TOTAL SECURITY 2012

Manuel d’utilisation

Copyright© 2011/2012 Bitdefender

Bitdefender Total Security 2012
Manuel d'utilisation

Date de publication 2011.07.21

Copyright© 2011/2012 Bitdefender

Notice Légale

Tous droits réservés. Aucune partie de ce manuel ne peut être reproduite ou transmise, sous aucune forme et d'aucune façon, électronique ou physique, y compris photocopies, enregistrement, ou par quelque moyen de sauvegarde ou de restauration que ce soit, sans une autorisation écrite d'un représentant officiel de Bitdefender. L'inclusion de courtes citations dans des textes n'est possible qu'avec la mention de la source. Le contenu ne peut en aucun cas être modifié.

Avertissement. Ce produit et sa documentation sont protégés par copyright. Les informations de ce document sont données « à titre indicatif », sans garantie. Bien que toutes les précautions aient été prises lors de la préparation de ce document, les auteurs ne pourront être tenus responsables envers quiconque de toute perte ou dommage occasionné, ou supposé occasionné, directement ou indirectement par les informations contenues dans ce document.

Ce manuel contient des liens vers des sites Web de tiers qui ne sont pas sous le contrôle de BITDEFENDER, et BITDEFENDER n'est pas responsable du contenu de ces sites. Si vous accédez à l'un des sites Web d'une tierce partie fourni dans ce document, vous le ferez à vos propres risques. BITDEFENDER indique ces liens uniquement à titre informatif, et l'inclusion de ce lien n'implique pas que BITDEFENDER assume ou accepte la responsabilité du contenu de ce site Web d'un tiers.

Marques commerciales. Des noms de marques peuvent apparaître dans ce manuel. Toutes les marques, enregistrées ou non, citées dans ce document, sont la propriété exclusive de leurs propriétaires respectifs.

Bitdefender

Table des matières

1. Installation 1
1.1. Configuration requise 1
1.1.1. Configuration système minimale 1
1.1.2. Configuration système recommandée 1
1.1.3. Configuration logicielle requise 1
1.2. Préparation de l'installation 2
1.3. Installer votre produit Bitdefender 2
1.3.1. Mise à niveau à partir d'une version antérieure 6
2. Introduction 7
2.1. Ouverture de Bitdefender 7
2.2. À faire après l'installation 7
2.3. Enregistrement du Produit 8
2.3.1. Saisie de votre clé de licence 9
2.3.2. Connexion à MyBitdefender 9
2.3.3. Acheter ou renouveler des clés de licence 11
2.4. Correction des problèmes en cours. 11
2.4.1. Assistant de Correction des Problèmes 12
2.4.2. Configurer les alertes d'état 13
2.5. Événements 13
2.6. Auto-Pilot 14
2.7. Mode Jeu et Mode Portable 15
2.7.1. Mode Jeu 15
2.7.2. Mode Portable 17
2.8. Paramètres Bitdefender de la protection par mot de passe 18
2.9. Rapports d'utilisation anonymes 18
2.10. Réparer ou désinstaller Bitdefender 19
3. Interface de Bitdefender 20
3.1. Icône de la zone de notification 20
3.2. Fenêtre principale 21
3.2.1. Barre d'outils supérieure 22
3.2.2. Panneaux 23
3.3. Fenêtre de configuration 27
4. Comment 29
4.1. Comment améliorer les performances de mon système ? 29
4.1.1. Défragmentez votre disque dur 30
4.1.2. Nettoyez votre PC 30
4.1.3. Nettoyer le Registre Windows 30
4.1.4. Analysez votre système régulièrement 31
4.2. Comment enregistrer une version d'essai ? 31
4.3. Comment enregistrer Bitdefender sans connexion Internet ? 32
4.4. Comment mettre à niveau vers un autre produit Bitdefender 2012 ? 33
4.5. Quand devrais-je réinstaller Bitdefender ? 33
4.6. Quand ma protection Bitdefender expire-t-elle ? 33
4.7. Comment renouveler ma protection Bitdefender ? 34
4.8. Quel est le produit Bitdefender que j'utilise ? 34

4.9. Comment analyser un fichier ou un dossier ? ... 35
4.10. Comment analyser mon système ? ... 35
4.11. Comment créer une tâche d'analyse personnalisée ? ... 35
4.12. Comment exclure un dossier de l'analyse ? ... 36
4.13. Que faire lorsque Bitdefender a détecté un fichier sain comme étant infecté ? ... 36
4.14. Comment créer des comptes utilisateurs Windows ? ... 37
4.15. Comment protéger mes enfants des menaces sur Internet ? ... 38
4.16. Comment débloquer un site web bloqué par le Contrôle Parental ? ... 39
4.17. Comment protéger mes informations personnelles ? ... 40
4.18. Comment utiliser les coffres-forts ? ... 40
4.19. Où voir l'espace restant sur ma SafeBox ? ... 42
4.20. Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ? ... 42

5. Protection antivirus ... 44
5.1. Analyse à l'accès (protection en temps réel) ... 45
5.1.1. Vérification des malwares détectés par l'analyse à l'accès ... 45
5.1.2. Régler le niveau de protection en temps réel ... 46
5.1.3. Création d'un niveau de protection personnalisé ... 46
5.1.4. Restauration des paramètres par défaut ... 48
5.1.5. Activer ou désactiver la protection en temps réel ... 48
5.1.6. Actions appliquées à l'encontre des malwares détectés ... 49
5.2. Analyse à la demande ... 50
5.2.1. Analyse auto. ... 50
5.2.2. Rechercher des malwares dans un fichier ou un dossier ... 51
5.2.3. Exécuter une Analyse Rapide ... 51
5.2.4. Exécuter une Analyse Complète du Système ... 51
5.2.5. Configurer et exécuter une analyse personnalisée ... 52
5.2.6. Assistant d'analyse antivirus ... 54
5.2.7. Consulter les journaux d'analyse ... 57
5.3. Analyse automatique de supports amovibles ... 58
5.3.1. Comment cela fonctionne-t-il ? ... 58
5.3.2. Gérer l'analyse des supports amovibles ... 59
5.4. Configuration des exceptions d'analyse ... 60
5.4.1. Exclure de l'analyse des fichiers ou des dossiers ... 60
5.4.2. Exclure de l'analyse des extensions de fichiers ... 61
5.4.3. Gérer les exceptions d'analyse ... 61
5.5. Gérer les fichiers en quarantaine ... 62
5.6. Active Virus Control ... 63
5.6.1. Vérifier des applications détectées ... 63
5.6.2. Activer ou désactiver Active Virus Control ... 64
5.6.3. Régler la protection Active Virus Control ... 64
5.6.4. Gérer des processus exclus ... 64
5.7. Corriger les vulnérabilités du système ... 65
5.7.1. Analyser votre système à la recherche de vulnérabilités ... 66
5.7.2. Utiliser la surveillance des vulnérabilités automatique ... 67

6. Antispam ... 69
6.1. Aperçu de l'antispam ... 70

6.1.1. Filtres AntiSpam ... 70
6.1.2. Fonctionnement de l'Antispam ... 71
6.1.3. Mises à jour de l'antispam ... 72
6.1.4. Clients et protocoles de messagerie pris en charge ... 72
6.2. Activer ou désactiver la protection antispam ... 72
6.3. Utilisation de la barre d'outils Antispam dans la fenêtre de votre client de messagerie ... 73
6.3.1. Indiquer des erreurs de détection ... 74
6.3.2. Indiquer les messages de spam non détectés ... 74
6.3.3. Configuration des paramètres de la barre d'outils ... 75
6.4. Configuration de la liste des amis ... 75
6.5. Configuration de la liste des spammeurs ... 76
6.6. Régler le niveau de sensibilité ... 77
6.7. Configurer les filtres antispam locaux ... 78
6.8. Configurer la détection "in-the-cloud" ... 78

7. Contrôle Vie Privée ... 80
7.1. Protection antiphishing ... 80
7.1.1. Protection Bitdefender dans le navigateur web ... 82
7.1.2. Alertes Bitdefender dans le navigateur ... 83
7.2. Données ... 83
7.2.1. À propos de la protection des données ... 83
7.2.2. Configurer la protection des données ... 84
7.2.3. Gestion des règles ... 85
7.3. Messagerie Inst. ... 86
7.4. Cryptage de Fichiers ... 86
7.4.1. Gérer des coffres-forts à partir de l'interface de Bitdefender ... 87
7.4.2. Gérer les coffres-forts depuis Windows ... 92
7.5. Supprimer définitivement des fichiers ... 96

8. Contrôle Parental ... 97
8.1. Configuration du Contrôle Parental ... 97
8.1.1. Contrôle Web ... 99
8.1.2. Contrôle des Applications ... 100
8.1.3. Contrôle par mots-clés ... 101
8.1.4. Contrôle de messagerie instantanée ... 103
8.1.5. Filtrage par catégories ... 104
8.2. Surveiller les activités des enfants ... 105
8.2.1. Vérifier les journaux du Contrôle Parental ... 105
8.2.2. Configurer les notifications par e-mail ... 106
8.3. Contrôle Parental à Distance ... 107
8.3.1. Pré-requis à l'utilisation du Contrôle Parental à Distance ... 107
8.3.2. Activation du Contrôle Parental à Distance ... 107
8.3.3. Accès au Contrôle Parental à Distance ... 108
8.3.4. Surveiller les activités des enfants à distance ... 108
8.3.5. Modifier les paramètres du Contrôle Parental à distance ... 109

9. Pare-feu ... 112
9.1. Activer ou désactiver la protection pare-feu ... 113
9.2. Configurer les paramètres de connexion réseau ... 113
9.3. Système de détection d'intrusion ... 114

9.4. Configurer les paramètres du trafic 115
9.5. Règles générales 115
9.6. Règles d'applications 116
9.7. Règles d'adaptateurs 119
9.8. Surveiller l'activité du réseau 120

10. Optimisation 122
10.1. Nettoyage de votre PC 122
10.2. Défragmenter des volumes de disque dur 123
10.3. Rechercher les doublons 124
10.4. Nettoyer le Registre Windows 125
10.5. Restauration du registre nettoyé 127
10.6. Analyseur de Performances 128

11. Mappage réseau 129
11.1. Activation du réseau Bitdefender 129
11.2. Ajouter des ordinateurs au réseau de Bitdefender 130
11.3. Gérer le réseau Bitdefender 130

12. Mise à jour 133
12.1. Vérifier que Bitdefender est à jour 133
12.2. Mise à jour en cours 134
12.3. Activer ou désactiver la mise à jour automatique 134
12.4. Réglage des paramètres de mise à jour 135

13. Sauvegarde en ligne de SafeBox 137
13.1. Gérer les sauvegardes de SafeBox à partir de la fenêtre Bitdefender 137
13.2. Gérer les sauvegardes SafeBox à partir de Windows 138
13.2.1. Ajouter des dossiers à SafeBox 138
13.2.2. Suppression de dossiers de la SafeBox 139
13.2.3. Restauration des fichiers supprimés de SafeBox 139
13.3. Synchroniser des fichiers entre vos ordinateurs 140

14. Protection Safego pour réseaux sociaux 141

15. Résolution des problèmes 142
15.1. Mon système semble lent 142
15.2. L'analyse ne démarre pas 143
15.3. Je ne peux plus utiliser une application 144
15.4. Je ne peux pas me connecter à Internet 145
15.5. Je ne peux pas accéder à un périphérique de mon réseau 145
15.6. Mon Internet est lent 147
15.7. Comment mettre à jour Bitdefender avec une connexion Internet lente 148
15.8. Mon ordinateur n'est pas connecté à Internet. Comment puis-je mettre à jour Bitdefender ? 149
15.9. Le Services Bitdefender ne répondent pas 149
15.10. Le filtre antispam ne fonctionne pas correctement 150
15.10.1. Des messages légitimes sont signalés comme étant du [spam] 150
15.10.2. De nombreux messages de spam ne sont pas détectés 152
15.10.3. Le filtre antispam ne détecte aucun message de spam. 154
15.11. La désinstallation de Bitdefender a échoué 155
15.12. Mon système ne démarre pas après l'installation de Bitdefender 155

16. Suppression des malwares de votre système 157
16.1. Mode de Secours de Bitdefender 157
16.2. Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ? 159
16.3. Comment nettoyer un virus dans une archive ? 160
16.4. Comment nettoyer un virus dans une archive de messagerie ? 161
16.5. Que faire si je suspecte un fichier d'être dangereux ? 162
16.6. Comment nettoyer les fichiers infectés du System Volume Information ? 163
16.7. Que sont les fichiers protégés par mot de passe du journal d'analyse ? 164
16.8. Que sont les éléments ignorés du journal d'analyse ? 164
16.9. Que sont les fichiers ultra-compressés du journal d'analyse ? 165
16.10. Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ? ... 165
17. Obtenir de l'aide 166
17.1. Support 166
17.1.1. Ressources en ligne 166
17.1.2. Demander de l'aide 167
17.1.3. Support Technique Editions Profil / Bitdefender 169
17.2. Nous contacter 171
17.2.1. Adresses Web 171
17.2.2. Distributeurs locaux 171
17.2.3. Bureaux de Bitdefender 172
18. Informations utiles 174
18.1. Comment supprimer les autres solutions de sécurité ? 174
18.2. Comment redémarrer en mode sans échec ? 175
18.3. Est-ce que j'utilise une version de Windows de 32 ou 64 bits ? 175
18.4. Comment utiliser la Restauration du Système dans Windows ? 176
18.5. Comment afficher des objets masqués dans Windows ? 177
Glossaire 178

1. Installation

1.1. Configuration requise

Vous pouvez installer Bitdefender Total Security 2012 uniquement sur les ordinateurs fonctionnant avec les systèmes d'exploitation suivants :

- Windows XP avec Service Pack 3 (32 bits)
- Windows Vista avec Service Pack 2
- Windows 7 avec Service Pack 1

Avant d'installer le produit, vérifiez que votre ordinateur dispose de la configuration minimale requise.

Note

Pour vérifier quel système d'exploitation fonctionne actuellement sur votre ordinateur ainsi que des informations sur votre matériel, faites un clic-droit sur **Poste de travail** et sélectionnez **Propriétés** dans le menu.

1.1.1. Configuration système minimale

- 1,8 Go d'espace disque disponible (au moins 800 Mo sur le lecteur système)
- Processeur 800MHz
- 1 Go de mémoire (RAM)

1.1.2. Configuration système recommandée

- 2,8 Go d'espace disque disponible (au moins 800 Mo sur le lecteur système)
- Intel CORE Duo (1,66 GHz) ou processeur équivalent
- Mémoire (RAM) :
  - 1 Go pour Windows XP
  - 1,5 Go pour Windows Vista et Windows 7

1.1.3. Configuration logicielle requise

Pour pouvoir utiliser Bitdefender et l'ensemble de ses fonctionnalités, votre ordinateur doit disposer de la configuration logicielle suivante :

- Internet Explorer 7 ou version supérieure
- Mozilla Firefox 3.6 ou version supérieure
- Yahoo! Messenger 8.1 ou version supérieure
- Microsoft Outlook 2007 / 2010
- Microsoft Outlook Express et Windows Mail (sur les systèmes 32 bits)
- Mozilla Thunderbird 3.0.4

- .NET Framework 3

1.2. Préparation de l'installation

Avant d'installer Bitdefender Total Security 2012, procédez comme suit pour faciliter l'installation :

- Vérifiez que l'ordinateur où vous prévoyez d'installer Bitdefender dispose de la configuration minimale requise.Si l'ordinateur ne dispose pas de la configuration minimale requise, Bitdefender ne pourra pas être installé, ou, une fois installé, il ne fonctionnera pas correctement, ralentira le système et le rendra instable.Pour des informations détaillées sur la configuration nécessaire, veuillez consulter « *Configuration requise* » (p. 1).
- Connectez-vous à l'ordinateur en utilisant un compte Administrateur.
- Désinstallez tous les autres logiciels similaires de l'ordinateur.L'exécution de deux programmes de sécurité à la fois peut affecter leur fonctionnement et provoquer d'importants problèmes avec le système.Windows Defender sera désactivé pendant l'installation.
- Désactivez ou supprimez tout programme pare-feu s'exécutant sur l'ordinateur.L'exécution de deux pare-feux à la fois peut affecter leur fonctionnement et provoquer d'importants problèmes avec le système.Le Pare-Feu Windows sera désactivé pendant l'installation.
- Il est recommandé que votre ordinateur soit connecté à Internet pendant l'installation, même pour une installation à partir d'un CD/DVD. Si des versions plus récentes que les fichiers d'applications du package d'installation sont disponibles, Bitdefender les téléchargera et les installera.

1.3. Installer votre produit Bitdefender

Vous pouvez installer Bitdefender à partir du disque d'installation de Bitdefender ou en utilisant un programme d'installation téléchargé sur votre ordinateur à partir du site Internet de Bitdefender ou d'autres sites Internet autorisés (par exemple, le site d'un partenaire de Bitdefender ou une boutique en ligne).Vous pouvez télécharger le fichier d'installation sur le site Internet de Bitdefender à l'adresse suivante : http://www.bitdefender.com/site/Downloads/.

- Pour installer Bitdefender à partir du disque d'installation, insérez le disque dans le lecteur optique. Un écran de bienvenue devrait s'afficher dans quelques instants. Suivez les instructions pour lancer l'installation.

Note

L'écran d'accueil fournit une option pour copier le package d'installation à partir du disque d'installation sur un support de stockage USB.C'est utile si vous avez besoin d'installer Bitdefender sur un ordinateur ne disposant pas d'un lecteur de

disque (sur un netbook, par exemple). Branchez votre périphérique USB, puis cliquez sur **Copier vers un disque USB**.Ensuite, branchez votre disque USB sur un PC ne disposant pas de lecteur de disque et double-cliquez sur `runsetup.exe` depuis le répertoire dans lequel se trouve le package d'installation.

Si l'écran d'accueil n'apparaît pas, allez dans le répertoire racine du disque et double-cliquez sur le fichier `autorun.exe`.

- Pour installer Bitdefender à l'aide du programme d'installation téléchargé sur votre ordinateur, localisez le fichier et double-cliquez dessus.Cela lancera le téléchargement des fichiers d'installation, qui peut requérir un certain temps, en fonction de votre connexion Internet.

Bitdefender vérifiera d'abord votre système pour valider l'installation.

Si votre système ne dispose pas de la configuration minimale requise pour l'installation de Bitdefender, vous serez informé des zones devant être améliorées avant de pouvoir poursuivre.

Si un programme antivirus incompatible ou une version antérieure de Bitdefender est détecté, on vous demandera de le désinstaller de votre système. Veuillez suivre les indications pour supprimer les logiciels de votre système, évitant ainsi que des problèmes ne surviennent par la suite.

Note
Il est parfois nécessaire de redémarrer l'ordinateur pour terminer la désinstallation des programmes antivirus détectés.

Suivez les étapes de l'assistant de configuration pour installer Bitdefender Total Security 2012.

Étape 1 - Bienvenue

Veuillez lire l'Accord de Licence et sélectionnez **Accepter & Poursuivre**.L'Accord de Licence contient les termes et conditions d'utilisation de Bitdefender Total Security 2012.

Note

Si vous n'acceptez pas ces termes, fermez la fenêtre. Le processus d'installation sera abandonné et vous quitterez l'installation.

Étape 2 - Enregistrer votre produit

Pour terminer l'enregistrement de votre produit vous devez saisir une clé de licence et créer un compte MyBitdefender.Une connexion Internet active est requise.

Procédez selon votre situation :

- **J'ai acheté le produit**

Dans ce cas, enregistrez le produit en procédant comme suit :

1. Sélectionnez **J'ai acheté le produit et je souhaite l'enregistrer maintenant**.
2. Saisissez la clé de licence dans le champ correspondant.

   Note

   Vous trouverez votre clé d'activation :
   - sur l'étiquette du CD/DVD.
   - sur le manuel du produit.
   - sur l'e-mail d'achat en ligne.

3. Saisissez votre adresse e-mail dans le champ correspondant.

   Important

   Une adresse e-mail valide est requise. Un message de confirmation sera envoyé à l'adresse que vous avez indiquée.

4. Cliquez sur **S'enregistrer**.

- **Je veux évaluer Bitdefender**

  Dans ce cas, vous pouvez utiliser le produit pendant une période de 30 jours. Pour commencer la période d'essai, sélectionnez **Je veux évaluer ce produit**.

  Vous devez créer un compte MyBitdefender pour utiliser les fonctionnalités en ligne du produit.Pour créer un compte, saisissez votre adresse e-mail dans le champ correspondant.Un message de confirmation sera envoyé à l'adresse que vous avez indiquée. Si vous avez déjà un compte, saisissez l'adresse e-mail qui y est associée pour enregistrer le produit avec ce compte.

Paramètres personnalisés

Cette étape vous permet également de personnaliser les paramètres d'installation en cliquant sur **Paramètres personnalisés**.

Chemin d'installation

Par défaut, Bitdefender Total Security 2012 sera installé dans `C:\Program Files\Bitdefender\Bitdefender 2012`.Si vous souhaitez choisir un autre répertoire, cliquez sur **Modifier** et choisissez le répertoire d'installation de Bitdefender.

Configurer les paramètres du proxy

Bitdefender Total Security 2012 nécessite un accès à Internet pour l'enregistrement du produit, le téléchargement de mises à jour du produit et de sécurité, les composants de détection "in the cloud" etc.Si vous utilisez une connexion via un proxy au lieu d'une connexion Internet directe, vous devez sélectionner cette options et configurer les paramètres du proxy.

Les paramètres peuvent être importés à partir du navigateur par défaut ou vous pouvez les indiquer manuellement.

Activer la mise à jour P2P

Vous pouvez partager les fichiers du produit et les signatures avec d'autres utilisateurs de Bitdefender.Ainsi, les mises à jour de Bitdefender sont effectuées plus rapidement. Si vous ne souhaitez pas activer cette fonctionnalité, cochez la case correspondante.

Note

Aucune information personnelle identifiable ne sera partagée si cette fonction est activée.

Si vous souhaitez réduire l'impact du trafic réseau sur la performance du système au cours des mises à jour, choisissez l'option de partage des mises à jour.Bitdefender utilise les ports 8880 – 8889 pour la mise à jour peer-to-peer.

Envoyer des Rapports d'Utilisation Anonymes

Les Rapports d'Utilisation Anonymes sont activés par défaut.Si vous activez cette option, les rapports contenant des informations sur votre utilisation du produit seront envoyés aux serveurs Bitdefender.Ces informations sont essentielles pour améliorer le produit et nous aider à vous offrir un meilleur service à l'avenir. Veuillez noter que ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.

Cliquez sur **OK** pour confirmer vos préférences.

Cliquez sur **Installer** pour lancer l'installation.

Étape 3 - Avancement de l'installation

Patientez jusqu'à la fin de l'installation.Des informations détaillées sur l'avancement sont affichées.

Les zones critiques de votre système font l'objet d'une analyse antivirus, les dernières versions des fichiers d'applications sont téléchargées et installées et les services Bitdefender sont lancés. Cette étape peut prendre quelques minutes.

Étape 4 - Terminer

Un résumé de l'installation s'affiche. Si des malwares actifs ont été détectés et supprimés pendant l'installation, un redémarrage du système peut être nécessaire.

Cliquez sur **Terminer**.

Si votre ordinateur exécute Windows XP, l'assistant de configuration détectera tous les réseaux auxquels vous êtes connecté et vous demandera d'indiquer s'il s'agit de réseaux Domicile/Bureau ou Public.

1.3.1. Mise à niveau à partir d'une version antérieure

Si vous utilisez déjà une ancienne version de Bitdefender, vous pouvez la mettre à niveau vers Bitdefender Total Security 2012 de deux façons :

- Installez Bitdefender Total Security 2012 directement sur la version plus ancienne.Bitdefender détectera la version antérieure et vous aidera à la désinstaller avant d'installer la nouvelle version. Vous devrez redémarrer l'ordinateur pendant la mise à niveau.
- Désinstallez la version la plus ancienne, puis redémarrez l’ordinateur et installez la nouvelle version comme expliqué précédemment.Utilisez cette méthode de mise à niveau si l'autre échoue.

Note

La configuration et le contenu de la quarantaine de l'ancienne version ne seront pas importés.

2. Introduction

Une fois Bitdefender Total Security 2012 installé, votre ordinateur est protégé contre toutes sortes de malwares (comme les virus, les spywares et les chevaux de Troie) et les menaces Internet (comme les pirates, le phishing et le spam).

Le Pilotage Automatique est lancé par défaut et vous n'avez aucun paramètre à configurer. Cependant, vous pouvez souhaiter profiter des paramètres de Bitdefender pour ajuster et améliorer votre protection.

Bitdefender prendra pour vous la plupart des décisions de sécurité et affichera rarement des alertes pop-up.Des détails sur les actions prises et des informations sur le fonctionnement du programme sont disponibles dans la fenêtre Événements. Pour plus d'informations, reportez-vous à « *Événements* » (p. 13).

Il est recommandé d'ouvrir Bitdefender de temps en temps et de corriger les problèmes existants.Vous pouvez avoir à configurer des composants Bitdefender spécifiques ou appliquer des actions préventives afin de protéger votre ordinateur et vos données.

Si vous n'avez pas enregistré le produit (y compris si vous n'avez pas créé de compte MyBitdefender), pensez à le faire avant la fin de la période d'essai.Vous devez créer un compte pour utiliser les fonctionnalités en ligne du produit. Pour plus d'informations sur le processus d'enregistrement, reportez-vous à « *Enregistrement du Produit* » (p. 8).

2.1. Ouverture de Bitdefender

Pour accéder à l'interface principale de Bitdefender Total Security 2012, utilisez le menu Démarrer de Windows en suivant le chemin d'accès **Démarrer → Tous les programmes → Bitdefender 2012 → Bitdefender Total Security 2012**ou, plus rapide, double-cliquez sur l'icône Bitdefender dans la zone de notification.

Pour plus d'informations sur la fenêtre Bitdefender et l'icône de la zone de notification, reportez-vous à « *Interface de Bitdefender* » (p. 20).

2.2. À faire après l'installation

Si vous souhaitez que Bitdefender traite pour vous toutes les décisions liées à la sécurité, maintenez le Pilotage Automatique activé. Pour plus d'informations, reportez-vous à « *Auto-Pilot* » (p. 14).

Voici une liste de tâches que vous pouvez souhaitez effectuer après l'installation :

- Si votre ordinateur se connecte à Internet via un serveur proxy, vous devez configurer les paramètres du proxy comme indiqué dans « *Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?* » (p. 42).

- Si vous avez installé Bitdefender sur plusieurs ordinateurs de votre réseau domestique, vous pouvez administrer tous les produits Bitdefender à distance à partir d'un seul ordinateur. Pour plus d'informations, reportez-vous à « *Mappage réseau* » (p. 129).
- Si vous avez des enfants, vous pouvez utiliser le Contrôle Parental pour surveiller et limiter leurs activités sur l'ordinateur et sur Internet. Le Contrôle Parental est activé par défaut sur les comptes utilisateurs restreints de Windows et des règles de filtrage web adaptées aux adolescents sont appliquées. Pour plus d'informations, reportez-vous à « *Contrôle Parental* » (p. 97).
- Créez des règles de protection des données pour empêcher vos données personnelles importantes d'être divulguées sans votre accord. Pour plus d'informations, reportez-vous à « *Données* » (p. 83).

2.3. Enregistrement du Produit

Pour bénéficier de la protection de Bitdefender, vous devez enregistrer votre logiciel en saisissant une clé de licence et en créant un compte MyBitdefender.

La clé de licence indique pendant combien de temps vous pouvez utiliser le produit.Dès que la clé de licence expire, Bitdefender cesse de réaliser ses fonctions et de protéger votre ordinateur.

Nous vous recommandons d'acheter une clé de licence ou de renouveler votre licence quelques jours avant l'expiration de la clé utilisée.Pour plus d'informations, reportez-vous à « *Acheter ou renouveler des clés de licence* » (p. 11).Si vous utilisez une version d'essai de Bitdefender, vous devez l'enregistrer avec une clé de licence si vous souhaitez continuer à l'utiliser après la fin de la période d'évaluation.

Un compte MyBitdefender vous permet d'accéder aux mises à jour du produit et d'utiliser les services en ligne de Bitdefender Total Security 2012.Si vous avez déjà un compte, enregistrez votre produit Bitdefender avec ce compte.

