage pour remplir les champs du site Web.
- Ouvrir Norton Identity Safe :
Permet d'ouvrir la fenêtre principale de Norton Identity Safe.
- Fermer le centre de sauvegarde :
Indique si le centre de sauvegarde est ouvert/fermé. Vous pouvez cliquer sur cette option pour fermer le centre de

<p>PARTAGER SUR</p>	<p>sauvegarde.</p> <p>⚠ Vous devez fermer la fenêtre principale Norton Identity Safe avant de fermer le centre de sauvegarde à l'aide de la barre d'outils.</p> <p>⚠ Vous devez être connecté à un centre de sauvegarde Identity Safe pour accéder au menu Le centre est ouvert.</p> <p>Permet de partager le site Web avec vos amis via les réseaux sociaux les plus connus, tels que Facebook, Twitter, LinkedIn, Yahoo Mail, Hotmail ou Google Mail.</p> <p>⚠ Le partage des sites Web présentant des menaces de sécurité n'est pas autorisé.</p>
----------------------------	--

Icône Paramètres (●●●)	<p>Permet de configurer les paramètres de la barre d'outils Norton et de Norton Identity Safe.</p> <p>Vos options sont :</p> <ul style="list-style-type: none">■ Options de la barre d'outils : vous pouvez activer ou désactiver les fonctions de partage de Norton Safe et Norton Safe Search, disponibles dans la barre d'outils.■ Ouvrir les paramètres d'Identity Safe : vous pouvez configurer Identity Safe de manière à pouvoir y accéder depuis divers appareils et améliorer ses capacités et son efficacité.
--------------------------	--

Dans le navigateur Google Chrome, il est possible d'accéder à la **barre d'outils Norton** dans la liste des extensions Chrome. Dans la page Extensions du navigateur Chrome, vous pouvez activer ou désactiver la **barre d'outils Norton** et désinstaller la **barre d'outils Norton** de votre navigateur Chrome.

Si la **barre d'outils Norton** est activée, vous pouvez accéder aux options suivantes :

Autoriser en mode navigation privée

Permet de naviguer sur Internet en mode furtif sans que les données de votre session de navigation soient stockées dans les historiques de navigation ou de téléchargement.

Autoriser l'accès aux fichiers URL Permet d'afficher l'emplacement de l'URL du fichier téléchargé.



Si vous avez désinstallé la **barre d'outils Norton** de votre navigateur Chrome, vous devez réinstaller Norton Security pour pouvoir accéder de nouveau à la **barre d'outils Norton** dans votre navigateur Chrome.

Lorsque vous désinstallez Norton Security, vous pouvez continuer à utiliser la barre d'outils Norton gratuitement.



L'ordinateur doit être connecté à Internet pour que cette option soit disponible. Norton Security ne vous autorise pas à laisser la **barre d'outils Norton** installée si vous mettez à niveau le produit vers la version la plus récente ou décidez de réinstaller un autre produit Norton.

Désactivation et activation de la barre d'outils Norton

Vous pouvez masquer la **barre d'outils Norton** si vous ne souhaitez pas voir l'évaluation de tous les sites Web que vous visitez. Lorsque vous masquez la barre d'outils, Norton Identity Safe n'affiche pas la fenêtre contextuelle **Norton Safe Web**. Toutefois Identity Safe vous signale les sites suspects et connus comme frauduleux et vous prévient si une erreur nécessite votre attention.

Désactivation de la barre d'outils Norton dans les navigateurs Internet Explorer, Mozilla Firefox et Google Chrome

- ❖ Lancez votre navigateur Internet et effectuez l'une des actions suivantes :
 - Dans Internet Explorer, cliquez avec le bouton droit de la souris sur la barre de menu, désélectionnez **Barre d'outils Norton** puis cliquez sur **Désactiver** dans la boîte de dialogue **Désactiver un module complémentaire**.
 - Dans Mozilla Firefox, cliquez sur **Outils > Modules > Extensions**. Sur la page **Extensions**, sous **Barres d'outils Norton Identity Safe**, cliquez sur **Désactiver**.
 - Dans Google Chrome, accédez à l'URL suivante : <chrome://extensions>. Dans la page **Extensions**, sous **Protection Norton Identity**, désélectionnez **Activée**.

Activation de la barre d'outils Norton dans les navigateurs Internet Explorer, Mozilla Firefox et Google Chrome

- ❖ Lancez votre navigateur Internet et effectuez l'une des actions suivantes :
 - Dans Internet Explorer, cliquez avec le bouton droit de la souris sur la barre de menu, sélectionnez **Barre d'outils Norton** puis cliquez sur **Activer** dans la boîte de dialogue **Activer un module complémentaire**.
 - Dans Mozilla Firefox, cliquez sur **Outils > Modules > Extensions**. Sur la page **Extensions**, sous **Barres d'outils Norton Identity Safe**, cliquez sur **Activer**.
 - Dans Google Chrome, accédez à l'URL suivante : <chrome://extensions>. Dans la page **Extensions**, sous **Protection Norton Identity**, sélectionnez **Activée**.

Norton Identity Safe

Norton Identity Safe vous permet de stocker et de gérer vos informations sensibles telles que vos identifiants, vos informations personnelles et vos informations financières. Identity Safe chiffre et stocke toutes vos informations sensibles dans un centre de sauvegarde sur le cloud. Vous pouvez accéder au centre de sauvegarde sur le cloud à l'aide d'un mot de passe depuis un ordinateur de bureau, un ordinateur portable, une tablette, un smartphone et le site Web Norton Identity Safe.

Identity Safe fait office de référentiel d'informations sensibles et fournit également les fonctions suivantes :

- Il vous protège contre l'usurpation d'identité et les sites Web frauduleux ou suspects lors des transactions en ligne.
- Il vous permet de gérer facilement et de remplir automatiquement plusieurs informations concernant vos cartes de crédit.
- Il vous permet de transporter et d'utiliser vos informations sensibles en toute sécurité lorsque vous êtes en déplacement. En enregistrant vos données dans un centre de sauvegarde dans le cloud, vous pouvez accéder à vos données sensibles depuis un ordinateur où Norton Security est installé ou via le site Web Norton Identity Safe.

Foire aux questions

- [la section intitulée « Comment commencer avec Identity Safe ? »](#)
- [la section intitulée « Quel type d'informations puis-je stocker dans un centre de sauvegarde ? »](#)
- [la section intitulée « Pourquoi dois-je activer la barre d'outils Norton ? »](#)
- [la section intitulée « Dois-je sauvegarder mes données Identity Safe ? »](#)

Comment commencer avec Identity Safe ?

Lorsque vous accédez à Identity Safe pour la première fois, vous devez vous connecter à Identity Safe à l'aide des identifiants de votre compte Norton. Si vous n'avez pas de compte Norton, vous pouvez cliquer sur **Connexion** pour en créer un.

Après vous être connecté à votre compte Norton, vous devez créer votre centre de sauvegarde sur le cloud Identity Safe. Vous devez fournir un mot de passe pour créer votre centre de sauvegarde dans le cloud. Nous vous recommandons de définir un mot de passe fiable pour votre centre de sauvegarde dans le cloud, étant donné que celui-ci vous sert de référentiel pour toutes vos informations sensibles. Se reporter à "[création d'un centre de sauvegarde dans le cloud](#)" à la page 245.

Vous pouvez utiliser la fonction **Générateur de mot de passe** pour créer un mot de passe unique et fiable pour votre centre de sauvegarde.



Vous ne pouvez créer qu'un seul centre de sauvegarde dans le cloud par compte Norton.

Quel type d'informations puis-je stocker dans un centre de sauvegarde ?

Voici les catégories et les types d'informations que vous pouvez stocker dans votre centre de sauvegarde Identity Safe :

- **Identifiants** - Votre ID utilisateur et vos mots de passe pour les sites Web que vous consultez, tels que vos services bancaires en ligne, votre messagerie électronique et des sites Web d'achats. Se reporter à "[Gestion des identifiants](#)" à la page 263.
- **Adresses** - Vos informations personnelles, telles que votre nom, date de naissance, adresse postale, adresse électronique et vos numéros de téléphone. Se reporter à "[Gestion des adresses](#)" à la page 266.

- **Portefeuille** - Vos informations financières, telles que vos informations de carte de crédit et de compte bancaire. Se reporter à "[Gestion des portefeuilles](#)" à la page 271.
- **Notes** - Tout type de texte qui vous servira ultérieurement. Se reporter à "[Gestion des notes](#)" à la page 272.

Pourquoi dois-je activer la barre d'outils Norton ?

Vous devez activer la barre d'outils Norton afin d'accéder plus facilement à toutes les fonctions d'Identity Safe depuis votre navigateur Internet. La barre d'outils Norton comprend les fonctions suivantes :

Norton Safe Search	<p>Un moteur de recherche sécurisé qui utilise Ask.com pour générer les résultats de la recherche. Norton Safe Search classe les résultats de la recherche en fonction du niveau de sécurité du site et de l'évaluation Norton.</p> <p>Pour plus d'informations sur l'utilisation de la fonction Norton Safe Search, Se reporter à "Recherche sur le Web à l'aide de Norton Safe Search" à la page 233..</p>
Norton Safe Web	<p>Un indicateur de sécurité pour les sites Web que vous consultez. il analyse le niveau de sécurité des sites Web que vous consultez et indique s'ils sont sécurisés.</p>

Centre de sauvegarde Identity Safe	Un emplacement en ligne sécurisé où vous pouvez stocker vos informations sensibles telles que vos identifiants, vos informations personnelles et financières. Vous pouvez utiliser ces informations pour vous connecter à des sites Web, pour remplir automatiquement des formulaires en ligne et effectuer des paiements en ligne.
Fonction de partage de Norton Safe	Un moyen sécurisé de partager avec vos amis les sites Web que vous consultez. Vous pouvez les partager à l'aide de sites de réseaux sociaux tels que Facebook, Twitter, LinkedIn, Yahoo Mail, Outlook et Gmail.
Assistant de remplissage	<p>Une fonction qui vous permet de remplir facilement les longs formulaires en ligne qui vous demandent des informations personnelles et financières. Vous pouvez glisser-déplacer une adresse ou un portefeuille depuis le volet Assistant de remplissage pour remplir automatiquement les formulaires en ligne.</p> <p>Pour plus d'informations sur la fonction de remplissage automatique, Se reporter à "A propos de l'assistant de remplissage" à la page 274..</p>

Norton Security ajoute la barre d'outils Norton aux navigateurs Internet Explorer, Firefox et Chrome installés sur votre ordinateur. Si la barre d'outils Norton n'est pas activée automatiquement, vous pouvez l'activer manuellement. Pour plus d'informations sur l'activation de la barre d'outils Norton dans votre navigateur, Se reporter à "[Désactivation et activation de la barre d'outils Norton](#)" à la page 294..

Dois-je sauvegarder mes données Identity Safe ?

Norton Identity Safe sauvegarde automatiquement vos données Identity Safe sur votre ordinateur dans un fichier DAT. Cependant, vous pouvez également sauvegarder manuellement vos données Identity Safe sur votre ordinateur ou un périphérique de stockage portable. Vous pouvez ensuite importer les données sauvegardées dans votre centre de sauvegarde Identity Safe. Pour plus d'informations sur l'exportation ou la sauvegarde de vos données Identity Safe, se reporter à ["Exportation de vos données Identity Safe"](#) à la page 279..

Optimisation des performances de votre ordinateur

8

Ce chapitre traite des sujets suivants :

- A propos de la fragmentation du disque et du fichier
- Optimisation manuelle de vos disques permanents
- A propos de l'utilisation efficace de l'optimisation
- A propos du nettoyage de l'encombrement du disque
- Exécution d'une analyse pour nettoyer l'encombrement du disque
- Exécution du rapport de diagnostic
- Gestion des éléments de démarrage
- Désactivation ou activation des éléments de démarrage

A propos de la fragmentation du disque et du fichier

Le disque dur de votre ordinateur stocke tous vos fichiers, toutes vos applications ainsi que le système d'exploitation Windows. Avec le temps, les éléments d'information composant chaque fichier se dispersent sur tout le disque. Ce processus est appelé fragmentation. Plus vous utilisez votre ordinateur, plus la fragmentation de vos fichiers s'accroît.

Lorsque vous accédez à un fichier fragmenté, les performances du disque diminuent. Ceci s'explique par le fait que la tête du disque recherche, charge, enregistre et assure le suivi de tous les fragments d'un fichier. Si l'espace libre est également fragmenté, la tête du disque doit rechercher l'espace libre adéquat pour stocker les fichiers temporaires ou les fichiers ajoutés.

Norton Security optimise vos disques permanents pour améliorer la vitesse et l'efficacité de votre ordinateur. La procédure d'optimisation réorganise les fragments de fichiers dispersés dans des groupes proches ou contigus. Lorsque la tête de disque accède à toutes les données d'un fichier au même endroit, la lecture du fichier en mémoire est accélérée. L'optimisation consolide également l'espace libre afin d'éviter la fragmentation des fichiers récemment ajoutés. Il ajoute un espace supplémentaire après les structures de données majeures afin qu'elles puissent se développer sans se refragmenter immédiatement.

Optimisation manuelle de vos disques permanents

Optimiser les disques permanents de votre ordinateur peut améliorer les performances et la fiabilité. Norton Security vérifie automatiquement que vos disques permanents ne sont pas fragmentés et les optimise s'ils sont fragmentés à plus de 10 %. Vous pouvez à tout moment consulter les derniers rapports pour déterminer si une optimisation est nécessaire.



Vous pouvez exécuter l'Optimisation du disque seulement quand le disque dispose de plus de 15 pour cent d'espace disponible.

Certains programmes, comme les logiciels de montage vidéo ou les logiciels nécessitant de grandes quantités d'espace disque, fonctionnent plus efficacement quand les disques sont optimisés. Si vous ne voulez pas attendre que Norton Security effectue l'optimisation

automatique, vous pouvez optimiser vos disques manuellement.



Pendant le processus d'optimisation du disque, les disques SSD sont défragmentés uniquement dans Windows 8.

Optimisation manuelle des disques permanents

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Performances**, puis cliquez sur **Optimiser le disque**.
- 2 Lorsque l'activité est terminée, cliquez sur **Fermer**.

A propos de l'utilisation efficace de l'optimisation

Norton Security optimise automatiquement le disque permanent de votre ordinateur lorsque cela est nécessaire, sans nécessiter d'intervention de votre part. Néanmoins, certaines pratiques peuvent aider Norton Security à effectuer cette optimisation plus efficacement.

Les procédures suivantes contribuent à l'efficacité de l'optimisation automatique :

Laissez de temps en temps votre ordinateur allumé quand vous ne l'utilisez pas.

Norton Security effectue l'optimisation du disque quand l'ordinateur est inactif. Si vous éteignez toujours votre ordinateur dès que vous avez fini de l'utiliser, Norton Security ne pourra jamais effectuer l'optimisation automatique. Si vous éteignez votre ordinateur pendant l'optimisation, Norton Security reprend le processus quand vous rallumez l'ordinateur.

Définissez une planification pour l'optimisation	Norton Security optimise automatiquement le disque dur selon les besoins. Vous pouvez aussi définir une planification pour l'optimisation.
Supprimez les fichiers de grande taille dont vous n'avez plus besoin.	Les fichiers de grande taille sont souvent plus fragmentés que les petits. Ces fichiers fragmentés affectent les performances de votre ordinateur.

A propos du nettoyage de l'encombrement du disque

Au fil du temps, de nombreux fichiers temporaires et superflus peuvent s'accumuler sur le disque permanent de votre ordinateur. A la longue, ces fichiers peuvent réduire significativement l'espace de stockage disponible sur le disque et affecter les performances de votre ordinateur. Norton Security nettoie automatiquement les fichiers indésirables qui se sont accumulés.

Les fichiers temporaires qui encombrant votre ordinateur peuvent être générés par plusieurs sources :

Installations de logiciels	Lorsque vous installez un logiciel sur votre ordinateur, la procédure d'installation peut créer des fichiers temporaires. Dans certains cas, le programme d'installation ne nettoie pas ces fichiers temporaires à la fin de l'installation.
----------------------------	--

Navigation Web

Lorsque vous naviguez sur une page Web, votre navigateur télécharge le texte et les images qui la composent. Après avoir consulté une page, le navigateur peut laisser sur l'ordinateur le contenu téléchargé. Ce contenu téléchargé permet d'afficher une page Web plus rapidement quand vous la consultez de nouveau. Ces fichiers conservés par le navigateur s'accumulent au fil du temps.

Erreurs de programme

Dans le cadre du fonctionnement normal de votre ordinateur, certains programmes créent des fichiers temporaires pour améliorer les performances. Si une erreur provoque la fermeture inopinée d'un programme, ces fichiers temporaires peuvent ne pas être effacés.

Exécution d'une analyse pour nettoyer l'encombrement du disque

Diverses activités, comme une navigation intensive sur le Web ou des installations de logiciels successives produisent des fichiers temporaires. Vous pouvez exécuter manuellement une analyse de nettoyage pour supprimer les fichiers temporaires immédiatement.

Nettoyage manuelle de votre ordinateur

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Performances**, puis sur **Nettoyage de fichier**.
- 2 Lorsque l'activité est terminée, cliquez sur **Fermer**.

Exécution du rapport de diagnostic

Le rapport de diagnostic de Norton Security collecte des informations sur votre ordinateur, y compris le système d'exploitation, les programmes et le matériel. Vous pouvez utiliser ce rapport pour identifier et résoudre les problèmes.

Le rapport de diagnostic est un rapport en temps réel horodaté. Norton Security ne génère pas ce rapport automatiquement. Vous devez sélectionner l'option **Rapport de diagnostic** dans la fenêtre **Analyses** pour générer le rapport manuellement.

Si Norton Security détecte des problèmes sur votre ordinateur, vous pouvez utiliser l'option **Corriger** pour les résoudre.

Vous pouvez enregistrer, transmettre par message électronique ou imprimer le rapport pour le consulter en cas de besoin.

Exécution du rapport de diagnostic

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Exécuter des analyses**.
- 2 Dans la fenêtre **Analyses**, cliquez sur **Rapport de diagnostic**, puis sur **OK**.

Gestion des éléments de démarrage

Le gestionnaire de démarrage de Norton Security surveille et répertorie les programmes qui démarrent automatiquement lors de la mise en marche de votre ordinateur. Pour réduire le temps de démarrage de votre

ordinateur et améliorer les performances, vous pouvez retarder le démarrage de certains programmes à la mise en marche de votre ordinateur.