Un compte MyBitdefender vous permet de :

- Maintenez votre produit à jour.
- Récupérez votre clé de licence, si jamais vous la perdez.
- Contacter le Service Client de Bitdefender.
- Surveillez les activités de vos enfants et configurez les paramètres du Contrôle Parental où que vous soyez.
- Sauvegardez et synchronisez vos fichiers importants sur des serveurs en ligne sécurisés à l'aide de SafeBox.
- Protégez votre compte Facebook avec Safego.

2.3.1. Saisie de votre clé de licence

Si au cours de l'installation vous avez choisi d'évaluer le produit, vous pouvez l'utiliser pendant une période d'essai de 30 jours. Pour continuer à utiliser Bitdefender une fois la période d'essai terminée, vous devez l'enregistrer avec une clé de licence.

Pour enregistrer le produit avec une clé de licence ou modifier la clé de licence actuelle, cliquez sur le lien **Informations de Licence** situé en bas de la fenêtre de Bitdefender.La fenêtre d'enregistrement est alors affichée.

Vous pouvez visualiser l'état de votre enregistrement Bitdefender, votre clé d'activation actuelle ou voir dans combien de jours la licence arrivera à son terme.

Pour enregistrer Bitdefender Total Security 2012 :

1. Entrez la clé d'activation dans le champ de saisie.

Note

Vous trouverez votre clé d'activation :

- sur l'étiquette du CD.
- sur le manuel du produit.
- sur l'e-mail d'achat en ligne.

Si vous n'avez pas de clé de licence Bitdefender, cliquez sur le lien de la fenêtre pour ouvrir une page web vous permettant d'en acheter une.

2. Cliquez sur **S'enregistrer**.

2.3.2. Connexion à MyBitdefender

Si vous avez indiqué une adresse e-mail pendant l'installation, un e-mail de confirmation a été envoyé à cette adresse. Cliquez sur le lien de l'e-mail pour terminer l'enregistrement.

Si vous n'avez pas terminé l'enregistrement, Bitdefender vous avertira qu'il est nécessaire de le faire.

Important

Vous devez vous connecter à un compte dans les 30 jours qui suivent l'installation de Bitdefender.Dans le cas contraire, Bitdefender ne se mettra plus à jour.

Pour créer un compte MyBitdefender ou vous connecter à un compte existant, cliquez sur le lien **Terminer l'enregistrement** / **MyBitdefender**, situé en bas de la fenêtre Bitdefender.

La fenêtre MyBitdefender s'ouvrira. Procédez selon votre situation.

Je souhaite créer un compte MyBitdefender

Pour créer un compte MyBitdefender, suivez ces étapes :

1. Sélectionnez **Créer un nouveau compte**.

   Une nouvelle fenêtre s'affiche.

2. Tapez les informations requises dans les champs correspondants. Les informations communiquées ici resteront confidentielles.

   - **Nom** - entrez un nom d'utilisateur pour votre compte. Ce champ est optionnel.
   - **E-mail** - indiquez votre adresse e-mail.
   - **Mot de passe** - saisissez un mot de passe pour votre compte.Le mot de passe doit contenir au moins 6 caractères.
   - **Confirmer le mot de passe** - ressaisissez le mot de passe.
   - Si vous le souhaitez, Bitdefender peut vous tenir informé de ses offres spéciales et promotions via l'adresse e-mail de votre compte.Pour activer cette option, sélectionnez **J'autorise Bitdefender à m'envoyer des e-mails**.

   Note
   Une fois le compte créé, vous pouvez utiliser l'adresse e-mail et le mot de passe indiqués pour vous connecter à votre compte sur http://my.bitdefender.com.

3. Cliquez sur **Envoyer**.
4. Vous devez terminer l'enregistrement de votre compte avant de pouvoir l'utiliser.Consultez votre messagerie et suivez les instructions de l'e-mail de confirmation envoyé par Bitdefender.

Note

Vous pouvez également vous connecter à l'aide de votre compte Facebook ou Google. Pour plus d'informations, reportez-vous à« Je souhaite me connecter à l'aide de compte Facebook ou Google » (p. 10)

Je souhaite me connecter à l'aide de compte Facebook ou Google

Pour vous connecter avec votre compte Facebook ou Google, procédez comme suit :

1. Cliquez sur l'icône du service que vous souhaitez utiliser pour vous connecter. Vous serez redirigé vers la page de connexion de ce service.
2. Suivez les instructions du service sélectionné pour lier votre compte à Bitdefender.

Note

Bitdefender n'accède à aucune information confidentielle telle que le mot de passe du compte que vous utilisez pour vous connecter, ou les informations personnelles de vos amis et contacts.

J'ai déjà un compte MyBitdefender

Si vous vous êtes connecté auparavant à un compte à partir de votre produit, Bitdefender le détectera et vous connectera à ce compte.Vous pouvez consulter votre compte sur http://my.bitdefender.com en cliquant sur **Aller dans MyBitdefender**.

Si vous souhaitez vous connecter à un autre compte, cliquez sur le lien correspondant et suivez les instructions des sections antérieures.

Si vous avez déjà un compte actif, mais que Bitdefender ne le détecte pas, suivez ces étapes pour vous connecter à ce compte :

1. Tapez l'adresse e-mail et le mot de passe de votre compte dans les champs correspondants.

   Note
   Si vous avez oublié votre mot de passe, cliquez sur **Mot de passe oublié** et suivez les instructions pour le retrouver.

2. Cliquez sur **Connexion**.

2.3.3. Acheter ou renouveler des clés de licence

Si la période d'essai est sur le point d'expirer, vous devez acheter une clé de licence et enregistrer votre produit.De même, si votre clé de licence actuelle est sur le point d'expirer, vous devez renouveler votre licence.

Bitdefender vous avertira à l'approche de la date d'expiration de votre licence. Suivez les instructions de l'alerte pour acheter une nouvelle licence.

Vous pouvez vous rendre sur une page web où vous pouvez acheter une clé de licence à tout moment, en procédant comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le lien **Informations de Licence**, situé en bas de la fenêtre Bitdefender pour ouvrir la fenêtre d'enregistrement du produit.
3. Cliquez sur le lien de la partie inférieure de la fenêtre.

2.4. Correction des problèmes en cours.

Bitdefender utilise un système de contrôle pour détecter la présence de problèmes pouvant affecter la sécurité de votre ordinateur et de vos données et vous en informer. Par défaut, il surveille seulement un ensemble de problèmes considérés comme très importants. Cependant, vous pouvez le configurer selon vos besoins en sélectionnant les problèmes spécifiques au sujet desquels vous souhaitez être averti(e).

Les problèmes détectés comprennent d'importants paramètres de protection qui sont désactivés et d'autres conditions pouvant constituer un risque pour la sécurité. Ils sont regroupés en deux catégories :

- **Problèmes critiques** - ils empêchent Bitdefender de vous protéger contre les malwares ou constituent un risque majeur pour la sécurité.
- **Problèmes mineurs (non critiques)** - ils peuvent affecter votre protection dans un avenir proche.

L'icône Bitdefender de la zone de notification signale les problèmes en attente en changeant de couleur comme suit :

Couleur rouge : D'importants problèmes affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.

Couleur jaune : Des problèmes non critiques affectent la sécurité de votre système. Vérifiez-les et réglez-les lorsque vous aurez le temps.

Si vous passez le curseur de la souris sur l'icône, une fenêtre de notification confirmera la présence de problèmes en attente.

Lorsque vous ouvrez la fenêtre de Bitdefender, la zone d'état de Sécurité de la barre d'outils supérieure indique le nombre et la nature des problèmes affectant votre système.

2.4.1. Assistant de Correction des Problèmes

Pour corriger les problèmes détectés, suivez l'assistant de **Correction des problèmes**.

1. Pour ouvrir l'assistant, procédez comme indiqué :
   - Faites un clic droit sur l'icône Bitdefender de la zone de notification et sélectionnez **Tout corriger**.En fonction des problèmes détectés, l'icône est rouge (indiquant des problèmes critiques) ou jaune (indiquant des problèmes non critiques).
   - Ouvrez la fenêtre de Bitdefender et cliquez dans la zone d'état de sécurité de la barre d'outils supérieure (vous pouvez par exemple cliquer sur le bouton **Tout corriger**).
2. Vous pouvez voir les problèmes affectant la sécurité de votre ordinateur et de vos données. Tous les problèmes présents sont sélectionnés pour être corrigés.

   Si vous ne souhaitez pas corriger un problème spécifique immédiatement, décochez la case correspondante. On vous demandera de spécifier pendant combien de temps vous souhaitez reporter la correction du problème. Sélectionnez l'option souhaitée dans le menu et cliquez sur **OK**.Pour cesser de surveiller cette catégorie de problème, sélectionnez **En permanence**.

L'état du problème deviendra **Reporter** et aucune action ne sera adoptée pour corriger le problème.

3. Pour corriger les problèmes sélectionnés, cliquez sur **Démarrer**. Certains problèmes sont corrigés immédiatement. Pour d'autres, un assistant vous aide à les corriger.

Les problèmes que cet assistant vous aide à corriger peuvent être regroupés dans les catégories suivantes :

- **Paramètres de sécurité désactivés.** Ces problèmes sont corrigés immédiatement en activant les paramètres de sécurité correspondants.
- **Tâches de sécurité préventives que vous avez besoin de réaliser.** Un assistant vous aide à corriger ces problèmes.

2.4.2. Configurer les alertes d'état

Le système d'alerte est préconfiguré pour surveiller et signaler les problèmes les plus importants qui peuvent compromettre la sécurité de votre ordinateur et de vos données.Outre les problèmes surveillés par défaut, plusieurs autres problèmes peuvent vous être signalés.

Vous pouvez configurer le système d'alertes afin de répondre au mieux à vos besoins de sécurité en choisissant des problèmes spécifiques sur lesquels vous souhaitez être informé.Suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Général** dans le menu de gauche puis sur l'onglet **Avancé**.
4. Recherchez et cliquez sur le lien **Configurer les alertes d'état**.
5. Cliquez sur les boutons pour activer ou désactiver les alertes d'état en fonction de vos préférences.

2.5. Événements

Bitdefender tient un journal détaillé des événements concernant son activité sur votre ordinateur (comprenant également les activités surveillées par le Contrôle Parental).Les événements sont un outil très important pour la surveillance et la gestion de votre protection Bitdefender.Par exemple, vous pouvez facilement vérifier qu'une mise à jour s'est effectuée correctement, s'il y a eu des malwares détectés sur votre ordinateur, etc.Vous pouvez également adopter d'autres actions si nécessaire ou modifier les actions appliquées par Bitdefender.

Pour ouvrir la fenêtre Événements, ouvrez la fenêtre Bitdefender et cliquez sur le bouton **Événements** de la barre d'outils supérieure.

Pour vous aider à filtrer les événements Bitdefender, les catégories suivantes sont disponibles dans le menu de gauche :

- **Antivirus**
- **Antispam**
- **Contrôle Parental**
- **Contrôle Vie Privée**
- **Pare-feu**
- **Optimisation**
- **SafeBox**
- **Mappage réseau**
- **Mise à jour**
- **SafeGo**
- **Enregistrement**

Une liste d'événements est disponible pour chaque catégorie. Pour des informations sur un événement de la liste, cliquez dessus. Des détails sur l'événement s'affichent alors dans la partie inférieure de la fenêtre. Chaque événement est accompagné des informations suivantes : une brève description, l'action que Bitdefender a appliqué et la date et l'heure de l'événement. Des options peuvent permettre d'appliquer une action supplémentaire si nécessaire.

Vous pouvez filtrer les événements en fonction de leur importance. Il y a trois types d'événements, chacun étant signalé par une icône spécifique :

Les événements **Informations** indiquent des opérations réussies.
Les événements d'**avertissement** indiquent des problèmes non critiques. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
Les événements **critiques** indiquent des problèmes critiques. Nous vous recommandons de les vérifier immédiatement.

Pour vous aider à gérer facilement les événements enregistrés, chaque section de la fenêtre Événements fournit des options permettant de supprimer ou de marquer comme lus tous les événements de cette section.

2.6. Auto-Pilot

Pour les utilisateurs qui souhaitent que leur solution de sécurité les protège sans les interrompre, Bitdefender Total Security 2012 dispose d'un mode de Pilotage Automatique intégré.

En Pilotage Automatique, Bitdefender applique une configuration de sécurité optimale et prend pour vous toutes les décisions de sécurité.Cela signifie qu'aucune fenêtre pop-up ni alerte ne s'affichera et que vous n'aurez aucun paramètre à configurer.

En mode de Pilotage Automatique, Bitdefender corrige automatiquement les problèmes critiques et gère :

- La protection antivirus, fournie par l'analyse à l'accès et l'analyse en continu.

- Protection pare-feu.
- La protection de la vie privée, fournie par le filtrage antiphishing et antimalware pour votre navigation web.
- Mises à jour automatiques.

Le Pilotage Automatique est lancé par défaut au moment où l'installation de Bitdefender se termine. Tant que le Pilotage Automatique sera activé, l'icône Bitdefender de la zone de notification deviendra .

Pour activer ou désactiver le Pilotage Automatique, ouvrez la fenêtre Bitdefender et cliquez sur le bouton **Auto-Pilot** de la barre d'outils supérieure.

Important
Lorsque le Pilotage Automatique est activé, modifier l'un des paramètres qu'il gère conduit à sa désactivation.

Pour afficher un historique des actions réalisées par Bitdefender alors que le Pilotage Automatique était en cours, ouvrez la fenêtre Événements.

2.7. Mode Jeu et Mode Portable

Certaines utilisations de l'ordinateur, comme les jeux ou les présentations, nécessitent plus de performance et de réactivité du système, et aucune interruption.Lorsque votre ordinateur portable est alimenté par sa batterie, il vaut mieux que les opérations non indispensables, qui consomment de l'énergie supplémentaire, soient reportées jusqu'au moment où l'ordinateur portable sera branché sur secteur.

Pour s'adapter à ces situations particulières, Bitdefender Total Security 2012 comprend deux modes de fonctionnement spéciaux :

- Mode Jeu
- Mode Portable

2.7.1. Mode Jeu

Le Mode Jeu modifie temporairement les paramètres de protection afin de minimiser leur impact sur les performances du système.Les paramètres suivants sont appliqués lorsque vous êtes en Mode Jeu :

- Toutes les alertes et fenêtres pop-up Bitdefender sont désactivées.
- L'Analyse automatique est désactivée.L'Analyse automatique détecte et utilise les moments pendant lesquels l'utilisation des ressources du système passe sous un certain seuil pour effectuer des analyses périodiques de l'ensemble du système.
- Le pare-feu Bitdefender est en mode normal (le **Mode paranoïaque** est désactivé).Cela signifie que toutes les nouvelles connexions (tant entrantes que

sortantes) seront automatiquement autorisées, et ce quels que soient le port et le protocole utilisés.

- La mise à jour automatique est désactivée.
- La synchronisation automatique est désactivée.
- La barre d'outils Bitdefender de votre navigateur web est désactivée lorsque vous jouez à des jeux pour navigateurs en ligne.

Lorsque vous êtes en Mode Jeu, vous pouvez voir la lettre G incrustée sur l'icône Bitdefender.

Utilisation du Mode Jeu

Par défaut, Bitdefender passe automatiquement en Mode Jeu lorsque vous lancez un jeu figurant dans la liste des jeux connus de Bitdefender, ou lorsqu'une application s'exécute en mode plein écran.Bitdefender reprendra automatiquement le mode de fonctionnement normal lorsque vous fermerez le jeu ou lorsque l'application détectée quittera le mode plein écran.

Si vous souhaitez activer manuellement le Mode Jeu, utilisez l'une des méthodes suivantes :

- Faites un Clic-droit sur l'icône Bitdefender dans la barre d'état et sélectionnez **Activer le Mode Jeu**.
- Appuyez sur les touches `Ctrl+Shift+Alt+G` (le raccourci clavier par défaut).

Important
N'oubliez pas de désactiver le Mode Jeu lorsque vous aurez fini. Pour cela, utilisez les mêmes méthodes que celles utilisées pour l'activer.

Changer le raccourci clavier pour passer en Mode Jeu

Vous pouvez passer manuellement en Mode Jeu en utilisant le raccourci clavier par défaut `Ctrl+Alt+Shift+G`.Pour changer le raccourci clavier, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Général** dans le menu de gauche puis sur l'onglet **Configuration**.
4. Sous l'option **Activer le raccourci clavier pour passer en Mode Jeu**, indiquez la touche de raccourci souhaitée :
   a. Choisissez la touche que vous souhaitez utiliser en cochant l'une des suivantes : touche Contrôle (`Ctrl`), Touche Shift(`Shift`) ou touche Alt (`Alt`).
   b. Dans le champ éditable, entrez la lettre que vous souhaitez utiliser.

Par exemple, si vous souhaitez utiliser le raccourci `Ctrl+Alt+D`, vous devez cocher seulement `Ctrl` et `Alt` et tapez `D`.

Note
Pour désactiver la touche de raccourci, désactivez l'option **Activer les raccourcis clavier pour passer en Mode Jeu**.

Activer ou désactiver le mode jeu automatique

Pour activer ou désactiver le mode jeu automatique, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Général** dans le menu de gauche puis sur l'onglet **Configuration**.
4. Activez ou désactivez le mode jeu automatique en cliquant sur le bouton correspondant.

2.7.2. Mode Portable

Le Mode Portable est spécialement conçu pour les utilisateurs d'ordinateurs portables et de notebooks. Son objectif est de minimiser l'impact de Bitdefender sur la consommation d'énergie lorsque ces périphériques sont alimentés par leur batterie.Quand Bitdefender fonctionne en Mode Portable, les fonctionnalités d'Analyse Automatique, de Mise à jour Automatique et de Synchronisation Automatique sont désactivées car elles nécessitent plus de ressources système et font donc augmenter la consommation d'énergie.

Bitdefender détecte le passage d'une alimentation secteur à une alimentation sur batterie et passe automatiquement en Mode Portable.De la même manière, Bitdefender quitte automatiquement le Mode Portable lorsqu'il détecte que l'ordinateur portable ne fonctionne plus sur batterie.

Pour activer ou désactiver le mode portable automatique, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Général** dans le menu de gauche puis sur l'onglet **Configuration**.
4. Activez ou désactivez le mode portable automatique en cliquant sur le bouton correspondant.

Si Bitdefender n'est pas installé sur un ordinateur portable, désactivez le mode portable automatique.

2.8. Paramètres Bitdefender de la protection par mot de passe

Si vous n'êtes pas le seul utilisateur avec des droits d'administrateur qui utilise cet ordinateur, il vous est recommandé de protéger vos paramètres Bitdefender par un mot de passe.

Pour configurer la protection par mot de passe des paramètres de Bitdefender, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Général** dans le menu de gauche puis sur l'onglet **Configuration**.
4. Dans la section **Paramètres de protection par mot de passe**, activez la protection par mot de passe en cliquant sur le bouton.
5. Cliquez sur le lien **Changer de mot de passe**.
6. Entrez le mot de passe dans les deux champs puis cliquez sur **OK**.(8 caractères minimum)

Une fois que vous avez défini un mot de passe, toute personne essayant de modifier les paramètres de Bitdefender devra indiquer ce mot de passe.

Important

N'oubliez pas votre mot de passe ou conservez-le en lieu sûr. Si vous oubliez le mot de passe, vous devrez réinstaller le programme ou contacter le support Bitdefender.

Pour supprimer la protection par mot de passe, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Général** dans le menu de gauche puis sur l'onglet **Configuration**.
4. Dans la section **Paramètres de protection par mot de passe**, désactivez la protection par mot de passe en cliquant sur le bouton.
5. Entrez le mot de passe puis cliquez sur **OK**.

2.9. Rapports d'utilisation anonymes

Par défaut, Bitdefender envoie des rapports contenant des informations sur votre utilisation aux serveurs Bitdefender.Ces informations sont essentielles pour améliorer le produit et nous aider à vous offrir un meilleur service à l'avenir. Veuillez noter que ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.

Si vous souhaitez cesser d'envoyer des rapports d'utilisation anonymes, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Général** dans le menu de gauche puis sur l'onglet **Avancé**.
4. Désactivez les rapports d'utilisation anonymes en cliquant sur le bouton correspondant.

2.10. Réparer ou désinstaller Bitdefender

Si vous souhaitez réparer ou supprimer Bitdefender Total Security 2012, suivez ce chemin à partir du menu Démarrer de Windows : **Démarrer → Tous les programmes → Bitdefender 2012 → Réparer ou Supprimer**.

Sélectionnez l'action que vous voulez effectuer.

- **Réparer** - pour réinstaller tous les composants du programme.
- **Supprimer** - pour supprimer tous les composants installés.

Note

Nous vous recommandons de sélectionner **Supprimer** pour que la réinstallation soit saine.

Veuillez attendre que Bitdefender termine l'action que vous avez sélectionnée. Cela prendra quelques minutes.

Vous aurez besoin de redémarrer l'ordinateur pour terminer le processus.

3. Interface de Bitdefender

Bitdefender Total Security 2012 répond aux besoins de tous les utilisateurs, qu'ils soient débutants ou armés de solides connaissances techniques. Son interface utilisateur graphique est conçue pour s'adapter à chaque catégorie d'utilisateurs.

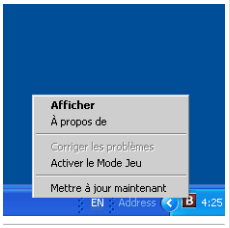
Pour afficher l'état du produit et effectuer des tâches essentielles, l'icône de la zone de notification de Bitdefender est disponible à tout moment.

La fenêtre principale vous permet d'accéder rapidement aux modules et aux informations importantes du produit, et vous permet d'effectuer les tâches courantes.

Pour configurer votre produit Bitdefender en détail et effectuer des tâches administratives avancées, vous trouverez tous les outils dont vous avez besoin dans la fenêtre de configuration.

3.1. Icône de la zone de notification

Pour gérer l'ensemble du produit plus rapidement, vous pouvez utiliser l'icône Bitdefender de la zone de notification.Double-cliquez sur cette icône pour ouvrir Bitdefender. Si vous effectuez un clic droit sur cette icône, le menu contextuel qui apparaît vous permettra de gérer le produit Bitdefender plus rapidement.



Icône

- **Afficher** - ouvre la fenêtre principale de Bitdefender.
- **À propos de** - Affichage d'une fenêtre contenant des informations relatives à Bitdefender, ainsi que des éléments d'aide si vous rencontrez une situation anormale.
- **Tout corriger** - vous aide à résoudre les problèmes de vulnérabilité de votre ordinateur en matière de sécurité.Si l'option n'est pas disponible, c'est qu'il n'y a pas de problème à corriger.Pour plus d'informations, reportez-vous à « *Correction des problèmes en cours.* » (p. 11).
- **Activer / désactiver le Mode Jeu** - active / désactive le Mode Jeu.
- **Mettre à jour** - effectue une mise à jour immédiate.Vous pouvez suivre l'état de mise à jour dans le panneau Mise à jour de la fenêtre principale de Bitdefender.

L'icône de la zone de notification de Bitdefender vous informe de la présence de problèmes affectant la sécurité de votre ordinateur et du fonctionnement du programme en affichant un symbole spécial :

D'importants problèmes affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.

Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.

Le produit fonctionne en Mode jeu.

Bitdefender Auto Pilot is engaged.

Si Bitdefender ne fonctionne pas, l'icône de la zone de notification apparaît sur un fond gris : .Cela se produit généralement lorsque la clé de licence expire. Cela peut également avoir lieu lorsque les services Bitdefender ne répondent pas ou lorsque d'autres erreurs affectent le fonctionnement normal de Bitdefender.

3.2. Fenêtre principale

La fenêtre principale de Bitdefender permet d'effectuer des tâches courantes, de corriger rapidement des problèmes de sécurité, d'afficher des informations sur des événements concernant le fonctionnement du produit et de personnaliser la configuration du produit. Tout se trouve à quelques clics.

La fenêtre est organisée en deux zones principales :

Barre d'outils supérieure
: Vous pouvez vérifier ici l'état de sécurité de votre ordinateur et accéder aux tâches importantes.

Panneaux
: Vous pouvez gérer ici les principaux modules de Bitdefender.

Vous trouverez également plusieurs liens utiles dans la partie inférieure de la fenêtre :

Lien	Description
Votre avis	Ouvre une page web dans votre navigateur où vous pouvez répondre à une petite enquête au sujet de votre utilisation du produit. Nous avons besoin de votre avis pour améliorer nos produits Bitdefender.
Terminer l'enregistrement / MyBitdefender	Ouvre la fenêtre MyBitdefender vous permettant de créer un compte ou de vous connecter à un compte existant. Un compte MyBitdefender est requis pour recevoir des mises à jour et bénéficier des fonctionnalités en ligne de votre produit. Pour plus d'informations sur la création d'un compte et les avantages que cela apporte, veuillez vous reporter à « *Connexion à MyBitdefender* » (p. 9).

Lien	Description
Informations de Licence	Ouvre une fenêtre où vous pouvez voir des informations sur la clé de licence actuelle et enregistrer votre produit avec une nouvelle clé de licence.
Aide et Support	Cliquez sur ce lien si vous avez besoin d'aide avec Bitdefender.
	Ajoute des points d'interrogation à différents endroits de la fenêtre Bitdefender afin de vous aider à trouver facilement des informations sur les différents éléments de l'interface. Placez le curseur de votre souris sur un point d'interrogation pour disposer rapidement d'informations sur l'élément qui se trouve à côté.

3.2.1. Barre d'outils supérieure

La barre d'outils supérieure contient les éléments suivants :

- La **Zone d'État de Sécurité** à gauche de la barre d'outils vous indique si des problèmes affectent la sécurité de votre ordinateur et vous aide à les corriger.

  La couleur de la zone d'état de sécurité change en fonction des problèmes détectés et différents messages s'affichent :

  - **La zone est en vert.** Il n'y a pas de problèmes à corriger. Votre ordinateur et vos données sont protégés.
  - **La zone est en jaune.** Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
  - **La zone est en rouge.** Des problèmes critiques affectent la sécurité de votre système. Nous vous recommandons de vous occuper de ces problèmes immédiatement.

  En cliquant sur le bouton **Afficher les problèmes** au centre de la barre d'outils ou ailleurs dans la zone d'état de sécurité à gauche, vous pouvez accéder à un assistant qui vous aidera à supprimer facilement toutes les menaces de votre ordinateur. Pour plus d'informations, reportez-vous à « *Correction des problèmes en cours.* » (p. 11).

- **Événements** vous permet d'accéder à un historique détaillé des événements importants survenus lors de l'activité du produit. Pour plus d'informations, reportez-vous à « *Événements* » (p. 13).
- **Configuration** vous permet d'accéder à une fenêtre où vous pouvez configurer les paramètres du produit. Pour plus d'informations, reportez-vous à « *Fenêtre de configuration* » (p. 27).

- **Auto-Pilot** vous permet de lancer le pilotage automatique et de profiter d'une sécurité totalement silencieuse.Pour plus d'informations, reportez-vous à « *Auto-Pilot* » (p. 14).

3.2.2. Panneaux

La zone des panneaux vous permet de gérer directement les modules Bitdefender.

Vous pouvez organiser les panneaux comme vous le souhaitez. Pour réorganiser la zone en fonction de vos besoins, faites glisser les panneaux individuels et déposez-les à d'autres endroits.

Pour accéder aux panneaux, utilisez le curseur sous les panneaux ou les flèches situées à droite et à gauche.

De haut en bas, chaque panneau du module contient les éléments suivants :

- Le nom du module.
- Un message d'état.
- L'icône du module. Cliquez sur l'icône d'un module pour configurer ses paramètres dans la fenêtre de configuration.
- Un bouton qui vous permet d'effectuer des tâches importantes liées au module.
- Un bouton est disponible sur certains panneaux vous permettant d'activer ou de désactiver une importante fonctionnalité du module.

Les panneaux disponibles dans cette zone sont :

Antivirus

La protection antivirus est la base de votre sécurité. Bitdefender vous protège en temps réel et à la demande contre toutes sortes de malwares tels que les virus, les chevaux de Troie, les spywares, les adwares etc.

Le panneau Antivirus vous permet d'accéder facilement aux principales tâches d'analyse. Cliquez sur **Analyser** et sélectionnez une tâche dans le menu déroulant :

- Analyse Rapide
- Analyse Complète
- Analyse personnalisée
- Vulnérabilité
- Mode de secours

Le bouton **Analyse Auto.** vous permet d'activer et de désactiver la fonctionnalité d'Analyse automatique.

Pour plus d'informations sur les tâches d'analyse et sur comment configurer la protection antivirus, reportez-vous à « *Protection antivirus* » (p. 44).

Pare-feu

Le pare-feu vous protège lorsque vous êtes connecté à des réseaux et à Internet en filtrant toute tentative de connexion.

En cliquant sur **Informations sur le réseau** dans le panneau Pare-feu, vous pouvez configurer les paramètres de connexion réseau.

Le bouton Pare-feu vous permet d'activer et de désactiver la protection pare-feu.

Avertissement

La désactivation du pare-feu exposant votre ordinateur à des connexions non autorisées, il devrait s'agir d'une mesure temporaire. Réactivez le pare-feu dès que possible.

Pour plus d'informations sur la configuration du pare-feu, reportez-vous à « *Pare-feu* » (p. 112).

Antispam

Le module antispam Bitdefender protège votre boîte de réception contre les e-mails indésirables en filtrant le trafic de messagerie POP3.

Cliquez sur **Gérer** dans le panneau Antispam et sélectionnez Amis ou Spammeurs dans le menu déroulant pour modifier la liste d'adresses correspondante.

Le bouton Antispam vous permet d'activer et de désactiver la protection antispam.

Pour plus d'informations sur la configuration de la protection antispam, reportez-vous à « *Antispam* » (p. 69).

Mise à jour

Dans un monde où les cybercriminels recherchent sans cesse de nouveaux moyens de nuire, il est essentiel de maintenir sa solution de sécurité à jour afin de conserver une longueur d'avance sur eux.

Par défaut, Bitdefender recherche automatiquement des mises à jour toutes les heures. Si vous souhaitez désactiver les mises à jour automatiques, utilisez le bouton **Automatique** du panneau Mise à jour.

Avertissement

Cela peut poser un problème de sécurité important. Nous vous recommandons de désactiver la mise à jour automatique pendant le moins de temps possible. Si Bitdefender n'est pas régulièrement mis à jour, il ne pourra pas vous protéger contre les dernières menaces.

Cliquez sur le bouton **Mettre à jour maintenant** du panneau pour lancer immédiatement une mise à jour.

Pour plus d'informations sur la configuration des mises à jour, reportez-vous à « *Mise à jour* » (p. 133).

Contrôle Parental

Bitdefender Total Security 2012 propose un ensemble complet de contrôles parentaux qui vous aide à protéger et à surveiller l'utilisation de l'ordinateur de vos enfants.

Cliquez sur **Gérer les comptes** dans le panneau du Contrôle Parental pour configurer les paramètres des comptes utilisateurs Windows de l'ordinateur.

Pour plus d'informations sur la configuration du Contrôle Parental, reportez-vous à « *Contrôle Parental* » (p. 97).

Contrôle Vie Privée

Le module contrôle vie privée vous aide à assurer la confidentialité de vos données personnelles importantes. Il vous protège lorsque vous êtes sur Internet contre les attaques de phishing, les tentatives de fraude, les fuites d'informations confidentielles etc.

Cliquez sur le bouton **Crypter** du panneau Contrôle vie privée et sélectionnez une tâche dans le menu déroulant :

- **Ajout au coffre-fort** - lance un assistant vous permettant d'ajouter vos fichiers importants à un coffre-fort sécurisé, crypté.
- **Destructeur de Fichiers** - lance un assistant qui vous permet de supprimer définitivement des fichiers.

Le bouton Antiphishing vous permet d'activer et de désactiver la protection antiphishing.

Pour plus d'informations sur comment configurer Bitdefender pour protéger votre vie privée, reportez-vous à « *Contrôle Vie Privée* » (p. 80).

SafeBox

SafeBox vous permet de sauvegarder vos fichiers importants sur des serveurs en ligne sécurisés et de les partager entre des ordinateurs disposant de Bitdefender Total Security 2012.

Cliquer sur **Gérer** vous permet de sélectionner une tâche dans le menu déroulant :

- **Sauvegarder** - synchronise immédiatement les dossiers locaux ajoutés à SafeBox avec les dossiers distants (en ligne).
- **Gérer les dossiers** - vous permet d'ajouter ou de retirer des dossiers de SafeBox, ou de modifier la façon dont les dossiers SafeBox locaux et distants sont liés.

Le bouton Sync. auto. vous permet d'activer et de désactiver la synchronisation pour les dossiers SafeBox.

Pour plus d'informations, reportez-vous à « *Sauvegarde en ligne de SafeBox* » (p. 137).

Mappage réseau

Le Mappage Réseau vous permet de gérer facilement la sécurité des ordinateurs de votre domicile à partir d'un seul ordinateur.

Pour commencer, cliquez sur **Gérer** dans le panneau Mappage Réseau et sélectionnez **Activer le réseau**.

Une fois le réseau activé, cliquer sur **Gérer** dans le panneau Mappage Réseau vous donnera accès aux options suivantes.

- **Désactiver la connexion** - permet de désactiver le réseau.
- **Tout analyser** - permet de lancer une analyse rapide ou une analyse complète du système sur les ordinateurs administrés.
- **Mise à jour de tous les ordinateurs** - permet de mettre à jour les produits Bitdefender sur les ordinateurs gérés.

Pour plus d'informations, reportez-vous à « *Mappage réseau* » (p. 129).

Optimisation

Bitdefender Total Security 2012 offre plus que de la sécurité, et contribue également aux bonnes performances de votre ordinateur.

Cliquer sur **Optimiser** dans le panneau Optimisation vous donne accès à un nombre d'outils utiles :

- Nettoyage du PC
- Défragmentation
- Détecteur de doublons
- Nettoyage du Registre
- Restauration Registre

Pour plus d'informations sur les outils d'optimisation des performances, veuillez vous référer à « *Optimisation* » (p. 122).

Safego

Pour vous aider à profiter de Facebook en toute sécurité, vous pouvez accéder à Safego, la solution de sécurité Bitdefender pour réseaux sociaux, directement à partir de votre logiciel.

Cliquez sur **Activer** pour activer et gérer Safego à partir de votre compte Facebook.

Si vous avez déjà activé Safego, vous aurez accès à des statistiques sur son activité en cliquant sur le bouton **Afficher les rapports**.

Pour plus d'informations, reportez-vous à « *Protection Safego pour réseaux sociaux* » (p. 141).

3.3. Fenêtre de configuration

La fenêtre de configuration vous permet d'accéder à chaque composant du produit et de le personnaliser. Vous pouvez configurer ici Bitdefender en détail.

À gauche de la fenêtre figure un menu contenant l'intégralité des modules de sécurité.Chaque module comprend un ou plusieurs onglet(s) où vous pouvez configurer les paramètres de sécurité correspondants, et effectuer des actions de sécurité ou des tâches administratives.La liste suivante décrit brièvement chaque module.

Général
: Vous permet de configurer les paramètres généraux du produit, tels que le mot de passe des paramètres, le Mode Jeu, le Mode Portable, les paramètres du proxy et les alertes d'état.

Antivirus
: Vous permet de configurer votre protection contre les malwares, de détecter et de corriger les vulnérabilités de votre système, de définir des exceptions d'analyse et de gérer les fichiers en quarantaine.

Antispam
: Vous permet de conserver votre boîte de réception sans SPAM et de configurer les paramètres antispam en détail.

Contrôle Parental
: Vous permet de protéger vos enfants contre les contenus inappropriés en appliquant vos droits d'accès personnalisés à l'ordinateur.

Contrôle Vie Privée
: Vous permet d'éviter le vol de données sur votre ordinateur et de protéger votre vie privée lorsque vous êtes en ligne.Configurez la protection de votre navigateur web, de vos logiciels de messagerie instantanée, gérez la protection des données et plus encore.

Pare-feu
: Vous permet de configurer les paramètres généraux du pare-feu, les règles de pare-feu, la détection d'intrusion, et de surveiller l'activité du réseau.

SafeBox
: Vous permet de configurer des sauvegardes et une synchronisation des données en ligne entre vos ordinateurs disposant de Bitdefender Total Security 2012.

Optimisation
: Vous permet d'améliorer les performances de votre ordinateur en défragmentant votre disque dur, en nettoyant le Registre Windows, en supprimant les doublons, etc.

Mappage réseau
Vous permet de configurer et de gérer les produits Bitdefender installés sur tous les ordinateurs de votre foyer à partir d'un seul et même ordinateur.

Mise à jour
Vous permet d'obtenir des informations sur les dernières mises à jour, de mettre à jour votre produit et de configurer en détail le processus de mise à jour.

Vous trouverez également plusieurs liens utiles dans la partie inférieure de la fenêtre :

Lien	Description
Votre avis	Ouvre une page web dans votre navigateur où vous pouvez répondre à une petite enquête au sujet de votre utilisation du produit. Nous avons besoin de votre avis pour améliorer nos produits Bitdefender.
Terminer l'enregistrement / MyBitdefender	Ouvre la fenêtre MyBitdefender vous permettant de créer un compte ou de vous connecter à un compte existant. Un compte MyBitdefender est requis pour recevoir des mises à jour et bénéficier des fonctionnalités en ligne de votre produit. Pour plus d'informations sur la création d'un compte et les avantages que cela apporte, veuillez vous reporter à « *Connexion à MyBitdefender* » (p. 9).
Informations de Licence	Ouvre une fenêtre où vous pouvez voir des informations sur la clé de licence actuelle et enregistrer votre produit avec une nouvelle clé de licence.
Aide et Support	Cliquez sur ce lien si vous avez besoin d'aide avec Bitdefender.
	Ajoute des points d'interrogation à différents endroits de la fenêtre Bitdefender afin de vous aider à trouver facilement des informations sur les différents éléments de l'interface. Placez le curseur de votre souris sur un point d'interrogation pour disposer rapidement d'informations sur l'élément qui se trouve à côté.

Pour revenir à la fenêtre principale, cliquez sur le bouton **Accueil** dans l'angle supérieur droit de la fenêtre.

4. Comment

Ce chapitre fournit des instructions pas à pas pour configurer les paramètres couramment utilisés ou pour terminer les tâches courantes avec Bitdefender.Certains sujets font référence à d'autres sujets où vous pouvez trouver des informations détaillées.

- « *Comment améliorer les performances de mon système ?* » (p. 29)
- « *Comment enregistrer une version d'essai ?* » (p. 31)
- « *Comment enregistrer Bitdefender sans connexion Internet ?* » (p. 32)
- « *Comment mettre à niveau vers un autre produit Bitdefender 2012 ?* » (p. 33)
- « *Quand devrais-je réinstaller Bitdefender ?* » (p. 33)
- « *Quand ma protection Bitdefender expire-t-elle ?* » (p. 33)
- « *Comment renouveler ma protection Bitdefender ?* » (p. 34)
- « *Quel est le produit Bitdefender que j'utilise ?* » (p. 34)
- « *Comment analyser un fichier ou un dossier ?* » (p. 35)
- « *Comment analyser mon système ?* » (p. 35)
- « *Comment créer une tâche d'analyse personnalisée ?* » (p. 35)
- « *Comment exclure un dossier de l'analyse ?* » (p. 36)
- « *Que faire lorsque Bitdefender a détecté un fichier sain comme étant infecté ?* » (p. 36)
- « *Comment créer des comptes utilisateurs Windows ?* » (p. 37)
- « *Comment protéger mes enfants des menaces sur Internet ?* » (p. 38)
- « *Comment débloquer un site web bloqué par le Contrôle Parental ?* » (p. 39)
- « *Comment protéger mes informations personnelles ?* » (p. 40)
- « *Comment utiliser les coffres-forts ?* » (p. 40)
- « *Où voir l'espace restant sur ma SafeBox ?* » (p. 42)
- « *Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?* » (p. 42)

4.1. Comment améliorer les performances de mon système ?

Les performances système dépendent entre autres de la configuration matérielle, comme la charge du processeur, l'utilisation de la mémoire et l'espace sur le disque dur.Il est aussi lié directement à votre configuration logicielle et à la gestion de vos données.

Voici les principales actions que vous pouvez appliquer avec Bitdefender pour améliorer la vitesse et les performances de votre système :

- « *Défragmentez votre disque dur* » (p. 30)
- « *Nettoyez votre PC* » (p. 30)
- « *Nettoyer le Registre Windows* » (p. 30)
- « *Analysez votre système régulièrement* » (p. 31)

4.1.1. Défragmentez votre disque dur

Nous vous recommandons de défragmenter le disque dur afin d'accéder aux fichiers plus rapidement et d'améliorer la performance globale du système. La Défragmentation vous aide à réduire la fragmentation des fichiers et améliore les performances de votre système.

Pour lancer la défragmentation, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Optimisation**.
3. Cliquez sur **Optimiser** et sélectionnez **Défragmentation** dans le menu déroulant.
4. Suivez les étapes de l'assistant.

4.1.2. Nettoyez votre PC

Le Nettoyage du PC améliore les performances du système en supprimant les fichiers qui ne sont plus utiles comme les fichiers Internet temporaires, les cookies et les fichiers temporaires du système.

Pour lancer le Nettoyage du PC, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Optimisation**.
3. Cliquez sur **Optimiser** et sélectionnez **Nettoyage du PC** dans le menu déroulant.
4. Suivez les étapes de l'assistant.

4.1.3. Nettoyer le Registre Windows

Nettoyer le Registre Windows peut améliorer les performances de votre système. Pour cela, utilisez le Nettoyage du Registre.Le Nettoyage du Registre analyse le Registre Windows et supprime les clés de registre non valides.

Pour lancer le Nettoyage du Registre, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Optimisation**.

3. Cliquez sur **Optimiser** et sélectionnez **Nettoyage du Registre** dans le menu déroulant.
4. Suivez les étapes de l'assistant.

4.1.4. Analysez votre système régulièrement

La vitesse de votre système et son comportement général peuvent également être affectés par des malwares.

Veillez à analyser votre système régulièrement, au moins une fois par semaine.

Il est recommandé d'utiliser l'Analyse Complète car elle recherche tous les types de malwares menaçant la sécurité de votre système et analyse également l'intérieur des archives.

Pour lancer l'Analyse Complète du Système, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Antivirus**.
3. Cliquez sur **Analyser** et sélectionnez **Analyse Complète** dans le menu déroulant.
4. Suivez les étapes de l'assistant.

4.2. Comment enregistrer une version d'essai ?

Si vous avez installé une version d'essai, vous ne pourrez l'utiliser que pendant une période limitée. Pour continuer à utiliser Bitdefender une fois la période d'essai terminée, vous devez enregistrer votre produit avec une clé de licence et créer un compte MyBitdefender.

- Pour enregistrer Bitdefender, procédez comme suit :
  1. Ouvrez la fenêtre de Bitdefender.
  2. Cliquez sur le lien **Informations de Licence** en bas de la fenêtre.La fenêtre d'enregistrement est alors affichée.
  3. Saisissez la clé de licence, puis cliquez sur **S'enregistrer**.

     Si vous n'avez pas de clé de licence, cliquez sur le lien de la fenêtre pour vous rendre sur une page web vous permettant d'en acheter une.
  4. Attendez la fin du processus d'enregistrement et fermez la fenêtre.
- Pour créer un compte MyBitdefender, suivez ces étapes :
  1. Ouvrez la fenêtre de Bitdefender.
  2. Cliquez sur le lien **Terminer l'enregistrement** en bas de la fenêtre. La fenêtre du compte s'affichera.
  3. Sélectionnez le lien correspondant pour créer un nouveau compte.

4. Tapez les informations requises dans les champs correspondants. Les informations communiquées ici resteront confidentielles.

   Cliquez sur **Envoyer**.

5. Consultez votre messagerie et suivez les instructions reçues afin de terminer l'enregistrement.

Note
Vous pouvez utiliser l'adresse e-mail et le mot de passe indiqués pour vous connecter à votre compte sur http://my.bitdefender.com.

4.3. Comment enregistrer Bitdefender sans connexion Internet ?

Si vous venez d'acheter Bitdefender et que vous n'avez pas de connexion Internet, vous pouvez enregistrer Bitdefender hors ligne.

Pour enregistrer Bitdefender avec votre clé de licence, procédez comme suit :

1. Allez sur un PC connecté à Internet. Vous pouvez par exemple utiliser l'ordinateur d'un ami ou un PC à partir d'un emplacement public.
2. Allez dans https://my.bitdefender.com pour créer un compte MyBitdefender.
3. Connectez-vous à votre compte et sélectionnez **Enregistrement hors connexion**.
4. Saisissez la clé de licence que vous avez achetée.
5. Cliquez sur **Soumettre** pour obtenir un code de confirmation.

Important
Notez le code de confirmation.

6. Retournez à votre PC avec le code de confirmation.
7. Ouvrez la fenêtre de Bitdefender.
8. Cliquez sur le lien **Informations de Licence** en bas de la fenêtre.La fenêtre d'enregistrement est alors affichée.
9. Sélectionnez l'option pour enregistrer le produit avec un code de confirmation.
10. Saisissez le code de confirmation dans le champ correspondant et cliquez sur **Soumettre**.
11. Attendez la fin du processus d'enregistrement et cliquez sur **Terminer**.

4.4. Comment mettre à niveau vers un autre produit Bitdefender 2012 ?

Vous pouvez facilement effectuer une mise à niveau d'un produit Bitdefender 2012 à un autre.

Il vous suffit d'acheter une clé de licence pour le produit Bitdefender 2012 vers lequel vous souhaitez mettre à niveau et de la saisir dans la fenêtre d'enregistrement du produit Bitdefender 2012 que vous utilisez actuellement.

Suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le lien **Informations de Licence** en bas de la fenêtre.La fenêtre d'enregistrement est alors affichée.
3. Saisissez la clé de licence, puis cliquez sur **S'enregistrer**.
4. Bitdefender vous indiquera que la clé de licence est destinée à un produit différent et vous donnera la possibilité de l'installer.Cliquez sur le lien correspondant, puis suivez la procédure pour effectuer la mise à niveau.

4.5. Quand devrais-je réinstaller Bitdefender ?

Dans certains cas, vous pouvez avoir besoin de réinstaller votre produit Bitdefender.

Quelques situations typiques nécessitant de réinstaller Bitdefender :

- vous avez réinstallé le système d'exploitation
- vous avez acheté un nouvel ordinateur
- vous souhaitez modifier la langue d'affichage de l'interface de Bitdefender

Pour réinstaller Bitdefender, vous pouvez utiliser le disque d'installation que vous avez acheté ou télécharger une nouvelle version sur le site web de Bitdefender.

Au cours de l'installation, on vous demandera d'enregistrer le produit avec votre clé de licence.

Si vous perdez votre clé de licence, vous pouvez la retrouver en vous connectant à https://my.bitdefender.com.Tapez l'adresse e-mail et le mot de passe de votre compte dans les champs correspondants.

4.6. Quand ma protection Bitdefender expire-t-elle ?

Pour connaître le nombre de jours restants de votre clé de licence, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le lien **Informations de Licence** en bas de la fenêtre.
3. La fenêtre **Enregistrez votre produit** indique le nombre de jours restants.

4.7. Comment renouveler ma protection Bitdefender ?

Lorsque votre protection Bitdefender est sur le point d'expirer, vous devez renouveler votre clé de licence.

- Suivez ces étapes pour visiter un site web où vous pouvez renouveler votre clé de licence Bitdefender :
  1. Ouvrez la fenêtre de Bitdefender.
  2. Cliquez sur le lien **Informations de Licence** en bas de la fenêtre.
  3. Cliquez sur **Vous n'avez pas de clé de licence ? Achetez-en une maintenant !**
  4. Une page web s'ouvrira dans votre navigateur web, vous permettant d'acheter une clé de licence Bitdefender.

  Note
  Vous pouvez également contacter le revendeur vous ayant vendu votre produit Bitdefender.

- Suivez ces étapes pour enregistrer votre Bitdefender avec la nouvelle clé de licence :
  1. Ouvrez la fenêtre de Bitdefender.
  2. Cliquez sur le lien **Informations de Licence** en bas de la fenêtre.La fenêtre d'enregistrement est alors affichée.
  3. Saisissez la clé de licence, puis cliquez sur **S'enregistrer**.
  4. Attendez la fin du processus d'enregistrement et fermez la fenêtre.

Pour plus d'informations, vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Support* » (p. 166).

4.8. Quel est le produit Bitdefender que j'utilise ?

Pour découvrir quel programme Bitdefender vous avez installé, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. En haut de la fenêtre devrait apparaître l'un des éléments suivants :
   - Bitdefender Antivirus Plus 2012
   - Bitdefender Internet Security 2012
   - Bitdefender Total Security 2012

4.9. Comment analyser un fichier ou un dossier ?

La méthode la plus simple, et celle que nous vous recommandons, pour analyser un fichier ou un dossier consiste à faire un clic droit sur l'objet que vous souhaitez analyser et à sélectionner **Analyser avec Bitdefender** dans le menu.Pour terminer l'analyse, suivez l'assistant d'analyse antivirus.

Cette méthode d'analyse est à utiliser dans des situations typiques qui englobent les cas suivants :

- Vous soupçonnez un fichier ou un dossier donné d'être infecté.
- Quand vous téléchargez sur Internet des fichiers dont vous pensez qu'ils pourraient être dangereux.
- Analysez un dossier partager sur le réseau avant de copier des fichiers sur votre ordinateur.

4.10. Comment analyser mon système ?

Pour effectuer une analyse complète du système, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Antivirus**.
3. Cliquez sur **Analyser** et sélectionnez **Analyse Complète** dans le menu déroulant.
4. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse.

4.11. Comment créer une tâche d’analyse personnalisée ?

Pour créer une tâche d'analyse personnalisée, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Antivirus**.
3. Cliquez sur **Analyser** et sélectionnez **Analyse personnalisée** dans le menu déroulant.
4. Cliquez sur **Ajouter cible** pour sélectionner les fichiers ou les dossiers à analyser.
5. Si vous souhaitez configurer les options d’analyse en détail, cliquez sur **Options d'analyse**.

   Vous pouvez sélectionner l'option **Éteindre l'ordinateur**.

   Si aucune menace n'est détectée pendant l'analyse, votre ordinateur sera éteint une fois l'analyse terminée. N'oubliez pas qu'il s'agira du comportement par défaut à chaque fois que vous exécuterez cette tâche.
6. Cliquez sur **Démarrer l'analyse** pour exécuter la tâche.

4.12. Comment exclure un dossier de l'analyse ?

Bitdefender vous permet d'exclure de l'analyse certains fichiers, dossiers ou extensions de fichiers.

Les exclusions doivent être employées par des utilisateurs ayant un niveau avancé en informatique et uniquement dans les situations suivantes :

- Vous avez un dossier important sur votre système où se trouvent des films et de la musique.
- Vous avez une archive importante sur votre système où se trouvent différentes données.
- Vous gardez un dossier où vous installez différents types de logiciels et applications à des fins de test. L'analyse du dossier peut conduire à la perte de certaines données.

Pour ajouter le dossier à la liste d'exceptions, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Exclusions**.
4. Cliquez sur le lien **Fichiers et dossiers exclus**.
5. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
6. Cliquez sur **Parcourir**, sélectionnez le dossier à exclure de l'analyse, puis cliquez sur **OK**.
7. Cliquez sur **Ajouter** puis sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

4.13. Que faire lorsque Bitdefender a détecté un fichier sain comme étant infecté ?

Il arrive parfois que Bitdefender indique par erreur qu'un fichier légitime est une menace (une fausse alerte).Pour corriger cette erreur, ajoutez le fichier à la zone des exclusions de Bitdefender :

1. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Ouvrez la fenêtre de Bitdefender.
   b. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
   c. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Résident**.
   d. Cliquez sur le bouton pour désactiver **l'analyse à l'accès**.

2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, reportez-vous à « *Comment afficher des objets masqués dans Windows ?* » (p. 177).
3. Restaurer le fichier à partir de la zone de Quarantaine :
   a. Ouvrez la fenêtre de Bitdefender.
   b. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
   c. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Quarantaine**.
   d. Sélectionnez le fichier et cliquez sur **Restaurer**.
4. Ajouter le fichier à la liste d'exceptions. Pour savoir comment faire cela, reportez-vous à « *Comment exclure un dossier de l'analyse ?* » (p. 36).
5. Activez la protection antivirus en temps réel de Bitdefender.
6. Contactez les représentants de notre support technique afin que nous puissions supprimer la signature de détection. Pour savoir comment faire cela, reportez-vous à « *Demander de l'aide* » (p. 167).

4.14. Comment créer des comptes utilisateurs Windows ?

Un compte utilisateur Windows est un profil unique qui inclut tous les paramètres, privilèges et fichiers personnels de chaque utilisateur.Les comptes Windows permettent à l'administrateur des PC de contrôler l'accès de chaque utilisateur.

Il s'avère pratique de créer des comptes utilisateur lorsque le PC est utilisé à la fois par les parents et les enfants ; un parent peut créer des comptes pour chaque enfant.

Choisissez le système d'exploitation que vous avez, afin de savoir comment créer des comptes Windows.

- Windows XP :
  1. Connectez-vous à votre ordinateur en tant qu'administrateur.
  2. Cliquez sur Démarrer, Panneau de configuration puis sur Comptes d'utilisateur.
  3. Cliquez sur Créer un nouveau compte.
  4. Saisissez le nom de l'utilisateur. Vous pouvez utiliser le nom complet de la personne, son prénom ou un surnom. Cliquez ensuite sur Suivant.
  5. Concernant le type de compte, choisissez Limité, puis Créer un compte. Les comptes limités sont adaptés aux enfants car ils ne peuvent pas faire de modification globale dans le système ou installer certaines applications.
  6. Votre nouveau compte aura été créé et apparaîtra dans l'écran Gérer les comptes.
- Windows Vista ou Windows 7 :

1. Connectez-vous à votre ordinateur en tant qu'administrateur.
2. Cliquez sur Démarrer, Panneau de configuration puis sur Comptes d'utilisateur.
3. Cliquez sur Créer un nouveau compte.
4. Saisissez le nom de l'utilisateur. Vous pouvez utiliser le nom complet de la personne, son prénom ou un surnom. Cliquez ensuite sur Suivant.
5. Pour le type de compte, cliquez sur Standard, puis sur Créer un compte. Les comptes limités conviennent particulièrement aux enfants car ils ne peuvent pas effectuer de modifications portant sur le système ni installer certaines applications.
6. Votre nouveau compte aura été créé et apparaîtra dans l'écran Gérer les comptes.

Note
Maintenant que vous avez ajouté de nouveaux comptes utilisateurs, vous pouvez créer des mots de passe pour ces comptes.

4.15. Comment protéger mes enfants des menaces sur Internet ?

Le Contrôle Parental de Bitdefender vous permet de limiter l'accès à Internet et à certaines applications, empêchant ainsi vos enfants de visualiser du contenu inapproprié en votre absence.

Vous pouvez configurer le contrôle parental pour bloquer :

- aux pages Web indésirables.
- l'accès à Internet, pour des périodes bien définies (l'heure des devoirs, par exemple).
- les pages Internet, les e-mails et les messages instantanées comportant des mots clés spécifiques.
- les applications comme des jeux, des chats, des programmes de partage de fichiers et autres.
- les messages instantanées envoyés par des contacts de messagerie instantanée autres que ceux autorisés.

Pour configurer le contrôle parental, suivez ces étapes :

1. Créez un compte utilisateur Windows limité (standard) destiné à vos enfants.Pour plus d'informations, reportez-vous à « *Comment créer des comptes utilisateurs Windows ?* » (p. 37).
2. Assurez-vous d'être connecté à l'ordinateur en utilisant un compte administrateur.Seuls les utilisateurs ayant des droits d'administrateur sur le système peuvent avoir accès et configurer le contrôle parental.

3. Configurer le Contrôle Parental du compte utilisateur Windows utilisé par vos enfants.
   a. Ouvrez la fenêtre de Bitdefender.
   b. Allez dans le panneau **Parental**.
   c. Cliquez sur **Gérer les comptes** et vérifiez que le contrôle parental est activé pour le compte utilisateur de votre enfant.
   d. Définissez l'âge de votre enfant en sélectionnant l'une des cases correspondant à l'option **Age**.Si vous précisez l'âge de l'enfant, des paramètres considérés comme étant adaptés à cet âge seront automatiquement chargés, basés sur les normes de développement de l'enfant.
   e. Si vous souhaitez configurer tous les paramètres du Contrôle Parental en détail, cliquez sur **Configuration**.