Norton Security retarde le démarrage des programmes retardés de cinq minutes. Le premier programme retardé de la fenêtre **Gestionnaire de démarrage** démarre cinq minutes après le démarrage de votre ordinateur. Tous les autres programmes retardés démarrent avec un délai supplémentaire de dix secondes.

Retardement des éléments de démarrage

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Performances**, puis sur **Gestionnaire de démarrage**.
- 2 Dans la fenêtre **Gestionnaire de démarrage**, dans la colonne **Retarder le démarrage**, sélectionnez le programme à différer.
- 3 Cliquez sur **Appliquer**.
- 4 Cliquez sur **Fermer**.

Exécution manuelle des éléments de démarrage différés

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Performances**, puis sur **Gestionnaire de démarrage**.
- 2 Dans la fenêtre **Gestionnaire de démarrage**, cliquez sur **Exécuter les éléments différés maintenant**.
- 3 Lorsque le programme est lancé, dans la fenêtre **Gestionnaire de démarrage**, cliquez sur **Fermer**.

Désactivation ou activation des éléments de démarrage

Chaque fois que vous démarrez votre ordinateur, certains programmes démarrent automatiquement et s'exécutent en parallèle. Ces programmes sont nommés éléments de démarrage. Les éléments de démarrage augmentent le temps de démarrage de votre ordinateur.

Le gestionnaire de démarrage vous aide à gérer avec efficacité les éléments de démarrage de votre ordinateur. Si vous ne souhaitez pas qu'un programme démarre automatiquement au démarrage de votre ordinateur, vous pouvez désactiver le programme dans le gestionnaire de démarrage. Vous pouvez également retarder un élément de démarrage, de sorte qu'il soit exécuté ultérieurement.

Désactivation des éléments de démarrage

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Performances**, puis cliquez sur **Gestionnaire de démarrage**.
- 2 Dans la colonne **Marche/Arrêt**, décochez les programmes que vous ne souhaitez pas lancer automatiquement au démarrage de votre ordinateur.
- 3 Cliquez sur **Appliquer** pour enregistrer les modifications.
- 4 Cliquez sur **Fermer**.

Activation des éléments de démarrage

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Performances**, puis cliquez sur **Gestionnaire de démarrage**.
- 2 Dans la colonne **Marche/Arrêt**, cochez les programmes que vous souhaitez lancer automatiquement au démarrage de votre ordinateur.
- 3 Cliquez sur **Appliquer** pour enregistrer les modifications.
- 4 Cliquez sur **Fermer**.

Ce chapitre traite des sujets suivants :

- [A propos de l'Historique de la sécurité](#)

A propos de l'Historique de la sécurité

La fenêtre **Historique de la sécurité** vous permet d'effectuer ce qui suit :

- Afficher le résumé des alertes et des messages sur les événements
- Afficher les résultats des analyses qui sont exécutées sur votre ordinateur
- Afficher les éléments que vous avez transmis au site Web Symantec Security Response.
- Gérer les éléments mis en quarantaine
- Contrôler les tâches de sécurité que vos produits effectuent en l'arrière-plan

L'historique de la sécurité permet de superviser les tâches de sécurité effectuées par votre produit en arrière-plan. En outre, les alertes reçues sont consultables en permanence dans l'historique de la sécurité. Si vous n'êtes pas en mesure d'examiner une alerte lorsqu'elle vous parvient, vous pouvez l'examiner ultérieurement dans l'historique de la sécurité.

Les alertes, les résultats d'analyse et les autres éléments de sécurité liés aux différentes fonctions des produits apparaissent sous leurs catégories respectives dans la fenêtre **Historique de la sécurité**. Par exemple,

les éléments de sécurité liés à la fonctionnalité Quarantaine apparaissent sous la catégorie **Quarantaine** de la fenêtre Historique de la sécurité. En outre, la fenêtre **Historique de la sécurité** affiche les détails relatifs à chaque élément dans le volet **Détails**.

En fonction de leur fonctionnalités, l'Historique de la sécurité organise largement toutes les catégories dans les groupes suivants :

- **Toute l'activité**
- **Protection et performances**
- **Soumissions et erreurs**
- **Performances**
- **Informations**

Par défaut, les catégories d'informations suivantes sont disponibles dans la fenêtre **Historique de la sécurité** :

- **Historique récent**
- **Historique complet**
- **Résultats de l'analyse**
- **Risques de sécurité résolus**
- **Risques de sécurité non résolus**
- **Quarantaine**
- **Activité SONAR**
- **Pare-feu - Réseau et connexions**
- **Pare-feu - Activités**
- **Prévention d'intrusion**
- **Protection pour les réseaux sociaux**
- **Diagnostic des téléchargements**
- **Antispam**
- **Identité**
- **Protection contre les falsifications du produit Norton**
- **Alertes de performances**
- **Limitation de l'utilisation réseau**
- **Sites signalés à Symantec**

- Rapport d'erreur Norton
- Erreurs de courriers électroniques
- Communauté de veille Norton
- Nettoyage des fichiers
- Optimisation du disque
- Mode silencieux
- LiveUpdate

Vous pouvez afficher les éléments de sécurité en fonction de la catégorie des événements sélectionnés et de la chaîne de recherche fournie. Votre produit Norton limite le nombre de résultats de la recherche apparaissant sur chaque page de la fenêtre **Historique de la sécurité**. Par conséquent, l'historique de la sécurité sépare les éléments qui sont renvoyés pour chaque critère de recherche et les affiche sur des pages distinctes. Vous pouvez utiliser la défilement au bas de la fenêtre pour parcourir les différentes pages successivement. Si vous voulez afficher une page spécifique, vous pouvez utiliser l'option **Aller à la page** pour ouvrir la page. Le nombre maximal d'éléments pouvant être affichés sur une page est 100.

Vous pouvez prendre une mesure appropriée pour résoudre un risque ou une menace en fonction de l'état de la sécurité d'un élément d'une catégorie d'informations. Les actions que vous pouvez effectuer incluent les actions suivantes :

- Restaurer et exclure un élément mis en quarantaine.
- Supprimer un élément de l'historique de la sécurité.
- Transmettre un élément à Symantec pour une analyse approfondie.
- Approuver ou restreindre les périphériques sur un réseau sélectionné.
- Supprimer l'état approuvé ou restreint des périphériques sur le réseau sélectionné.
- Autoriser le programme sélectionné à accéder à Internet.

- Configurer votre produit Norton pour être averti lorsqu'il bloque une signature d'attaque sélectionnée.

Votre produit Norton vous permet également d'enregistrer l'historique des événements de sécurité. Vous pouvez afficher les informations d'événement de sécurité quand vous le souhaitez. Si vous souhaitez analyser les événements de sécurité un certain jour, vous pouvez enregistrer les fichiers journaux de l'Historique de la sécurité du jour en question. Vous pouvez importer ultérieurement le fichier journal dans l'Historique de la sécurité et analyser les données.

Ouverture de l'historique de la sécurité

L'historique de la sécurité fournit un enregistrement de toutes les activités que Norton Security a effectué sur votre ordinateur.

Vous pouvez accéder à l'historique de la sécurité à partir des emplacements suivants :

- Onglet **Sécurité** de la fenêtre principale du produit
- Diverses fenêtres et notifications d'alerte
- Zone de notification de la barre des tâches Windows
- Section **Menaces détectées** dans plusieurs fenêtres **Analyse**

Affichage d'éléments de l' historique de la sécurité

L'historique de la sécurité fournit un enregistrement de toutes les activités que votre produit Norton a effectué sur votre ordinateur.

Vous pouvez afficher toutes les activités, y compris :

- Alertes et messages sur les événements de l'Historique de la sécurité
- Résultats des différentes analyses
- Informations que vous avez soumises au site Web Symantec Security Response
- Éléments mis en quarantaine
- Activités de Norton Firewall

- Activités de nettoyage de fichier
- Tâches de sécurité que votre produit Norton effectuée en arrière-plan

Selon leurs fonctionnalités, toutes les catégories de l'historique de la sécurité s'affichent sous les groupes suivants dans la liste déroulante pour l' **affichage** :

- **Toute l'activité**
- **Protection et performances**
- **Soumissions et erreurs**
- **Performances**
- **Informations**

Les éléments liés aux différentes fonctions des produits apparaissent sous leurs catégories respectives dans la fenêtre **Historique de la sécurité**. Par exemple, les éléments de sécurité liés à la fonctionnalité Quarantaine apparaissent sous la catégorie **Quarantaine** de la fenêtre **Historique de la sécurité**. En outre, la fenêtre **Historique de la sécurité** affiche les détails relatifs à chaque élément dans le volet **Détails**.

Affichage des éléments dans l'historique de la sécurité

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Historique**.

- 2 Dans la liste déroulante **Affichage**, de la fenêtre **Historique de la sécurité**, sélectionnez la catégorie d'éléments que vous souhaitez afficher. Vos options sont :

<p>Historique récent</p>	<p>La vue Historique récent de la fenêtre Historique de la sécurité affiche les alertes que vous avez reçues au cours des sept derniers jours. Elle énumère l'historique de certains événements de sécurité récents.</p>
<p>Historique complet</p>	<p>La vue Historique complet de la fenêtre Historique de la sécurité affiche l'historique complet de la sécurité.</p>
<p>Résultats de l'analyse</p>	<p>Vous pouvez analyser votre ordinateur pour vérifier s'il est infecté par des virus, des spywares, des malwares ou s'il est exposé à des risques de sécurité.</p> <p>La vue Résultats de l'analyse de la fenêtre Historique de la sécurité affiche les détails des analyses que vous avez exécutées sur votre ordinateur.</p>

Risques de sécurité résolus	<p>Les risques de sécurité incluent les programmes suspects susceptibles de compromettre la sécurité de votre ordinateur.</p> <p>La vue Risques de sécurité résolus de la fenêtre Historique de la sécurité affiche une liste des risques de sécurité que votre produit Norton a détectés puis réparés, mis en quarantaine ou supprimés. Les éléments en quarantaine sont répertoriés dans la vue Quarantaine. Vous pouvez également afficher les éléments mis en quarantaine dans la vue Quarantaine.</p>
Risques de sécurité non résolus	<p>Les risques de sécurité incluent les programmes suspects susceptibles de compromettre la sécurité de votre ordinateur.</p> <p>La vue Risques de sécurité non résolus de la fenêtre Historique de la sécurité affiche une liste des risques de sécurité que votre produit Norton n'a pas pu réparer, supprimer ou mettre en quarantaine.</p> <p>Certaines menaces requièrent un redémarrage du système. Les journaux de ces menaces peuvent être supprimés uniquement après le redémarrage du système.</p>

Quarantaine

La quarantaine de l'historique de la sécurité constitue un emplacement sécurisé de l'ordinateur où les éléments peuvent être isolés en attendant que vous décidiez des mesures à prendre.

La vue **Quarantaine** de la fenêtre **Historique de la sécurité** affiche tous les risques de sécurité isolés dans la quarantaine de l'historique de la sécurité.

Activité SONAR

Symantec Online Network for Advanced Response (SONAR) identifie de nouvelles menaces sur la base du comportement suspect des applications. SONAR détecte et protège votre ordinateur contre tout code malveillant, avant même que les définitions de virus ne soient disponibles sur LiveUpdate.

La vue **Activité SONAR** de la fenêtre **Historique de la sécurité** affiche les détails sur les risques de sécurité détectés par SONAR. Cette catégorie répertorie également toute activité modifiant la configuration ou les paramètres de votre ordinateur.

L'option **Plus d'infos** de cette catégorie fournit des informations supplémentaires sur les ressources affectées par cette activité.

Pare-feu - Réseau et connexions

Le pare-feu surveille les communications entre votre ordinateur et les autres ordinateurs sur Internet.

La catégorie **Pare-feu - Réseaux et connexions** de la fenêtre **Historique de la sécurité** affiche des informations sur les réseaux auxquels votre ordinateur se connecte. Elle affiche également les actions effectuées pour approuver ou restreindre les réseaux et les ordinateurs.

Cette catégorie affiche également un historique de toutes les connexions réseau TCP/IP effectuées avec votre ordinateur. Les connexions sont consignées lors de leur fermeture.

La fenêtre **Historique de la sécurité - Détails avancés** de cette catégorie vous permet de modifier les paramètres d'approbation et de restriction pour les ordinateurs et les réseaux.

Pare-feu - Activités

Le pare-feu surveille les communications entre votre ordinateur et les autres ordinateurs sur Internet. Le pare-feu gère les règles de contrôle de l'accès Internet vers et de votre ordinateur.

La vue **Pare-feu - Activités** de la fenêtre **Historique de la sécurité** affiche les règles créées par le pare-feu. Les règles que vous créez apparaissent également dans cette vue.

La fenêtre **Historique de la sécurité - Détails avancés** pour cette catégorie affiche les règles de programme qui ont été créées. Elle vous permet aussi d'autoriser une règle de programme bloquée.

Prévention d'intrusion

La Prévention d'intrusion analyse tout le trafic réseau en provenance ou à destination de votre ordinateur à la recherche de menaces connues.

La vue **Prévention d'intrusion** de la fenêtre **Historique de la sécurité** affiche des détails au sujet des activités récentes de prévention d'intrusion.

La fenêtre **Historique de la sécurité - Détails avancés** de cette catégorie vous permet de choisir d'être averti ou non quand la prévention d'intrusion détecte une signature de **Prévention d'intrusion**.

Protection pour les réseaux sociaux

La protection pour les réseaux sociaux répertorie les menaces que votre produit Norton a détectées lors de vos activités sur des réseaux sociaux.

Ces menaces sont généralement des escroqueries que les fraudeurs en ligne utilisent pour profiter des différentes fonctions de partage des sites Web de réseaux sociaux. Votre produit Norton fournit un aperçu et une analyse de toutes les activités de menace sur les réseaux sociaux. Le rapport est basé sur des données issues du Symantec Global Intelligence Network, que les analystes Symantec utilisent pour identifier, analyser et fournir des commentaires sur les tendances émergentes dans le paysage dynamique des menaces.

Vous pouvez sélectionner une menace spécifique et cliquer sur l'option **En savoir plus** pour en savoir plus sur la manière de rester protégé contre une menace sociale particulière.

Diagnostic des téléchargements

Diagnostic des téléchargements traite tout fichier exécutable que vous téléchargez en vue d'effectuer une analyse de son niveau de fiabilité. Il vous informe des résultats du traitement en fonction des paramètres définis pour Diagnostic des téléchargements.

La vue **Diagnostic des téléchargements** de la fenêtre de **Historique de la sécurité** affiche les détails de tous les événements que Diagnostic des téléchargements traite et signale. Cette vue contient également des informations sur les actions que vous effectuez selon les données de réputation des événements.

Antispam

Norton AntiSpam vous aide à protéger votre ordinateur contre l'exposition à des messages non sollicités.

La vue **AntiSpam** de la fenêtre **Historique de la sécurité** affiche les détails des messages électroniques traités par l'antispam.

Identité

Les diverses fonctions d'Identity Safe vous aident à gérer vos identités et offrent davantage de sécurité lorsque vous effectuez des transactions en ligne.

La vue **Identité** de la fenêtre **Historique de la sécurité** affiche les définitions Antiphishing que votre produit Norton télécharge lorsque vous exécutez LiveUpdate pour obtenir les définitions de virus les plus récentes.

Protection contre les falsifications du produit Norton

La Protection contre les falsifications du produit Norton vous permet de protéger votre produit Norton contre une attaque ou une modification par des applications inconnues, suspectes ou malveillantes.

La vue **Protection contre les falsifications du produit Norton** de la fenêtre **Historique de la sécurité** affiche les détails des tentatives non autorisées de modification des processus de Symantec. Les tâches bloquées par votre produit Symantec apparaissent également dans la liste.

Alerte de performances

La fonction d'alerte de performances vous permet d'afficher, de surveiller et d'analyser l'impact des activités du système sur votre ordinateur.

La vue **Alerte de performances** de la fenêtre **Historique de la sécurité** donne des détails sur l'impact des processus exécutés sur votre ordinateur. Vous y trouverez notamment le nom du processus, les ressources utilisées, dans quelle mesure les ressources ont été utilisées et l'impact global du processus sur votre ordinateur. De plus, les journaux relatifs aux alertes de performances et aux programmes que vous avez exclus des alertes de performances figurent aussi dans la liste.

Limitation de l'utilisation réseau

L'option Limitation de l'utilisation réseau vous permet de configurer des politiques et de restreindre l'utilisation d'Internet de votre produit Norton. Vous pouvez définir la quantité de bande passante réseau utilisée par votre produit Norton.

Le vue Limitation de l'utilisation réseau, dans la fenêtre Historique de la sécurité, fournit des détails sur les actions que vous avez entreprises pour restreindre l'utilisation d'Internet du produit Norton.

Sites signalés à Symantec

Dans certains cas, vous pouvez avoir envoyé l'évaluation de certaines pages Web à Symantec.

L'affichage des **Sites signalés à Symantec** dans la **fenêtre Historique de la sécurité** affiche tous les sites Web que vous avez signalés à Symantec afin d'en vérifier l'authenticité.

Rapport d'erreur Norton

Votre produit Norton peut générer des erreurs dans certains cas. Par exemple, une erreur peut se produire quand vous exécutez LiveUpdate ou analysez un dossier. Elles incluent les erreurs de moteur, de dépassement de délai et de programme.

La vue **Rapport d'erreur Norton** de la fenêtre **Historique de la sécurité** affiche les erreurs générées par votre produit Norton.

Erreurs de courrier électronique

Les erreurs de courrier électronique incluent tout échec se produisant lorsque votre produit Norton essaie d'envoyer, de télécharger ou d'analyser un message électronique que vous envoyez ou recevez.

La vue **Erreurs de courrier électronique** dans l'historique de la sécurité affiche les détails des alertes d'erreur de courrier électronique que vous recevez lorsqu'une erreur de courrier électronique se produit. Les détails incluent l' **ID** et le **message** d'erreur. Cette vue affiche également des informations sur le sujet, l'adresse de l'expéditeur et du destinataire associées au courrier électronique de l'alerte.

**Communauté de veille
Norton**

La fonctionnalité Communauté de veille Norton vous permet de transmettre les données d'application ou de sécurité suspectes à Symantec à des fins d'analyse. Symantec étudie ces données pour identifier de nouvelles menaces.