Pour des informations détaillées sur l'utilisation du Contrôle Parental, reportez-vous à « *Contrôle Parental* » (p. 97).

4.16. Comment débloquer un site web bloqué par le Contrôle Parental ?

Le Contrôle Parental de Bitdefender vous permet de contrôler le contenu auquel vos enfants accèdent lorsqu'ils utilisent l'ordinateur.

Si vous définissez la catégorie d'âge pour votre enfant dans le Contrôle Parental et n'utilisez qu'un compte Windows, vous ne pourrez pas accéder aux sites web considérés comme inadaptés à la catégorie d'âge sélectionnée.

Si le Contrôle Parental bloque l'accès à un site Web, vous pouvez créer une règle pour autoriser explicitement l'accès à ce site Web.

Pour autoriser l'accès à un site web, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Parental**.
3. Cliquez sur **Gérer les comptes**.
4. Cliquez sur le bouton **Configuration** pour configurer les paramètres utilisateur.
5. Cliquez sur **Autoriser le site Web**.
6. Saisissez l'adresse du site Internet dans le champ **Site Web**.
7. Sélectionnez l'action souhaitée pour cette règle - **Autoriser** et cliquez sur **Terminer** pour ajouter la règle.
8. Ouvrez votre navigateur et accédez au site web.

4.17. Comment protéger mes informations personnelles ?

Le Contrôle Vie Privée surveille les données quittant votre ordinateur via des formulaires web, des e-mails ou des messages instantanés.

Pour vous assurer qu'aucune donnée à caractère personnel ne quitte votre ordinateur sans votre accord, vous devez créer des règles de protection des données et les exceptions à ces règles.

Les règles de protection des données indiquent les informations à bloquer.

Pour créer une règle de Protection des données, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Contrôle Vie Privée** dans le menu de gauche puis sur l'onglet **Protection des données**.
4. Si la **Protection des données** est désactivée, activez-la à l'aide du bouton correspondant.
5. Sélectionnez l'option **Ajouter une règle** pour lancer l'assistant de Protection des données.
6. Suivez les étapes de l'assistant.

4.18. Comment utiliser les coffres-forts ?

La fonction Coffre-fort de Bitdefender vous permet de créer des disques logiques cryptés et protégés par mot de passe (appelés « coffres-forts ») sur votre ordinateur, afin d'y stocker vos documents confidentiels et sensibles.Physiquement, le coffre-fort est un fichier stocké sur le disque dur en local et ayant une extension .bvd.

Lorsque vous créez un coffre-fort, deux éléments sont importants : la taille et le mot de passe. La taille par défaut de 50 Mo devrait suffire pour vos documents personnels, fichiers Excel etc. Vous pouvez cependant avoir besoin de plus d'espace pour des vidéos ou d'autres fichiers volumineux.

Pour stocker en toute sécurité vos fichiers ou dossiers confidentiels ou sensibles dans des coffres-forts Bitdefender, procédez comme suit :

- **Créez un coffre-fort et définissez un mot de passe sécurisé pour celui-ci.**

  Pour créer un coffre-fort, faites un clic droit sur une zone vide du Bureau ou dans un dossier de votre ordinateur, pointez sur Coffre-fort Bitdefender et sélectionnez **Créer un coffre-fort** .

  Une nouvelle fenêtre apparaîtra. Procédez comme suit :

  1. Cliquez sur **Parcourir** pour sélectionner l'emplacement du coffre-fort et sauvegardez le coffre-fort sous le nom que vous souhaitez.

2. Choisissez une lettre de lecteur à partir du menu. Quand vous ouvrez le coffre, un disque virtuel indexé avec la lettre choisie apparaît dans **Poste de travail**.
3. Saisissez le mot de passe du coffre-fort dans les champs **Mot de passe** et **Confirmer**.
4. Si vous souhaitez modifier la taille par défaut du coffre-fort (50 Mo), entrez la valeur souhaitée dans le champ **Taille du coffre-fort**.
5. Cliquez sur Créer si vous ne souhaitez créer le coffre qu'à l'emplacement sélectionné. Pour créer et afficher le coffre comme disque dur virtuel dans **Poste de travail**, cliquez sur **Créer et ouvrir**.

Note

Lorsque vous ouvrez le coffre-fort, un disque virtuel apparaît dans **Poste de travail**. Le disque se voit attribuer la lettre correspondant au coffre.

- **Ajoutez les fichiers ou les dossiers que vous voulez protéger au coffre-fort.**

  Vous devez d'abord ouvrir le coffre-fort pour y ajouter un fichier.

  1. Parcourir pour sélectionner le fichier coffer-fort .bvd.
  2. Faites un clic droit sur le coffre-fort, pointez sur Coffre-fort Bitdefender et sélectionnez **Ouvrir**.
  3. Dans la fenêtre qui apparaît, sélectionnez une lettre de lecteur à attribuer au coffre-fort, saisissez le mot de passe et cliquez sur **Ouvrir**.

  Vous pouvez maintenant effectuer des opérations sur le lecteur correspondant au coffre-fort souhaité en utilisant Windows Explorer, comme vous le feriez avec un lecteur normal. Pour ajouter un fichier à un coffre-fort ouvert, vous pouvez également faire un clic droit sur le fichier, pointer sur Coffre-fort Bitdefender, puis sélectionner **Ajouter au coffre-fort**.

- **Maintenez toujours le coffre-fort verrouillé.**

  Ouvrez uniquement les coffres-forts lorsque vous avez besoin d'y accéder ou de gérer leur contenu. Pour verrouiller un coffre-fort, faites un clic droit sur le disque dur virtuel correspondant dans **Poste de travail**, sélectionnez **Coffre-fort Bitdefender**, puis choisissez **Verrouiller**.

- **Veillez à ne pas supprimer le coffre-fort .bvd.**

  En supprimant le fichier vous supprimez également le contenu du coffre-fort.

Pour plus d'informations sur l'utilisation des coffres-forts, reportez-vous à « *Cryptage de Fichiers* » (p. 86).

4.19. Où voir l'espace restant sur ma SafeBox ?

Pour connaître l'espace restant de votre SafeBox, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **SafeBox** dans le menu de gauche.
4. La section **Espace utilisé** permet de voir l'espace restant.

4.20. Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?

Si votre ordinateur se connecte à Internet via un serveur proxy, vous devez configurer Bitdefender avec les paramètres du proxy. Normalement, Bitdefender détecte et importe automatiquement les paramètres proxy de votre système.

Important

Les connexions domestiques à Internet n'utilisent normalement pas de serveur proxy. En règle générale, vérifiez et configurez les paramètres de connexion proxy de votre programme Bitdefender lorsque aucune mise à jour n'est en cours. Si Bitdefender peut effectuer des mises à jour, alors il est correctement configuré pour se connecter à Internet.

Pour gérer les paramètres proxy, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Général** dans le menu de gauche puis sur l'onglet **Avancé**.
4. Dans la section **Paramètres du proxy**, activez l'utilisation du proxy en cliquant sur le bouton.
5. Cliquez sur le lien **Gérer Proxy**.
6. Deux options permettent de définir les paramètres du proxy :
   - **Importer les paramètres proxy à partir du navigateur par défaut** - paramètres du proxy de l'utilisateur actuel provenant du navigateur par défaut. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, vous devez les indiquer dans les champs correspondants.

Note

Bitdefender peut importer les paramètres proxy des principaux navigateurs, y compris des dernières versions d'Internet Explorer, de Mozilla Firefox et d'Opera.

- **Paramètres proxy personnalisés** - paramètres proxy que vous pouvez configurer vous-même. Voici les paramètres à spécifier:
  - **Adresse** - saisissez l'IP du serveur proxy.
  - **Port** - saisissez le port utilisé par Bitdefender pour se connecter au serveur proxy.
  - **Nom d'utilisateur** - indiquez un nom d'utilisateur reconnu par le serveur proxy.
  - **Mot de passe** - saisissez le mot de passe valide de l'utilisateur dont le nom vient d'être indiqué.

7. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Bitdefender utilisera les paramètres proxy disponibles jusqu'à ce qu'il parvienne à se connecter à Internet.

Important
N'oubliez pas de désactiver l'utilisation du proxy lorsque vous passez à une connexion Internet directe.

5. Protection antivirus

Bitdefender protège votre ordinateur contre tous les types de logiciels malveillants (virus, chevaux de Troie, spywares, rootkits, etc.).La protection offerte par Bitdefender est divisée en deux catégories:

- Analyse à l'accès - empêche les nouvelles menaces d'infecter votre système.Bitdefender analysera par exemple un document Word quand vous l'ouvrez, et les e-mails lors de leur réception.

  L'analyse à l'accès assure une protection en temps réel contre les malwares, et constitue un composant essentiel de tout programme de sécurité informatique.

  Important
  Pour empêcher l'infection de votre ordinateur par des virus, maintenez l' **analyse à l'accès** activée.

- Analyse à la demande - permet de détecter et de supprimer les codes malveillants déjà présents dans le système.C'est l'analyse classique antivirus déclenchée par l'utilisateur – vous choisissez le lecteur, dossier ou fichier que Bitdefender doit analyser et Bitdefender le fait – A la demande.

  Lorsque l'Analyse automatique est activée, il est inutile de lancer manuellement des analyses antimalwares.L'Analyse automatique analysera votre ordinateur encore et encore, et adoptera les mesures appropriées lorsque des malwares seront détectés. L'Analyse automatique s'exécute uniquement lorsque suffisamment de ressources système sont disponibles, afin de ne pas ralentir l'ordinateur.

Bitdefender analyse automatiquement tout support amovible connecté à l'ordinateur afin de s'assurer que son accès ne pose pas de problème de sécurité. Pour plus d'informations, reportez-vous à « *Analyse automatique de supports amovibles* » (p. 58).

Les utilisateurs avancés peuvent configurer des exceptions d'analyse s'ils ne souhaitent pas que certains fichiers ou types de fichiers soient analysés. Pour plus d'informations, reportez-vous à « *Configuration des exceptions d'analyse* » (p. 60).

Lorsqu'il détecte un virus ou un autre malware, Bitdefender tente automatiquement de supprimer le code du malware du fichier infecté et de reconstruire le fichier d'origine.Cette opération est appelée désinfection.Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Pour plus d'informations, reportez-vous à « *Gérer les fichiers en quarantaine* » (p. 62).

Si votre ordinateur a été infecté par des malwares, veuillez vous référer à « *Suppression des malwares de votre système* » (p. 157).Pour vous aider à supprimer les malwares qui ne peuvent pas l'être à partir du système d'exploitation Windows, Bitdefender vous fournit le Mode de secours.Il s'agit d'un environnement de

confiance, spécialement conçu pour la suppression de malwares, qui vous permet de faire redémarrer votre ordinateur indépendamment de Windows. Lorsque l'ordinateur s'exécute en Mode de Secours, les malwares Windows sont inactifs, ce qui rend leur suppression facile.

Pour vous protéger contre les applications malveillantes inconnues, Bitdefender utilise Active Virus Control, une technologie heuristique avancée, qui surveille en permanence les applications en cours d'exécution sur votre système. Active Virus Control bloque automatiquement les applications ayant un comportement similaire à celui des malwares afin de les empêcher d'endommager votre ordinateur. Des applications légitimes sont parfois bloquées. Vous pouvez dans ce cas configurer Active Virus Control afin qu'il ne bloque plus ces applications en créant des règles d'exclusion. Pour en savoir plus, reportez-vous à « *Active Virus Control* » (p. 63).

De nombreuses formes de malwares sont conçues pour infecter des systèmes en exploitant leurs vulnérabilités, telles que des mises à jour de systèmes d'exploitation manquantes ou des applications non à jour. Bitdefender vous aide à identifier et à corriger facilement les vulnérabilités du système afin de renforcer la protection de votre ordinateur contre les malwares et les hackers.Pour plus d'informations, reportez-vous à « *Corriger les vulnérabilités du système* » (p. 65).

5.1. Analyse à l'accès (protection en temps réel)

Bitdefender protège votre ordinateur de manière continue et en temps réel contre toutes les menaces de codes malveillants en analysant tous les fichiers à l'accès, les e-mails et les communications via les applications de messagerie instantanée (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Le réglage par défaut de la protection en temps réel assure un bon niveau de protection contre les malwares, avec un impact minimal sur les performances système.Vous pouvez facilement modifier les paramètres de la protection en temps réel selon vos besoins en choisissant un des niveaux de protection prédéfinis.Si vous êtes un utilisateur avancé, vous pouvez également configurer les paramètres d'analyse en détail en créant un niveau de protection personnalisé.

5.1.1. Vérification des malwares détectés par l'analyse à l'accès

Pour vérifier les malwares détectés par l'analyse à l'accès, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Événements** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Analyses Antivirus**.Cette section vous permet de trouver tous les événements d'analyse antimalware, y compris les menaces détectées par l'analyse à l'accès, les analyses lancées par un utilisateur et les modifications d'état pour les analyses automatiques.

4. Cliquez sur un événement pour afficher des informations à son sujet.

5.1.2. Régler le niveau de protection en temps réel

Le niveau de protection en temps réel détermine les paramètres d'analyse pour la protection en temps réel.Vous pouvez facilement modifier les paramètres de la protection en temps réel selon vos besoins en choisissant un des niveaux de protection prédéfinis.

Pour régler le niveau de protection en temps réel, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Résident**.
4. Déplacez le curseur sur l'échelle pour choisir le niveau de protection souhaité.Reportez-vous à la description à droite de l'échelle pour choisir le niveau de protection le plus adapté à vos besoins de sécurité.

5.1.3. Création d'un niveau de protection personnalisé

Les utilisateurs avancés peuvent profiter des paramètres d'analyse proposés par Bitdefender.Vous pouvez configurer les paramètres de protection en temps réel en détail en créant un niveau de protection personnalisé.

Pour créer un niveau de protection personnalisé, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Résident**.
4. Cliquez sur **Personnaliser**.
5. Configurez les paramètres d'analyse selon vos besoins.
6. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Ces informations peuvent vous être utiles :

- Si vous n'êtes pas familiarisé avec certains des termes, consultez le glossaire.Vous pouvez également rechercher des informations sur Internet.
- **Options d'analyse pour les fichiers auxquels on accède.** Vous pouvez régler Bitdefender pour analyser tous les types de fichiers auxquels vous accédez ou uniquement les applications (fichiers programmes).L'analyse de tous les fichiers auxquels on a accédé offre une protection maximale alors que l'analyse des applications uniquement peut être utilisée pour obtenir de meilleures performances du système.

Les applications (ou les fichiers de programmes) sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers.Cette catégorie comprend les extensions de fichiers suivantes :

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Analyse dans les archives.** L'analyse à l'intérieur des archives est un processus lent et consommant beaucoup de ressources, qui n'est donc pas recommandé pour une protection en temps réel. Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système.Les malwares peuvent affecter votre système uniquement si le fichier infecté est extrait de l'archive et exécuté dans que la protection en temps réel ne soit activée.

  Si vous décidez d'utiliser cette option, vous pouvez définir une limite de taille pour les archives à analyser à l'accès.Cochez la case correspondante et tapez la taille maximale des archives (en Mo).

- **Options d'analyse pour le trafic e-mail, web et de messagerie instantanée.** Afin d'éviter que des malwares soient téléchargés sur votre ordinateur, Bitdefender analyse automatiquement les points d'entrée des malwares suivants :
  - e-mails entrants et sortants
  - trafic Web
  - fichiers reçus via Yahoo! Messenger et Windows Live Messenger

  L'analyse du trafic web peut ralentir un peu la navigation sur Internet, mais elle bloquera les malwares provenant d'Internet, y compris les téléchargements de type "drive-by".

  Bien que ce ne soit pas recommandé, vous pouvez désactiver l'analyse antivirus du trafic Internet, de la messagerie électronique et de la messagerie instantanée pour améliorer les performances du système.Si vous désactivez les options

d'analyse correspondantes, les e-mails et les fichiers reçus ou téléchargés sur Internet ne seront pas analysés, ce qui permettra aux fichiers infectés d'être enregistrés sur votre ordinateur. Ce n'est pas une menace majeure car la protection en temps réel bloquera le malware lorsque vous tenterez d'accéder (ouvrir, déplacer, copier ou exécuter) aux fichiers infectés.

- **Analyser les secteurs de boot.** Vous pouvez paramétrer Bitdefender pour qu'il analyse les secteurs boot de votre disque dur.Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus de boot.Quand un virus infecte le secteur de boot, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
- **Analyser uniquement les fichiers nouveaux et modifiés.** En n'analysant que les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.

5.1.4. Restauration des paramètres par défaut

Le réglage par défaut de la protection en temps réel assure un bon niveau de protection contre les malwares, avec un impact minimal sur les performances système.

Pour restaurer les paramètres de protection en temps réel par défaut, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Résident**.
4. Cliquez sur **Par défaut**.

5.1.5. Activer ou désactiver la protection en temps réel

Pour activer ou désactiver la protection en temps réel contre les malwares, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Résident**.
4. Cliquez sur le bouton pour activer ou désactiver l'analyse à l'accès.
5. Si vous tentez de désactiver la protection en temps réel, une fenêtre d'avertissement apparaît.Vous devez confirmer votre choix en sélectionnant dans le menu la durée pendant laquelle vous souhaitez désactiver la protection en

temps réel. Vous pouvez désactiver la protection en temps réel pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.

Avertissement
Cela peut poser un problème de sécurité important. Nous vous recommandons de désactiver la protection en temps réel pendant le moins de temps possible. Si la protection en temps réel est désactivée, vous ne serez pas protégé contre les menaces de codes malveillants.

5.1.6. Actions appliquées à l'encontre des malwares détectés

Les fichiers détectés par la protection en temps réel sont regroupés dans deux catégories :

- **Fichiers infectés .** Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender.Bitdefender peut généralement supprimer le code malveillant d'un fichier infecté et reconstruire le fichier d'origine. Cette opération est appelée désinfection.

Note
Les signatures de malwares sont des fragments de codes extraits à partir de malwares réels. Elles sont utilisées par les programmes antivirus pour rechercher certaines caractéristiques et détecter les malwares.
La base de données de signatures de malwares Bitdefender rassemble des signatures de malwares mises à jour toutes les heures par les chercheurs de malwares Bitdefender.

- **Fichiers suspects.** Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique.B-HAVE étant une technologie d'analyse heuristique, Bitdefender ne peut être certain que le fichier est réellement infecté par des malwares. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible.

En fonction du type de fichier détecté, les actions suivantes sont menées automatiquement :

- Si un fichier infecté est détecté, Bitdefender tente automatiquement de le désinfecter.Si la désinfection échoue, le fichier est placé en quarantaine afin de contenir l'infection.

Important
Pour certains types de malware, la désinfection n'est pas possible car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

- Si un fichier suspect est détecté, il est placé en quarantaine afin d'empêcher une infection potentielle.

  Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux Laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender.Si la présence de malwares est confirmée, une signature est publiée afin de permettre de supprimer des malwares.

5.2. Analyse à la demande

L'objectif principal de Bitdefender est de conserver votre PC sans virus. Cela est assuré avant tout par l'analyse antivirus des emails que vous recevez et des fichiers que vous téléchargez ou copiez sur votre système.

Il y a cependant un risque qu'un virus soit déjà logé dans votre système, avant même l'installation de Bitdefender. C'est pourquoi il est prudent d'analyser votre ordinateur après l'installation de Bitdefender. Et c'est encore plus prudent d'analyser régulièrement votre ordinateur contre les virus.

L'analyse sur demande est basée sur les tâches d'analyse. Les tâches d'analyse permettent de spécifier les options d'analyse et les objets à analyser.Vous pouvez analyser l'ordinateur quand vous le souhaitez en exécutant les tâches par défaut ou vos propres tâches d'analyse (tâches définies par l'utilisateur). Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée.

5.2.1. Analyse auto.

L'analyse automatique est une analyse légère à la demande qui analyse en silence toutes vos données à la recherche de malwares et adopte les mesures appropriées lorsque des infections sont détectées. L'Analyse automatique détecte et utilise les moments pendant lesquels l'utilisation des ressources du système passe sous un certain seuil pour effectuer des analyses périodiques de l'ensemble du système.

Avantages de l'Analyse automatique :

- N'a pratiquement aucun impact sur le système.
- En pré-analysant le disque dur, les futures tâches à la demande seront effectuées extrêmement rapidement.
- L'analyse à l'accès sera également bien plus rapide.

Pour activer ou désactiver l'analyse automatique, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Antivirus**.
3. Cliquez sur le bouton pour activer ou désactiver l'analyse automatique.

5.2.2. Rechercher des malwares dans un fichier ou un dossier

Il est conseillé d'analyser les fichiers et les dossiers chaque fois que vous soupçonnez qu'ils peuvent être infectés.Faites un clic droit sur le fichier ou le dossier que vous souhaitez analyser et sélectionnez **Analyser avec Bitdefender**.L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse.

5.2.3. Exécuter une Analyse Rapide

Quick Scan utilise l'analyse 'in-the-cloud' pour détecter les malwares présents sur votre système.La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.

Pour effectuer une analyse rapide, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Antivirus**.
3. Cliquez sur **Analyser** et sélectionnez **Analyse Rapide** dans le menu déroulant.
4. Suivez les indications de l'Assistant d'analyse antivirus pour terminer l'analyse.

5.2.4. Exécuter une Analyse Complète du Système

La tâche d'Analyse Complète du Système analyse l'ensemble de votre ordinateur en vue de détecter tous les types de logiciels malveillants menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.Si vous avez désactivé l'Analyse auto., nous vous recommandons d'exécuter une Analyse Complète du Système au moins une fois par semaine.

Note

L'Analyse Complète du système effectuant une analyse approfondie de l'ensemble du système, elle peut prendre quelque temps. Il est donc recommandé d'exécuter cette tâche lorsque vous n'utilisez pas votre ordinateur.

Avant d'exécuter une Analyse Complète du Système, nous vous recommandons ceci :

- Vérifiez que Bitdefender dispose de signatures de malwares à jour. L'analyse de votre ordinateur à l'aide d'une base de signatures non à jour peut empêcher Bitdefender de détecter les malwares connus depuis la dernière mise à jour.Pour plus d'informations, reportez-vous à « *Mise à jour* » (p. 133).
- Fermez tous les programmes ouverts.

Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée.Pour plus

d'informations, reportez-vous à « *Configurer et exécuter une analyse personnalisée* » (p. 52).

Pour exécuter une Analyse Complète du Système, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Antivirus**.
3. Cliquez sur **Analyser** et sélectionnez **Analyse Complète** dans le menu déroulant.
4. Suivez les indications de l'Assistant d'analyse antivirus pour terminer l'analyse.

5.2.5. Configurer et exécuter une analyse personnalisée

Pour configurer une analyse antimalware en détail et l'exécuter, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Antivirus**.
3. Cliquez sur **Analyser** et sélectionnez **Analyse personnalisée** dans le menu déroulant.
4. Cliquez sur **Ajouter cible**, cochez les cases correspondant aux emplacements que vous souhaitez analyser à la recherche de malwares puis cliquez sur **OK**.
5. Cliquez sur **Options d'analyse** si vous souhaitez configurer les options d'analyse. Une nouvelle fenêtre s'affiche.Suivez ces étapes :

   a. Vous pouvez facilement configurer les options d'analyse en réglant le niveau d'analyse. Déplacez le curseur sur l'échelle pour définir le niveau d'analyse souhaité.Reportez-vous à la description à droite de l'échelle pour identifier le niveau d'analyse le plus adapté à vos besoins.

      Les utilisateurs avancés peuvent profiter des paramètres d'analyse proposés par Bitdefender.Pour configurer les options d'analyse en détail, cliquez sur **Personnaliser**. Vous trouverez des informations à leur sujet à la fin de cette section.

   b. Par défaut, Bitdefender tente de supprimer le code malveillant des fichiers infectés ou, si la désinfection échoue, de les placer en quarantaine. Si ces deux actions échouent, l'on vous demandera de spécifier une action à appliquer aux menaces non résolues.

      Si vous souhaitez uniquement détecter des malwares, sans appliquer d'autre action, cochez la case correspondante dans la section **Actions**.

   c. Vous pouvez aussi configurer ces options générales :

      - **Exécuter la tâche en priorité basse.** Décroît la priorité du processus d'analyse. Vous allez permettre aux autres logiciels d'être exécutés à une

vitesse supérieure et d'augmenter le temps nécessaire pour le final du processus d'analyse.

- **Réduire l'assistant d'analyse dans la zone de notification.** Réduit la fenêtre d'analyse dans la barre d'état système. Double-cliquez sur l'icône de Bitdefender pour l'ouvrir.
- Spécifiez l'action à mener si aucune menace n'a été trouvée.

d. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

6. Cliquez sur **Démarrer l'analyse** et suivez l'Assistant d'analyse antivirus pour terminer l'analyse. En fonction des emplacements à analyser, l'analyse peut prendre quelque temps.

Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

- Si vous n'êtes pas familiarisé avec certains des termes, consultez le glossaire.Vous pouvez également rechercher des informations sur Internet.
- **Analyser les fichiers.** Vous pouvez régler Bitdefender pour analyser tous les types de fichiers ou uniquement les applications (fichiers programmes).L'analyse de tous les fichiers consultés offre une protection maximale alors que l'analyse des applications uniquement peut être utilisée pour que l'analyse soit plus rapide.

  Les applications (ou les fichiers de programmes) sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers.Cette catégorie comprend les extensions de fichiers suivantes : 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Options d'analyse pour les archives.** Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système.Les malwares peuvent affecter votre système uniquement si le fichier infecté est extrait de l'archive et exécuté dans que la protection en temps réel ne soit activée. Il est toutefois recommandé d'utiliser cette option afin de détecter et de supprimer toute menace potentielle, même si celle-ci n'est pas imminente.

  Note
  L'analyse des fichiers compressés augmente le temps d'analyse global et demande plus de ressources système.

- **Analyser les secteurs de boot.** Vous pouvez paramétrer Bitdefender pour qu'il analyse les secteurs boot de votre disque dur.Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus de boot.Quand un virus infecte le secteur de boot, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
- **Analyse de la mémoire.** Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire de votre système.
- **Analyse la base de registre.** Sélectionnez cette option pour analyser les clés de registre. Le Registre Windows est une base de données qui contient les paramètres et les options de configuration des composants du système d'exploitation Windows, ainsi que des applications installées.
- **Analyse les cookies.** Sélectionnez cette option pour analyser les cookies stockés par les navigateurs sur votre ordinateur.
- **Analyser uniquement les fichiers nouveaux et modifiés.** En n'analysant que les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
- **Ignorer les keyloggers commerciaux.** Sélectionnez cette option si vous avez installé et utilisez un keylogger commercial sur votre ordinateur. Les keyloggers commerciaux sont des logiciels de surveillance légitimes dont la fonction principale consiste à enregistrer tout ce qui est tapé au clavier.

5.2.6. Assistant d'analyse antivirus

À chaque fois que vous initierez une analyse à la demande (par exemple en faisant un clic droit sur un dossier et en sélectionnant **Analyser avec Bitdefender**), l'assistant de l'analyse antivirus s'affichera.Suivez l'assistant pour terminer le processus d'analyse.

Note

Si l'assistant d'analyse ne s'affiche pas, il est possible que l'analyse soit paramétrée pour s'exécuter invisiblement, en tâche de fond.Recherchez l'icône de l'avancement de l'analyse dans la barre des tâches.Vous pouvez cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

Étape 1 - Sélectionner les cibles d'analyse

Cette étape apparaît uniquement lorsque vous utilisez l'Analyse personnalisée. Pour plus d'informations, reportez-vous à « *Configurer et exécuter une analyse personnalisée* » (p. 52).

Étape 2 - Effectuer l'analyse

Bitdefender commence à analyser les objets sélectionnés.

Le statut et les statistiques de l'analyse s'affichent (vitesse d'analyse, temps écoulé, nombre d'objets analysés / infectés / suspects / cachés, etc.).

Patientez jusqu'à ce que Bitdefender ait terminé l'analyse.

Note

L'analyse peut durer un certain temps, suivant sa complexité.

Archives protégées par mot de passe. Lorsqu'une archive protégée par mot de passe est détectée, en fonction des paramètres de l'analyse, on peut vous demander d'indiquer son mot de passe. Les archives protégées par mot de passe ne peuvent pas être analysées à moins que vous ne communiquiez le mot de passe.Voici les options proposées :

- **Entrer le mot de passe.** Si vous souhaitez que Bitdefender analyse l'archive, sélectionnez cette option et entrez le mot de passe.Si vous ne connaissez pas le mot de passe, choisissez l'une des autres options.
- **Ne pas demander le mot de passe et ne pas analyser cet objet.** Sélectionnez cette option pour ne pas analyser cette archive.
- **Ne pas analyser les éléments protégés par mot de passe.** Sélectionnez cette option si vous ne voulez pas être dérangé au sujet des archives protégées par mot de passe.Bitdefender ne pourra pas les analyser, mais un rapport sera conservé dans le journal des analyses.

Cliquez sur **OK** pour continuer l'analyse.

Arrêt ou pause de l'analyse. Vous pouvez arrêter l'analyse à tout moment en cliquant sur **Arrêter et Oui**. Vous vous retrouverez alors à la dernière étape de l'assistant.Pour suspendre temporairement le processus d'analyse, cliquez sur **Pause**. Pour reprendre l'analyse, cliquez sur **Reprendre**.

Étape 3 - Choisir des actions

Une fois l'analyse terminée, une nouvelle fenêtre apparaît affichant les résultats de l'analyse.

S'il n'y a pas de menaces non résolues, cliquez sur **Continuer**.Sinon, vous devez configurer de nouvelles actions à mener sur les menaces non résolues pour protéger votre système.

Les objets infectés sont affichés dans des groupes, basés sur les malwares les ayant infectés.Cliquez sur le lien correspondant à une menace pour obtenir plus d'informations sur les éléments infectés.

Vous pouvez sélectionner une action globale à mener pour l'ensemble des problèmes de sécurité ou sélectionner des actions spécifiques pour chaque groupe de problèmes.Une ou plusieurs des options qui suivent peuvent apparaître dans le menu :

Ne pas mener d'action
Aucune action ne sera menée sur les fichiers détectés.Une fois l'analyse terminée, vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.

Désinfecter
Supprime le code malveillant des fichiers infectés.

Supprimer
Supprime du disque les fichiers détectés.

Quarantaine
Déplace les fichiers detectés dans la zone de quarantaine.Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.Pour plus d'informations, reportez-vous à « *Gérer les fichiers en quarantaine* » (p. 62).

Renommer
Modifie le nom des fichiers cachés en y ajoutant le suffixe `.bd.ren`.Vous pourrez ainsi rechercher ce type de fichiers sur votre ordinateur, et les trouver s'il en existe.

Veuillez noter que ces fichiers cachés ne sont pas ceux que vous avez choisi de ne pas afficher dans Windows. Ce sont des fichiers qui ont été cachés par des programmes particuliers, connus sous le nom de rootkits.Les rootkits ne sont pas malveillants en eux-mêmes. Ils sont cependant couramment utilisés pour rendre les virus et les spywares indétectables par les programmes antivirus habituels.

Cliquez sur **Continuer** pour appliquer les actions spécifiées.

Étape 4 - Résumé

Une fois que les problèmes de sécurité auront été corrigés par Bitdefender, les résultats de l'analyse apparaîtront dans une nouvelle fenêtre.Si vous souhaitez consulter des informations complètes sur le processus d'analyse, cliquez sur **Afficher journal** pour afficher le journal d'analyse.

Important
Si cela est nécessaire, il vous sera demandé de redémarrer votre système pour terminer le processus d'installation.

Cliquez sur **Fermer** pour fermer la fenêtre.

Bitdefender n'a pas pu corriger certains problèmes

Dans la plupart des cas, Bitdefender désinfecte ou isole l'infection des fichiers infectés qu'il détecte.Il y a toutefois des problèmes qui ne peuvent pas être résolus automatiquement.Pour plus d'informations et d'instructions sur la méthode permettant de supprimer des malwares manuellement, reportez-vous à « *Suppression des malwares de votre système* » (p. 157).

Bitdefender a détecté des fichiers suspects

Les fichiers suspects sont des fichiers détectés par l'analyse heuristique pouvant être infectés par des malwares et pour lesquels une signature n'a pas encore été publiée.

Lorsque des fichiers suspects seront détectés durant l'analyse, vous serez invité à les envoyer au laboratoire Bitdefender.Cliquez sur **OK** pour envoyer ces fichiers aux laboratoires Bitdefender pour une analyse plus approfondie.

5.2.7. Consulter les journaux d'analyse

À chaque fois que vous effectuez une analyse, un journal d'analyse est créé. Le rapport d'analyse contient des informations détaillées sur le processus d'analyse, telles que les options d'analyse, la cible de l'analyse, les menaces trouvées et les actions prises à l'encontre de ces menaces.

Vous pouvez ouvrir le journal d'analyse directement à partir de l'assistant d'analyse, une fois l'analyse terminée, en cliquant sur **Afficher le Journal**.

Pour consulter les journaux d'analyse ultérieurement, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Événements** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Analyses Antivirus**.Cette section vous permet de trouver tous les événements d'analyse antimalware, y compris les menaces détectées par l'analyse à l'accès, les analyses

lancées par un utilisateur et les modifications d'état pour les analyses automatiques.

4. Dans la liste des événements, vous pouvez consulter les analyses ayant été réalisées récemment.Cliquez sur un événement pour afficher des informations à son sujet.
5. Pour ouvrir le journal d'analyse, cliquez sur **Journal**.Le journal d'analyse s'affichera dans votre navigateur Internet par défaut.

5.3. Analyse automatique de supports amovibles

Bitdefender détecte automatiquement la connexion d'un périphérique de stockage amovible à votre ordinateur et l'analyse en tâche de fond.Ceci est recommandé afin d'empêcher que des virus ou autres malwares n'infectent votre ordinateur.

Les périphériques détectés appartiennent à l'une des catégories suivantes :

- CD/DVD
- Des mémoires USB, tels que des clés flash et des disques durs externes
- disques réseau (distants) connectés

Vous pouvez configurer l'analyse automatique séparément pour chaque catégorie de périphériques de stockage. L'analyse automatique des disques réseau connectés est désactivée par défaut.

5.3.1. Comment cela fonctionne-t-il ?

Lorsqu'il détecte un périphérique de stockage amovible, Bitdefender commence à l'analyser en tâche de fond à la recherche de malwares (à condition que l'analyse automatique soit activée pour ce type de périphérique). Une icône d'analyse de Bitdefender apparaîtra dans la zone de notification.Vous pouvez cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

Si le Pilotage automatique est activé, vous n'aurez pas à vous inquiéter de l'analyse. L'analyse sera seulement enregistrée et des informations à son sujet seront disponibles dans la fenêtre Événements.

Si le Pilotage automatique est désactivé :

1. Vous serez averti via une fenêtre pop-up qu'une nouveau périphérique a été détecté et est en cours d'analyse.
2. Lorsqu'une archive protégée par mot de passe est détectée au cours de l'analyse, on peut vous demander d'indiquer son mot de passe. Les archives protégées par mot de passe ne peuvent pas être analysées à moins que vous ne communiquiez le mot de passe.Vous pouvez choisir d'indiquer le mot de passe, de ne pas analyser le fichier ou de désactiver la détection des archives protégées par mot de passe.

3. Dans la plupart des cas, Bitdefender supprime automatiquement les malwares détectés ou isole les fichiers infectés en quarantaine. S'il y a des menaces non résolues après l'analyse, on vous demandera de choisir les actions à leur appliquer.

Note

Veuillez prendre en compte le fait qu'aucune mesure ne sera prise à l'encontre des fichiers infectés ou suspects détectés sur des CD/DVD. Ni à l'encontre des fichiers suspects détectés sur des lecteurs mappés du réseau si vous ne disposez pas des privilèges appropriés.

4. Lorsque l'analyse est terminée, la fenêtre des résultats de l'analyse s'affiche afin de vous informer si vous pouvez accéder aux fichiers en toute sécurité sur le support amovible.

Ces informations peuvent vous être utiles :

- Soyez prudent lorsque vous utilisez un CD/DVD infecté par des malwares car les malwares ne peuvent pas être supprimés du disque (le support est en lecture seule). Vérifiez que la protection en temps réel est activée pour empêcher la diffusion de malwares sur votre système. Il est recommandé de copier toutes les données essentielles du disque sur le système avant de se séparer du disque.
- Bitdefender n'est parfois pas en mesure de supprimer les malwares de certains fichiers en raison de contraintes légales ou techniques. C'est le cas par exemple des fichiers archivés à l'aide d'une technologie propriétaire (car l'archive ne peut pas être recréée correctement).

  Pour savoir comment traiter les malwares, reportez-vous à « *Suppression des malwares de votre système* » (p. 157).

5.3.2. Gérer l'analyse des supports amovibles

Pour gérer l'analyse automatique de supports amovibles, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Exclusions**.
4. Dans la section **Analyser les périphériques détectés**, choisissez les types de périphériques de stockage que vous souhaitez analyser automatiquement. Cliquez sur les boutons pour activer ou désactiver l'analyse automatique.

Pour une meilleure protection, nous vous recommandons d'activer l'analyse automatique de tous les types de périphériques de stockage amovibles.

Les options d'analyse sont déjà configurées pour que la détection soit la meilleure possible.Si des fichiers infectés sont détectés, Bitdefender essaiera de les désinfecter (supprimer le code malveillant) ou de les placer en quarantaine. Si ces actions

échouent, l'Assistant d'analyse antivirus vous permettra de spécifier d'autres actions à appliquer aux fichiers infectés. Les options d'analyse sont standard et vous ne pouvez pas les modifier.

5.4. Configuration des exceptions d’analyse

Bitdefender permet d'exclure de l'analyse certains fichiers, dossiers ou extensions de fichiers. Cette fonctionnalité est conçue pour éviter d'interférer avec votre travail et peut également contribuer à améliorer les performances du système. Les exclusions doivent être employées par des utilisateurs ayant un niveau avancé en informatique ou, sinon, selon les recommandations d'un représentant de Bitdefender.

Vous pouvez configurer des exclusions à appliquer uniquement à l'analyse à l'accès ou à la demande, ou aux deux. Les objets exclus d'une analyse à l'accès ne sont pas analysés, que ce soit vous-même ou une application qui y accédiez.

Note

Les exclusions ne sont PAS appliquées pour l’analyse contextuelle.L'analyse contextuelle est un type d'analyse à la demande : vous faites un clic droit sur le fichier ou le dossier que vous souhaitez analyser et vous sélectionnez **Analyser avec Bitdefender**.

5.4.1. Exclure de l'analyse des fichiers ou des dossiers

Pour exclure de l'analyse des fichiers ou des dossiers, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Exclusions**.
4. Activez les exceptions d'analyse pour les fichiers à l'aide du bouton correspondant.
5. Cliquez sur le lien **Fichiers et dossiers exclus**.La fenêtre qui s'affiche vous permet de gérer les fichiers et dossiers exclus de l'analyse.
6. Ajoutez des exclusions en suivant ces étapes :
   a. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
   b. Cliquez sur **Parcourir**, sélectionnez le fichier ou le dossier à exclure de l'analyse, puis cliquez sur **OK**.Vous pouvez également taper (ou copier coller) le chemin vers le fichier ou le dossier dans le champ de saisie.
   c. Par défaut, le fichier ou dossier sélectionné est exclu à la fois de l'analyse à l'accès et à la demande. Pour modifier les conditions d'application de l'exclusion, sélectionnez l'une des autres options.
   d. Cliquez sur **Ajouter**.
7. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

5.4.2. Exclure de l'analyse des extensions de fichiers

Lorsque vous excluez de l'analyse une extension de fichier, Bitdefender n'analysera plus les fichiers avec cette extension, quel que soit leur emplacement sur votre ordinateur. L'exclusion s'applique également aux fichiers de supports amovibles tels que les CD, les DVD, les périphériques de stockage USB ou les disques réseau.

Important
Soyez prudent lorsque vous excluez de l'analyse des extensions car celles-ci peuvent rendre votre ordinateur vulnérable aux malwares.

Pour exclure de l'analyse des extensions de fichiers, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Exclusions**.
4. Activez les exceptions d'analyse pour les fichiers à l'aide du bouton correspondant.
5. Cliquez sur le lien **Extensions exclues**.La fenêtre qui s'affiche vous permet de gérer les extensions de fichiers exclues de l'analyse.
6. Ajoutez des exclusions en suivant ces étapes :
   a. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
   b. Indiquez les extensions que vous ne souhaitez pas analyser, en les séparant par des points-virgules (;).Voici un exemple :

      ```
      txt;avi;jpg
      ```

   c. Par défaut, tous les fichiers ayant les extensions indiquées sont exclus à la fois de l'analyse à l'accès et à la demande. Pour modifier les conditions d'application de l'exclusion, sélectionnez l'une des autres options.
   d. Cliquez sur **Ajouter**.
7. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

5.4.3. Gérer les exceptions d'analyse

Si les exceptions d'analyse configurées ne sont plus nécessaires, il est recommandé de les supprimer ou de les désactiver.

Pour gérer les exceptions d'analyse, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Exclusions**.Utilisez les options de la section **Fichiers et dossiers** pour gérer les exceptions d'analyse.

4. Pour supprimer ou éditer des exceptions d'analyse, cliquez sur l'un des liens. Procédez comme suit :
   - Pour supprimer une entrée du tableau, sélectionnez-la et cliquez sur le bouton **Supprimer**.
   - Pour modifier une entrée du tableau, double-cliquez dessus (ou sélectionnez-la et cliquez sur le bouton **Modifier**.)Une nouvelle fenêtre apparaît vous permettant de modifier l'extension ou le chemin à exclure et le type d'analyse dont vous souhaitez les exclure, le cas échéant. Effectuez les modifications nécessaires, puis cliquez sur **Modifier**.
5. Pour désactiver les exceptions d'analyse, cliquez sur le bouton correspondant.

5.5. Gérer les fichiers en quarantaine

Bitdefender isole les fichiers infectés par des malwares qu'il ne peut pas désinfecter et les fichiers suspects dans une zone sécurisée nommée quarantaine. Quand un virus est en quarantaine, il ne peut faire aucun dégât car il ne peut ni être exécuté ni lu.

Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux Laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender.Si la présence de malwares est confirmée, une signature est publiée afin de permettre de supprimer des malwares.

Bitdefender analyse également les fichiers en quarantaine après chaque mise à jour de signatures de malware.Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

Pour consulter et gérer les fichiers de la quarantaine, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Quarantaine**.
4. Les fichiers en quarantaine sont gérés automatiquement par Bitdefender en fonction des paramètres de quarantaine par défaut. Bien que ce ne soit pas recommandé, vous pouvez régler les paramètres de quarantaine en fonction de vos préférences.

   Analyser la quarantaine après la mise à jour des définitions de virus
   Maintenez cette option activée pour analyser automatiquement les fichiers en quarantaine après chaque mise à jour des définitions de virus.Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

Envoyer les fichiers en quarantaine à Bitdefender pour une analyse plus approfondie

Maintenez cette option activée pour envoyer automatiquement les fichiers de la quarantaine aux laboratoires de Bitdefender.Les fichiers exemples seront analysés par les spécialistes des malwares de Bitdefender.Si la présence de malwares est confirmée, une signature est publiée afin de permettre de supprimer des malwares.

Supprimer le contenu de plus de {30} jours

Par défaut, les fichiers placés en quarantaine depuis plus de 30 jours sont automatiquement supprimés.Si vous souhaitez modifier cet intervalle, entrez une nouvelle valeur dans le champ correspondant.Pour désactiver la suppression automatique des anciens fichiers de la quarantaine, tapez 0.

5. Pour supprimer un fichier en quarantaine, sélectionnez-le, puis cliquez sur le bouton **Supprimer**.Si vous souhaitez restaurer un fichier mis en quarantaine à son emplacement d'origine, sélectionnez-le, puis cliquez sur **Restaurer**.

5.6. Active Virus Control

Bitdefender Active Virus Control est une technologie de détection proactive innovante qui utilise des méthodes heuristiques de pointe pour détecter de nouvelles menaces potentielles en temps réel.

Active Virus Control surveille en permanence les applications en cours d'exécution sur l'ordinateur, à la recherche d'actions ressemblant à celles des malwares. Chacune de ces actions est notée et une note globale est calculée pour chaque processus. Lorsque la note globale d'un processus atteint un seuil donné, le processus est considéré comme malveillant et est automatiquement bloqué.

Si le Pilotage automatique est désactivé, vous serez averti via une fenêtre pop-up sur l'application bloquée. Sinon, l'application sera bloquée sans notification. Vous pouvez vérifier les applications détectées par Active Virus Control dans la fenêtre Événements.

5.6.1. Vérifier des applications détectées

Pour contrôler les applications détectées par Active Virus Control, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Événements** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Active Virus Control**.
4. Cliquez sur un événement pour afficher des informations à son sujet.

5. Si vous considérez que l'application est fiable, vous pouvez configurer Active Virus Control afin qu'il ne la bloque plus en cliquant sur **Autoriser et surveiller**.Active Virus Control continuera à surveiller les applications exclues. Si Active Virus Control détecte qu'une application exclue effectue des activités suspectes, l'événement sera simplement enregistré et signalé au Cloud Bitdefender comme erreur de détection.

5.6.2. Activer ou désactiver Active Virus Control

Pour activer ou désactiver Active Virus Control, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Résident**.
4. Cliquez sur le bouton pour activer ou désactiver Active Virus Control.

5.6.3. Régler la protection Active Virus Control

Si vous remarquez qu'Active Virus Control détecte souvent des applications légitimes, optez pour un niveau de protection moins strict.

Pour régler la protection Active Virus Control, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Résident**.
4. Vérifiez qu'Active Virus Control est activé.
5. Déplacez le curseur sur l'échelle pour choisir le niveau de protection souhaité.Reportez-vous à la description à droite de l'échelle pour choisir le niveau de protection le plus adapté à vos besoins de sécurité.

Note

Si vous élevez le niveau de protection, Active Virus Control aura besoin de moins de signes de comportements similaires à ceux des malwares pour signaler un processus. Cela conduira au signalement d'un nombre plus important d'applications et, en même temps, à un risque plus élevé de faux positifs (des applications saines détectées comme étant malveillantes).

5.6.4. Gérer des processus exclus

Vous pouvez configurer des règles d'exceptions pour les applications de confiance afin qu'Active Virus Control ne les bloque pas si elles effectuent des actions ressemblant à celles de malwares. Active Virus Control continuera à surveiller les applications exclues. Si Active Virus Control détecte qu'une application exclue

effectue des activités suspectes, l'événement sera simplement enregistré et signalé au Cloud Bitdefender comme erreur de détection.

Pour gérer les exclusions de processus Active Virus Control, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Exclusions**.
4. Cliquez sur le lien **Processus exclus**.Dans la fenêtre qui apparaît, vous pouvez gérer les exclusions de processus Active Virus Control.

   Note
   Les exclusions de processus s'appliquent également au Système de Détection d'Intrusion inclus dans le pare-feu Bitdefender.

5. Ajoutez des exclusions en suivant ces étapes :
   a. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
   b. Cliquez sur **Parcourir**, sélectionnez l'application que vous souhaitez exclure, puis cliquez sur **OK**.
   c. Gardez l'option **Autoriser** sélectionnée pour empêcher Active Virus Control de bloquer l'application.
   d. Cliquez sur **Ajouter**.
6. Pour supprimer ou éditer des exclusions, procédez comme suit :
   - Pour supprimer une entrée du tableau, sélectionnez-la et cliquez sur le bouton **Supprimer**.
   - Pour modifier une entrée du tableau, double-cliquez dessus (ou sélectionnez-la et cliquez sur le bouton **Modifier**.)Effectuez les modifications nécessaires, puis cliquez sur **Modifier**.
7. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

5.7. Corriger les vulnérabilités du système

Une étape importante permettant de préserver votre ordinateur contre les personnes malveillantes et les menaces est de maintenir à jour votre système d'exploitation et vos principales applications.Vous devriez également envisager de désactiver les paramètres Windows qui rendent le système plus vulnérable aux malwares. De plus, afin de prévenir tout accès physique non autorisé à votre ordinateur, il est recommandé d'utiliser des mots de passe complexes (qui ne peuvent pas être devinés trop facilement) pour chaque compte utilisateur Windows.

Bitdefender fournit deux manières simples de corriger les vulnérabilités de votre système :

- Vous pouvez rechercher des vulnérabilités sur votre système et les corriger pas à pas à l'aide de l'assistant de l'**Analyse de Vulnérabilité**.
- La surveillance des vulnérabilités automatique vous permet de vérifier et de corriger les vulnérabilités détectées dans la fenêtre Événements.

Nous vous recommandons de vérifier et de corriger les vulnérabilités du système toutes les semaines, ou une fois toutes les deux semaines.

5.7.1. Analyser votre système à la recherche de vulnérabilités

Pour corriger les vulnérabilités du système à l'aide de l'assistant de l'Analyse de Vulnérabilité, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Antivirus**.
3. Cliquez sur **Analyser** puis sélectionnez **Analyse de Vulnérabilité**.
4. Suivez la procédure en six étapes pour supprimer les vulnérabilités de votre système. Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.

   a. **Protection de votre PC**

   Sélectionnez les vulnérabilités à rechercher.

   b. **Vérification des problèmes**

   Patientez jusqu'à ce que Bitdefender ait terminé l'analyse des vulnérabilités de votre système.

   c. **Mises à jour Windows**

   Vous pouvez voir la liste des mises à jour Windows (critiques et non-critiques) qui ne sont pas installées actuellement sur votre ordinateur.Sélectionnez les mises à jour que vous souhaitez installer.

   Pour lancer l'installation des mises à jour sélectionnées, cliquez sur **Suivant**.Veuillez noter que l'installation des mises à jour peut durer un certain temps et que certaines peuvent nécessiter un redémarrage du système. Si nécessaire, redémarrez le système dès que possible.

   d. **Mises à jour d'applications**

   Si une application n'est pas à jour, cliquez sur le lien fourni pour télécharger la dernière version.

   e. **Mots de passe vulnérables**

   Vous pouvez voir une liste des comptes utilisateur Windows configurés sur votre ordinateur ainsi que le niveau de protection que leur mot de passe respectif apportent.

Cliquez sur **Corriger** pour modifier les mots de passe vulnérables.Vous pouvez choisir entre demander à l'utilisateur de modifier le mot de passe lors de sa prochaine connexion ou modifier le mot de passe par vous-même immédiatement. Pour avoir un mot de passe sécurisé, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

f. **Résumé**

Cette étape vous permet d'afficher le résultat de l'opération.

5.7.2. Utiliser la surveillance des vulnérabilités automatique

Bitdefender analyse régulièrement votre système à la recherche de vulnérabilités, en tâche de fond, et enregistre les problèmes détectés dans la fenêtre Événements.

Pour vérifier et corriger les problèmes détectés, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Événements** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Vulnérabilité**.
4. Vous pouvez consulter des informations détaillées au sujet des vulnérabilités du système détectées. En fonction du problème, procédez comme suit pour corriger une vulnérabilité spécifique :
   - Si des mises à jour Windows sont disponibles, cliquez sur **Mettre à jour** pour ouvrir l'assistant de l'Analyse de Vulnérabilité et les installer.
   - Si une application n'est pas à jour, cliquez sur **Mettre à jour maintenant** pour trouver un lien vers la page Web du fournisseur d'où vous pourrez installer la dernière version de l'application.
   - Si un compte utilisateur Windows a un mot de passe vulnérable, cliquez sur **Corriger le mot de passe** pour obliger l'utilisateur à modifier son mot de passe lors de la prochaine connexion ou pour changer le mot de passe par vous-même.Pour avoir un mot de passe sécurisé, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).
   - Si la fonctionnalité Autorun de Windows est activée, cliquez sur **Désactiver** pour la désactiver.

Pour configurer les paramètres de surveillance des vulnérabilités, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Vulnérabilité**.

4. Cliquez sur le bouton pour activer ou désactiver l'Analyse de Vulnérabilité Automatique.

Important
Pour être automatiquement averti en cas de vulnérabilités du système ou des applications, veuillez garder l'option **Analyse de Vulnérabilité Automatique** activée.

5. Choisissez les vulnérabilités du système que vous souhaitez vérifier régulièrement à l'aide des boutons correspondants.

Mises à jour Windows critiques
Vérifiez que votre système d'exploitation Windows dispose des dernières mises à jour de sécurité critiques de Microsoft.

Mises à jour Windows régulières
Vérifiez que votre système d'exploitation Windows dispose des dernières mises à jour de sécurité de Microsoft.

Mises à jour d'applications
Vérifiez que les applications web essentielles installées sur votre système sont à jour. Des applications non à jour peuvent être exploitées par des logiciels malveillants, rendant votre PC vulnérable aux attaques extérieures.

Mots de passe vulnérables
Vérifiez si les mots de passe des comptes Windows configurés sur le système sont faciles à deviner. Choisir des mots de passe difficiles à deviner rend difficile l'introduction dans votre système de hackers.Un mot de passe sécurisé est constitué d'une association de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

Exécution automatique des médias
Vérifiez l'état de la fonctionnalité Autorun de Windows.Cette fonctionnalité permet aux applications d'être automatiquement lancées à partir de CD, DVD, lecteurs USB ou autres périphériques externes.

Certains types de malwares utilisent la fonction Autorun pour passer automatiquement des supports amovibles vers le PC. Nous vous recommandons donc de désactiver cette fonctionnalité Windows.

Note
Si vous désactivez la surveillance d'une certaine vulnérabilité, les problèmes qui y sont liés ne seront plus enregistrés dans la fenêtre Événements.

6. Antispam

Le spam est un terme utilisé pour décrire les e-mails non sollicités. Le Spam est un problème grandissant, à la fois pour les particuliers et les entreprises. Vous ne voudriez pas que vos enfants tombent sur certains emails, vous pourriez perdre votre travail (pour une perte de temps trop grande ou parce que vous recevez trop de messages à caractère pornographique sur votre e-mail professionnel) et vous ne pouvez pas empêchez les gens d'en envoyer. L'idéal serait de pouvoir arrêter de les recevoir. Malheureusement, le SPAM arrive dans un large éventail de formes et de tailles, et il en existe beaucoup.

Bitdefender Antispam utilise des innovations technologiques de pointe et des filtres antispam répondant aux normes industrielles qui permettent d'éliminer les spams avant qu'ils n'atteignent la boîte aux lettres de l'utilisateur.Pour plus d'informations, reportez-vous à « *Aperçu de l'antispam* » (p. 70).

La protection Bitdefender Antispam est disponible seulement pour les clients de messagerie configurés pour recevoir des e-mails via le protocole POP3.POP3 est l'un des protocoles les plus utilisés pour télécharger des e-mails à partir d'un serveur de messagerie.

Note

Bitdefender ne fournit pas de protection antispam pour les comptes de messagerie auxquels vous accédez via un service de webmail.

Les messages de spam détectés par Bitdefender sont marqués avec le préfixe `[spam]` dans la ligne Objet.Bitdefender place automatiquement les messages de spam dans un dossier spécifique, comme indiqué :

- Dans Microsoft Outlook, les messages de spam sont placés dans le dossier **Spam**, situé dans le dossier **Éléments supprimés**.Le dossier **Spam** est créé lors de l'installation de Bitdefender.
- Dans Outlook Express et Windows Mail, les messages de spam sont placés directement dans **Éléments Supprimés**.
- Dans Mozilla Thunderbird, les messages de spam sont placés dans le dossier **Spam**, situé dans le dossier **Corbeille**.Le dossier **Spam** est créé lors de l'installation de Bitdefender.

Si vous utilisez d'autres clients de messagerie, vous devez créer une règle pour déplacer les e-mails marqués comme`[spam]`par Bitdefender vers un dossier de quarantaine personnalisé.

6.1. Aperçu de l'antispam

6.1.1. Filtres AntiSpam

Le moteur antispam de Bitdefender intègre plusieurs filtres qui préservent votre messagerie du spam : Liste des amis, Liste des spammeurs, Filtre de caractères, Filtre de liens, Filtre des signatures, Filtre NeuNet (heuristique) et détection "in the cloud".