La vue **Communauté de veille Norton** de la fenêtre **Historique de la sécurité** affiche une liste des fichiers que vous avez transmis à Symantec à des fins d'analyse. Les fichiers, à divers stades de la transmission, apparaissent également dans la liste.

Nettoyage des fichiers

La fonction Nettoyage des fichiers supprime les fichiers temporaires indésirables, y compris les restes de fichiers du navigateur Internet, les clés de recherche sur Internet et les autres fichiers temporaires.

La vue **Nettoyage des fichiers** de la fenêtre **Historique de la sécurité** affiche la liste des activités de Nettoyage des fichiers qui ont été effectuées sur votre ordinateur.

Optimisation du disque

L'optimisation du disque est un processus qui permet de rationaliser l'emplacement physique des fichiers. Les fichiers et les métadonnées sont réorganisés de manière à améliorer le temps d'accès aux données.

La vue Optimisation du disque de la fenêtre **Historique de la sécurité** affiche la liste des activités d'optimisation du disque qui ont été effectuées sur votre ordinateur.

Mode silencieux

Le Mode silencieux supprime les alertes et les notifications et suspend momentanément la majorité des activités d'arrière-plan.

La vue du **Mode silencieux** dans la fenêtre **Historique de la sécurité** affiche le récapitulatif des sessions en Mode silencieux.

Vous y trouvez les informations suivantes :

- Type de mode silencieux (Mode silencieux ou Mode discret par exemple)
- Type de programme activant le mode silencieux comme la gravure de disque ou l'exécution d'un programme en mode plein écran
- Nom du programme spécifié par l'utilisateur qui active le mode silencieux.
- Etat du mode silencieux (activé ou désactivé).

LiveUpdate

LiveUpdate permet d'obtenir les dernières mises à jour de définition et de programme pour tous les produits Symantec installés sur votre ordinateur. Ces mises à jour permettent la protection contre les nouvelles menaces.

La vue **LiveUpdate** de la fenêtre **Historique de la sécurité** affiche les détails relatifs aux activités de LiveUpdate effectuées sur votre ordinateur. Ces détails comprennent notamment la gravité, l'état et la durée des sessions de LiveUpdate sur votre ordinateur.

- 3 Cliquez sur une ligne pour afficher les détails de l'élément.
 Si vous souhaitez afficher des informations supplémentaires sur un élément, cliquez sur l'option **Plus d'options** dans le volet **Détails** ou cliquez deux fois sur la ligne souhaitée. Vous pouvez afficher les détails avancés concernant l'élément dans la fenêtre **Historique de la sécurité - Détails avancés** et prendre les mesures appropriées. Pour certaines catégories, l'option **Plus d'options** ouvre la fenêtre **Diagnostic des fichiers** qui affiche les détails à propos de l'événement sélectionné dans l'historique de la sécurité. Vous devez utiliser le lien **Options** situé dans la fenêtre **Historique de la sécurité** pour sélectionner une action que votre produit Norton doit effectuer sur un élément de ces catégories. Le lien **Options** est également disponible dans la fenêtre **Diagnostic des fichiers** pour certains éléments. Vous devez utiliser le lien **Restaurer** dans la fenêtre **Historique de la sécurité** pour restaurer un élément mis en quarantaine sélectionné à son emplacement d'origine. Le lien **Restaurer** est également disponible dans la fenêtre **Diagnostic des fichiers** pour certains éléments.

A propos de la fenêtre Diagnostic des fichiers

La fenêtre **Diagnostic des fichiers** donne des détails concernant tout fichier d'intérêt disponible sur votre ordinateur. Cette option d'analyse de fichier est disponible pour les fichiers que vous téléchargez, analysez ou utilisez pour réaliser une activité.

Vous pouvez accéder à la fenêtre **Diagnostic des fichiers** de différente manière. Par exemple, vous pouvez utiliser les différentes fenêtres d'alerte, de notification, d'analyse et de performances et le menu de raccourci des différents fichiers présents sur votre ordinateur pour ouvrir la fenêtre. L'Historique de la sécurité offre un emplacement centralisé où vous pouvez accéder aux fenêtres **Diagnostic des fichiers** de

différents événements relatifs aux Risques de sécurité, au Diagnostic des téléchargements et à la Performance.

La fenêtre Diagnostic des fichiers vous permet d'afficher des détails supplémentaires des événements appartenant à certaines des catégories suivantes dans la fenêtre **Historique de la sécurité** :

Risques de sécurité résolus	<p>Vous permet d'afficher les informations détaillées relatives aux risques de sécurité résolus de manière organisée.</p> <p>La catégorie Risques de sécurité résolus comprend les fichiers infectés que Norton Security répare, supprime ou met en quarantaine. Cette catégorie contient la plupart des risques moyens et élevés qui sont soit mis en quarantaine soit bloqués.</p> <p>La fenêtre Diagnostic des fichiers fournit des détails sur le niveau de risque, l'origine et le rapport d'activité des risques de sécurité résolus sur votre système.</p>
------------------------------------	---

Risques de sécurité non résolus

Vous permet d'afficher les informations détaillées relatives aux risques de sécurité non résolus de manière organisée.

La catégorie **Risques de sécurité non résolus** comprend les fichiers infectés pour lesquels Norton Security n'était pas capable d'intervenir. Cette catégorie comprend la plupart des risques faibles qui nécessitent votre attention et une intervention adéquate.

La fenêtre **Diagnostic des fichiers** fournit des détails sur le niveau de risque, l'origine et le rapport d'activité des risques de sécurité non résolus sur votre système.

Quarantaine

Vous permet d'afficher les informations détaillées relatives aux risques de sécurité mis en quarantaine de manière organisée.

La catégorie **Quarantaine** comprend les fichiers infectés qui sont isolés du reste de votre ordinateur pendant qu'ils attendent de votre part une intervention adéquate.

La fenêtre **Diagnostic des fichiers** fournit des détails sur le niveau de risque, l'origine et le rapport d'activité des risques de sécurité devant être mis en quarantaine sur votre système.

<p>Diagnostic des téléchargements</p>	<p>Vous permet d'afficher les détails de réputation d'un fichier que vous téléchargez.</p> <p>Vous pouvez utiliser ces détails pour définir le niveau de sécurité du fichier et ensuite décider de l'action que vous souhaitez prendre.</p>
<p>Alerte de performances</p>	<p>Vous permet d'afficher les détails de performance de n'importe quel Fichier d'intérêt disponible sur votre ordinateur.</p> <p>Les informations incluent les détails généraux, des informations sur le lignage et l'origine, l'utilisation des ressources et les actions exécutées par le fichier sur votre système.</p>

La fenêtre **Diagnostic des fichiers** fournit divers détails à propos de l'élément de l' **Historique de la sécurité**. Ces détails sont classés dans différents onglets de la fenêtre **Diagnostic des fichiers**.

A propos de la fenêtre Menace détectée

La fenêtre **Menace détectée** s'affiche chaque fois que le produit Norton détecte un risque de sécurité sur votre ordinateur. Vous pouvez utiliser cette fenêtre pour afficher des détails sur le risque et sélectionner une action à entreprendre. Il se peut que vous deviez parfois accéder à nouveau à la fenêtre **Menace détectée** pour le même risque. Dans ce cas, vous pouvez ouvrir la fenêtre à n'importe quel moment depuis l'historique de la sécurité. L'Historique de la sécurité est l'emplacement centralisé où vous pouvez accéder aux fenêtres **Menace**

détectée relatives à des risques appartenant à une des catégories suivantes :

Risques de sécurité résolus	Cette catégorie comprend les risques de sécurité ou fichiers infectés que le produit Norton a détectés puis réparés, mis en quarantaine ou supprimés.
Risques de sécurité non résolus	Cette catégorie comprend les risques de sécurité ou les fichiers infectés que le produit Norton n'a pas été en mesure de réparer, supprimer ou mettre en quarantaine.
Quarantaine	Cette catégorie comprend les éléments de risque de sécurité qui sont isolés du reste de votre ordinateur le temps que vous effectuiez l'action adéquate.

Les options d'action dans la fenêtre **Menace détectée** pour un risque varient en fonction du type de risque et de son degré de gravité. Les options suivantes sont disponibles dans cette fenêtre :

Restaurer	Remplace le risque de sécurité en quarantaine à son emplacement d'origine dans votre ordinateur
Restaurer et exclure ce fichier	Renvoie l'élément mis en quarantaine sélectionné vers son emplacement d'origine sans le réparer et exclut cet élément des détections des analyses ultérieures.

Supprimer ce fichier	Supprime le risque de sécurité de votre ordinateur et le met en quarantaine
Exclure ce programme	Exclut ce risque de sécurité des analyses futures
Supprimer de l'historique	Supprime l'élément représentant un risque de sécurité sélectionné du journal de l'Historique de la sécurité
Obtenir de l'aide	Renvoie au site Web Symantec Security Response
Transmettre à Symantec	Envoie l'élément sélectionné à Symantec

Recherche dans l'historique de la sécurité

Vous pouvez rechercher les éléments répertoriés dans l'historique de la sécurité. Vous pouvez utiliser l'option **Recherche rapide** pour trouver des éléments à l'aide d'un mot-clé ou du nom d'un risque de sécurité. Si vous souhaitez afficher tous les éléments de l'Historique de la sécurité relatifs à un certain risque pour la sécurité, vous pouvez filtrer les éléments à l'aide de la fonction **Recherche rapide**. Par exemple, si vous souhaitez afficher toutes les alertes que la fonction Auto-Protect a générées, vous pouvez saisir Auto-Protect et filtrer la liste.

Vous pouvez effacer les résultats de la recherche et retourner à la liste actuelle de l'Historique de la sécurité en cliquant sur l'icône de la croix noire (x) dans la case **Recherche rapide**.

L'option **Recherche rapide** opère uniquement sur la vue en cours. Si vous voulez que votre recherche porte

sur tous les éléments de l'historique de la sécurité, vous devez sélectionner la vue **Historique complet**.

Recherche dans l'historique de la sécurité

- 1 Dans la fenêtre **Historique de la sécurité**, saisissez le nom de l'élément à rechercher dans la zone de texte **Recherche rapide**.
- 2 Cliquez sur **OK**.

Exportation ou importation des informations de l'historique de la sécurité

Votre produit Norton vous permet également d'exporter l'historique des événements de sécurité vers un fichier. Vous pouvez exporter et enregistrer les événements de l'historique de la sécurité et les afficher à loisir.

Par exemple, vous pouvez rechercher tous les événements de sécurité pour une date particulière. Vous pouvez pour cela utiliser l'option **Recherche rapide** pour obtenir une liste de tous les éléments qui sont liés à un risque de sécurité particulier. Vous pouvez alors utiliser l'option **Exporter** pour enregistrer la liste dans le journal de l'Historique de la sécurité. Vous pouvez plus tard importer le fichier journal et analyser les données.

L'Historique de la sécurité stocke les informations dans un fichier séparé. Quand la taille du fichier atteint sa limite de taille maximale, les informations liées à de nouveaux événements écrasent les informations liées à des événements plus anciens. Vous pouvez exporter le journal périodiquement, si vous voulez garder toutes les informations de l'Historique de la sécurité.

Vous pouvez enregistrer votre fichier journal dans l'un des formats de fichier suivants :

- Fichiers journaux de l'historique de la sécurité (*.mcf)
Le format de fichier des journaux de l'Historique de la sécurité est .mcf, format propriétaire de Symantec.

Quand vous utilisez cette option de type de fichier, vous pouvez afficher le fichier dans la fenêtre **Historique de la sécurité**.

■ Fichiers texte (.txt)

Les données sont enregistrées dans une mise en forme de texte séparée par une virgule.

Quand vous utilisez cette option de type de fichier, vous pouvez afficher le fichier en externe sans la fenêtre Historique de la sécurité.

Vous pouvez uniquement importer les fichiers journaux ayant une extension de fichier .mcf. Quand vous importez un fichier journal, la liste exportée des informations de l'Historique de la sécurité du fichier journal apparaît. Cette liste remplace la liste actuelle des événements de sécurité. Vous pouvez sélectionner une option dans la liste déroulante **Afficher** pour afficher les détails spécifiques aux options enregistrées dans le fichier journal. Vous pouvez revenir sur la liste d'historique de la sécurité actuelle en cliquant sur le lien **Fermer le fichier :nom_fichier.mcf**.

Exportation des informations de l'historique de la sécurité

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Historique**.
- 2 Dans la fenêtre **Historique de la sécurité**, dans la liste déroulante **Afficher**, sélectionnez une option.
- 3 Cliquez sur **Exporter**.
- 4 Dans la boîte de dialogue **Enregistrer sous** qui apparaît, naviguez vers un emplacement et spécifiez le nom pour le fichier.
Le nom de catégorie de la liste déroulante **Afficher** apparaît comme nom de fichier par défaut. Vous pouvez donner le nom de votre choix au fichier.
- 5 Dans la boîte de dialogue **Enregistrer sous**, sélectionnez l'emplacement auquel vous souhaitez enregistrer le fichier journal.
- 6 Cliquez sur **Enregistrer**.

Importation des informations de l'historique de la sécurité

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Historique**.
- 2 Dans la fenêtre **Historique de la sécurité**, cliquez sur **Importer**.
- 3 Dans la boîte de dialogue **Ouvrir** qui apparaît, indiquez le dossier contenant le fichier que vous voulez importer.
- 4 Sélectionnez le fichier .mcf et cliquez sur **Ouvrir**. Vous pouvez seulement ouvrir des fichiers journaux au format .mcf dans la fenêtre **Historique de la sécurité**. Vous pouvez ouvrir et afficher en externe les fichiers journaux .txt sans utiliser l'Historique de la sécurité.

Dans le mode d'importation, vous ne pouvez pas apporter des modifications aux informations. Par exemple, vous ne pouvez pas effacer les journaux. Vous pouvez revenir à la liste de l'Historique de la sécurité courante en fermant le fichier.

Gestion des éléments en quarantaine

La quarantaine de l'historique de la sécurité constitue un emplacement sécurisé de l'ordinateur où les éléments peuvent être isolés en attendant que vous décidiez des mesures à prendre. Les éléments en quarantaine sont isolés du reste de l'ordinateur, de sorte qu'ils ne peuvent pas se propager ni provoquer de nouvelles infections. Dans certains cas, vous pouvez suspecter qu'un élément est infecté, même si les analyses du produit Norton ne l'ont pas détecté comme tel. Vous pouvez placer manuellement ces éléments en quarantaine.

Vous ne pouvez pas ouvrir cet élément accidentellement et propager le virus, mais vous pouvez toujours l'analyser et déterminer s'il doit être soumis à Symantec.

La quarantaine comprend les groupes d'éléments suivants :

Risques de sécurité	<p>Inclut des éléments tels que les spywares et logiciels publicitaires qui présentent généralement un risque faible et qui sont nécessaires au fonctionnement d'un autre programme.</p> <p>Vous pouvez restaurer ces éléments si nécessaire.</p>
Menaces de sécurité	<p>Inclut les virus et les autres éléments à haut risque.</p>

Plusieurs options s'offrent à vous une fois un élément placé en quarantaine. Toutes les actions concernant des éléments en quarantaine doivent être exécutées à partir de la quarantaine de l'historique de la sécurité.

Exécution d'une action sur un élément en quarantaine

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Historique**.
- 2 Dans le volet **Détails**, cliquez sur **Options**.
 Vous pouvez utiliser le lien **Plus d'options** pour afficher plus de détails concernant l'élément avant de choisir l'action qui lui sera appliquée. Le lien ouvre la fenêtre **Diagnostic des fichiers** qui contient plus d'informations sur le risque.

- 3 Dans la fenêtre **Menace détectée**, sélectionnez l'action que vous voulez effectuer. Certaines options sont les suivantes :

<p>Restaurer</p>	<p>Replaces le risque de sécurité mis en quarantaine à son emplacement d'origine sur l'ordinateur.</p> <p>Cette option est disponible uniquement pour les éléments mis en quarantaine manuellement.</p>
<p>Restaurer et exclure ce fichier</p>	<p>Renvoie l'élément mis en quarantaine sélectionné vers son emplacement d'origine sans le réparer et exclut cet élément des détections des analyses ultérieures.</p> <p>Cette option n'est disponible que pour les menaces virales et non virales détectées.</p>
<p>Supprimer de l'historique</p>	<p>Supprime l'élément sélectionné du journal de l'historique de la sécurité</p>

Transmettre à Symantec	Envoie l'élément sélectionné à Symantec pour évaluer le risque de sécurité Dans certains cas, vous pouvez suspecter l'infection d'un élément, même si le produit Norton ne l'a pas identifié comme une menace de sécurité. En de tels cas, vous pouvez utiliser cette option pour transmettre l'élément à Symantec à des fins d'analyse approfondie.
-------------------------------	---

Vous pouvez également vous rendre à cette fenêtre à l'aide du lien **Options** de la fenêtre **Diagnostic des fichiers** pour certains risques.

- 4 Suivez les instructions à l'écran.

Ajout d'éléments à la quarantaine

La quarantaine de l'historique de la sécurité constitue un emplacement sécurisé de l'ordinateur où les éléments peuvent être isolés en attendant que vous décidiez des mesures à prendre.

La vue **Quarantaine** de la fenêtre **Historique de sécurité** affiche une liste des éléments en quarantaine. Vous pouvez afficher le nom et l'état de risque de chaque élément en quarantaine.

Vous pouvez ajouter manuellement des éléments à la quarantaine de l'historique de la sécurité. Vous pouvez utiliser l'option **Ajouter un élément à la quarantaine** de la vue **Quarantaine** de l' **Historique de la sécurité** pour mettre en quarantaine les éléments dont vous suspectez l'infection. Elle n'a aucun effet sur les fichiers déjà en quarantaine.



Vous ne pouvez pas mettre un bon fichier connu ou une application Windows en quarantaine.

Ajout d'un élément à la quarantaine

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Historique**.
- 2 Dans l' **Historique de la sécurité**, vue **Quarantaine**, cliquez sur **Ajouter un élément à la quarantaine**.
- 3 Dans la boîte de dialogue **Quarantaine manuelle**, zone de texte **Description**, saisissez un nom bref pour l'élément à ajouter.
Ce texte apparaît dans la quarantaine et doit être explicite.
- 4 Cliquez sur **Parcourir**.
- 5 Dans la boîte de dialogue **Sélectionner le fichier à mettre en quarantaine**, localisez et sélectionnez l'élément à mettre en quarantaine, puis cliquez sur **Ouvrir**.
- 6 Cliquez sur **Ajouter**.
- 7 Dans la fenêtre **Historique de la sécurité**, cliquez sur **Fermer**.