Liste d'Amis / Liste des Spammeurs

La majorité des utilisateurs communiquent régulièrement avec un groupe de personnes ou reçoivent des messages de la part des entreprises et compagnies du même domaine. En utilisant **les listes amis/spammeurs**, vous pouvez déterminer aisément de quelles personnes vous voulez recevoir des messages et de quelles personnes vous ne voulez plus en recevoir.

Note

Nous vous suggérons d'ajouter les noms de vos amis et leurs adresses mail à la **Liste des Amis**. Bitdefender ne bloque pas les messages provenant de ces personnes; pour cela, ajouter des amis vous aide à laisser passer les messages légitimes.

Filtre jeu de caractères

De nombreux spams sont écrits en caractères cyrilliques et/ou asiatiques. Le filtre de caractères détecte ce type de messages et les enregistre en tant que SPAM.

Filtre de liens

La plupart des spams comportent des liens vers des destinations Web. Ces destinations sont souvent des pages à caractères publicitaires offrant la possibilité de faire des achats et sont parfois utilisées pour le phishing.

Bitdefender maintient une base de données de ce type de liens.Le filtre de liens compare toutes les URL d'un message à sa base de données. En cas de concordance, le message est marqué comme SPAM.

Filtre des signatures

Les spécialistes Bitdefender du spam analysent en permanence les e-mails de spam en circulation et publient des signatures de spam permettant de les détecter.

Le Filtre des signatures compare les e-mails aux signatures de spam de la base de données locale. En cas de concordance, le message est signalé comme étant du SPAM.

Note
Contrairement aux autres filtres, le Filtre des signatures ne peut pas être désactivé indépendamment de la protection antispam.

Filtre NeuNet (heuristique)

Le **Filtre Heuristique** effectue des tests sur tous les composants du message (pas seulement l'en-tête mais aussi le corps du message en html ou format texte), cherchant des mots spécifiques, phrases, liens ou autres caractéristiques du spam.En fonction des résultats de l'analyse, l'e-mail recevra un score de spam.

Si le score de spam dépasse le seuil, l'e-mail est considéré comme étant du SPAM. Le seuil est défini par le niveau de sensibilité de l'antispam. Pour plus d'informations, reportez-vous à « *Régler le niveau de sensibilité* » (p. 77).

Le filtre détecte aussi les messages marqués comme SEXUELLEMENT EXPLICITES dans leur objet et les enregistre en tant que SPAM.

Note
Depuis le 19 mai 2004, le spam avec un contenu sexuel doit inclure l'avertissement SEXUELLEMENT EXPLICITE dans l'objet, contre risque d'amendes pour violation de la loi.

Détection "in-the-cloud"

La détection "in the cloud" utilise les services Cloud de Bitdefender pour vous fournir une protection antispam efficace et toujours à jour.

Les e-mails sont vérifiés dans les nuages uniquement si les filtres antispam locaux ne fournissent pas de résultat probant.

6.1.2. Fonctionnement de l'Antispam

Le Moteur de Bitdefender Antispam utilise tous les filtres antispam combinés pour déterminer si un e-mail doit ou non accéder à votre **Boîte de réception**.

Chaque e-mail provenant du réseau Internet est d'abord vérifié à l'aide du filtre Liste des amis/Liste des spammeurs. Si l'adresse de l'expéditeur est identifiée dans la Liste des amis, alors l'e-mail est directement déplacé vers votre **boîte de réception**.

Sinon, le filtre Liste des spammeurs analysera à son tour l'e-mail pour vérifier si l'adresse de l'expéditeur figure dans sa liste. En cas de correspondance, l'e-mail sera étiqueté comme étant du SPAM et déplacé dans le dossier **Spam**.

Autrement, le filtre Jeu de caractères vérifiera si l'email est écrit en carctères cyrilliques ou en asiatiques. Si tel est le cas, le message sera marqué comme Spam et déplacé vers le dossier **Spam**.

Le Filtre de liens comparera les liens trouvés dans l'e-mail avec les liens connus comme étant du spam, contenus dans la base de données de Bitdefender. En cas de correspondance, l'e-mail sera considéré comme étant du SPAM.

Ensuite, le Filtre des signatures compare l'e-mail aux signatures de spam de la base de données locale. En cas de concordance, le message est signalé comme étant du SPAM.

Le Filtre Heuristique NeuNet effectuera toutes sortes de tests sur les composants du message, recherchant des mots, des expressions, des liens ou d'autres caractéristiques propres au SPAM. En fonction des résultats de l'analyse, l'e-mail recevra un score de spam.

Note

Si l'e-mail est marqué comme SEXUALLY EXPLICIT dans sa ligne de sujet, Bitdefender le considérera comme du SPAM.

Si le score de spam dépasse le seuil, l'e-mail est considéré comme étant du SPAM. Le seuil est défini par le niveau de protection antispam. Pour plus d'informations, reportez-vous à « *Régler le niveau de sensibilité* » (p. 77).

Si les filtres antispam locaux ne fournissent pas de résultat probant, l'e-mail est vérifié à l'aide de la détection dans les nuages, qui détermine en dernier lieu si l'e-mail est un spam ou est légitime.

6.1.3. Mises à jour de l'antispam

À chaque fois qu'une mise à jour est effectuée, de nouvelles signatures d'e-mails et de liens de spam connus sont ajoutées aux bases de données. Cette manipulation aide à renforcer l'efficacité du moteur Antispam.

Pour vous protéger des Spammeurs, Bitdefender peut effectuer des mise à jour automatiques. Maintenez l'option **Mise à jour automatique** activée.

6.1.4. Clients et protocoles de messagerie pris en charge

La protection antispam fonctionne avec tous les clients de messagerie POP3/SMTP.La barre Antispam Bitdefender ne s'affiche cependant que dans :

- Microsoft Outlook 2007 / 2010
- Microsoft Outlook Express et Windows Mail (sur les systèmes 32 bits)
- Mozilla Thunderbird 3.0.4

6.2. Activer ou désactiver la protection antispam

Pour activer ou désactiver la protection antispam, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Antispam**.

3. Cliquez sur le bouton pour activer ou désactiver la protection antispam.

6.3. Utilisation de la barre d'outils Antispam dans la fenêtre de votre client de messagerie

La barre d'outils Antispam se trouve dans la partie supérieure de votre client de messagerie.La barre d'outils Antispam vous aide à gérer la protection antispam directement à partir de votre client de messagerie. Vous pouvez facilement corriger Bitdefender s'il a indiqué comme SPAM un message légitime.

Important

Bitdefender s'intègre dans la plupart des clients de messagerie via une barre d'outils antispam facile à utiliser.Pour une liste complète des clients de messagerie pris en charge, veuillez vous référer à « *Clients et protocoles de messagerie pris en charge* » (p. 72).

Chaque bouton de la barre d'outils de Bitdefender sera expliqué ci-dessous:

Spam - indique que le message sélectionné est un spam. L'e-mail sera immédiatement placé dans le dossier **Spam**.Si les services cloud antispam sont activés, le message est envoyé au Cloud Bitdefender pour une analyse plus approfondie.

Pas Spam - indique que l'e-mail sélectionné n'est pas du spam et que Bitdefender ne devrait pas l'avoir signalé comme tel.Cet email sera retiré du dossier **Spam** et placé dans la **Boîte de réception**.Si les services cloud antispam sont activés, le message est envoyé au Cloud Bitdefender pour une analyse plus approfondie.

Important

Le bouton **Pas Spam** devient actif quand vous choisissez un message marqué spam par Bitdefender (ces messages se trouvent d'habitude dans le répertoire **Spam**).

Ajouter Spammeur - ajoute l'expéditeur de l'e-mail sélectionné à la liste des Spammeurs.Il se peut que vous ayez besoin de cliquer sur **OK** pour valider.Les messages provenant d'adresses qui figurent dans la liste de Spammeurs seront automatiquement considérés comme étant du `[spam]`.

Ajouter Ami - ajoute l'expéditeur de l'e-mail sélectionné à la liste d'Amis.Il se peut que vous ayez besoin de cliquer sur **OK** pour valider.Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.

Spammeurs - ouvre la liste des **Spammeurs**qui contient toutes les adresses e-mail dont vous ne voulez recevoir aucun message, quel que soit son contenu.Pour plus d'informations, reportez-vous à « *Configuration de la liste des spammeurs* » (p. 76).

Amis - ouvre la **Liste d'amis** qui contient tous les emails que vous souhaitez recevoir quel qu'en soit le contenu.Pour plus d'informations, reportez-vous à « *Configuration de la liste des amis* » (p. 75).

Configuration - ouvre une fenêtre qui vous permet de configurer les filtres antispam et les paramètres de la barre d'outils.

6.3.1. Indiquer des erreurs de détection

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement corriger le filtre antispam (en indiquant quels e-mails n'auraient pas dû être signalés comme étant du `[spam]`). Cela contribue à améliorer l'efficacité du filtre antispam.Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans le dossier de courrier indésirable dans lequel les messages de spam sont placés.
3. Sélectionnez le message légitime considéré à tort comme étant du `[spam]` par Bitdefender.
4. Cliquez sur le bouton **Ajouter un ami** de la barre d'outils antispam Bitdefender pour ajouter l'expéditeur à la liste d'Amis.Il se peut que vous ayez besoin de cliquer sur **OK** pour valider.Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.
5. Cliquez sur le bouton **Pas Spam** de la barre d'outils antispam de Bitdefender (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Le message d'e-mail sera placé dans la boîte de réception.

6.3.2. Indiquer les messages de spam non détectés

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement indiquer quels e-mails auraient dû être détectés comme étant du spam. Cela contribue à améliorer considérablement l'efficacité du filtrage antispam.Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans la boîte de Réception.
3. Sélectionnez les messages de spam non détectés.
4. Cliquez sur le bouton **Spam** de la barre d'outils antispam de Bitdefender(généralement située dans la partie supérieure de la fenêtre du client de messagerie). Les messages sont immédiatement signalés comme étant du `[spam]` et son placés dans le dossier de courrier indésirable.

6.3.3. Configuration des paramètres de la barre d'outils

Pour configurer les paramètres de la barre d'outils antispam de votre client de messagerie, cliquez sur le bouton **Configuration** de la barre d'outils puis sur l'onglet **Paramètres de la barre d'outils**.

Les paramètres sont regroupés en deux catégories :

- Dans la catégorie **Règles de messagerie**, vous pouvez configurer les règles de traitement des e-mails de spam détectés par Bitdefender.
  - **Placer le message dans les éléments supprimés** (uniquement pour Microsoft Outlook Express / Windows Mail)

    Note
    Dans Microsoft Outlook / Mozilla Thunderbird, les messages de spam détectés sont automatiquement placés dans un dossier Spam, situé dans le dossier Éléments supprimés / Corbeille.

  - **Signaler les messages spam comme 'lus'** - signale automatiquement les messages spam comme lus, de manière à éviter le dérangement que provoque leur arrivée.
- Dans la catégorie **Notifications** vous pouvez choisir d'afficher ou non des fenêtres de confirmation lorsque vous cliquez sur les boutons **Ajouter spammeur** et **Ajouter ami** de la barre d'outils antispam. Les fenêtres de confirmation peuvent empêcher d'ajouter accidentellement des expéditeurs d'e-mails à la liste d'Amis / de Spammeurs.

6.4. Configuration de la liste des amis

La **liste d'amis** est une liste de toutes les adresses email dont vous accepterez les messages, quel que soit leur contenu. Les messages de vos amis ne seront jamais considérés comme spam, même si leur contenu ressemble au spam.

Note
Tout message provenant d'une adresse contenue dans la **liste d'amis** sera automatiquement déposé dans votre boîte de réception sans autre traitement.

Pour configurer et gérer la liste d'Amis :

- Si vous utilisez Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, cliquez sur le bouton **Amis** de la barre d'outils antispam Bitdefender intégrée à votre client de messagerie.
- Vous pouvez également procéder comme suit :
  1. Ouvrez la fenêtre de Bitdefender.
  2. Allez dans le panneau **Antispam**.
  3. Cliquez sur **Gérer** et sélectionnez **Amis** dans le menu.

Pour ajouter une adresse e-mail, sélectionnez l'option **Adresse e-mail**, indiquez l'adresse puis cliquez sur **Ajouter**.Syntaxe: name@domain.com.

Pour ajouter toutes les adresses e-mail d'un domaine particulier, sélectionnez l'option **Nom de domaine**, indiquez le nom de domaine puis cliquez sur **Ajouter**.Syntaxe:

- @domain.com, *domain.com et domain.com - tous les messages en provenance de domain.com seront dirigés vers votre **Boîte de réception** quel que soit leur contenu;
- *domain* - tous les messages provenant de domain (quel que soit le suffixe) seront dirigés vers votre **Boîte de réception** quel que soit leur contenu;
- *com - tous les messages ayant comme suffixe du domaine com seront dirigés vers votre **Boîte de réception** quel que soit leur contenu;

Il est recommandé d'éviter d'ajouter des noms de domaines entiers, mais cela peut être utile dans certaines situations.Vous pouvez, par exemple, ajouter le domaine de messagerie électronique de la société pour laquelle vous travaillez ou les domaines de partenaires en qui vous avez confiance.

Pour retirer un élément de la liste, cliquez sur le lien correspondant **Supprimer**.Pour supprimer toutes les entrées de la liste, cliquez sur le bouton **Nettoyer** puis sur **Oui** pour confirmer.

Vous pouvez enregistrer la liste d'amis dans un fichier afin de pouvoir l'utilisersur un autre ordinateur ou si vous réinstallez le produit.Pour enregistrer la liste d'Amis, cliquez sur le bouton **Enregistrer** et enregistrez-la à l'emplacement désiré.Le fichier aura l'extension `.bwl`.

Pour charger une liste d'Amis enregistrée préalablement, cliquez sur le bouton **Charger** et ouvrez le fichier `.bwl` correspondant.Pour supprimer le contenu de la liste en cours d'utilisation lorsque vous chargez une liste enregistrée auparavant, sélectionnez **Écraser la liste en cours**.

Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

6.5. Configuration de la liste des spammeurs

La **liste des spammeurs** est une liste de toutes les adresses e-mail de la part de lesquelles vous ne voulez recevoir aucun message, quel que soit son contenu.Tout message en provenance d'une adresse de la **liste des spammeurs** sera automatiquement marqué SPAM sans autre traitement.

Pour configurer et gérer la liste des Spammeurs :

- Si vous utilisez Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, cliquez sur le bouton **Spammeurs** de la barre d'outils antispam Bitdefender intégrée à votre client de messagerie.
- Vous pouvez également procéder comme suit :
  1. Ouvrez la fenêtre de Bitdefender.

2. Allez dans le panneau **Antispam**.
3. Cliquez sur **Gérer** et sélectionnez **Spammeurs** dans le menu.

Pour ajouter une adresse e-mail, sélectionnez l'option **Adresse e-mail**, indiquez l'adresse puis cliquez sur **Ajouter**.Syntaxe: name@domain.com.

Pour ajouter toutes les adresses e-mail d'un domaine particulier, sélectionnez l'option **Nom de domaine**, indiquez le nom de domaine puis cliquez sur **Ajouter**.Syntaxe:

- @domain.com, *domain.com et domain.com - tous les messages provenant de domain.com seront étiquetés comme SPAM;
- *domain* - tous les messages de domain (quel que soit le suffixe) seront étiquetés comme SPAM;
- *com - tous les messages provenant d'un domaine avec un suffixe com seront étiquetés comme SPAM.

Il est recommandé d'éviter d'ajouter des noms de domaines entiers, mais cela peut être utile dans certaines situations.

Avertissement

N'ajoutez pas de domaines de services de webmail légitimes (tels que Yahoo, Gmail, Hotmail ou d'autres) à la liste de Spammeurs. Sinon, les e-mails envoyés par les utilisateurs de ces services seront identifiés comme étant du spam.Si par exemple, vous ajoutez `yahoo.com` à la liste des Spammeurs, tous les e-mails provenant d'adresses `yahoo.com` seront identifiés comme étant du `[spam]`.

Pour retirer un élément de la liste, cliquez sur le lien correspondant **Supprimer**.Pour supprimer toutes les entrées de la liste, cliquez sur le bouton **Nettoyer** puis sur **Oui** pour confirmer.

Vous pouvez enregistrer la liste des spammeurs dans un fichier afin de pouvoirl'utiliser sur un autre ordinateur ou si vous réinstallez le produit.Pour enregistrer la liste des Spammeurs, cliquez sur le bouton **Enregistrer** et enregistrez-la à l'emplacement désiré.Le fichier aura l'extension `.bwl`.

Pour charger une liste de Spammeurs enregistrée préalablement, cliquez sur le bouton **Charger** et ouvrez le fichier `.bwl` correspondant.Pour supprimer le contenu de la liste en cours d'utilisation lorsque vous chargez une liste enregistrée auparavant, sélectionnez **Écraser la liste en cours**.

Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

6.6. Régler le niveau de sensibilité

Si vous remarquez que certains e-mails légitimes sont signalés comme étant du spam, ou que de nombreux e-mails de spam ne sont pas détectés, vous pouvez essayer d'ajuster le niveau de sensibilité de l'antispam pour régler le problème. Cependant, plutôt que de modifier par vous-même le niveau de sensibilité, nous

vous recommandons de commencer par lire « *Le filtre antispam ne fonctionne pas correctement* » (p. 150) et de suivre les instructions pour corriger le problème.

Pour régler le niveau de sensibilité de l'antispam, suivez ces étapes :

1. Lancer Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antispam** dans le menu de gauche puis sur l'onglet **Paramètres**.
4. Reportez-vous à la description à droite de l'échelle pour choisir le niveau de sensibilité le plus adapté à vos besoins de sécurité. La description vous informe également des actions supplémentaires à appliquer afin d'éviter des problèmes éventuels ou d'améliorer l'efficacité de la détection du spam.

6.7. Configurer les filtres antispam locaux

Comme cela est décrit dans « *Aperçu de l'antispam* » (p. 70), Bitdefender utilise une combinaison de divers filtres antispam pour identifier le spam.Les filtres antispam sont préconfigurés pour une protection efficace.

Important

Selon que vous recevez ou non des e-mails légitimes rédigés avec des caractères asiatiques ou cyrilliques, désactivez ou activez le paramètre bloquant automatiquement ces e-mails. Le paramètre correspondant est désactivé dans les versions localisées du programme utilisant ces jeux de caractères (par exemple, dans la version russe ou chinoise).

Pour configurer les filtres antispam locaux, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antispam** dans le menu de gauche puis sur l'onglet **Paramètres**.
4. Cliquez sur les boutons pour activer ou désactiver les filtres antispam locaux.

Si vous utilisez Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, vous pouvez configurer les filtres antispam locaux directement à partir de votre client de messagerie. Cliquez sur le bouton **Configuration** de la barre d'outils antispam de Bitdefender (généralement situé dans la partie supérieure de la fenêtre du client de messagerie) puis sur l'onglet **Filtres Antispam**.

6.8. Configurer la détection "in-the-cloud"

La détection "in the cloud" utilise les services Cloud de Bitdefender pour vous fournir une protection antispam efficace et toujours à jour.

Pour configurer la détection "in-the-cloud", suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antispam** dans le menu de gauche puis sur l'onglet **Cloud**.
4. Cliquez sur le bouton pour activer ou désactiver la détection "in-the-cloud".
5. Des échantillons d'e-mails de spam ou légitimes peuvent être envoyés au Cloud Bitdefender lorsque vous indiquez des erreurs de détection ou des e-mails de spam non détectés. Cela contribue à améliorer la détection antispam de Bitdefender.Configurez l'envoi d'échantillons d'e-mails au Cloud Bitdefender en sélectionnant les options souhaitées.

Si vous utilisez Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, vous pouvez configurer la détection "in-the-cloud" directement à partir de votre client de messagerie. Cliquez sur le bouton **Configuration** de la barre d'outils antispam de Bitdefender (généralement situé dans la partie supérieure de la fenêtre du client de messagerie) puis sur l'onglet **Configuration du Cloud**.

7. Contrôle Vie Privée

Vos informations confidentielles sont une cible constante des cybercriminels.Les menaces ayant atteint la quasi totalité des activités en ligne, la consultation d'e-mails, l'utilisation de services de messagerie et la navigation sur Internet sans protection adaptée peuvent conduire à des fuites susceptibles de menacer votre vie privée.

De plus, des fichiers importants que vous conservez sur votre ordinateur peuvent se retrouver un jour entre de mauvaises mains.

Le Contrôle Vie Privée de Bitdefender s'attaque à toutes ces menaces avec de nombreux composants.

- Protection Antiphishing - propose un ensemble complet de fonctionnalités qui vous permettent de naviguer sur Internet en toute sécurité, en vous évitant de divulguer des informations personnelles à des sites web frauduleux se faisant passer pour légitimes.
- Données - vous aide à vérifier que vos informations personnelles ne quittent pas votre ordinateur sans votre accord. Analyse les e-mails et les messages instantanées envoyés à partir de votre ordinateur ainsi que les données transmises via des pages web, et bloque toute information protégée par les règles de protection des données que vous avez créées.
- Cryptage de Messagerie Instantanée - chiffre vos conversations de messagerie instantanée afin de garantir la confidentialité de celles-ci.
- Cryptage de Fichiers - vous permet de créer des disques (ou coffres) cryptés, protégés par mot de passe, sur votre ordinateur, dans lesquels vous pouvez stocker vos documents confidentiels ou sensibles en toute sécurité.
- Destructeur de fichiers - efface définitivement des fichiers et toute trace de ceux-ci sur votre ordinateur.

7.1. Protection antiphishing

L'antiphishing Bitdefender empêche la divulgation de vos informations personnelles sur Internet en vous alertant sur les pages Internet potentiellement de type phishing.

Bitdefender fournit une protection antiphishing en temps réel pour :

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Pour configurer les paramètres Antiphishing, les étapes sont les suivantes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Contrôle Vie Privée** dans le menu de gauche puis sur l'onglet **Antiphishing**.

Les paramètres sont regroupés en deux catégories.

Fonctions de la barre d'outils

Cliquez sur les boutons pour activer ou désactiver :

- Affichage de la barre d'outils Bitdefender dans le navigateur web.
- Search advisor, un composant qui évalue les résultats de vos recherches Google, Bing et Yahoo!, ainsi que tous les liens Facebook et Twitter en plaçant une icône devant chaque résultat :

  Nous vous déconseillons de consulter cette page web.

  Cette page web peut contenir du contenu dangereux. Soyez prudent si vous décidez de la consulter.

  Cette page peut être consultée en toute sécurité.
- Analyse du trafic web SSL.

  Des attaques plus sophistiquées peuvent utiliser le trafic web sécurisé pour induire en erreur leurs victimes.Nous vous recommandons donc d'activer l'analyse SSL.

Protection des navigateurs web

Cliquez sur les boutons pour activer ou désactiver :

- Protection contre les escroqueries.
- Protection contre le phishing.
- Protection de la messagerie instantanée.

Vous pouvez créer une liste de sites Web qui ne seront pas analysés par les moteurs Antiphishing de Bitdefender.La liste ne doit contenir que des sites web de confiance.Par exemple, ajoutez les sites Web sur lesquels vous avez l'habitude de faire vos achats en ligne.

Pour configurer et gérer la liste blanche antiphishing, cliquez sur le lien **Liste Blanche**.Une nouvelle fenêtre s'affiche.

Pour ajouter un site à la liste blanche, entrez son adresse dans le champ correspond et cliquez sur **Ajouter**.

Pour supprimer un site web de la liste, sélectionnez-le dans la liste et cliquez sur le lien **Supprimer**.

Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

7.1.1. Protection Bitdefender dans le navigateur web

Bitdefender s'intègre directement et au moyen d'une barre d'outils intuitive et conviviale aux navigateurs Internet suivants :

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera

La barre d'outils de Bitdefender n'est pas votre barre d'outils de navigateur typique. La seule chose qu'il ajoute à votre navigateur est un petit bouton en haut de chaque page web.Cliquez dessus pour voir la barre d'outils.

La barre d'outils Bitdefender contient les éléments suivants :

Résultat de la page

En fonction de la façon dont Bitdefender classifie la page web que vous affichez, l'un des résultats suivants s'affiche dans la partie gauche de la barre d'outils :

- Le message "Cette page n'est pas sûre" apparaît sur un fond rouge - nous vous recommandons de quitter immédiatement la page web.
- Le message "Nous vous recommandons d'être vigilant" apparaît sur un fond orange - le contenu de cette page web peut être dangereux.Soyez prudent si vous décidez de le consulter.
- Le message "Cette page est sûre" apparaît sur un fond vert - il s'agit d'une page sûre que vous pouvez consulter.

Bac à sable

Cliquez sur pour lancer le navigateur dans un environnement fourni par Bitdefender, l'isolant du système d'exploitation. Cela empêche les menaces de navigateur d'exploiter les vulnérabilités des navigateurs pour prendre le contrôle de votre système. Utilisez le Bac à sable lorsque vous consultez des pages web que vous suspectez de contenir des malwares.

Note
Le Bac à sable n'est pas disponible sur les ordinateurs fonctionnant sous Windows XP.

Configuration

Cliquez sur pour sélectionner les fonctionnalités individuelles à activer ou désactiver :

- Filtre Antiphishing
- Filtre Antimalware

- Search Advisor

Bouton marche/arrêt

Pour activer / désactiver complètement les fonctionnalités de la barre d'outils, cliquez sur sur le côté droit de la barre d'outils.

7.1.2. Alertes Bitdefender dans le navigateur

Lorsque vous essayez de consulter un site Web considéré comme non sûr, ce site web est bloqué et une page d'avertissement s'affiche dans votre navigateur.

La page contient des informations telles que l'URL du site web et la menace détectée.

Vous devez décider quoi faire ensuite. Les options suivantes sont disponibles :

- Quittez la page web.
- Pour vous rendre sur le site web, malgré l'avertissement, cliquez sur **Je comprends les risques, je souhaite quand même consulter cette page**.
- Ajoutez la page à la liste blanche antiphishing en cliquant sur **Ajouter à la liste blanche**.Cette page ne sera plus analysée par les moteurs Antiphishing de Bitdefender.

7.2. Données

La protection des données empêche les fuites de données sensibles lorsque vous êtes en ligne.

Prenons un exemple simple : vous avez créé une règle de protection des données qui protège votre numéro de carte bancaire.Si un logiciel spyware parvient à s'installer sur votre ordinateur, il ne peut pas transmettre votre numéro de carte bancaire par e-mail, messages instantanés ou pages web. De plus, vos enfants ne peuvent pas l'utiliser pour faire des achats en ligne ou le révéler à des personnes rencontrées sur Internet.

Pour en savoir plus, reportez-vous à ces sujets :

- « *À propos de la protection des données* » (p. 83).
- « *Configurer la protection des données* » (p. 84).
- « *Gestion des règles* » (p. 85).

7.2.1. À propos de la protection des données

Qu'il s'agisse de votre adresse email ou de votre numéro de carte bancaire, si ces informations tombent dans de mauvaises mains vous pouvez en subir les conséquences: crouler sous le spam ou retrouver votre compte bancaire vide.

En se basant sur les règles que vous avez créées, la Protection des Données analyse le trafic Internet, de messagerie et de messagerie instantanée partant de votre ordinateur, pour y rechercher des chaînes de texte spécifiques que vous avez définies

(par exemple, votre numéro de carte bancaire). En cas de correspondance, la page Web, l'e-mail ou l'échange de messagerie instantanée concerné est bloqué.

Vous pouvez créer des règles pour protéger toutes les informations que vous considérez comme personnelles ou confidentielle, votre numéro de téléphone, votre adresse e-mail ou votre Numéro de compte bancaire...Le support multi-utilisateur est fourni pour que les utilisateurs connectés sur des comptes Windows différents puissent configurer et utiliser leurs propres règles.Si votre compte Windows est un compte administrateur, les règles que vous créez peuvent être configurées pour s'appliquer également lorsque d'autres utilisateurs de l'ordinateur sont connectés à leurs comptes utilisateurs Windows.

7.2.2. Configurer la protection des données

Si vous souhaitez utiliser la protection des données, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Contrôle Vie Privée** dans le menu de gauche puis sur l'onglet **Protection des données**.
4. Vérifiez que la protection des données est activée.
5. Définissez les règles nécessaires à la protection de vos données sensibles.Pour plus d'informations, reportez-vous à « *Créer des règles de protection des données* » (p. 84).