Restauration d'un élément à partir de la quarantaine

Certains programmes utilisent d'autres programmes considérés comme étant des risques de sécurité. Le programme peut ne pas fonctionner si un fichier spécifique est supprimé. Tous les risques de sécurité supprimés sont automatiquement sauvegardés dans la quarantaine de l'historique de la sécurité. Si un programme utile cesse de fonctionner, le produit Norton vous permet ainsi de restaurer le programme à risque.

Par exemple, un logiciel shareware ou gratuit que vous téléchargez peut utiliser des logiciels publicitaires pour maintenir son coût à un niveau peu élevé. Dans ce cas, vous pouvez autoriser ce risque de sécurité à rester sur votre ordinateur ou le restaurer si la protection contre les spywares l'a supprimé.

Certains éléments en quarantaine sont correctement désinfectés après une nouvelle analyse du produit Norton. Vous pouvez également restaurer ce type d'éléments.



Si vous restaurez un élément dans un répertoire différent de son emplacement d'origine, il risque de ne pas fonctionner correctement. Par conséquent, il est recommandé de réinstaller le programme.

Restauration d'un élément à partir de la quarantaine

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Historique**.
- 2 Dans l' **Historique de la sécurité**, dans la vue **Quarantaine**, sélectionnez l'élément à restaurer.
- 3 Dans le volet **Détails**, cliquez sur **Options**.
- 4 Dans la fenêtre **Menace détectée**, effectuez l'une des opérations suivantes :
 - Cliquez sur **Restaurer et exclure ce fichier**.
Cette option renvoie l'élément mis en quarantaine sélectionné vers son emplacement d'origine sans le réparer et exclut cet élément des détections des analyses ultérieures.
 - Cliquez sur **Restaurer**.
Cette option renvoie l'élément sélectionné vers son emplacement d'origine sans le réparer. Cette option est disponible uniquement pour les éléments mis en quarantaine manuellement.
- 5 Dans la fenêtre **Restauration de la quarantaine**, cliquez sur **Oui**.
En cas de menaces non virales, vous pouvez utiliser l'option disponible dans cette fenêtre pour exclure le risque de sécurité. Votre produit Norton ne détecte pas les risques de sécurité exclus des analyses ultérieures.
- 6 Dans la boîte de dialogue **Parcourir**, sélectionnez le dossier ou le disque sur lequel vous souhaitez restaurer le fichier, puis cliquez sur **OK**.
- 7 Cliquez sur **Fermer**.

Transmission manuelle d'un élément à Symantec

Lorsqu'un virus ou un autre danger est détecté, il est automatiquement soumis pour analyse au site Web

Symantec Security Response. Si vous avez désactivé l'option de transmission automatique des risques, vous pouvez les transmettre manuellement à partir de la quarantaine de l'histoire de la sécurité. Vous devez disposer d'une connexion Internet pour transmettre un élément.

Lorsque vous transmettez automatiquement ou manuellement des fichiers à Symantec, vous contribuez à l'efficacité de votre produit Symantec. Par exemple, vous pouvez transmettre un élément qui n'a pas été détecté pendant l'analyse et dont vous pensez qu'il constitue un risque de sécurité. Symantec Security Response analysera le fichier. S'il est identifié comme risque de sécurité, il sera ajouté à une future mise à jour des définitions.

Les transmissions n'incluent jamais d'informations personnellement identifiables.

Dans certains cas, il est nécessaire que Symantec Security Response bloque la transmission de certains types ou volumes. Ces éléments apparaissent sous l'intitulé **Non transmis** dans l'histoire de la sécurité.

Envoi manuel d'un élément à Symantec

- 1 Dans la fenêtre principale de Norton Security, cliquez deux fois sur **Sécurité**, puis cliquez sur **Historique**.
- 2 Dans l' **Historique de la sécurité**, vue **Quarantaine**, sélectionnez l'élément à transmettre à Symantec.
- 3 Dans le volet **Détails**, cliquez sur **Options**.
- 4 Dans la fenêtre **Menace détectée**, cliquez sur **Transmettre à Symantec**.
- 5 Dans la boîte de dialogue qui apparaît, cliquez sur **OK**.

Personnalisation des fonctions de protection

10

Ce chapitre traite des sujets suivants :

- [Résumé des fonctionnalités](#)
- [A propos de la désactivation des fonctions automatiques](#)

Résumé des fonctionnalités

Les informations de cette section vous permettront de vous familiariser avec le produit.

Vous y trouvez les informations suivantes :

- une liste de toutes les fonctions du produit,
- une brève description de chaque fonction.

Le résumé des fonctionnalités peut vous aider à déterminer celle à utiliser pour résoudre un problème. Lisez les descriptions de fonction pour repérer le composant à utiliser.

Pour plus d'informations, sélectionnez l'une des sous-entrées de cette rubrique d'aide.

A propos de protection contre les virus et les risques de sécurité

Les fonctions de protection contre les virus et les risques de sécurité sont conçus pour prévenir les infections virales et détecter les risques sur votre ordinateur. Les virus connus sont automatiquement détectés et réparés.

Les pièces jointes au courrier électronique et aux messages instantanés, les téléchargements Internet et autres fichiers entrants sont analysés. En outre, les mises à jour des définitions qu'Automatic LiveUpdate télécharge lorsque votre ordinateur est connecté à Internet vous préparent à lutter contre les risques de sécurité les plus récents.

Votre ordinateur est surveillé de façon continue et protégé contre les menaces connues et inconnues grâce aux fonctions suivantes :

<p>Auto-Protect</p>	<p>Recherche des virus et d'autres risques de sécurité chaque fois que vous exécutez des programmes sur votre ordinateur. Auto-Protect vous permet de personnaliser la protection de votre ordinateur. Les options Auto-Protect sont les suivantes :</p> <ul style="list-style-type: none"> ■ Se charge en mémoire au démarrage de Windows et vous protège en permanence pendant que vous travaillez. ■ Recherche les virus et risques de sécurité chaque fois que vous exécutez des programmes sur votre ordinateur. Il recherche également les virus lorsque vous insérez des disquettes ou tout autre média amovible, accédez à Internet ou utilisez des fichiers de documents. ■ Surveille l'ordinateur pour détecter les symptômes inhabituels pouvant indiquer une menace active.
----------------------------	--

<p>LiveUpdate automatique</p>	<p>Vous prévient lorsque des mises à jour du programme sont disponibles et télécharge automatiquement les mises à jour des définitions.</p> <p>Se reporter à "A propos de Norton LiveUpdate" à la page 36.</p>
<p>Analyse de fichier compressé</p>	<p>Détecte les virus, les spywares et les autres risques de sécurité au sein des fichiers compressés au cours des analyses manuelles.</p> <p>Se reporter à "Mesures à prendre en cas de détection d'un virus" à la page 130.</p>
<p>Protection du courrier</p>	<p>Protège votre ordinateur contre les menaces présentes dans les pièces jointes à un message électronique.</p> <p>Vous pouvez utiliser les options Analyse antivirus du courrier et antispam afin de configurer votre programme de messagerie pour la protection contre des virus et autres menaces.</p>
<p>Protection heuristique</p>	<p>Détecte les virus nouveaux et inconnus en analysant la structure et le comportement du fichier exécutable. Analyse également d'autres attributs comme la logique de programmation, les instructions machine et toutes les données contenues dans le fichier.</p>

<p>Analyse rapide</p>	<p>Recherche les infections comportant des processus en cours d'exécution dans la mémoire, ainsi que les infections référencées par des dossiers et des fichiers de démarrage.</p> <p>Se reporter à "Exécution d'une analyse rapide" à la page 89.</p>
------------------------------	--

A propos de Norton Family

L'option **Norton Family** vous permet de créer votre compte Norton Family. Norton Family est une application de contrôle parental offrant une manière intelligente de protéger les activités de vos enfants sur Internet. Norton Family aide les parents à mieux comprendre ce que font leurs enfants en ligne, et ainsi à mieux les protéger et les guider.

Vous pouvez utiliser l'icône **Family** située dans la section **Plus de Norton** de la fenêtre principale pour créer votre compte Norton Family. Cette icône peut ne pas être disponible dans certaines versions de Norton Security. Dans ce cas, vous ne pouvez pas accéder aux options de Norton Family. Vous devez installer le client Norton Family sur tous les ordinateurs utilisés par vos enfants. Si vos enfants utilisent le même ordinateur, vous devez créer des comptes utilisateur pour chacun et installer le client Norton Family sur l'ordinateur.

Pour créer votre compte Norton Family, vous pouvez également utiliser le lien **Norton Family** dans le volet **Protection Web** de la fenêtre avancée de Norton Security. Symantec vous recommande d'utiliser les informations d'authentification de votre compte Norton pour vous inscrire à Norton Family.

Une fois votre compte configuré, vous pouvez définir les paramètres sur le site Web de Norton Family afin de contrôler les activités de vos enfants sur Internet. Vous pouvez vous connecter à votre compte Norton

Family à tout moment afin d'afficher leurs activités sur Internet. Vous pouvez également utiliser l'icône **Family** située dans la fenêtre principale pour vous connecter à votre compte et afficher les activités de vos enfants sur Internet.

Les fonctionnalités suivantes de Norton Family vous permettent de gérer les activités Internet de vos enfants :

- surveillance des appareils Android ;
- surveillance et blocage des sites Web ;
- application de limites de temps ;
- surveillance des réseaux sociaux ;
- surveillance des recherches ;
- application des règles de la maison.



Norton Family peut ne pas être disponible dans certaines versions de Norton Security. Dans ce cas, vous ne pouvez pas accéder aux options de Norton Family.

A propos de la désactivation des fonctions automatiques

Votre produit Symantec est configuré par défaut pour fournir une protection complète à votre ordinateur. Un grand nombre de paramètres incluent des fonctions automatiques qui offrent une protection continue. Dans certains cas, vous pouvez être amené à les désactiver pour réaliser une tâche donnée.



N'oubliez pas de réactiver la fonction automatique que vous avez désactivée une fois la tâche terminée.

Se reporter à
"Désactivation
temporaire et
réactivation
d'Auto-Protect"
à la page 351.

Se reporter à
"Désactivation ou
activation du filtrage
antispam"
à la page 352.

Désactivation temporaire et réactivation d'Auto-Protect

Si vous n'avez pas modifié les paramètres par défaut, Auto-Protect se charge au démarrage de l'ordinateur. La fonction vous protège également contre la plupart des virus, des chevaux de Troie, des vers et des autres menaces. Elle recherche les virus dans les programmes actifs et surveille toute activité de l'ordinateur. Elle recherche également sur les médias amovibles les activités susceptibles d'indiquer la présence d'un virus. Auto-Protect vous avertit lorsqu'elle détecte un virus ou une activité suspecte.

Dans certains cas, Auto-Protect peut vous signaler un virus alors que vous savez qu'il ne s'agit pas d'un virus. Si vous effectuez une activité qui génère ces symptômes et voulez éviter de recevoir l'avertissement correspondant, désactivez la protection automatique.

Si vous avez défini un mot de passe pour les paramètres, Norton Security vous le demande pour pouvoir les afficher ou les modifier.



Lorsque vous désactivez **Auto-Protect**, vous désactivez également les fonctions **Protection SONAR** et **Diagnostic des téléchargements**.

Pour désactiver Auto-Protect temporairement :

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antivirus**.

- 3 A la ligne **Auto-Protect**, faites glisser le curseur **Ac./Désac.** vers la droite sur la position **Désactivé**.
- 4 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**.
- 5 Dans la boîte de dialogue qui s'affiche, dans la liste déroulante **Sélectionner la durée**, sélectionnez la durée de désactivation de la fonction Auto-Protect, puis cliquez sur **OK**.

Activation d'Auto-Protect

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antivirus**.
- 3 A la ligne **Auto-Protect**, faites glisser le curseur **Ac./Désac.** vers la gauche sur la position **Activé**.
- 4 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**.

Désactivation ou activation du filtrage antispam

Avec l'utilisation accrue du courrier électronique, de nombreux utilisateurs reçoivent un grand nombre de messages électroniques commerciaux non sollicités ou indésirables appelés spam. Le spam complique l'identification des messages utiles et peut contenir des textes ou des images choquants.

Pour contrôler ces spam, vous pouvez utiliser le filtrage antispam. La protection antispam est activée par défaut. Si, pour une quelconque raison, vous souhaitez la désactiver, vous pouvez le faire depuis le programme lui-même.



La désactivation de Norton AntiSpam augmente l'exposition aux messages électroniques indésirables.

Désactivation du filtrage antispam

- 1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.

- 3 Dans l'onglet **Filtre**, à la ligne **Antispam**, déplacez le curseur **Ac./Désac.** vers la droite, sur la position **Désactivé**.
- 4 Cliquez sur **Appliquer**.
- 5 Dans la liste déroulante **Sélectionner la durée** de la fenêtre **Alerte de sécurité**, sélectionnez la durée pendant laquelle vous souhaitez désactiver le filtrage antispam.
- 6 Cliquez sur **OK**.
- 7 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Activation du filtrage antispam

- 1 Dans la fenêtre principale du produit Norton, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Antispam**.
- 3 Dans l'onglet **Filtre**, à la ligne **Antispam**, déplacez le curseur **Ac./Désac.** vers la droite, sur la position **Désactivé**.
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Activation ou désactivation de la fonction Communauté de veille Norton

La communauté de veille Norton permet d'identifier de nouveaux risques de sécurité grâce à la transmission à Symantec de données de sécurité et d'applications sélectionnées en vue de leur analyse. Cela permet à Symantec de fournir des solutions identifiant plus efficacement les nouvelles menaces et les nouveaux risques. Symantec évalue ces données afin de déterminer les nouvelles menaces ainsi que leurs sources. Les efforts collectifs des utilisateurs de produits de sécurité Norton permettent d'identifier rapidement des solutions à ces menaces et risques.

Vous pouvez utiliser l'option **Communauté de veille Norton** pour envoyer des informations concernant un fichier suspect à Symantec pour analyse. Symantec évalue ces données afin de déterminer les nouvelles

menaces ainsi que leurs sources. La fonction Norton Insight utilise les informations évaluées par Symantec pour détecter les menaces de sécurité.



La Communauté de veille Norton collecte et transmet les données détaillées concernant uniquement les erreurs et composants propres à Norton. Il ne collecte ou ne stocke pas les informations personnelles des utilisateurs.

La fenêtre **Historique de la sécurité** permet d'étudier les informations envoyées à Symantec.

Désactivation ou activation de la fonction Communauté de veille Norton

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Dans la fenêtre **Paramètres administratifs**, à la ligne **Communauté de veille Norton**, effectuez l'une des opérations suivantes :
 - Pour désactiver la Communauté de veille Norton, déplacez le curseur **Ac./Désac.** vers la droite sur la position **Désactivé**.
 - Pour activer la Communauté de veille Norton, déplacez le curseur **Ac./Désac.** vers la gauche sur la position **Activé**.
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Désactivation ou activation des fonctions de protection de la sécurité

Il peut parfois être utile de désactiver une fonction de protection de la sécurité. Par exemple, le Pare-feu intelligent peut perturber l'affichage d'une page Web.

La désactivation des fonctionnalités de protection réduit la sécurité de votre système. Lorsque vous désactivez une fonction, vous pouvez spécifier son délai d'inactivation. Une fois le délai expiré, la fonction est réactivée automatiquement.

Pour que votre ordinateur reste protégé, vous pouvez réactiver manuellement les fonctions de protection avant l'expiration du délai que vous avez spécifié.

Pour désactiver une fonction de protection

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Sur la ligne **Paramètres généraux**, à la ligne **Pare-feu intelligent**, déplacez le curseur **Ac./Désac.** vers la droite, sur la position **Désactivé**.
- 4 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 5 Dans la ligne **Prévention d'intrusion**, faites glisser le curseur **Ac./Désac.** vers la droite sur la position **Désactivé**.
- 6 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**.
- 7 Dans la **liste déroulante Sélectionner la durée**, sélectionnez la durée de désactivation de la fonction de protection de la sécurité, puis cliquez sur **OK**.

Pour que votre ordinateur reste protégé, vous pouvez réactiver manuellement les fonctions de protection avant l'expiration du délai que vous avez spécifié.

Pour activer une fonction de protection

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Pare-feu**.
- 3 Sur la ligne **Paramètres généraux**, à la ligne **Pare-feu intelligent**, déplacez le curseur **Ac./Désac.** vers la gauche, sur la position **Activé**.
- 4 Cliquez sur l'onglet **Protection navigateur/intrusions**.
- 5 Dans la ligne **Prévention d'intrusion**, faites glisser le curseur **Ac./Désac.** vers la gauche sur la position **Activé**.
- 6 Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**.

Personnalisation des paramètres

11

Ce chapitre traite des sujets suivants :

- [Personnalisation des paramètres de Norton Security](#)
- [Activation et désactivation des Commandes rapides](#)
- [A propos des paramètres de la protection automatique](#)
- [A propos des paramètres Analyses et risques](#)
- [A propos des paramètres Antispyware et mises à jour](#)
- [A propos des paramètres de protection contre les intrusions et de protection du navigateur](#)
- [Activation ou désactivation de la gestion à distance](#)
- [Réinitialisation du mot de passe des configurations de votre produit Norton](#)
- [Désactivation du mot de passe des paramètres du produit Norton](#)
- [Sécurisation des paramètres de votre produit Norton à l'aide d'un mot de passe](#)
- [A propos de Protection contre les falsifications du produit Norton](#)

Personnalisation des paramètres de Norton Security

Les paramètres par défaut du produit Norton permettent de protéger votre ordinateur de manière sécurisée, automatique et efficace. Cependant, si vous souhaitez modifier ou personnaliser vos paramètres de protection, vous pouvez accéder à la plupart des fonctionnalités à partir de la fenêtre **Paramètres**.

Vous pouvez configurer le produit Norton comme suit :

- Vous pouvez utiliser le commutateur **Marche/Arrêt** pour activer ou désactiver une fonction. Lorsque vous désactivez une fonction, la couleur du commutateur **Marche/Arrêt** devient rouge, ce qui indique que votre ordinateur est vulnérable aux menaces de sécurité. Lorsque vous activez une fonction, la couleur du commutateur **Marche/Arrêt** devient verte, ce qui indique que votre ordinateur est protégé contre les menaces de sécurité.
- Vous pouvez faire glisser le curseur d'une fonction de protection pour définir votre paramètre préféré. Le plus souvent, Norton Security fournit le paramètre de curseur pour que vous décidiez si Norton Security doit résoudre automatiquement les menaces de sécurité ou vous demander avant de prendre des mesures.
- Vous pouvez configurer une fonction de protection en sélectionnant les options fournies pour la configuration ou en fournissant les informations requises. La plupart de ces options sont disponibles en tant que cases à sélectionner ou à désélectionner. Vous pouvez utiliser l'option **Par défaut** pour réinitialiser la configuration sur le niveau par défaut.
- Vous pouvez sélectionner une option préférée dans la liste déroulante.
- Vous pouvez sélectionner ou désélectionner les options **Commandes rapides** pour activer ou désactiver une fonction.

Le produit Norton fournit aussi l'option **Utiliser les paramètres par défaut** dans la plupart des fenêtres **Paramètres**. Vous pouvez utiliser cette option pour réinitialiser la configuration sur le niveau par défaut.

Personnalisation des paramètres du produit Norton

- 1 Dans la fenêtre principale Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, cliquez sur la fonction de protection à personnaliser.
- 3 Dans la fenêtre qui apparaît, définissez l'option sur vos paramètres préférés.
Il peut être nécessaire de cliquer sur un onglet pour accéder aux paramètres qui y sont répertoriés.
- 4 Dans la fenêtre **Paramètres**, effectuez l'une des opérations suivantes :
 - Pour enregistrer les modifications, cliquez sur **Appliquer**.
 - Pour fermer la fenêtre sans enregistrer les modifications, cliquez sur **Fermer**.

Activation et désactivation des Commandes rapides

A partir de la fenêtre **Paramètres**, vous pouvez activer ou désactiver les services **Commandes rapides** suivants :

- **Mode silencieux**
- **Navigation sécurisée**
- **Identity Safe**
- **LiveUpdate automatique**
- **Pare-feu intelligent**
- **Protection contre les falsifications de Norton**

Il est recommandé de laisser tous les services activés à l'exception du mode silencieux.

A propos des paramètres de la protection automatique**Activation ou désactivation des commandes rapides**

- 1 Dans la fenêtre principale Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Commandes rapides**, effectuez l'une des opérations suivantes :
 - Pour activer un service, sélectionnez la case correspondante.
 - Pour désactiver un service, désélectionnez la case correspondante.Si une alerte ou un message s'affiche, sélectionnez la durée dans le menu déroulant, puis cliquez sur **OK**.

A propos des paramètres de la protection automatique

L'option **Protection au démarrage** de l'onglet **Protection automatique** assure un niveau de sécurité amélioré dès le moment où vous démarrez votre ordinateur. Cette option garantit une meilleure sécurité en exécutant tous les composants nécessaires utiles pour la protection de l'ordinateur aussitôt que vous démarrez l'ordinateur.

Les paramètres **Protection en temps réel** de l'onglet **Protection automatique** vous permettent de contrôler l'analyse et la surveillance de votre ordinateur. Ils protègent votre ordinateur en recherchant en permanence les virus et autres risques de sécurité.

Vous utilisez les options de **Protection en temps réel** pour déterminer ce qui doit être analysé et ce que recherche l'analyse. Ces paramètres assurent également une protection avancée en détectant proactivement les risques de sécurité inconnus sur votre ordinateur. Vous pouvez déterminer ce qui se produit lorsqu'un risque de sécurité ou une activité risquée est détectée.

A propos des paramètres de la protection automatique

Vous pouvez utiliser les options de **Protection en temps réel** suivants :

Auto-Protect	
--------------	--

Auto-Protect se charge en mémoire et vous protège en permanence pendant que vous travaillez. Auto-Protect recherche des virus et autres risques de sécurité chaque fois que vous exécutez des programmes sur votre ordinateur.

Il recherche également les virus lorsque vous insérez des disquettes ou tout autre média amovible, accédez à Internet ou utilisez des fichiers de documents que vous recevez ou créez. Il surveille également l'ordinateur pour détecter les symptômes inhabituels pouvant indiquer une menace active.

Pour rester protégé, activez les options suivantes :

■ **Analyse de média amovible**

Recherche les virus de secteur de démarrage à chaque accès à des médias amovibles.

Lorsque le média amovible a été analysé, il ne l'est plus avant d'être réinséré ou formaté. Si vous pensez que le média amovible est infecté par un virus d'amorce, vérifiez qu'Auto-Protect est activé pour réanalyser le média, insérez le média amovible et ouvrez-le à

A propos des paramètres de la protection automatique

partir du Poste de travail. Insérez alors le média amovible et ouvrez-le à partir du Poste de travail pour qu'Auto-Protect l'analyse de nouveau. Vous pouvez également l'analyser manuellement pour vérifier qu'il n'est pas infecté.

Protection SONAR	
------------------	--

Symantec Online Network for Advanced Response (SONAR) assure une protection en temps réel contre les menaces en détectant proactivement les risques de sécurité inconnus sur votre ordinateur.

SONAR identifie les menaces naissantes en fonction du comportement des applications. Il est plus rapide que les techniques basées sur les signatures traditionnelles de détection des menaces. SONAR détecte et protège votre ordinateur contre tout code malveillant, avant même que les définitions de virus ne soient disponibles sur LiveUpdate.

La **Protection SONAR** inclut les options suivantes :

■ **Protection de lecteur réseau**

Cette option protège les lecteurs réseau connectés à votre ordinateur. Vous pouvez activer ou désactiver la protection de vos lecteurs réseau. Les lecteurs réseau étant particulièrement sujets à l'infection, Symantec recommande de garder cette option activée.

■ **Mode avancé SONAR**

Le produit Norton vous donne le contrôle sur les

A propos des paramètres de la protection automatique

menaces à faible probabilité uniquement si cette option est activée.

■ Supprimer les risques automatiquement

Cette option permet aux menaces à faible probabilité de se comporter comme des menaces à forte probabilité lorsque le **Mode avancé SONAR** est activé. Dans ce cas, le produit Norton supprime automatiquement les menaces et vous en avertit.

■ Supprimer les risques en mon absence

Cette option permet au produit Norton de supprimer automatiquement des menaces à faible probabilité s'il n'obtient aucune réponse de votre part lorsque le **Mode avancé SONAR** est activé.

■ Afficher les notifications de blocage SONAR

Cette option vous permet d'activer ou de désactiver les notifications de blocage SONAR. Le produit Norton supprime les notifications de blocage SONAR quand vous configurez l'option **Afficher les notifications de blocage SONAR** sur **Consigner uniquement**.

Protection antimalware au démarrage	Cette fonction améliore la protection en exécutant tous les composants du produit Norton nécessaires pour bloquer les intrusions de malwares au démarrage de l'ordinateur.  Cette fonction n'est disponible que sous Windows 8.
--	---

A propos des paramètres **Analyses et risques**

Les paramètres **Analyses et risques** permettent de personnaliser les analyses que le produit Norton effectue sur votre ordinateur. Vous pouvez configurer une analyse en fonction de la signature numérique et du niveau d'approbation des fichiers de votre ordinateur. Vous pouvez définir comment le produit Norton doit se comporter lorsqu'il analyse les messages électroniques.

Vous pouvez utiliser les paramètres **Analyses et risques** suivants :

Analyses d'ordinateur	
------------------------------	--

Le produit Norton vous permet d'exécuter différents types d'analyses pour détecter et empêcher toute infection virale sur votre ordinateur. Les analyses possibles sont : l'analyse rapide, l'analyse complète du système et les analyses personnalisées. Vous pouvez utiliser les options Analyses d'ordinateur pour personnaliser les analyses que le produit Norton effectue sur votre ordinateur. Vous pouvez également spécifier l'analyse des fichiers compressés.

Les options d'Analyse d'ordinateur vous ont également permis de spécifier des analyses détectent des rootkits, d'autres éléments furtifs, cookies de suivi et des menaces de sécurité inconnues. Vos options sont :

■ **Analyse des fichiers compressés**

Analyse et répare les fichiers au sein de fichiers compressés.

Lorsque vous activez cette fonction, le produit Norton analyse et détecte les virus et autres risques de sécurité dans les fichiers des fichiers compressés et supprime les fichiers compressés.

■ **Analyse des rootkits et des éléments furtifs**

Analyse en vue de la détection des rootkits et d'autres risques de sécurité

qui pourraient se cacher sur votre ordinateur

■ **Analyse des lecteurs réseau**

Analyse les lecteurs réseau connectés à votre ordinateur.

Le produit Norton effectue une **analyse des lecteurs réseau** pendant une **analyse complète du système** et une **analyse personnalisée**. Par défaut, l'option **Analyse des lecteurs réseau** est activée. Si vous désactivez cette option, le produit Norton n'effectue pas l'analyse des lecteurs réseau.

■ **Protection heuristique**

Analyse votre ordinateur pour le protéger contre les menaces de sécurité inconnues.

Le produit Norton utilise la technologie heuristique pour vérifier les caractéristiques suspectes d'un fichier afin de le classer comme étant infecté. Cette méthode consiste à comparer les caractéristiques d'un fichier à celle d'un fichier infecté connu. Si le fichier montre des caractéristiques suspectes suffisantes, le produit Norton l'identifie comme étant infecté par une menace.

Ports protégés

■ Analyse des cookies de suivi

Analyse les petits fichiers enregistrés sur l'ordinateur et utilisés par les sites Web pour suivre vos activités.

■ Analyse complète du système

L'analyse complète du système examine l'intégralité de l'ordinateur en profondeur et recherche les virus, spywares et différentes vulnérabilités portant sur la sécurité. Vous pouvez utiliser l'option **Configurer** pour planifier l'analyse complète du système.

Les paramètres des ports protégés vous permettent de protéger les ports POP3 et SMTP de votre programme de messagerie électronique.

Vous pouvez utiliser cette option pour configurer manuellement vos ports de messagerie électronique POP3 et SMTP afin de protéger votre courrier électronique. Si les numéros de ports SMTP et POP3 fournis par votre fournisseur d'accès Internet (FAI) pour votre programme de messagerie électronique sont différents des numéros de ports SMTP et POP3 par défaut, vous devez configurer le produit Norton pour qu'il protège les ports.

Analyse antivirus du courrier

L'analyse antivirus du courrier vous protège contre les menaces envoyées ou reçues dans des pièces jointes.

Vous pouvez utiliser les valeurs de l'option Analyse antivirus du courrier pour définir comment le produit Norton doit se comporter lorsqu'il analyse les messages électroniques. Selon les options que vous choisissez, le produit Norton analyse automatiquement les messages électroniques que vous envoyez ou recevez.

Exclusions/risques faibles	
---------------------------------------	--

En utilisant cette option, vous pouvez spécifier des fichiers, dossiers ou disques à exclure des analyses du produit Norton. Les analyses, les signatures et les éléments à faible risque peuvent faire partie des exclusions.

Les options d'exclusion vous permettent également de choisir les catégories de risques que le produit Norton doit détecter. Vos options sont :

■ **Risques faibles**

Vous permet de gérer les éléments à faible risque trouvés sur votre ordinateur.

Vous pouvez sélectionner la réponse du produit Norton aux éléments de risque faible.

■ **Éléments à exclure des analyses**

Vous permet de déterminer les lecteurs, dossiers ou fichiers à exclure de l'analyse des risques.

Vous pouvez ajouter de nouveaux éléments d'exclusion ou modifier les éléments ajoutés à la liste des éléments exclus. Vous pouvez également supprimer des éléments de cette liste.

■ **Éléments à exclure de la détection des fonctions Auto-Protect, SONAR et Diagnostic des téléchargements**

Vous permet de déterminer les lecteurs, dossiers ou fichiers à exclure des analyses Auto-Protect et SONAR.

Vous pouvez ajouter les nouveaux éléments à exclure ou modifier les éléments déjà exclus. Vous pouvez également supprimer des éléments de cette liste.

■ **Signatures à exclure de toutes les détections**

Vous permet de connaître le nom des risques et de supprimer le nom d'un risque de la liste des éléments exclus

Vous pouvez également afficher l'impact du risque en fonction des performances, de la confidentialité, de la suppression et de la furtivité.

■ **Effacer tous les ID de fichiers exclus lors des analyses**

Permet de supprimer toutes les informations de réputation des fichiers exclus des analyses.

Vous pouvez utiliser l'option **Tout effacer** pour effacer les informations de réputation des fichiers exclus des analyses.

⚠ Les exclusions diminuant votre protection, utilisez-les uniquement en cas de besoin spécifique.

A propos des paramètres Antispyware et mises à jour

L'antispyware protège votre ordinateur contre les risques de sécurité qui peuvent compromettre vos informations personnelles et votre confidentialité.

Votre produit Norton protège votre ordinateur des vulnérabilités via les dernières mises à jour de programmes et de définitions. LiveUpdate automatique obtient les dernières définitions de virus via les mises à jour des définitions et protège votre ordinateur contre les nouvelles menaces de sécurité.

Vous disposez des paramètres Antispyware et mises à jour suivants :

Antispyware	Les options Antispyware vous permettent de choisir les catégories de risque que Norton Security doit détecter au cours des analyses Auto-Protect, manuelles et du courrier électronique.
--------------------	--

Mises à jour	
---------------------	--

Les mises à jour des définitions contiennent les informations qui permettent à votre produit Norton de détecter la présence d'un virus ou d'une menace de sécurité spécifique et de vous en alerter. Vous pouvez utiliser les options disponibles sous **Mises à jour** pour obtenir les dernières définitions de virus par la mise à jour des définitions et protéger votre ordinateur contre les dernières menaces de sécurité. Vos options sont :

■ **LiveUpdate automatique**

La fonction LiveUpdate automatique recherche automatiquement les mises à jour des définitions et des programmes lorsque vous êtes connecté à Internet.

■ **Appliquer les mises à jour uniquement au redémarrage**

Permet de choisir la méthode d'application des mises à jour de programme téléchargées par LiveUpdate automatique sur votre ordinateur. Certaines mises à jour de programmes nécessitent un redémarrage de l'ordinateur.

Lorsque cette option est activée, les mises à jour de programme qui nécessitent un redémarrage du système sont appliquées automatiquement au prochain redémarrage de l'ordinateur. Les mises à

A propos des paramètres de protection contre les intrusions et de protection du navigateur

	<p>jour de programme qui ne requièrent pas de redémarrage du système sont, quant à elles, appliquées instantanément. Cette option est désactivée par défaut.</p> <p>⏏ Cette fonction est disponible uniquement sous Windows 7 ou version ultérieure.</p>
--	--

A propos des paramètres de protection contre les intrusions et de protection du navigateur

La Prévention d'intrusion analyse tout le trafic entrant et sortant sur votre ordinateur et compare ces informations à un ensemble de signatures d'attaque. Une signature d'attaque contient des informations identifiant une tentative de piratage visant à exploiter une vulnérabilité connue du système d'exploitation ou d'un programme. La Prévention d'intrusion protège votre ordinateur contre les attaques Internet les plus fréquentes.

Si des informations transmises correspondent à une signature d'attaque, la Prévention d'intrusion rejette automatiquement le paquet et interrompt la connexion avec l'ordinateur à l'origine de l'envoi des données. L'ordinateur est ainsi protégé contre les attaques possibles.

Pour détecter et bloquer les activités réseau douteuses, la Prévention d'intrusion s'appuie sur une liste de signatures d'attaque. Le produit Norton exécute LiveUpdate automatiquement pour maintenir à jour la liste de signatures d'attaque. Si vous n'utilisez pas la

A propos des paramètres de protection contre les intrusions et de protection du navigateur

fonction LiveUpdate automatique, nous vous conseillons d'exécuter LiveUpdate une fois par semaine.

Le produit Norton fournit également la fonction de protection du navigateur, qui protège votre navigateur Web contre les programmes malveillants.



La fonction Protection du navigateur est disponible pour Internet Explorer 7.0 ou version ultérieure, Chrome 17.0 ou version ultérieure et pour Firefox 10.0 ou version ultérieure.

Avec l'augmentation croissante de l'utilisation d'Internet, votre navigateur peut être sujet aux attaques par des sites Web malveillants. Ces sites détectent et exploitent la vulnérabilité de votre navigateur Web pour télécharger des malwares dans votre système sans votre consentement ou à votre insu. Ces programmes malveillants sont également appelés des téléchargements non sollicités. Votre produit Norton protège votre navigateur contre les téléchargements non sollicités des sites Web malveillants.

Le paramètre **Protection navigateur/intrusions** inclut également l'option **Diagnostic des téléchargements** pour protéger votre ordinateur contre tout fichier risqué que vous téléchargez via un navigateur Web. Le diagnostic des téléchargements donne des informations sur le niveau de réputation des fichiers exécutables que vous téléchargez à l'aide du navigateur. Le diagnostic des téléchargements prend en charge uniquement les téléchargements qui utilisent le protocole HTTP, le navigateur Internet Explorer 6.0 ou ultérieur, le navigateur Chrome 10.0 ou ultérieur et le navigateur Firefox 3.6 ou ultérieur. Les détails de la réputation que le diagnostic des téléchargements fournit indiquent si le fichier téléchargé est sûr. Vous pouvez utiliser ces détails pour décider si vous voulez installer le fichier exécutable.

Activation ou désactivation de la gestion à distance

La fonction de gestion à distance permet de gérer à distance le produit Norton à l'aide de votre compte Norton et de l'application Norton Studio. Norton Studio est une application du Windows Store et ne fonctionne que sous Windows 8. L'activation de l'option **Gestion à distance** vous permet de visualiser les informations de votre produit Norton et de résoudre les problèmes de sécurité de votre appareil.

Lorsque l'option **Gestion à distance** est activée, le produit Norton envoie ces informations à votre compte Norton et à l'application Norton Studio. Lorsque cette option est désactivée, le produit Norton ne publie pas ses informations.

L'option **Gestion à distance** est désactivée par défaut.

Dans certains cas, vous êtes invité à saisir le mot de passe de votre compte Norton lors de l'activation de l'option **Gestion à distance**.