Créer des règles de protection des données

Pour créer un règle, cliquez sur le bouton **Ajouter une règle** et suivez les indications de l'assistant de configuration. Vous pouvez naviguer dans l'assistant à l'aide des boutons **Suivant** et **Retour**. Pour quitter l'assistant, cliquez sur **Annuler**.

1. **Définition des types de règles et de données**

   Vous devez définir les paramètres suivants:

   - **Nom de la règle** - saisissez le nom de la règle dans ce champ de saisie.
   - **Type de règle** - détermine le type de règle (addresse, nom, carte de crédit, code PIN, etc.)
   - **Données de la règle** - saisissez les données que vous voulez protéger dans ce champ de saisie.Si par exemple vous voulez protéger votre numéro de carte de crédit, saisissez ici l'intégralité ou une partie de celui-ci.

     Important
     Si vous saisissez moins de trois caractères, vous serez invité à valider les données. Nous vous recommandons de saisir au moins trois caractères afin d'éviter le blocage erroné de messages et de pages Web.

Toutes les données que vous enregistrez sont cryptées. Pour plus de sécurité, n'entrez pas toutes les données que vous souhaitez protéger.

2. **Sélectionnez les types de trafic et les utilisateurs**

   a. Sélectionnez le type de trafic que Bitdefender doit analyser.

   - **Analyse Web (trafic HTTP)** - analyse le trafic Web (HTTP) et bloque les données sortantes correspondant aux données de la règle.
   - **Analyse e-mail (trafic SMTP)** - analyse le trafic mail (SMTP) et bloque les e-mails sortants qui contiennent les éléments déterminés dans la règle de gestion des données.
   - **Analyse du trafic de Messagerie Instantanée** - analyse le trafic de Messagerie Instantanée et bloque les échanges sortants qui contiennent les éléments déterminés dans la règle de gestion des données.

   Vous pouvez choisir d'appliquer la règle uniquement si les données de la règle correspondent à tous les mots ou à la chaîne de caractères détectée.

   b. Spécifiez les utilisateurs pour lesquels la règle s'applique.

   - **Seulement pour moi (utilisateur actuel)** - la règle s'appliquera seulement à votre compte utilisateur.
   - **Comptes utilisateurs limités** - la règle s'appliquera à vous et aux comptes Windows limités.
   - **Tous les utilisateurs** - la règle s'appliquera à tous les comptes Windows.

3. **Décrire la règle**

   Entrez une description courte de la règle dans le champ correspondant.Puisque les données bloquées (chaines de caractères) ne sont pas affichées sous forme de texte clair quand vous accédez à la règle, la description devrait vous aider à l'identifier rapidement.

   Cliquez sur **Terminer**.La règle apparaîtra dans le tableau.

Désormais, toute tentative d'envoi des données spécifiées (via e-mail, messagerie instantanée ou sur une page web) échouera. Une entrée apparaîtra dans le fenêtre Événements indiquant que Bitdefender a bloqué l'envoi de contenu lié à l'identité.

7.2.3. Gestion des règles

Pour gérer les règles de protection des données :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Contrôle Vie Privée** dans le menu de gauche puis sur l'onglet **Protection des données**.

Vous pouvez voir les règles existantes dans le tableau.

Pour supprimer une règle, sélectionnez-la, puis cliquez sur le bouton **Supprimer**.

Pour modifier une règle, sélectionnez-la, puis cliquez sur le bouton **Modifier la règle**. Une nouvelle fenêtre s'affiche alors.Dans cette rubrique, vous pouvez modifier le nom, la description et les paramètres de la règle (type, données et trafic). Cliquez sur **OK** pour enregistrer les modifications.

7.3. Messagerie Inst.

Le contenu de vos messages instantanés doit rester entre vous et votre interlocuteur.En cryptant vos conversations, vous pouvez vous assurer que toute personne qui tentera de les intercepter en cours de route, depuis et vers vos contacts, ne pourra pas en lire le contenu.

Par défaut, Bitdefender crypte toutes vos sessions de messagerie instantanée, à condition que :

- Votre correspondant a installé un produit Bitdefender qui prend en charge le cryptage de messagerie instantanée, et le cryptage est activé pour l'application de messagerie instantanée utilisée pour converser.
- vous et votre correspondant utilisiez soit Yahoo Messenger, soit Windows Live (MSN) Messenger.

Important

Bitdefender ne cryptera pas la conversation si le correspondant utilise une application à interface Web, telle que Meebo, ou si l'un des correspondants utilise Yahoo! et l'autre Windows Live (MSN).

Pour configurer le cryptage de messagerie instantanée :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Contrôle Vie Privée** dans le menu de gauche puis sur l'onglet **Cryptage**.

Par défaut, le cryptage de messagerie instantanée est activé pour Yahoo Messenger et Windows Live (MSN) Messenger.Vous pouvez désactiver le Cryptage de Messagerie Instantanée pour une application ou pour les deux en cliquant sur le bouton correspondant.

7.4. Cryptage de Fichiers

Le Cryptage de Fichiers Bitdefender vous permet de créer des disques (ou coffres) cryptés, protégés par mot de passe, sur votre ordinateur, dans lesquels vous pouvez stocker vos documents confidentiels ou sensibles en toute sécurité.Les données

stockées dans le coffre-fort ne sont accessibles qu'aux utilisateurs connaissant le mot de passe.

Le mot de passe vous permet d'ouvrir le coffre-fort pour y stocker vos données et de le refermer tout en préservant sa sécurité.Pendant qu'un coffre est ouvert, vous pouvez ajouter de nouveaux fichiers, accéder au fichiers courrants ou les modifier.

Physiquement, le coffre-fort est un fichier stocké sur votre disque dur local avec l'extension `.bvd`.Même si les fichiers représentant les coffres peuvent être atteints depuis un système d'exploitation différent comme Linux, les informations stockées dedans ne peuvent être lues car elles sont cryptées.

Le Cryptage de Fichiers est désactivé par défaut.Pour l'activer, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Contrôle Vie Privée** dans le menu de gauche puis sur l'onglet **Cryptage**.
4. Cliquez sur le bouton **Accès au coffre-fort** pour l'activer.

Les coffres-forts peuvent être gérés depuis la fenêtre de Bitdefender ou à l'aide du menu contextuel Windows et du disque logique associé au coffre-fort.

7.4.1. Gérer des coffres-forts à partir de l'interface de Bitdefender

Pour gérer vos coffres-forts à partir de l'interface de Bitdefender, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Contrôle Vie Privée** dans le menu de gauche puis sur l'onglet **Cryptage**.

Les coffres-forts existants apparaissent dans le tableau dans la partie inférieure de la fenêtre.Pour actualiser la liste, faites un clic droit à l'intérieur du tableau et sélectionnez **Actualiser les coffres-forts** dans le menu qui apparaît.

Créer des coffres-forts

Pour créer un nouveau coffre-fort, faites un clic droit sur l'en-tête du tableau des coffres-forts et sélectionnez **Créer un nouveau coffre-fort**.

Une nouvelle fenêtre s'affiche.

1. Spécifiez l'emplacement et le nom du coffre-fort.
   - Cliquez sur **Parcourir** pour sélectionner l'emplacement du coffre-fort et sauvegardez le coffre-fort sous le nom que vous souhaitez.

- Entrez le nom et le chemin d'accès du fichier du coffre-fort sur le disque dans les champs correspondants.

2. Choisissez une lettre de lecteur à partir du menu.Quand vous ouvrez le coffre, un disque virtuel indexé avec la lettre choisie apparaît dans Poste de travail.
3. Si vous souhaitez modifier la taille par défaut du coffre-fort (50 Mo), entrez la valeur souhaitée dans le champ **Taille du coffre-fort**.
4. Tapez le mot de passe souhaité pour le coffre-fort dans les champs **Mot de passe** et **Confirmation**.Toutes personnes essayant d'ouvrir le coffre et d'utiliser les fichiers doit fournir le mot de passe.
5. Cliquez sur **Créer** si vous souhaitez créer le coffre-fort seulement à l'emplacement sélectionné.Pour créer et afficher le coffre-fort comme disque virtuel dans Poste de travail, cliquez sur **Créer&Ouvrir**.

Bitdefender vous informera immédiatement du résultat de l'opération.Si une erreur s'est produite, utilisez le message d'erreur pour essayer de régler le problème. Cliquez sur **OK** pour fermer la fenêtre.

Note

Il peut être pratique d'enregistrer tous les coffres-forts au même emplacement. De cette façon, vous les retrouverez plus vite.

Ouverture de coffres-forts

Pour accéder aux fichiers contenus dans un coffre et pouvoir travailler avec ces fichiers, il faut d'abord ouvrir le coffre.Quand vous ouvrez le coffre, un disque virtuel s'affiche dans le Poste de travail.Le disque se voit attribuer la lettre correspondant au coffre.

Pour ouvrir un coffre-fort, suivez ces étapes :

1. Cliquez sur le coffre-fort dans le tableau et sélectionnez **Ouvrir** dans le menu qui s'affiche.

   Note

   Si un coffre-fort existant n'apparaît pas dans le tableau, faites un clic droit sur l'en-tête du tableau des coffres-forts, sélectionnez **Ajouter un coffre-fort existant** et accédez à son emplacement.

2. Une nouvelle fenêtre s'affiche.

   Le nom du coffre-fort et son emplacement s'affichent.Choisissez une lettre de lecteur à partir du menu.
3. Entrez le mot de passe du coffre-fort dans le champ **Mot de Passe**.
4. Cliquez sur **Ouvrir**.

Bitdefender vous informera immédiatement du résultat de l'opération.Si une erreur s'est produite, utilisez le message d'erreur pour essayer de régler le problème.

Ajout de fichiers aux coffres-forts

Pour lancer un assistant qui vous permettra d'ajouter des fichiers à un coffre, cliquez sur **Choisir une Action** dans la zone de Cryptage des Fichiers puis sélectionnez **Ajouter des fichiers au coffre-fort** dans le menu déroulant.

Vous pouvez naviguer dans l'assistant à l'aide des boutons **Suivant** et **Retour**. Pour quitter l'assistant, cliquez sur **Annuler**.

1. **Sélectionnez des fichiers & des dossiers**

   Cliquez sur **Ajouter cible** pour sélectionner les fichiers/dossiers qui seront ajoutés au coffre-fort.

2. **Choisir un coffre-fort**

   Vous pouvez sélectionner un coffre-fort existant, rechercher un coffre-fort déjà créé ou en créer un nouveau dans lequel ajouter les fichiers.

3. **Créer un Coffre-Fort**

   Si vous avez choisi de créer un nouveau coffre-fort, vous pouvez indiquer ici les informations nécessaires à son sujet. Pour plus d'informations, veuillez vous référer à « *Créer des coffres-forts* » (p. 87)

4. **Entrer le mot de passe**

   Si vous avez sélectionné un coffre-fort verrouillé, vous devez indiquer son mot de passe pour l'ouvrir.

5. **Confirmer**

   Cette étape vous permet de vérifier les choix faits au cours des étapes précédentes.

   Note

   Si vous avez choisi de créer un nouveau coffre-fort, Bitdefender vous demandera de formater le lecteur qui y est associé. Sélectionnez les options de formatage et cliquez sur **Démarrer** pour formater le lecteur.

6. **Contenu**

   Cette étape vous permet d'afficher le contenu du coffre-fort.

Verrouiller des coffres-forts

Quand vous avez fini de travailler avec les fichiers d'un coffre-fort, vous devez le verrouiller pour protéger vos données.En verrouillant le coffre-fort, le disque virtuel

correspondant disparaît de Poste de travail. L'accès aux données stockées dans le coffre-fort est donc complètement bloqué.

Pour verrouiller un coffre-fort, cliquez dessus dans le tableau et sélectionnez **Verrouiller** dans le menu qui s'affiche.

Vous pouvez également lancer un assistant qui vous permettra de verrouiller un coffre-fort en cliquant sur **Choisir une Action** dans la zone de Cryptage des Fichiers puis sélectionnez **Verrouiller le coffre-fort** dans le menu déroulant.

Vous pouvez naviguer dans l'assistant à l'aide des boutons **Suivant** et **Retour**. Pour quitter l'assistant, cliquez sur **Annuler**.

1. **Choisir un coffre-fort**

   Cette étape vous permet de spécifier le coffre-fort à verrouiller.

2. **Confirmer**

   Cette étape vous permet de vérifier les choix faits au cours des étapes précédentes.

3. **Terminer**

   Cette étape vous permet d'afficher le résultat de l'opération.

Bitdefender vous informera immédiatement du résultat de l'opération.Si une erreur s'est produite, utilisez le message d'erreur pour essayer de régler le problème. Cliquez sur **OK** pour fermer la fenêtre.

Supprimer des fichiers des coffres-forts

Pour lancer un assistant qui vous permettra de retirer des fichiers d'un coffre, cliquez sur **Choisir une Action** dans la zone de Cryptage des Fichiers puis sélectionnez **Supprimer les fichiers** dans le menu déroulant.

Vous pouvez naviguer dans l'assistant à l'aide des boutons **Suivant** et **Retour**. Pour quitter l'assistant, cliquez sur **Annuler**.

1. **Choisir un coffre-fort**

   Cette étape vous permet de spécifier le coffre-fort duquel vous voulez supprimer des fichiers.

2. **Entrer le mot de passe**

   Si vous avez sélectionné un coffre-fort verrouillé, vous devez indiquer son mot de passe pour l'ouvrir.

3. **Contenu**

   Sélectionnez les fichiers ou dossiers à supprimer du coffre-fort.

4. **Confirmer**

Cette étape vous permet de vérifier les choix faits au cours des étapes précédentes.

5. **Terminer**

   Cette étape vous permet d'afficher le résultat de l'opération.

Afficher les contenus des coffres-forts

Pour lancer un assistant qui vous permettra d'afficher le contenu d'un coffre-fort, cliquez sur **Choisir une Action** dans la zone de Cryptage des Fichiers puis sélectionnez **Afficher les fichiers du coffre-fort** dans le menu déroulant.

Vous pouvez naviguer dans l'assistant à l'aide des boutons **Suivant** et **Retour**. Pour quitter l'assistant, cliquez sur **Annuler**.

1. **Choisir un coffre-fort**

   Cette étape vous permet de spécifier le coffre-fort dont vous souhaitez afficher les fichiers.

2. **Entrer le mot de passe**

   Si vous avez sélectionné un coffre-fort verrouillé, vous devez indiquer son mot de passe pour l'ouvrir.

3. **Confirmer**

   Cette étape vous permet de vérifier les choix faits au cours des étapes précédentes.

4. **Contenu**

   Cette étape vous permet d'afficher le résultat de l'opération.

Changer le mot de passe du coffre-fort

Le coffre-fort doit être verrouillé pour que vous puissiez modifier son mot de passe. Pour modifier le mot de passe d'un coffre-fort, suivez ces étapes :

1. Cliquez sur le coffre-fort dans le tableau et sélectionnez **Changer de mot de passe** dans le menu qui s'affiche.

   Une nouvelle fenêtre s'affiche.

2. Entrez le mot de passe actuel du coffre-fort dans le champ **Ancien mot de Passe**.

3. Entrez le nom du nouveau mot de passe champ **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**.

Note

Le mot de passe doit comporter au moins 8 caractères.Pour avoir un mot de passe sécurisé, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

4. Cliquez sur **OK** pour changer le mot de passe.

Bitdefender vous informera immédiatement du résultat de l'opération.Si une erreur s'est produite, utilisez le message d'erreur pour essayer de régler le problème. Cliquez sur **OK** pour fermer la fenêtre.

7.4.2. Gérer les coffres-forts depuis Windows

Bitdefender s'intègre dans Windows pour vous aider à gérer vos coffres-forts plus facilement.

Le menu contextuel de Windows s'affiche si vous faites un clic droit sur un fichier ou un dossier ou sur des objets placés sur votre bureau.Pointez simplement sur Coffre-Fort Bitdefender dans ce menu et vous aurez accès à toutes les opérations disponibles pour les coffres-forts.

De plus, quand vous ouvrez (montez) un coffre-fort, un nouveau disque (une nouvelle partition logique) apparaîtra.Ouvrez simplement le Poste de travail pour voir apparaître un nouveau disque basé sur votre coffre-fort. Vous pouvez y effectuer les différentes manipulations de fichiers courantes (copie, suppression, modification, etc.). Les fichiers sont protégés tant qu'ils sont conservés sur ce disque (car un mot de passe est demandé lors du montage du fichier).Lorsque vous avez terminé, verrouillez (c'est-à-dire démontez) votre coffre-fort afin d'activer la protection de son contenu.

Vous pouvez facilement identifier les coffres-forts Bitdefender de votre ordinateur par l'icône Bitdefender et l'extension `.bvd`.

Création de coffres-forts

Gardez à l'esprit qu'un coffre-fort est en fait simplement un fichier avec l'extension `.bvd`.Lorsque vous ouvrez le coffre-fort, un disque virtuel apparaît dans Poste de Travail où vous pouvez stocker des fichiers en toute sécurité. Lorsque vous créez un coffre-fort, vous devez spécifier où et sous quel nom l'enregistrer dans votre ordinateur. Vous devez également indiquer un mot de passe pour protéger son contenu.Seuls les utilisateurs connaissant le mot de passe peuvent ouvrir le coffre-fort et accéder aux documents et aux données qu'il contient.

Pour créer un coffre-fort, procédez comme suit :

1. Faites un clic droit sur votre bureau ou sur un dossier/fichier de votre ordinateur, allez sur **Coffre-fort Bitdefender** et sélectionnez **Créer un Coffre-Fort**.Une nouvelle fenêtre s'affiche.

2. Spécifiez l'emplacement et le nom du coffre-fort.
   - Cliquez sur **Parcourir** pour sélectionner l'emplacement du coffre-fort et sauvegardez le coffre-fort sous le nom que vous souhaitez.
   - Entrez le nom et le chemin d'accès du fichier du coffre-fort sur le disque dans les champs correspondants.
3. Choisissez une lettre de lecteur à partir du menu.Quand vous ouvrez le coffre, un disque virtuel indexé avec la lettre choisie apparaît dans Poste de travail.
4. Si vous souhaitez modifier la taille par défaut du coffre-fort (50 Mo), entrez la valeur souhaitée dans le champ **Taille du coffre-fort**.
5. Indiquez le mot de passe souhaité pour le coffre-fort dans le**Mot de passe**et**Confirmer**champs.Toutes personnes essayant d'ouvrir le coffre et d'utiliser les fichiers doit fournir le mot de passe.
6. Cliquez sur **Créer** si vous souhaitez créer le coffre-fort seulement à l'emplacement sélectionné.Pour créer et afficher le coffre-fort comme disque virtuel dans Poste de travail, cliquez sur **Créer&Ouvrir**.

Bitdefender vous informera immédiatement du résultat de l'opération.Si une erreur s'est produite, utilisez le message d'erreur pour essayer de régler le problème. Cliquez sur **OK** pour fermer la fenêtre.

Note
Il peut être pratique d'enregistrer tous les coffres-forts au même emplacement. De cette façon, vous les retrouverez plus vite.

Ouvrir des coffres-forts

Pour accéder aux fichiers contenus dans un coffre et pouvoir travailler avec ces fichiers, il faut d'abord ouvrir le coffre.Quand vous ouvrez le coffre, un disque virtuel s'affiche dans le Poste de travail.Le disque se voit attribuer la lettre correspondant au coffre.

Pour ouvrir un coffre-fort, suivez ces étapes :

1. Localisez sur votre ordinateur le fichier `.bvd` correspondant au coffre-fort que vous voulez ouvrir.
2. Faites un clic droit sur le fichier, allez sur **Coffre-fort Bitdefender** et sélectionnez **Ouvrir**.Des méthodes plus rapides sont possibles : double-cliquez sur le fichier, ou faites un clic droit dessus et sélectionnez **Ouvrir**.Une nouvelle fenêtre s'affiche.
3. Choisissez une lettre de lecteur à partir du menu.
4. Entrez le mot de passe du coffre-fort dans le champ **Mot de Passe**.
5. Cliquez sur **Ouvrir**.

Bitdefender vous informera immédiatement du résultat de l'opération.Si une erreur s'est produite, utilisez le message d'erreur pour essayer de régler le problème. Cliquez sur **OK** pour fermer la fenêtre.

Ajout de fichiers aux coffres-forts

Avant de pouvoir ajouter des fichiers ou des dossiers à un coffre-fort, vous devez ouvrir le coffre-fort. Lorsqu'un coffre-fort est ouvert, vous pouvez facilement y stocker des fichiers ou des dossiers en utilisant le menu contextuel. Faites un clic droit sur le fichier ou le dossier que vous voulez copier dans un coffre-fort, allez sur **Coffre-Fort Bitdefender** et cliquez sur **Ajouter au coffre-fort**.

- Si un seul coffre-fort est ouvert, le fichier ou le dossier est copié directement dans ce coffre-fort.
- Si plusieurs coffres-forts sont ouverts, on vous demandera de choisir le coffre-fort où copier l'élément. Sélectionnez dans le menu la lettre de lecteur correspondant au coffre-fort souhaité et cliquez sur **OK** pour copier l'élément.

Vous pouvez également utiliser le disque virtuel correspondant au coffre-fort.Suivez ces étapes :

1. Ouvrez le Poste de travail : dans le menu Démarrer de Windows, cliquez sur **Ordinateur** (sous Windows Vista et 7) ou sur **Poste de travail** (sous Windows XP).
2. Entrez le disque virtuel correspondant au coffre-fort.Recherchez la lettre de lecteur que vous avez attribuée au coffre-fort lorsque vous l'avez ouvert.
3. Copiez-collez ou glissez-déposez des fichiers et des dossiers directement dans ce disque virtuel.

Verrouiller des coffres-forts

Quand vous avez fini de travailler avec les fichiers d'un coffre-fort, vous devez le verrouiller pour protéger vos données.En verrouillant le coffre-fort, le disque virtuel correspondant disparaît de Poste de travail. L'accès aux données stockées dans le coffre-fort est donc complètement bloqué.

Pour verrouiller un coffre-fort, suivez ces étapes :

1. Ouvrez le Poste de travail : dans le menu Démarrer de Windows, cliquez sur **Ordinateur** (sous Windows Vista et 7) ou sur **Poste de travail** (sous Windows XP).
2. Identifiez le disque virtuel correspondant au coffre-fort que vous voulez fermer. Recherchez la lettre de lecteur que vous avez attribuée au coffre-fort lorsque vous l'avez ouvert.
3. Faites un clic droit sur le disque virtuel correspondant, allez sur **Coffre-fort Bitdefender** et cliquez sur **Verrouiller**.

Vous pouvez également faire un clic droit sur le fichier .bvd représentant le coffre-fort, aller dans **Coffre-Fort Bitdefender** et cliquer sur **Verrouiller**.

Bitdefender vous informera immédiatement du résultat de l'opération.Si une erreur s'est produite, utilisez le message d'erreur pour essayer de régler le problème. Cliquez sur **OK** pour fermer la fenêtre.

Supprimer des fichiers des coffres-forts

Pour pouvoir supprimer des fichiers ou des dossiers d'un coffre-fort, le coffre-fort doit être ouvert.Pour supprimer des fichiers ou des dossiers d'un coffre-fort, procédez comme suit :

1. Ouvrez le Poste de travail : dans le menu Démarrer de Windows, cliquez sur **Ordinateur** (sous Windows Vista et 7) ou sur **Poste de travail** (sous Windows XP).
2. Entrez le disque virtuel correspondant au coffre-fort.Recherchez la lettre de lecteur que vous avez attribuée au coffre-fort lorsque vous l'avez ouvert.
3. Supprimez des fichiers ou des dossiers comme vous le faites habituellement avec Windows (par exemple, faites un clic droit sur un fichier que vous souhaitez supprimer et sélectionnez **Supprimer**).

Changer le mot de passe du coffre-fort

Le mot de passe protège le contenu d'un coffre-fort contre les accès non autorisés. Seuls les utilisateurs connaissant le mot de passe peuvent ouvrir le coffre-fort et accéder aux documents et aux données qu'il contient.

Le coffre-fort doit être verrouillé pour que vous puissiez modifier son mot de passe. Pour modifier le mot de passe d'un coffre-fort, suivez ces étapes :

1. Localisez sur votre ordinateur le fichier .bvd correspondant au coffre-fort.
2. Faites un clic droit sur le fichier, allez sur **Coffre-fort Bitdefender** et sélectionnez **Modifier le mot de passe du coffre-fort**.Une nouvelle fenêtre s'affiche.
3. Entrez le mot de passe actuel du coffre-fort dans le champ **Ancien mot de Passe**.
4. Tapez le nouveau mot de passe souhaité pour le coffre-fort dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**.

   Note

   Le mot de passe doit comporter au moins 8 caractères.Pour avoir un mot de passe sécurisé, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

5. Cliquez sur **OK** pour changer le mot de passe.

Bitdefender vous informera immédiatement du résultat de l'opération.Si une erreur s'est produite, utilisez le message d'erreur pour essayer de régler le problème. Cliquez sur **OK** pour fermer la fenêtre.

7.5. Supprimer définitivement des fichiers

Lorsque vous supprimez un fichier, vous ne pouvez plus y accéder par le chemin habituel. Toutefois, ce fichier continue d'être stocké sur le disque dur jusqu'à ce qu'il soit remplacé lors de la copie de nouveaux fichiers.

Le Destructeur de Fichiers Bitdefender vous aidera à supprimer définitivement des données en les supprimant physiquement de votre disque dur.

Vous pouvez détruire rapidement des fichiers ou dossiers de votre ordinateur à l'aide du menu contextuel de Windows, en procédant comme suit :

1. Faites un clic droit sur le fichier ou le dossier que vous souhaitez supprimer définitivement et sélectionnez **Destructeur de Fichiers**.
2. Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour lancer l'assistant du Destructeur de Fichiers.
3. Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.
4. Les résultats sont affichés.Cliquez sur **Fermer** pour quitter l'assistant.

Vous pouvez également détruire des fichiers à partir de l'interface de Bitdefender.

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Confidentialité**.
3. Cliquez sur **Crypter** et sélectionnez **Destructeur de Fichiers** dans le menu déroulant.
4. Suivez l'assistant du Destructeur de Fichiers :
   a. **Sélectionnez un fichier/dossier**

      Ajoutez les fichiers ou les dossiers que vous souhaitez supprimer définitivement.

   b. **Destruction de Fichiers**

      Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.

   c. **Résultats**

      Les résultats sont affichés.Cliquez sur **Fermer** pour quitter l'assistant.

8. Contrôle Parental

Le module de contrôle parental de Bitdefender vous permet de contrôler l'accès à Internet et à des applications spécifiques pour chaque utilisateur disposant d'un compte utilisateur sur le système.

Vous pouvez configurer le contrôle parental pour bloquer :

- aux pages Web indésirables.
- l'accès à Internet, pour des périodes bien définies (l'heure des devoirs, par exemple).
- les pages Internet, les e-mails et les messages instantanées comportant des mots clés spécifiques.
- les applications comme des jeux, des chats, des programmes de partage de fichiers et autres.
- les messages instantanées envoyés par des contacts de messagerie instantanée autres que ceux autorisés.

Important

Seuls les utilisateurs ayant des droits d'administrateur sur le système peuvent avoir accès et configurer le contrôle parental.Pour vous assurer que vous serez la seule personne à pouvoir modifier les paramètres du contrôle parental pour tous les utilisateurs, protégez ces paramètres avec un mot de passe.

Une fois le contrôle parental configuré, il est facile pour vous de connaître les activités de vos enfants sur l'ordinateur.

Même lorsque vous n'êtes pas chez vous, vous pouvez surveiller les activités de vos enfants et modifier les paramètres du Contrôle Parental à l'aide du Contrôle Parental à Distance.

8.1. Configuration du Contrôle Parental

Avant de configurer le Contrôle Parental, créez un compte utilisateur Windows pour chaque enfant. Cela vous permettra de connaître exactement les activités de chacun d'entre eux sur l'ordinateur. Nous vous recommandons de créer des comptes utilisateur limités (standard) afin qu'ils ne puissent pas modifier les paramètres du Contrôle Parental. Pour plus d'informations, reportez-vous à « *Comment créer des comptes utilisateurs Windows ?* » (p. 37).

Si vos enfants peuvent accéder à un compte administrateur sur leur ordinateur, vous devez configurer un mot de passe pour protéger les paramètres du Contrôle Parental. Pour plus d'informations, reportez-vous à « *Paramètres Bitdefender de la protection par mot de passe* » (p. 18).