Activation de la gestion à distance

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 A la ligne **Gestion à distance**, déplacez le curseur **Ac./Désac.** vers la gauche sur la position **Activé**.
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Désactivation de la gestion à distance

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 A la ligne **Gestion à distance**, faites glisser le curseur **Ac./Désac.** vers la droite, sur la position **Désactivé**.

- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Réinitialisation du mot de passe des configurations de votre produit Norton

Si vous oubliez votre mot de passe des configurations Norton, vous pouvez le réinitialiser. Vous pouvez réinitialiser le mot de passe des configurations de votre produit Norton à l'aide de l'option **Réinitialiser le mot de passe d'accès aux paramètres** dans la fenêtre **Sélectionnez votre préférence de désinstallation**.

Pour accéder à la fenêtre **Sélectionnez votre préférence de désinstallation**, vous devez choisir de désinstaller votre produit Norton. Il n'est toutefois pas nécessaire de désinstaller le produit pour réinitialiser le mot de passe des configurations.



L'option **Réinitialiser le mot de passe d'accès aux paramètres** s'affiche dans la fenêtre **Sélectionnez votre préférence de désinstallation** uniquement lorsque l'option **Paramètres de protection par mot de passe** est activée. Pour utiliser l'option **Paramètres de protection par mot de passe**, ouvrez la fenêtre principale de votre produit Norton, puis cliquez sur **Paramètres > Paramètres administratifs > Sécurité de produit**.

Réinitialisation du mot de passe des configurations de votre produit Norton

- 1 Dans la barre des tâches Windows, effectuez l'une des opérations suivantes :
 - Sous Windows XP, Windows Vista ou Windows 7, sélectionnez **Démarrer > Panneau de configuration**.
 - Sous Windows 8, dans l'écran **Apps**, sous **Système Windows**, cliquez sur **Panneau de configuration**.

Désactivation du mot de passe des paramètres du produit Norton

- 2 Dans le **Panneau de configuration de Windows**, effectuez l'une des opérations suivantes :
 - Sous Windows XP, cliquez deux fois sur **Ajout/Suppression de programmes**.
 - Dans Windows Vista, cliquez deux fois sur **Programmes et fonctionnalités**.
 - Dans Windows 7 ou Windows 8, cliquez sur **Programmes > Programmes et fonctionnalités**.
L'option **Programmes** de Windows 7 ou Windows 8 est disponible en sélectionnant l'option **Catégorie** dans la liste déroulante **Afficher par**.
- 3 Dans la liste des programmes installés, effectuez l'une des opérations suivantes :
 - Sous Windows XP, cliquez sur **Norton Security**, puis sur **Modifier/Supprimer**.
 - Sous Windows Vista, Windows 7 ou Windows 8, cliquez sur **Norton Security**, puis sur **Désinstaller/Modifier**.
- 4 En bas de la fenêtre **Sélectionnez votre préférence de désinstallation**, cliquez sur **Réinitialiser le mot de passe des configurations**.
- 5 Dans la boîte de dialogue qui s'affiche, saisissez dans la case la clé générée de manière aléatoire qui s'affiche en regard de la case **Réinitialiser la clé de mot de passe**
- 6 Dans la case **Nouveau mot de passe**, saisissez le nouveau mot de passe.
- 7 Dans la case **Confirmer le nouveau mot de passe**, saisissez une nouvelle fois le nouveau mot de passe.
- 8 Cliquez sur **OK**.

Désactivation du mot de passe des paramètres du produit Norton

Vous pouvez protéger vos paramètres du produit Norton à l'aide d'un mot de passe en utilisant l'option **Paramètres de protection par mot de passe**. Si

Sécurisation des paramètres de votre produit Norton à l'aide d'un mot de passe

l'option **Paramètres de protection par mot de passe** est activée, vous devez saisir le mot de passe des paramètres à chaque fois que vous voulez afficher ou configurer les paramètres du produit Norton. Vous ne pouvez pas accéder aux paramètres du produit sans fournir le mot de passe.



Si vous oubliez votre mot de passe de paramètres, vous pouvez le réinitialiser à l'aide de l'option **Réinitialiser le mot de passe d'accès aux paramètres** de la fenêtre **Sélectionnez votre préférence de désinstallation**.

Vous pouvez désactiver l'option **Paramètres de protection par mot de passe** si vous n'avez pas besoin de protéger par un mot de passe les configurations du produit Norton.

Désactivation du mot de passe des paramètres du produit Norton

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Dans la boîte de dialogue qui apparaît, saisissez votre mot de passe des configurations dans la case **Mot de passe**, puis cliquez sur **OK**.
- 4 Sous **Sécurité du produit**, à la ligne **Paramètres de protection par mot de passe**, mettez le commutateur **Marche/Arrêt** sur la droite à la position **Arrêt**.
- 5 Cliquez sur **Appliquer**, puis sur **Fermer**.

Sécurisation des paramètres de votre produit Norton à l'aide d'un mot de passe

Vous pouvez sécuriser les paramètres de votre produit Norton contre les accès non autorisés en définissant un mot de passe. L'option **Paramètres de protection par mot de passe** de la fenêtre **Paramètres administratifs**

Sécurisation des paramètres de votre produit Norton à l'aide d'un mot de passe

vous permet de sécuriser les configurations de votre produit Norton à l'aide d'un mot de passe.

Une fois que vous avez configuré un mot de passe pour les paramètres du produit Norton, vous devez saisir le mot de passe à chaque fois que vous affichez ou configurez les paramètres du produit.

Par défaut, l'option **Paramètres de protection par mot de passe** est désactivée. Vous devez activer l'option **Paramètres de protection par mot de passe** pour définir un mot de passe permettant d'accéder à vos configurations.



Le mot de passe doit être constitué de 8 à 256 caractères de longueur.

Sécurisation des paramètres de votre produit Norton à l'aide d'un mot de passe

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Sécurité de produit**, à la ligne **Paramètres de protection par mot de passe**, mettez le commutateur **Marche/Arrêt** sur la gauche à la position **Marche**.
- 4 Effectuez l'une des opérations suivantes :
 - A la ligne **Paramètres de protection par mot de passe**, cliquez sur **Configurer**.
 - Dans la fenêtre **Paramètres**, cliquez sur **Appliquer**.
- 5 Dans la boîte de dialogue qui apparaît, saisissez un mot de passe dans la case **Mot de passe**.
- 6 Dans la case **Confirmer le mot de passe**, saisissez à nouveau le mot de passe.
- 7 Cliquez sur **OK**.
- 8 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

A propos de Protection contre les falsifications du produit Norton

L'option Protection contre les falsifications du produit Norton permet d'éviter que des programmes extérieurs effectuent des modifications sur le produit Norton. Cette fonction de sécurité permet aussi d'éviter que la restauration de système de Windows ne modifie des fichiers Norton, donnant lieu au message **Restauration incomplète**.

L'option Protection contre les falsifications du produit Norton protège Norton Security contre les attaques ou modifications par des virus ou d'autres menaces inconnues. Vous pouvez protéger le produit contre des modifications ou des suppressions accidentelles en maintenant l'option **Protection contre les falsifications du produit Norton** activée.

Si vous souhaitez désactiver temporairement l'option **Protection contre les falsifications du produit Norton**, vous pouvez le faire pour une durée spécifiée.



Vous ne pouvez pas exécuter de restauration de système sur votre ordinateur quand l'option **Protection contre les falsifications du produit Norton** est activée. Vous devez désactiver temporairement l'option **Protection contre les falsifications du produit Norton** pour exécuter correctement une restauration de système.

Activation ou désactivation de l'option Protection contre les falsifications du produit Norton

L'option Protection contre les falsifications du produit Norton protège les fichiers du produit Norton contre les attaques ou modifications par des virus ou d'autres menaces inconnues. Vous pouvez protéger le produit contre des modifications ou des suppressions accidentelles en maintenant l'option **Protection contre les falsifications du produit Norton** activée.

Si vous souhaitez désactiver temporairement l'option **Protection contre les falsifications du produit Norton**, vous pouvez le faire pour une durée spécifiée.



Vous ne pouvez pas exécuter de restauration de système sur votre ordinateur quand l'option **Protection contre les falsifications du produit Norton** est activée. Vous devez désactiver temporairement l'option **Protection contre les falsifications du produit Norton** pour exécuter correctement une restauration de système.

Désactivation de l'option Protection contre les falsifications du produit Norton

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Sous **Sécurité de produit**, à la ligne **Protection contre les falsifications du produit Norton**, mettez le commutateur **Ac./Désac.** sur la droite à la position **Désactivé**.
- 3 Cliquez sur **Appliquer**.
- 4 Dans la boîte de dialogue **Alerte de sécurité** de la liste déroulante **Sélectionner la durée**, sélectionnez pendant combien de temps vous souhaitez désactiver l'option Protection contre les falsifications du produit Norton.
- 5 Cliquez sur **OK**.
- 6 Dans la fenêtre **Paramètres**, cliquez sur **Fermer**.

Activation de l'option Protection contre les falsifications du produit Norton

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Paramètres**.
- 2 Dans la fenêtre **Paramètres**, sous **Paramètres détaillés**, cliquez sur **Paramètres administratifs**.
- 3 Sous **Sécurité du produit**, à la ligne **Protection contre les falsifications du produit Norton**, mettez le commutateur **Marche/Arrêt** sur la gauche à la position **Marche**.
- 4 Cliquez sur **Appliquer**, puis sur **Fermer**.

Ce chapitre traite des sujets suivants :

- Recherche du numéro de version de votre produit
- Accès au contrat de licence d'utilisateur final
- A propos de la mise à niveau de votre produit
- Résolutions des problèmes avec Norton Autofix
- Raisons expliquant l'échec de l'option Corriger
- A propos du support
- Désinstallation de votre produit Norton

Recherche du numéro de version de votre produit

Si vous souhaitez mettre à niveau votre produit Norton ou contacter le support clientèle pour obtenir de l'aide, vous devez connaître le numéro de version complet du produit Norton installé sur votre ordinateur. Cela assure d'obtenir la solution adaptée à vos problèmes.

Recherche du numéro de version de votre produit

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Aide**.

- 2 Dans le menu déroulant **Aide**, cliquez sur **A propos de**.
Vous pouvez voir le numéro de version de votre produit dans la fenêtre qui s'affiche.

Accès au contrat de licence d'utilisateur final

Un contrat de licence d'utilisateur est un document juridique que vous acceptez en installant le produit. Il contient des informations sur la restriction du partage ou de l'utilisation du logiciel, ainsi que les droits de l'utilisateur sur le logiciel, et d'autres conditions générales.

Pour en savoir plus sur les contrats de licence produit et les avis de tiers, rendez-vous sur la page CLUF.

Accès au contrat de licence d'utilisateur final

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Aide**.
- 2 Dans le menu déroulant **Aide**, cliquez sur **A propos de**, puis cliquez sur **Contrat de licence utilisateur**.
- 3 Lisez le contrat de licence Norton et cliquez sur **Fermer**.

A propos de la mise à niveau de votre produit

Norton Security vous aide à mettre votre produit à niveau si votre abonnement est actif. Vous pouvez mettre à niveau votre produit actuel à la version la plus récente gratuitement tant que l'abonnement de votre produit actuel est actif. Si une nouvelle version de votre produit est disponible, Norton Security permet de télécharger la nouvelle version.

L'option **Télécharger automatiquement la nouvelle version** télécharge automatiquement la dernière version

de Norton Security disponible et vous invite à l'installer gratuitement. Pour obtenir la dernière version de Norton Security dès sa publication par Symantec, vous devez activer l'option **Télécharger automatiquement la nouvelle version**. Pour activer l'option **Télécharger automatiquement la nouvelle version**, accédez à la fenêtre principale de Norton Security, puis cliquez sur **Paramètres > Paramètres administratifs > Télécharger automatiquement la nouvelle version > Activé**.

Si vous choisissez d'installer la version la plus récente du produit, Norton Security télécharge la version la plus récente et l'installe automatiquement. Assurez-vous d'avoir correctement enregistré toutes vos données importantes, telles que vos photos et données financières, avant d'installer la nouvelle version du produit.

Si vous téléchargez et installez la dernière version de votre produit, l'état de votre abonnement reste le même que la version précédente du produit. Par exemple, vous disposez de 200 jours d'abonnement restants avec votre version actuelle du produit et vous mettez à jour votre produit. Dans ce cas, l'état de l'abonnement de votre produit mis à jour reste de 200 jours.

Si aucune nouvelle version n'est disponible, la page Web vous en informe et vous confirme que votre produit est à jour. Symantec vous recommande d'avoir la dernière version du produit, car elle contient de nouvelles fonctionnalités améliorées offrant une meilleure protection contre les menaces de sécurité.

La mise à niveau du produit est différente des mises à jour de protection effectuées par LiveUpdate. Les principales différences sont les suivantes :

- La mise à jour du produit permet de télécharger et d'installer une nouvelle version du produit complet.
- Les mises à jour de protection sont des fichiers destinés à maintenir Norton Security à jour avec les technologies de protection contre les menaces les plus récentes.

Si une nouvelle version du produit n'est pas disponible, assurez-vous de disposer de toutes les mises à jour de protection les plus récentes. LiveUpdate automatise l'obtention et l'installation des mises à jour de protection. Vous pouvez exécuter LiveUpdate ou activer LiveUpdate automatique pour obtenir les dernières mises à jour.

Le processus de mise à jour risque de ne pas fonctionner si votre navigateur ne peut pas communiquer avec les serveurs Symantec. Les navigateurs pris en charge sont Internet Explorer 6.0 ou version ultérieure, Chrome 10.0 ou version ultérieure et Firefox 3.6 ou version ultérieure.



Votre produit doit être activé et vous devez disposer d'une connexion Internet pour vérifier et installer la nouvelle version du produit.

Recherche de la nouvelle version du produit

Vous pouvez mettre à jour votre produit si votre abonnement est actif. Si une nouvelle version est mise à disposition par Symantec, vous pouvez télécharger et installer la nouvelle version de votre produit. Vous pouvez également autoriser Norton Security à vous avertir lorsqu'une nouvelle version du produit est disponible. Pour ce faire, activez l'option **Télécharger automatiquement la nouvelle version** dans la fenêtre **Paramètres administratifs**. La version la plus récente de votre produit peut contenir des fonctionnalités nouvelles et améliorées afin d'offrir une meilleure protection contre les menaces de sécurité.

Lorsque vous vérifiez s'il existe une nouvelle version, les informations de votre produit, tels que le nom du produit et la version sont envoyés aux serveurs Symantec. Les serveurs vérifient si une nouvelle version du produit précisé est disponible ou non.

Si une nouvelle version est disponible, vous pouvez la télécharger et l'installer à partir de la page Web. Si aucune nouvelle version n'est disponible, la page Web vous l'indique. Dans ce cas, vous pouvez exécuter LiveUpdate afin d'obtenir les dernières mises à jour des

définitions et des programmes, ainsi que de conserver la version existante de votre produit à jour.

Le processus de mise à jour risque de ne pas fonctionner si votre navigateur ne peut pas communiquer avec les serveurs Symantec. Les navigateurs pris en charge sont Internet Explorer 6.0 ou version ultérieure, Chrome 10.0 ou version ultérieure et Firefox 3.6 ou version ultérieure.



Votre produit doit être activé et vous devez disposer d'une connexion Internet pour rechercher et installer la nouvelle version du produit.

Recherche d'une nouvelle version du produit

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Aide**.
- 2 Dans le menu déroulant **Aide**, cliquez sur **Dernière version**.
La site Web indique si une nouvelle version est disponible ou non.



Cette option est uniquement disponible si vous disposez d'un abonnement ou d'un service actif.

- 3 Si une nouvelle version est disponible, suivez les instructions à l'écran pour télécharger le nouveau produit.

Résolutions des problèmes avec Norton Autofix



Votre appareil doit être connecté à Internet pour résoudre les problèmes liés à l'utilisation de Norton Autofix.

Norton Autofix fournit un support supplémentaire au produit par un simple clic dans la fenêtre principale de Norton Security. Le logiciel effectue une analyse rapide de votre ordinateur et répare les problèmes sans aucune intervention de votre part. Si le problème persiste, utilisez l'option **Ouvrir le site Web du support**

technique pour accéder au site Web du support Norton et obtenir une aide par téléphone, courrier électronique, chat ou sur le forum.

De plus, le site Web de support Norton vous permet d'accéder aux articles de la base de connaissances. Ces articles peuvent vous aider à résoudre vos problèmes techniques.

Les techniciens du support technique peuvent vous aider à résoudre des problèmes plus complexes par le biais de l'assistance à distance. La technologie d'assistance à distance permet aux techniciens du support technique de Symantec d'avoir accès à votre ordinateur en tant qu'utilisateurs à distance afin de pouvoir effectuer la maintenance ou l'entretien.



Les offres d'assistance technique peuvent varier en fonction de la langue ou du produit.

Lorsque vous cliquez sur l'option **Support technique** dans le menu déroulant **Aide**, Norton Security vérifie votre connexion Internet. Pour avoir accès à Norton Autofix, vérifiez que votre ordinateur est connecté à Internet. Si vous passez par un serveur proxy pour vous connecter à Internet, vous devez configurer les paramètres de proxy de Norton Security. Pour plus d'informations, se reporter à "[Configuration des paramètres de proxy réseau](#)" à la page 43.

Si vous ne connaissez pas vos paramètres proxy, contactez votre fournisseur d'accès Internet ou administrateur réseau pour obtenir de l'aide.

Résolution des problèmes avec Norton Autofix

- 1 Dans la fenêtre principale de Norton Security, cliquez sur **Aide**.
- 2 Dans le menu déroulant Aide, cliquez sur **Support technique**.

- 3 Dans la fenêtre Norton Autofix, effectuez l'une des opérations suivantes :
 - Si vous rencontrez un problème de connexion à Internet, assurez-vous que votre appareil est connecté, puis cliquez sur **Réessayer** pour terminer le processus Autofix.
 - Si vous rencontrez toujours des problèmes de connexion à Internet, cliquez sur **Ignorer** pour continuer et passer aux autres processus Norton Autofix.
 - Si le problème n'a pas été réparé automatiquement, cliquez sur **Ouvrir le site Web du support technique** pour obtenir une aide supplémentaire.
 - Si vous ne parvenez pas à vous connecter au site Web de support technique, utilisez le lien **cliquez ici** pour obtenir les numéros des contacts du support.
 - Si le problème a été réparé, cliquez sur **Fermer**.

Raisons expliquant l'échec de l'option Corriger

Votre produit Norton fonctionne en mode silencieux en arrière-plan pour vous protéger contre tous types de menaces de sécurité. Si Norton détecte des problèmes importants susceptibles de bloquer votre protection ou de réduire les performances du système, il exécute une tâche Corriger.

Il arrive que cette tâche échoue.

Voici les raisons à l'origine d'un échec de la tâche Corriger et des moyens d'y remédier :

- **Expiration de l'abonnement**

Vérifiez que votre abonnement est actif. Pour vérifier votre abonnement, accédez à la fenêtre principale et cliquez sur **Aide**, puis sur **Etat de l'abonnement**.
- **Lenteur de la connexion Internet**

Votre produit récupère des mises à jour sur les serveurs Symantec. Si votre connexion Internet est lente, les mises à jour nécessaires à la résolution des problèmes détectés par votre produit ne peuvent pas être téléchargées. Vérifiez que votre connexion bénéficie d'une vitesse suffisante pour pouvoir télécharger toutes les définitions de virus.

■ **Ordinateur complètement infecté**

Si votre ordinateur est gravement infecté et que le produit ne possède pas suffisamment de mises à jour pour le débarrasser des virus, la tâche **Corriger** peut échouer. Exécutez **Norton Power Eraser** pour nettoyer votre ordinateur. Pour obtenir des instructions, se reporter à "[Analyse de l'ordinateur à l'aide de Norton Power Eraser](#)" à la page 105.

■ **Suppression partielle des menaces**

Lorsque les menaces sont supprimées, le produit Norton vous invite à redémarrer votre ordinateur. Si vous ignorez l'étape de redémarrage, la tâche **Corriger** peut échouer à un stade ultérieur lorsque vous l'exécutez.

■ **Mises à jour de protection obsolètes**

Dans certains cas, il est possible que vous ne disposiez pas des dernières mises à jour de protection si vous avez effectué une mise à niveau vers la dernière version du produit. Exécutez **LiveUpdate** à plusieurs reprises pour bénéficier des dernières mises à jour de la protection. Pour obtenir des instructions, se reporter à "[Exécution manuelle de Norton LiveUpdate](#)" à la page 40.

■ **Echec de LiveUpdate**

Si **LiveUpdate** échoue, la tâche **Corriger** échoue également. Pour résoudre les problèmes courants associés à **LiveUpdate**,

■ **Absence de connexion Internet**

Vérifiez que l'appareil est connecté à Internet. Vérifiez que les paramètres de contrôle parental et les paramètres de proxy ne bloquent pas votre connexion.

■ **La limitation de l'utilisation réseau est définie sur Economie ou Aucun trafic**

Si l'option Limitation de l'utilisation réseau est définie sur le mode **Economie** ou **Aucun trafic**, votre ordinateur ne peut pas obtenir les dernières mises à jour. Pour modifier ce paramètre, Se reporter à "[Définir l'utilisation de bande passante de Norton Security](#)" à la page 225.

■ **Le pare-feu bloque le trafic**

Vérifiez que les paramètres de pare-feu de votre produit autorisent le trafic. Pour plus d'informations, Se reporter à "[Désactivation ou activation du pare-feu intelligent](#)" à la page 151.

■ **La date et l'heure sont incorrectes**

Si la date et l'heure de votre ordinateur ont été modifiées manuellement ou sont incorrectes, la tâche **Corriger** peut échouer. Vérifiez que la date et l'heure sont correctes.

■ **Espace insuffisant sur l'ordinateur**

Si la quantité d'espace libre sur le disque ne permet pas d'installer les mises à jour, la tâche **Corriger** peut échouer. Libérez de l'espace sur le disque et exécutez **LiveUpdate**. Pour plus d'informations, Se reporter à "[Exécution manuelle de Norton LiveUpdate](#)" à la page 40.

A propos du support

Si vous avez acheté Norton Security, vous pouvez accéder au support à partir du produit.



Les offres de support peuvent varier selon la langue ou le produit.

A propos du support Norton

Le site Web de Support Norton offre une gamme complète d'options d'aide autonome. Vous pouvez accéder au support Norton à partir du produit.

A l'aide du site Web de support Norton, vous pouvez effectuer les actions suivantes :

- Trouver de l'aide à propos du téléchargement du produit, de l'abonnement au produit, de l'activation et de l'installation du produit et d'autres thèmes encore.
- Télécharger d'anciens manuels du produit.
- Gérer vos produits et services à l'aide de votre compte Norton.
- Effectuer une recherche sur Norton Forum pour trouver de l'aide supplémentaire pour l'installation, la configuration et le dépannage du produit. Vous pouvez publier vos questions sur le forum et recevoir des réponses d'autres utilisateurs et d'experts. Le forum est l'endroit idéal pour partager des astuces, des idées et faire des suggestions au sujet du produit Norton. Vous devez au préalable vous inscrire à Norton Forum pour pouvoir publier vos questions.
- Trouver des informations sur les derniers virus et risques et des astuces vous permettant de rester protégé.
- Accéder à la boutique en ligne Norton et à la page de téléchargement des produits Norton.



Les offres de support peuvent varier selon la zone géographique, la langue ou le produit.

Pour en savoir plus sur les offres de support, consultez la page Politique de support.

Outre les options d'aide sans assistance, vous pouvez utiliser l'option **Nous contacter** située en haut de la

page Web, pour entrer en contact avec l'équipe de support technique de la manière suivante :

Live Chat	Dialogue en temps réel avec un agent de support. Pour des problèmes techniques plus complexes, vous pouvez autoriser via chat un agent de support à se connecter à distance à votre ordinateur pour résoudre votre problème.
Téléphone	Parlez à un agent de support en temps réel.
Forums Norton	Trouvez de l'aide supplémentaire sur l'installation et la configuration du produit et sur les erreurs de dépannage.

A propos de la conservation de votre abonnement actuel

La durée de la période d'abonnement varie pour chaque produit Norton. Pour maintenir une protection ininterrompue, vous devez maintenir votre abonnement actif. Si votre abonnement expire, vous ne pouvez plus obtenir de mise à jour, quelle qu'elle soit, et votre logiciel ne fonctionne plus.

Vous pouvez utiliser le service de renouvellement automatique Norton pour obtenir une protection ininterrompue en renouvelant automatiquement votre abonnement au prix d'abonnement ordinaire. Pour plus d'informations sur ce service, accédez à la page de FAQ sur le service de renouvellement automatique Norton.

Lorsque vous renouvelez votre abonnement, des mises à jour de la protection et des nouvelles fonctions sont disponibles pendant la période d'abonnement. Veuillez noter que des fonctionnalités peuvent être ajoutées, modifiées ou supprimées pendant cette période.

Vous pouvez en savoir plus sur votre abonnement en visitant le site Web des comptes Norton. Pour accéder à votre compte Norton, dans la fenêtre principale de Norton Security, cliquez sur **Aide > Compte**.

Pour en savoir plus sur les différentes offres de Norton, rendez-vous à l'adresse <http://us.norton.com/comparaison/promo>.

Désinstallation de votre produit Norton

Vous pouvez supprimer votre produit Norton de votre ordinateur des manières suivantes :

- A partir du **Panneau de configuration** de Windows.
- A partir du menu **Démarrer**.
- A partir de l' **écran d'accueil** de Windows 8.



Avant de poursuivre la désinstallation, imprimez la rubrique d'aide Désinstallation de votre produit Norton. Vous ne pourrez pas accéder à l'aide en ligne pendant la désinstallation.

Si vous souhaitez réinstaller votre produit Norton, vous devez le désinstaller de votre ordinateur. Vous pouvez réinstaller votre produit à l'aide du fichier d'installation téléchargé à partir du site Web de Norton. Pour réinstaller votre produit Norton, consultez la page Téléchargement et installation de mon produit Norton sur mon appareil.

Lorsque vous le désinstallez, votre produit Norton vous autorise à utiliser gratuitement Norton Identity Safe pour effectuer des recherches et naviguer sur Internet en toute sécurité, même une fois le produit désinstallé. Vous pouvez choisir de conserver Norton Identity Safe qui offre gratuitement les fonctions Norton Safe Search

et Norton Safe Web. Norton Safe Search fournit, pour chaque résultat, l'état de sécurité du site ainsi que l'évaluation Norton. Norton Safe Web analyse les niveaux de sécurité des sites Web que vous visitez et vous indique si ces sites sont sûrs.



L'ordinateur doit être connecté à Internet pour que cette option soit disponible. Norton Security ne vous autorise pas à laisser la barre d'outils Norton installée si vous mettez à niveau le produit vers la version la plus récente ou décidez de réinstaller un autre produit Norton.

Désinstallation de votre produit Norton à l'aide du Panneau de configuration Windows

- 1 Effectuez l'une des opérations suivantes :
 - Dans la barre des tâches de Windows, cliquez sur **Démarrer > Panneau de configuration**.
 - Sous Windows 8, accédez à **Apps**, puis, sous **Système Windows**, cliquez sur **Panneau de configuration**.
- 2 Dans le **Panneau de configuration** de Windows, effectuez l'une des opérations suivantes :
 - Sous Windows XP, cliquez deux fois sur **Ajout/Suppression de programmes**.
 - Dans Windows Vista, cliquez deux fois sur **Programmes et fonctionnalités**.
 - Sous Windows 7 ou version ultérieure, cliquez sur **Programmes > Programmes et fonctionnalités**.

L'option **Programmes** sous Windows 7 ou version ultérieure est disponible si vous sélectionnez l'option **Catégorie** dans la liste déroulante **Afficher par**.

- 3 Dans la liste des programmes installés, effectuez l'une des opérations suivantes :
 - Sous Windows XP, cliquez sur **Norton Security**, puis sur **Modifier/Supprimer**.
 - Sous Windows Vista, Windows 7 ou Windows 8, cliquez sur **Norton Security**, puis sur **Désinstaller/Modifier**.
- 4 Dans la page qui s'affiche, sous **Sélectionnez vos préférences de désinstallation**, cliquez sur l'une des options suivantes :

<p>Je souhaite réinstaller un produit Norton. Merci de conserver mes paramètres.</p>	<p>Permet de conserver vos paramètres, mots de passe et préférences pour les fonctions Norton avant de désinstaller votre produit Norton.</p> <p>Sélectionnez cette option si vous souhaitez réinstaller votre produit Norton ou un autre produit Norton.</p>
<p>Merci de supprimer toutes les données utilisateur.</p>	<p>Permet de supprimer complètement votre produit Norton sans enregistrer vos paramètres, mots de passe et préférences.</p>

- 5 Si votre produit Norton propose d'installer la barre d'outils Norton après la désinstallation, procédez de l'une des manières suivantes :
 - Pour conserver la barre d'outils Norton après la désinstallation, cliquez sur **Conserver et continuer**.
 - Pour désinstaller votre produit Norton sans conserver la barre d'outils Norton, cliquez sur **Non, merci**.
- 6 Pour désinstaller votre produit Norton, cliquez sur **Suivant**.

- 7 Effectuez l'une des opérations suivantes :
- Cliquez sur **Redémarrer maintenant** (recommandé) pour redémarrer votre ordinateur.
 - Cliquez sur **Redémarrer ultérieurement** pour redémarrer l'ordinateur ultérieurement.
- Norton Security n'est complètement désinstallé qu'après avoir redémarré l'ordinateur.

Désinstallation de votre produit Norton à partir du menu Démarrer

- 1 Dans la barre des tâches de Windows, cliquez sur **Démarrer > Tous les programmes > Norton Security > Désinstaller Norton Security**.
- 2 Dans la page qui s'affiche, sous **Sélectionnez vos préférences de désinstallation**, cliquez sur l'une des options suivantes :

<p>Je souhaite réinstaller un produit Norton. Merci de conserver mes paramètres.</p>	<p>Permet de conserver vos paramètres, mots de passe et préférences pour les fonctions Norton avant de désinstaller votre produit Norton.</p> <p>Sélectionnez cette option si vous souhaitez réinstaller votre produit Norton ou un autre produit Norton.</p>
<p>Merci de supprimer toutes les données utilisateur.</p>	<p>Permet de supprimer complètement votre produit Norton sans enregistrer vos paramètres, mots de passe et préférences.</p>

- 3 Si votre produit Norton propose d'installer la barre d'outils Norton après la désinstallation, procédez de l'une des manières suivantes :
 - Pour conserver la barre d'outils Norton après la désinstallation, cliquez sur **Conserver et continuer**.
 - Pour désinstaller votre produit Norton sans conserver la barre d'outils Norton, cliquez sur **Non, merci**.
- 4 Pour désinstaller votre produit Norton, cliquez sur **Suivant**.
- 5 Effectuez l'une des opérations suivantes :
 - Cliquez sur **Redémarrer maintenant** (recommandé) pour redémarrer votre ordinateur.
 - Cliquez sur **Redémarrer ultérieurement** pour redémarrer l'ordinateur ultérieurement.

Norton Security n'est complètement désinstallé qu'après avoir redémarré l'ordinateur.

Désinstallation de votre produit Norton à partir de l'écran d'accueil de Windows 8

- 1 Sur l' **écran d'accueil**, cliquez avec le bouton droit de la souris sur **Norton Security**, puis sur **Désinstaller**.
- 2 Dans la liste des programmes actuellement installés, cliquez sur **Norton Security**, puis sur **Désinstaller/Modifier**.

- 3 Dans la page qui s'affiche, sous **Sélectionnez vos préférences de désinstallation**, cliquez sur l'une des options suivantes :

<p>Je souhaite réinstaller un produit Norton. Merci de conserver mes paramètres.</p>	<p>Permet de conserver vos paramètres, mots de passe et préférences pour les fonctions Norton avant de désinstaller votre produit Norton.</p> <p>Sélectionnez cette option si vous souhaitez réinstaller votre produit Norton ou un autre produit Norton.</p>
<p>Merci de supprimer toutes les données utilisateur.</p>	<p>Permet de supprimer complètement votre produit Norton sans enregistrer vos paramètres, mots de passe et préférences.</p>

- 4 Si votre produit Norton propose d'installer la barre d'outils Norton après la désinstallation, procédez de l'une des manières suivantes :
- Pour conserver Norton Identity Safe après la désinstallation, cliquez sur **Conserver et continuer**.
 - Pour désinstaller votre produit Norton sans conserver Norton Identity Safe, cliquez sur **Non, merci**.
- 5 Pour désinstaller votre produit Norton, cliquez sur **Suivant**.
- 6 Effectuez l'une des opérations suivantes :
- Cliquez sur **Redémarrer maintenant** (recommandé) pour redémarrer votre ordinateur.
 - Cliquez sur **Redémarrer ultérieurement** pour redémarrer l'ordinateur ultérieurement.
- Votre produit Norton n'est complètement désinstallé qu'après le redémarrage de l'ordinateur.

Index

A

- abonnement
 - conservation 397
- accès aux analyses de Norton Security
 - Analyse de l'ordinateur 85
 - Analyse de réputation 85
 - analyse Facebook 85
- activation
 - dépannage 12
 - problèmes 12
 - utilisation d'une licence ou d'une clé 8
- activités système
 - affichage des détails 50
- adresses
 - ajout aux Autorisés 214
 - ajout aux Bloqués 216
 - importer les Autorisés 214
- alerte
 - recherche 336
- alerte de performances
 - exclusion de programmes 58
- Alertes
 - historique de la sécurité 309
 - performances 51
- alertes
 - blocage des vers 138
 - alertes de performances
 - configuration du profil de ressource faible 57
 - configurer le seuil 55
 - désactivation et activation 53
 - suppression des programmes de la liste d'exclusions 59
- Analyse
 - Analyse de l'ordinateur 86
- analyse
 - analyses de sécurité et de performances 145
 - risque de sécurité détecté 130
- analysé
 - nombre total d'éléments analysés 90
- analyse à l'invite de commande
 - analyse depuis la ligne de commande 103
- Analyse complète du système
 - planification 100
- analyse complète du système
 - exécution d'une analyse 88
- Analyse de la Prévention d'intrusion
 - purge des périphériques 199
 - suppression des périphériques 199
- Analyse de Norton Security
 - analyse depuis la ligne de commande 103

- analyse de Norton Security
 - diagnostic des fichiers 331
- analyse de performances
 - planification 145
- analyse de prévention d'intrusion
 - liste d'exclusions 198
- analyse de sécurité
 - planification 145
- Analyse du mur Facebook
 - à propos 106
- analyse du mur Facebook
 - activation 109
- Analyse Norton Security
 - Analyse complète du système 88
 - Analyse de réputation 82
 - Analyse en période d'inactivité 82
 - Analyse réseau détaillée 82
 - Analyser l'ordinateur 82
- analyse Norton Security
 - à propos 82
 - accès aux analyses de Norton Security 85
 - analyse Facebook 82
 - Analyse rapide 89
- analyse planifiée
 - modification 102
- Analyse rapide
 - exécution d'une analyse 89
 - exécution d'une analyse rapide du réseau Insight 89
 - planification 101
- Analyse terminée
 - affichage après une analyse 141
- analyser
 - éléments individuels 89
 - ordinateur entier 88
- Analyses
 - Analyse complète du système 86
 - Analyse personnalisée 86
 - Analyse rapide 86
 - exécution d'analyses personnalisées 96
 - historique de la sécurité 309
 - ligne de commande 103
 - problèmes détectés au cours 141
- analyses
 - analyse Facebook 106, 109
 - analyse personnalisée 91, 144
 - détection de vers, alerte 138
 - disque dur 89
 - disquette 89
 - dossier 89
 - effacement des ID de fichiers 112
 - exclusion de menaces 110
 - fichier 89
 - fonctions de protection 346
 - lecteur amovible 89
 - modification d'une analyse personnalisée 95
 - modification d'une analyse planifiée 102
 - Norton Bootable Recovery Tool 28
 - Norton Power Eraser 105
 - planification d'analyses personnalisées 98
 - planification d'une analyse complète du système 100
 - planification d'une analyse rapide 101
 - suppression d'analyses personnalisées 97
- analyses de port 150
- analyses personnalisées
 - ajout de dossiers 94
 - ajout de fichiers 94

- configurer les options
 - d'analyse 91
- créer 94
- exécution d'une analyse
 - personnalisée 96
- modification 95
- planification 98
- sélectionner les éléments 92
- suppression d'une analyse 97
- antiphishing
 - à propos 235
 - activation 238
 - afficher la barre d'outils 294
 - désactivation 238
 - masquer la barre d'outils 294
- AntiSpam
 - Commentaires 218
 - Intégration client 210
 - Requête Web 219
- Antispam
 - Exclusions du carnet
 - d'adresses 212
 - liste Autorisés 214
 - liste Bloqués 216
- antiSpam
 - à propos 209
- antispyware
 - à propos 375
- Appliquer les mises à jour
 - uniquement au redémarrage
 - désactivation ou activation 41
- approbation du périphérique
 - ajouter un périphérique 201
- Assistant Ajouter une règle
 - ouverture 162
 - utilisation 163
- Assistant Norton Bootable Recovery Tool
 - téléchargement 23
- attaques
 - réseau 151

- Auto-Protect
 - désactivation ou activation 351
 - fonctionnalités 346
 - notifications 132
- AutoBlock
 - appareil 197
- AutoBlock d'intrusion
 - activation ou désactivation 195
 - blocage d'ordinateur de manière permanente 197
 - déblocage d'ordinateurs 196

B

- Bande passante
 - définir l'utilisation 225
- barre d'outils Norton
 - à propos 288
 - paramètres 252
- blocage
 - spam 209

C

- carte
 - à propos 267
- Cartes
 - ajout 269
 - copie 271
 - mise à jour 271
 - mise à jour d'image 269
 - suppression 271
- Clé de produit
 - localiser 10
 - Voir aussi* code PIN
- clients de messagerie électronique,
 - intégration 210
- code PIN
 - localiser 10
 - Voir aussi* clé de produit
- Commandes rapides
 - activation ou désactivation 358

Commentaire
 Norton AntiSpam 218
 communauté de veille Norton
 désactiver ou activer 353
 compte Norton
 à propos 68
 connexion 19
 création 19
 réinitialisation du mot de
 passe 19
 configuration
 alertes de performances 53
 délai d'inactivité 147
 Identity Safe 254
 Intégration client 210
 liste Bloqués 216
 LiveUpdate automatique 39
 mode silencieux 116
 protection antimalware au
 démarrage 125
 Rapport sur 30 jours 78
 tâches automatiques 143
 travail en arrière-plan 66
 Configurer
 limite de ressources 55
 mode discret 120
 mot de passe des
 paramètres 383
 notifications sur le Diagnostic
 des téléchargements 187
 protection au démarrage 124
 source d'alimentation 67
 connexions 128
 contrat de licence d'utilisateur final
 de Norton Security 388
 Contrôle automatique des
 programmes
 activation et désactivation 157
 Contrôle des programmes
 activation et désactivation 157

courrier électronique
 spam 209

D

délai d'inactivité
 configuration de la durée 147
 détection de vers, alerte
 réponse 138
 diagnostic des fichiers
 à propos 331
 Diagnostic des fraudes
 activer ou désactiver 234
 Diagnostic des téléchargements
 configuration d'alertes 188
 désactivation ou activation 185
 diagnostic du système
 à propos 45
 contrôle des activités 47
 graphique des événements 45
 schéma de performance 45
 disques
 nettoyage 304
 domaines
 ajout aux Autorisés 214
 ajout aux Bloqués 216
 Données personnelles
 sauvegarde 279

E

éléments de démarrage
 activer ou désactiver 307
 retard et exécution 306
 enregistrement automatique des
 frappes 207
 état de la sécurité
 réponse 32
 Exclusions de signatures
 exclure des éléments 111
 Exclusions du carnet d'adresses
 définition 212

extensions de fichier
des fichiers infectés 141

F

fenêtre d'analyse complète
apparaissant après une
analyse 88–89

Fenêtre de réparation manuelle
passage en revue des risques
restants dans 141

fenêtre de réparation manuelle
passage en revue des risques
restants 88
passant en revue les risques
restants dans 89

fenêtre principale
messages 126

filtrage
identification des expéditeurs de
courrier 214
identification des expéditeurs de
courrier électronique 216
Requête Web 219
SSL 209

filtre
importer les Autorisés 214

filtre antispam
activation ou désactivation 352

fonctions de protection
Auto-Protect 346, 351
désactivation 350
désactivation ou activation 354
LiveUpdate automatique 346
pare-feu intelligent 354
protection du courrier
électronique 346
protection heuristique 346

fragmentation du disque
à propos 301

G

Gérer
éléments de démarrage 306

gestion à distance
désactivation ou activation 380

gestion des identifiants
à propos 260

Gestionnaire de démarrage
activer ou désactiver des
éléments de démarrage 307
retard et exécution des éléments
en retard 306

graphique de l'état du système
détails des activités 50

Graphique de l'UC
obtention de données
historiques 60
processus consommant des
ressources 61

Graphique de la mémoire
obtention de données
historiques 60

graphique de la mémoire
à propos 59

Graphique des événements
accès 47
contrôle des activités 47

graphique des événements
indicateur d'utilisation de l'UC 59

H

Historique de la sécurité
résoudre les risques 141

historique de la sécurité
à propos 309
affichage des éléments 312
affichage des éléments en
quarantaine 312
ajout d'éléments à la
quarantaine 312

- alertes de trafic 312
- alertes du pare-feu 312
- alertes réseau 312
- historique des alertes
 - complet 312
- historique des alertes récentes 312
- importation ou exportation 337
- message suspect 312
- ouverture 312
- quarantaine 339
- recherche 336
- recherche rapide 336
- résultat de l'analyse manuelle 312
- transmission d'éléments à Symantec 312
- historique de sécurité
 - risques de sécurité 312

I

- icône de la zone de notification 126
- icônes de la barre des tâches
 - à propos 34
- ID de fichiers
 - effacement 112
- Identifiant
 - ajout manuel 263
 - configuration 254
 - création d'un nouveau dossier 263
 - enregistrement 261
 - gestion 263
 - modification 263
 - suppression 263
- Identity Safe
 - à propos 240
 - accès 252
 - barre d'outils Norton 253
 - configuration 254
 - connexion et déconnexion 253

- désactivation 243
- identifiants 260
- modification du mot de passe 287
- restauration des données 280
- sauvegarde 279

- indicateur de l'état de la sécurité
 - affichage 17

- Internet
 - problèmes de connexion 128

L

- Limitation de l'utilisation réseau
 - définition de la bande passante 225
- limitation de l'utilisation réseau
 - activation ou désactivation 224
- Liste Autorisés 214
- Liste Bloqués 216
- liste d'exclusion
 - supprimer un programme 59
- LiveUpdate
 - à propos 36
- LiveUpdate automatique
 - activation ou désactivation 39
- logiciel publicitaire
 - à propos 207
 - dans les programmes gratuits 207
- logiciels espions
 - détectés par Auto-Protect 132
- logiciels publicitaires
 - détectés par Auto-Protect 132

M

- Media Center Extender
 - mode silencieux 116
- Menaces
 - éléments infectés 92
 - résoudre un élément 92

- menaces
 - élimination 81
 - envoyer à partir de la quarantaine 344
 - Menace détectée, fenêtre 334
 - protection 150
- menaces de sécurité à haut risque
 - exclusion de l'analyse 110
- Menaces détectées
 - à propos de 92
 - résolution du risque 92
- messages 126
- mise à jour de la protection
 - à propos 375
 - date de la dernière mise à jour 41
- mise à jour de protection manuelle 40
- Mises à jour de la protection
 - mises à jour de programme 37
 - mises à jour des définitions 37
- Mode discret
 - activer ou désactiver 120
 - options 120
- mode discret
 - à propos 117
 - enregistrement de programmes TV 117
 - gravure de disque 117
- mode silencieux
 - activation automatique 116
 - activation manuelle 113
 - désactivation ou activation 113, 116
 - détection plein écran 116
 - programmes spécifiés par l'utilisateur 121
- mot de passe
 - enregistrement 261
 - fiable 296
 - modification 263, 287

- mot de passe des configurations
 - réinitialisation 381
- mot de passe des paramètres
 - désactivation 382

N

- Navigation
 - options 282
- Nettoyage
 - fichiers de cache 304
 - fichiers de cache du navigateur 304
 - Fichiers Internet temporaires 304
 - méthode 305
- nettoyage
 - fichiers de cache des sites Web 304
- niveau d'approbation
 - modification 203
 - périphérique 203
 - réseau 203
- Norton AntiSpam 209
 - à propos 209
 - Commentaires 218
 - Exclusions du carnet d'adresses 212
 - Requête Web 219
 - SSL 209
- Norton Autofix
 - résolution des problèmes 391
- Norton Bootable Recovery Tool
 - à propos 21
 - accès 28
 - création du fichier ISO 25
 - création sur DVD 24
 - création sur USB 26
 - mise à jour des définitions 31
 - utilisation 28
- Norton Family
 - à propos 349

- paramètres 349
 - Norton Firewall Diagnosis
 - à propos 178
 - Norton Insight
 - actualisation du niveau d'approbation 72
 - affichage des processus 72
 - fichiers approuvés 68
 - Fichiers d'intérêt 72
 - vérification du niveau d'approbation 75
 - Norton LiveUpdate
 - à propos 36
 - exécution 40
 - Norton Power Eraser
 - analyse 105
 - Norton Safe Search
 - navigation Web 233
 - Norton Safe Web
 - à propos 228
 - activation 109, 232
 - Analyse du mur Facebook 106
 - désactivation 232
 - Norton Security
 - activation 8
 - conservation de votre abonnement 397
 - Contrat de licence d'utilisateur 388
 - délai d'inactivité 147
 - démarrage à partir de l'invite de commande 31
 - désinstallation 398
 - état de la sécurité 32
 - état du système 12
 - fenêtre principale 12
 - gestion à distance 380
 - historique de la sécurité 309
 - icônes 34
 - menu de raccourcis 35
 - mise à niveau 388
 - mode discret 117
 - mode silencieux 113, 116
 - mot de passe 383
 - mot de passe des paramètres 382
 - Norton Autofix 391
 - nouvelle version 390
 - numéro de version 387
 - optimisation 301
 - paramètres 357
 - protection au démarrage 124
 - tâches personnalisées 144
 - Norton Security configurations
 - réinitialisation du mot de passe 381
 - Notes
 - enregistrement 272
 - mise à jour 272
 - suppression 272
 - notifications
 - Prévention d'intrusion 192
 - notifications de la prévention d'intrusion
 - activation ou désactivation 192
 - Notifications sur le Diagnostic des téléchargements
 - activer ou désactiver 187
 - nouvelle version
 - mise à niveau 388
 - rechercher 390
 - numéro de version
 - vérification 387
- ## O
- Optimisation
 - volume de démarrage 63
 - optimisation
 - à propos 62
 - défragmentation du volume de démarrage 64
 - exécution manuelle 302

- pratique d'excellence 303
- optimisation du disque
 - procédure 302
- Optimiseur du temps d'inactivité
 - à propos 64
- optimiseur du temps d'inactivité
 - activation ou désactivation 65
- Options
 - Intégration client 210
- options de navigation
 - à propos 282
- Ordinateur
 - protection 128
- ordinateur
 - blocage avec AutoBlock 195
 - état de la protection 17
- ordre de traitement
 - règles de filtrage 156

P

- page Web
 - rapport 239
- pages Web
 - protection 235
- paramètre
 - protection du navigateur 378
- Paramètres
 - Commandes rapides 358
 - protection du navigateur 184
- paramètres
 - analyses et risques 366
 - diagnostic des
 - téléchargements 185
 - gestion à distance 380
 - limitation de l'utilisation
 - réseau 225
 - personnalisation 357
- Protection contre les
 - falsifications du produit
 - Norton 385
 - protection contre les
 - intrusions 378
 - requête Web 221
- Paramètres d'Identity Safe
 - Détail des fraudes 234
- Paramètres de protection par mot
 - de passe
 - configuration 383
 - désactivation 382
 - réinitialisation 381
- Paramètres de proxy réseau
 - configuration 43
- pare-feu 150
- pare-feu intelligent
 - à propos 150
 - désactivation ou activation 151
- Performances
 - à propos des alertes 51
 - exécuter un nettoyage de
 - disque 305
 - nettoyage du disque 304
- performances
 - fragmentation du disque 301
 - fragmentation du fichier 301
 - optimisation du disque 302
 - optimisation du volume de
 - démarrage 63
 - suivi 60
- périphérique
 - modification du niveau
 - d'approbation 203
 - purge de la liste
 - d'exclusions 199
- Personnalisation
 - du Pare-feu intelligent 153
- personnalisation
 - liste Autorisés 214
- POP3, port 222
- port de messagerie électronique
 - suppression dans les ports
 - protégés 223

- ports protégés
 - ajout de ports POP3 et SMTP 222
 - suppression d'un port de messagerie électronique 223
- préparation aux situations d'urgence
 - protection permanente 81
- Prévention d'intrusion
 - Activation ou désactivation des notifications spécifiques 192
 - liste d'exclusions 198
- prévention d'intrusion
 - à propos 378
 - désactivation ou activation 354
- profil de ressource faible avec l'alimentation sur batterie
 - activation ou désactivation 57
- profils Identity Safe
 - à propos 244
- programme
 - suppression des règles de programme 161
- programme espion
 - gestion de la protection dans la fenêtre principale 207
- programmes
 - ajout aux règles de programme 158
 - configuration de l'accès à Internet 162
 - création de règles de filtrage 162
- Programmes spécifiés par l'utilisateur
 - ajout de programmes 122
 - suppression de programmes 123
- programmes spécifiés par l'utilisateur
 - à propos 121
 - mode silencieux 121
- protection
 - analyses du système 88
 - maintien 126
 - paramètres 359
 - préparation aux situations d'urgence 81
- protection antimalware au démarrage
 - désactivation ou activation 125
- protection antivirus
 - analyses du système 88
 - messagerie instantanée 346
- Protection au démarrage
 - configuration 124
- protection automatique
 - à propos 359
- Protection contre les falsifications du produit Norton
 - à propos 385
 - activation ou désactivation 385
- protection contre les virus
 - à propos de 346
 - mise à jour 346
- Protection du navigateur
 - activer ou désactiver 184
- protection du navigateur
 - à propos 378
- protection permanente
 - à propos de 81
 - élimination des risques de sécurité 81
- protection SONAR
 - activation ou désactivation 109
- Protection, fonctions
 - filtre antispam 352
- protection, fonctions
 - communauté de veille Norton 353

Q

- Quarantaine
 - historique de la sécurité 309
- quarantaine
 - ajout d'éléments 312
 - ajout d'un élément 342
 - envoyer pour analyse 344
 - fichier infecté par un ver 138
 - gestion des éléments 339
 - restauration d'éléments 343

R

- rapport
 - désactivation ou activation 78
- Rapport de diagnostic
 - en cours d'exécution 306
- Réaction
 - à propos 128
 - réaction aux urgences 128
- règle de programme
 - suppression de programmes 161
- règles
 - création 162–163
 - modification 163, 173
- règles de filtrage
 - à propos 153
 - activation et désactivation 176
 - ajout 162
 - création 163
 - modification 173
 - modification de l'ordre 175
 - ordre de traitement 175
 - suppression 176
- Règles de programme
 - suppression 176
- règles de programme
 - ajout 162
 - ajout de programmes 158
 - modification 173
 - personnalisation 161
- règles de trafic
 - ajout 162
 - modification 173
 - suppression 176
- réparation
 - actions 141
 - fichiers infectés 141
 - fichiers système 141
 - média amovible 141
- Requête Web
 - à propos 219
- requête Web
 - activation ou désactivation 221
- Réseau
 - modification du niveau d'approbation 203
- restauration
 - données de Identity Safe 278
- restauration d'éléments
 - quarantaine 343
- Résumé des résultats
 - nombre total d'éléments analysés 90
 - risques résolus 90
- résumé des résultats
 - à propos 90
 - risques résolus 90
- Risques
 - réponse à 141
- risques
 - ajouter à la quarantaine 342
 - analyses de port 150
 - détection 131
 - envoyer à partir de la quarantaine 344
 - intrusions 151
 - restauration de la quarantaine 343
 - risques de sécurité à propos 207

- analyses de port 150
- attaques 151
- autres programmes 207
- détectés par Auto-Protect 130, 132
- gestion de la protection en utilisant la fenêtre principale 207

S

- Safe Web
 - activation 232
 - désactivation 232
- sauvegarde
 - données de Identity Safe 278
- Sauvegarde et restauration à propos 278
- serveur proxy
 - configuration 43
- signatures
 - inclusion et exclusion 194
- situation d'urgence
 - préparations 81
- SMTP, port 222
- Source d'alimentation
 - configurer 67
- spyware
 - à propos 207
 - détection 131
 - paramètres 359
- SSL (Secure Sockets Layer)
 - Norton AntiSpam 209
- Support
 - chat, téléphone, forum 395
 - Support intégré 395
- support clientèle
 - à propos 395
- Support Norton
 - site Web 395
- support technique
 - à propos 395

- Symantec Security Response
 - affichage des fichiers transmis 312
 - envoi d'élément 344

T

- tâche personnalisée
 - LiveUpdate 144
 - nettoyage de fichier 144
 - optimisation du disque 144
 - sauvegarde 144
- tâches automatiques
 - activation ou désactivation 143
- transactions Internet
 - usurpation d'identité 240
- travail en arrière-plan
 - surveillance 66

U

- utilisation de l'UC
 - à propos 59
 - affichage 60

V

- vers
 - dans les messages électroniques 138
 - détectés par le Blocage des vers 138
- virus
 - description 346
 - détection 131
 - envoyer à partir de la quarantaine 344
 - menace inconnue 346
 - protection automatique 346
- virus et spyware
 - paramètres 359

Avec des fonctions antivirus, antisipam et antispyware, les produits Norton de Symantec protègent les utilisateurs contre les menaces traditionnelles. Ils assurent également une protection contre les bots, les téléchargements insidieux et le vol d'identité tout en n'ayant qu'un faible impact sur les ressources système. Symantec, la référence de la sécurité en ligne pour toute la famille, propose également des services, notamment la sauvegarde en ligne et l'optimisation des ordinateurs. Pour plus d'informations, cliquez sur l'un des liens suivants :

[Antivirus](#) | [Antispam](#) | [Antispyware](#) | [Sauvegarde en ligne](#)

Copyright © 2014 Symantec Corporation. Tous droits réservés. Symantec, Norton et le logo Norton sont des marques commerciales ou des marques déposées de Symantec Corporation et de ses filiales aux Etats-Unis et dans d'autres pays. Les autres noms peuvent être des marques commerciales de leurs propriétaires respectifs.