Pour configurer le contrôle parental :

1. Assurez-vous d'être connecté à l'ordinateur en utilisant un compte administrateur.Seuls les utilisateurs ayant des droits d'administrateur sur le système peuvent avoir accès et configurer le contrôle parental.
2. Ouvrez la fenêtre de Bitdefender.
3. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
4. Cliquez sur **Contrôle Parental** dans le menu de gauche puis sur l'onglet **Comptes**.Vous pouvez vérifier et configurer ici les paramètres du Contrôle Parental de chaque compte utilisateur Windows. Si le Contrôle Parental est activé, vous pouvez voir la catégorie d'âge sélectionnée et l'état des contrôles parentaux (qui seront décrits ci-après).

Pour configurer le contrôle parental pour un compte utilisateur spécifique :

1. Utilisez le bouton pour activer le Contrôle Parental sur ce compte utilisateur.
2. Définissez l'âge de votre enfant en sélectionnant l'une des cases correspondant à l'option **Age**.Si vous précisez l'âge de l'enfant, des paramètres considérés comme étant adaptés à cet âge seront automatiquement chargés, basés sur les normes de développement de l'enfant.
3. Si vous souhaitez configurer tous les paramètres du Contrôle Parental en détail, cliquez sur **Configuration**.Cliquez sur un onglet pour configurer la fonction de contrôle parental correspondante :

   - **Web** - permet de filtrer la navigation sur Internet et de mettre en place des restrictions horaires pour l'accès à Internet à l'aide de Contrôle Web.
   - **Applications** - permet de configurer le Contrôle des Applications pour bloquer ou limiter l'accès à certaines applications.
   - **Mots-clés** - pour filtrer l'accès à Internet, aux e-mails et à la messagerie instantanée en fonction de mots-clés à l'aide de Contrôle par mots-clés.
   - **Messagerie Instantanée** - permet de configurer le Contrôle de Messagerie Instantanée pour autoriser ou bloquer les conversations avec certains contacts de messagerie instantanée sur Yahoo! Messenger et Windows Live (MSN) Messenger.
   - **Catégories** - pour bloquer certaines catégories de contenu web à l'aide du Filtrage par catégories.

   Pour fermer la fenêtre des paramètres du Contrôle parental, cliquez sur le bouton X dans le coin supérieur droit. Les paramètres que vous avez configurés sont enregistrés automatiquement.

Pour configurer les options de surveillance des activités et du Contrôle Parental à Distance, allez dans l'onglet **Configuration**.Configurez les options de surveillance selon vos besoins :

Envoyer les rapports d'activité par e-mail
Une notification par e-mail est envoyée à chaque fois que le Contrôle Parental bloque une activité.Vous devez configurer les paramètres de notification.

Enregistrer un rapport de trafic Internet
Enregistre les sites Internet consultés par les utilisateurs pour lesquels le Contrôle Parental est activé.

Pour plus d'informations, reportez-vous à « *Surveiller les activités des enfants* » (p. 105).

Si vous souhaitez surveiller et limiter à distance les activités de vos enfants sur l'ordinateur et sur Internet, activez le Contrôle Parental à Distance à l'aide du bouton. Pour plus d'informations, reportez-vous à « *Contrôle Parental à Distance* » (p. 107).

8.1.1. Contrôle Web

Le Contrôle Web vous aide à bloquer les sites web au contenu inapproprié et à mettre en place des restrictions horaires pour l'accès à Internet.

Pour configurer le Contrôle Web pour un compte utilisateur spécifique :

1. Accédez à la fenêtre des paramètres de contrôle parental Bitdefender pour ce compte utilisateur.
2. Cliquez sur l'onglet **Web**.
3. Utilisez le bouton pour activer le Contrôle Web.
4. Vous pouvez, si vous le souhaitez, créer vos propres règles pour autoriser ou bloquer l'accès à des sites Web spécifiques.Si le contrôle parental bloque automatiquement l'accès à un site Web, vous pouvez créer une règle pour autoriser explicitement l'accès à ce site Web.
5. Vous pouvez définir des limites pour contrôler le temps que vos enfants passent sur Internet.Pour plus d'informations, reportez-vous à « Limiter l'accès à Internet en fonction de l'heure » (p. 100).

Création de règles de Contrôle Web

Pour autoriser ou bloquer l'accès à un site Web, suivez ces étapes :

1. Cliquez sur **Autoriser site** ou sur **Bloquer site**.
2. Saisissez l'adresse du site Internet dans le champ **Site Web**.
3. Sélectionnez l'action souhaitée pour cette règle - **Autoriser** ou **Bloquer**.
4. Cliquez sur **Terminer** pour ajouter la règle.

Gestion des règles de Contrôle Web

Les règles de Contrôle de Sites Web qui ont été configurées apparaissent dans le tableau situé en bas de la fenêtre. Pour chaque règle de Contrôle Web figurent l'adresse du site Web et son état actuel.

Pour supprimer une règle, sélectionnez-la, puis cliquez sur **Supprimer**.

Pour modifier une règle, double-cliquez dessus (ou sélectionnez-la et cliquez sur **Modifier**).Apportez les modifications nécessaires dans la fenêtre de configuration.

Limiter l'accès à Internet en fonction de l'heure

La section Planifier l'Accès à Internet vous permet de limiter le temps que votre enfant passe sur Internet.

Pour bloquer tout accès à Internet, sélectionnez **Bloquer l'Accès à Internet**.

Pour limiter l'accès à Internet à certaines heures de la journée :

1. Sélectionnez **Limiter l'accès à Internet**.
2. Cliquez sur **Modifier la planification**.
3. Sélectionnez dans la grille les intervalles de temps pendant lesquels l'accès à Internet est bloqué.Vous pouvez cliquer sur des cellules individuelles pour choisir des heures ou cliquer et faire glisser la souris sur plusieurs cellules pour bloquer de plus longues périodes.Pour démarrer une nouvelle sélection, cliquez sur **Tout Bloquer** ou **Tout Autoriser**.
4. Cliquez sur **Enregistrer**.

Note

Bitdefender effectuera des mises à jour toutes les heures même si l'accès à Internet est bloqué.

8.1.2. Contrôle des Applications

Le **Contrôle des Programmes** vous aide à bloquer des applications. Jeux, logiciel de messagerie, ou tout autre catégorie de logiciels et malware peuvent être bloqués de cette façon. Les applications bloquées de cette manière sont également protégées contre les modifications et ne peuvent pas être copiées ou déplacées.Vous pouvez bloquer les applications de façon permanente ou juste à certaines plages horaires, comme celles pendant lesquelles vos enfants doivent faire leurs devoirs.

Pour configurer le contrôle des applications pour un compte utilisateur spécifique :

1. Accédez à la fenêtre des paramètres de contrôle parental Bitdefender pour ce compte utilisateur.
2. Cliquez sur l'onglet **Applications**.

3. Utilisez le bouton pour activer le contrôle des applications.
4. Créez des règles pour les applications auxquelles vous souhaitez bloquer ou limiter l'accès.

Création de Règles du Contrôle des Applications

Pour bloquer ou limiter l'accès à une application, suivez ces étapes :

1. Cliquez sur **Bloquer** ou **Limiter**.
2. Cliquez sur **Parcourir** pour localiser l'application pour laquelle vous voulez bloquer/limiter l'accès.Les applications installées se trouvent généralement dans le dossier `C:\Program Files`.
3. Sélectionnez l'action pour la règle :
   - **Bloquer en permanence** pour bloquer complètement l'accès à l'application.
   - **Bloquer en fonction de ce tableau** pour limiter l'accès à certaines plages horaires.

   Si vous choisissez de limiter l'accès à l'application et non de la bloquer complètement, vous devez également sélectionner dans la grille les jours et les heures pendant lesquels l'accès est bloqué.Vous pouvez cliquer sur des cellules individuelles pour choisir des heures ou cliquer et faire glisser la souris sur plusieurs cellules pour bloquer de plus longues périodes.Pour démarrer une nouvelle sélection, cliquez sur **Tout Bloquer** ou **Tout Autoriser**.
4. Cliquez sur **Enregistrer** pour ajouter la règle.

Gestions des Règles du Contrôle des Applications

Les règles du Contrôle des Applications qui ont été configurées sont listées dans le tableau situé en bas de la fenêtre. Pour chaque règle du Contrôle des Applications figurent le nom de l'application, son chemin et son état actuel.

Pour supprimer une règle, sélectionnez-la, puis cliquez sur **Supprimer**.

Pour modifier une règle, double-cliquez dessus (ou sélectionnez-la et cliquez sur **Modifier**).Apportez les modifications nécessaires dans la fenêtre de configuration.

8.1.3. Contrôle par mots-clés

Le Contrôle par mots-clés vous aide à bloquer l'accès aux e-mails, pages Internet et messages instantanés contenant des mots spécifiques.L'utilisation du Contrôle par mots-clés permet d'empêcher que vos enfants voient des mots ou des phrases inappropriés lorsqu'ils sont sur Internet.En outre, vous pouvez faire en sorte qu'aucune information personnelle (adresse de domicile ou téléphone par exemple) ne soit fournie aux personnes rencontrées sur Internet.

Note
Le Contrôle par mots-clés des messages instantanés est uniquement disponible avec Yahoo Messenger et Windows Live (MSN) Messenger.

Pour configurer le Contrôle par Mots-clés pour un compte utilisateur spécifique :

1. Accédez à la fenêtre des paramètres de contrôle parental Bitdefender pour ce compte utilisateur.
2. Cliquez sur l'onglet **Mots-clés**.
3. Utilisez le bouton pour activer le Contrôle par Mots-clés.
4. Créez des règles de vérification des mots-clés de manière à éviter la diffusion de mots impropres ou l'envoi d'informations importantes.

Création de Règles de Contrôle par Mots-clés

Pour bloquer un mot ou une expression, suivez ces étapes :

1. Cliquez sur **Bloquer le mot-clé**.
2. Paramétrer les mots-clés.
   - **Mots-clés** - entrez dans ce champ le nom de la règle.
   - **Mot-clé** - entrez dans le champ le mot ou la phrase que vous souhaitez bloquer.Si vous souhaitez que seuls les mots entiers soient détectés sélectionnez la case **Uniquement les mots entiers**.
3. Sélectionnez le Type de filtrage.
   - **Bloquer l'affichage** - sélectionnez cette option pour les règles créées dans le but d'empêcher l'affichage de mots inappropriés.
   - **Bloquer l'envoi** - sélectionnez cette option pour les règles créées dans le but d'éviter l'envoi d'informations importantes.
4. Sélectionnez le type de trafic que Bitdefender doit analyser pour le mot spécifié.

Option	Description
Web	Les pages Web qui contiennent le mot clé sont bloquées
E-mail	Les emails qui contiennent le mot clé sont bloqués.
Messagerie instantanée	Les messages instantanés contenant le mot clé sont bloqués.

5. Cliquez sur **Terminer** pour ajouter la règle.

Désormais, toute tentative d'envoi des données spécifiées (via e-mail, messagerie instantanée ou sur une page web) échouera. Un message d'alerte s'affichera indiquant que Bitdefender a empêché l'envoi de contenu lié à l'identité.

Gestion des Règles de Contrôle par Mots-clés

Les règles de contrôle des mots clés qui ont été configurées sont listées dans le tableau. Des informations détaillées sont fournies pour chacune des règles.

Pour supprimer une règle, sélectionnez-la, puis cliquez sur **Supprimer**.

Pour modifier une règle, double-cliquez dessus (ou sélectionnez-la et cliquez sur **Modifier**).Apportez les modifications nécessaires dans la fenêtre de configuration.

8.1.4. Contrôle de messagerie instantanée

Le contrôle des Messageries Instantanées vous permet de définir avec quels contacts vos enfants sont autorisés à chatter.

Note
Le contrôle de la messagerie instantanée est uniquement disponible pour Yahoo Messenger et Windows Live (MSN) Messenger.

Pour configurer le contrôle de messagerie instantanée pour un compte utilisateur spécifique :

1. Accédez à la fenêtre des paramètres de contrôle parental Bitdefender pour ce compte utilisateur.
2. Cliquez sur l'onglet **Messagerie Instantanée**.
3. Utilisez le bouton pour activer le contrôle de messagerie instantanée.
4. Sélectionnez la méthode de filtrage préférée et, en fonction de votre choix, créez des règles adaptées.
   - **Autoriser l'utilisation de la messagerie instantanée avec tous les contacts, sauf ceux de la liste**

     Dans ce cas, vous devez préciser les contacts de messagerie instantanée à bloquer (les personnes à qui vos enfants ne doivent pas parler).
   - **Bloquer la messagerie instantanée avec tous les contacts sauf ceux de la liste**

     Dans ce cas, vous devez spécifier les contacts de messagerie instantanée avec lesquels votre enfant est expressément autorisé à chatter.Vous pouvez, par exemple, autoriser la messagerie instantanée avec des membres de la famille, des copains d'école et des voisins.

     Cette deuxième option est recommandée si votre enfant a moins de 14 ans.

Créer des règles de contrôle des messageries instantanées

Pour autoriser ou bloquer les conversations instantanées avec un contact, suivez ces étapes :

1. Cliquez sur **Bloquer contact** ou **Autoriser contact**.
2. Tapez l'adresse e-mail ou le nom d'utilisateur du contact de Messagerie Instantanée dans le champ **E-mail ou Identifiant**.
3. Choisir la messagerie Instantanée correspondant au contact.
4. Sélectionnez l'action souhaitée pour cette règle - **Autoriser** ou **Bloquer**.
5. Cliquez sur **Terminer** pour ajouter la règle.

Gérer les règles de contrôle des messageries instantanées

Les règles de contrôle de messagerie instantanée qui ont été configurées figurent dans le tableau, situé dans la partie inférieure de la fenêtre.

Pour supprimer une règle, sélectionnez-la, puis cliquez sur **Supprimer**.

Pour modifier une règle, double-cliquez dessus (ou sélectionnez-la et cliquez sur **Modifier**).Apportez les modifications nécessaires dans la fenêtre de configuration.

8.1.5. Filtrage par catégories

Le Filtrage par catégories filtre l'accès aux sites web de façon dynamique en fonction de leur contenu. Lorsque vous activez le Contrôle Parental et indiquez l'âge de votre enfant, le Filtrage par catégories est automatiquement configuré pour bloquer les catégories de sites web considérées comme inappropriées pour l'âge de votre enfant.Cette configuration convient à la plupart des cas.

Si vous souhaitez un plus grand contrôle du contenu web auquel votre enfant est exposé, vous pouvez choisir les catégories de sites web spécifiques à bloquer par le Filtrage par catégories.

Pour vérifier et configurer en détail les paramètres du Filtrage par catégories pour un compte utilisateur donné, procédez comme suit :

1. Accédez à la fenêtre des paramètres de contrôle parental Bitdefender pour ce compte utilisateur.
2. Cliquez sur l'onglet **Catégories**.
3. Le Contrôle par catégories est activé par défaut. Bien que ce ne soit pas recommandé, vous pouvez choisir de désactiver le Contrôle par Catégories et configurer une liste de sites web à bloquer à l'aide du Contrôle Web.
4. Vous pouvez vérifier les catégories Web bloquées/restreintes automatiquement pour les âges sélectionnés. Par exemple, si l'état de la catégorie Moteurs de recherche est **Bloqué**, votre enfant ne sera autorisé à utiliser aucun moteur de recherche. Si vous n'êtes pas satisfait des paramètres par défaut, vous pouvez les configurer selon vos besoins.

   Pour modifier l'action configurée pour une certaine catégorie de contenu web, cliquez sur l'état actuel et sélectionnez l'action souhaitée dans le menu.

8.2. Surveiller les activités des enfants

Bitdefender vous aide à surveiller ce que vos enfants font sur l'ordinateur même lorsque vous êtes absent(e).

Par défaut, lorsque le Contrôle Parental est activé, les activités de vos enfants sont enregistrées. De cette façon, vous pouvez toujours savoir exactement quels sites web ils ont consultés, quelles applications ils ont utilisées, quelles activités ont été bloquées par le Contrôle Parental etc.

Vous pouvez aussi configurer Bitdefender pour envoyer des notifications par email quand le contrôle parental bloque une activité.

8.2.1. Vérifier les journaux du Contrôle Parental

Pour vérifier les activités récentes de vos enfants sur l'ordinateur, accédez aux journaux du Contrôle Parental. Suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Événements** de la barre d'outils supérieure.
3. Cliquez sur **Contrôle Parental** dans le menu de gauche.

Note

Si vous ne partagez pas l'ordinateur avec vos enfants, vous pouvez configurer le réseau domestique de Bitdefender afin que vous puissiez accéder au journal du contrôle parental à distance (à partir de votre ordinateur).Pour plus d'informations, reportez-vous à « *Mappage réseau* » (p. 129).

Les journaux de contrôle parental fournissent des informations détaillées sur l'ordinateur et les activités de vos enfants sur Internet.Les informations sont organisées sous plusieurs onglets :

Événements

Vous aide à découvrir des informations détaillées sur l'activité du Contrôle Parental (par exemple, quand le Contrôle Parental a été activé/désactivé, quels événements ont été bloqués).

Cliquez sur un événement pour obtenir des informations à son sujet.

Utilisation des Applications

Vous aide à connaître les applications que vos enfants ont utilisées récemment.

Vous pouvez filtrer des informations par utilisateur et période. Cliquez sur un événement pour obtenir des informations à son sujet.

Journal Internet

Vous aide à connaître les sites web que vos enfants ont consultés récemment.

Vous pouvez filtrer des informations par utilisateur et période. Cliquez sur un événement pour obtenir des informations à son sujet.

8.2.2. Configurer les notifications par e-mail

Pour recevoir des notifications par e-mail lorsque le Contrôle Parental bloque une activité :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Contrôle Parental** dans le menu de gauche puis sur l'onglet **Configuration**.
4. Activez l'option **Envoyer les rapports d'activité par e-mail** à l'aide du bouton correspondant.
5. On vous demandera de configurer les paramètres de votre compte e-mail. Cliquez sur **Oui** pour ouvrir la fenêtre de configuration.

   Note
   Vous pouvez ouvrir la fenêtre de configuration plus tard en cliquant sur **Paramètres des Notifications**.

6. Saisissez l'adresse e-mail pour recevoir les notifications par e-mail.
7. Configurez les paramètres d'e-mail du serveur utilisé pour envoyer les notifications par e-mail.Trois options permettent de configurer les paramètres de messagerie :

   Utiliser les paramètres de ce client de messagerie
   Cette option est sélectionnée par défaut lorsque Bitdefender parvient à importer les paramètres de serveur de messagerie depuis votre client de messagerie.

   Effectuez la sélection à partir de l'un des serveurs connus
   Sélectionnez cette option si vous avez un compte de messagerie avec l'un des services de webmail de la liste.

   Je veux configurer les paramètres du serveur moi-même
   Si vous connaissez les paramètres du serveur de messagerie, sélectionnez cette option et configurez les paramètres comme suit :

   - **Serveur Sortant (SMTP)** - adresse du serveur de courrier électronique utilisé pour envoyer des e-mails.
   - Si le serveur utilise un port autre que celui par défaut -port 25-, entrez le numéro du port dans le champ correspondant.

- Si le serveur requiert une authentification, cochez la case **Mon serveur SMTP requiert une authentification** et tapez vos nom d'utilisateur et mot de passe dans les champs correspondants.
- Si le serveur requiert une connexion sécurisée SSL, cochez la case **Utiliser SSL**.

8. Cliquez sur **Tester** pour valider la configuration. Si des problèmes sont détectés pendant la validation, vous serez informé(e) que vous devez les corriger.
9. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

8.3. Contrôle Parental à Distance

Le contrôle parental à distance vous permet de surveiller les activités de vos enfants et de modifier les paramètres de contrôle parental, même si vous n'êtes pas chez vous.Il vous suffit d'un ordinateur avec accès Internet et d'un navigateur web.

Le contrôle parental à distance propose une manière discrète de surveiller ce que vos enfants font en ligne, sans trop s'immiscer.

8.3.1. Pré-requis à l'utilisation du Contrôle Parental à Distance

Afin d'utiliser le Contrôle Parental à Distance, les pré-requis suivants doivent être remplis :

1. Installez Bitdefender Internet Security 2012 ou Bitdefender Total Security 2012 sur l'ordinateur de vos enfants.
2. Veillez à terminer l'enregistrement du produit en associant votre produit à un compte MyBitdefender. Pour plus d'informations, reportez-vous à « *Enregistrement du Produit* » (p. 8).
3. Activer le Contrôle Parental à Distance.
4. L'ordinateur depuis lequel vous souhaitez accéder au contrôle parental à distance doit être connecté à Internet.

8.3.2. Activation du Contrôle Parental à Distance

Pour activer le contrôle parental à distance :

1. Connectez-vous à l'ordinateur sur lequel Bitdefender est installé à l'aide d'un compte administrateur.Vous pouvez utiliser le même compte que celui utilisé pour installer le programme.
2. Ouvrez la fenêtre de Bitdefender.
3. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
4. Cliquez sur **Contrôle Parental** dans le menu de gauche puis sur l'onglet **Configuration**.

5. Activez le Contrôle Parental à Distance à l'aide du bouton correspondant. Le Contrôle Parental à Distance sera activé pour tous les comptes utilisateur du système.

8.3.3. Accès au Contrôle Parental à Distance

Vous pouvez accéder au Contrôle Parental à Distance en vous connectant à MyBitdefender.

1. Sur un ordinateur connecté à Internet, ouvrez le navigateur Web et allez sur :

   https://myaccount.bitdefender.com/fr/MyAccount/login/

2. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
3. Dans le panneau Services, cliquez sur **Assistance pour les parents** pour accéder au tableau de bord du Contrôle Parental à Distance.
4. Vous pouvez voir tous vos ordinateurs sur lesquels le Contrôle Parental à Distance est activé et leurs comptes utilisateurs respectifs. Trois boutons sont disponibles pour chaque compte utilisateur :

   - **Alertes** - permet de vérifier les activités ayant été bloquées sur le compte utilisateur concerné depuis votre dernière connexion.
   - **Activités** - permet de vérifier les activités récentes de vos enfants.
   - **Configuration** - permet de modifier la configuration du Contrôle Parental pour le compte utilisateur concerné.

   Cliquer sur l'un de ces boutons ouvrira la page du Contrôle Parental à Distance de ce compte utilisateur.

8.3.4. Surveiller les activités des enfants à distance

Avant de pouvoir surveiller à distance les activités de vos enfants sur l'ordinateur et sur Internet, vous devez activer le Contrôle Parental à Distance sur leur ordinateur. Pour plus d'informations, reportez-vous à « *Activation du Contrôle Parental à Distance* » (p. 107).

Pour surveiller à distance les activités de vos enfants sur leur ordinateur :

1. Sur un ordinateur connecté à Internet, ouvrez le navigateur Web et allez sur :

   https://myaccount.bitdefender.com/fr/MyAccount/login/

2. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
3. Dans le panneau Services, cliquez sur **Assistance pour les parents** pour accéder au tableau de bord du Contrôle Parental à Distance.
4. Localisez le compte utilisateur de votre enfant et cliquez sur l'un de ces boutons :

- **Alertes** - permet de vérifier les activités ayant été bloquées sur le compte utilisateur concerné depuis votre dernière connexion.
- **Activités** - permet de vérifier les activités récentes de vos enfants.

Dans la page des alertes, vous pouvez connaître les sites Web, applications ou contacts de messagerie instantanée qui ont été bloqués depuis votre dernière connexion.Pour supprimer une restriction, cliquez sur le bouton **Autoriser** correspondant.

Sur la page Activités, vous trouverez des informations utiles sur les activités récentes de vos enfants :

- qui sont les sites Web les plus consultés et les sites Web les plus bloqués.
- qui sont les applications les plus utilisées et les plus bloquées.
- qui sont les contacts de messagerie instantanée les plus contactés et les plus bloqués.

Vous pouvez bloquer directement un site Web, une application ou un contact de messagerie instantanée en cliquant sur le bouton **Bloquer** correspondant.

Pour filtrer les enregistrements affichés, cliquez sur le menu **Afficher** et sélectionnez l'option souhaitée.

8.3.5. Modifier les paramètres du Contrôle Parental à distance

Avant de pouvoir modifier à distance les paramètres de contrôle parental configurés pour vos enfants, vous devez activer le contrôle parental à distance sur leurs ordinateurs.Pour plus d'informations, reportez-vous à « *Activation du Contrôle Parental à Distance* » (p. 107).

Pour modifier les paramètres du Contrôle Parental à distance :

1. Sur un ordinateur connecté à Internet, ouvrez le navigateur Web et allez sur :

   https://myaccount.bitdefender.com/fr/MyAccount/login/

2. Connectez-vous à votre compte Bitdefender à l'aide de votre nom d'utilisateur et de votre mot de passe.
3. Dans le panneau Services, cliquez sur **Assistance pour les parents** pour accéder au tableau de bord du Contrôle Parental à Distance. Vous pouvez voir tous les comptes utilisateur pour lesquels le Contrôle Parental est activé.
4. Localisez le compte utilisateur de votre enfant et cliquez sur l'un de ces boutons :
   - **Alertes** - permet de vérifier la liste des activités bloquées récemment et de supprimer des restrictions.
   - **Activités** - permet de vérifier les activités récentes de vos enfants et de bloquer les activités non souhaitées.

- **Configuration** - permet de modifier la configuration du Contrôle Parental pour le compte utilisateur concerné.

5. Appliquez et supprimez des restrictions en fonction de vos besoins.

Limiter l'accès à Internet en fonction de l'heure

Vous pouvez spécifier quand votre enfant est autorisé à accéder à Internet à l'aide des options de **Planification de l'accès à Internet** de la page **Configuration**.

Pour limiter l'accès à Internet à certaines heures de la journée :

1. Sélectionnez dans la grille les intervalles de temps pendant lesquels l'accès à Internet est bloqué.Pour démarrer une nouvelle sélection, cliquez sur **Tout Bloquer** ou **Tout Autoriser**.
2. Cliquez sur **Enregistrer**.

Pour bloquer complètement l'accès à Internet, cliquez sur le lien **Tout Bloquer** sous la grille horaire puis sur le lien **Enregistrer**.

Les modifications seront configurées et appliquées sur l'ordinateur de vos enfants après la prochaine synchronisation avec le site Web de contrôle parental à distance (dans un intervalle de 10 minutes).

Bloquer des sites web

Pour bloquer un site web :

1. Allez à la page **Configuration**.
2. Indiquez le site web dans le champ correspondant.
3. Cliquez sur **Envoyer**.Le site web sera ajouté à la liste des actions en attente. Si vous changez d'avis, cliquez sur le bouton **Annuler l'Action** correspondant.

Note

Vous pouvez également aller sur la page **Activités**, vérifier la liste des sites web consultés et cliquer sur le bouton correspondant **Bloquer** quand vous souhaitez bloquer un site web.

La règle sera configurée et appliquée sur l'ordinateur de vos enfants après la prochaine synchronisation avec le site Web de contrôle parental à distance (dans un intervalle de 10 minutes).

Bloquer des contacts de messagerie instantanée

Pour bloquer les messages instantanés avec un certain contact :

1. Allez à la page **Configuration**.
2. Saisissez le contact de messagerie instantanée dans le champ correspondant.

3. Cliquez sur **Bloquer**.Le contact de messagerie instantanée sera ajouté à la liste des actions en attente. Si vous changez d'avis, cliquez sur le bouton **Annuler l'Action** correspondant.

Note

Vous pouvez également aller sur la page **Activités**, consulter la liste des contacts de messagerie instantanée avec lesquels votre enfant a discuté et cliquer sur le bouton **Bloquer** correspondant lorsque vous trouvez un contact indésirable.

La règle sera configurée et appliquée sur l'ordinateur de vos enfants après la prochaine synchronisation avec le site Web de contrôle parental à distance (dans un intervalle de 10 minutes).

Bloquer des applications

Pour bloquer une application :

1. Allez à la page **Activités**.
2. Consultez la liste des applications utilisées et cliquez sur le bouton **Bloquer** correspondant lorsque vous repérez une applications indésirable.

La règle sera configurée et appliquée sur l'ordinateur de vos enfants après la prochaine synchronisation avec le site Web de contrôle parental à distance (dans un intervalle de 10 minutes).

Débloquer des sites web, des applications ou des contacts de messagerie instantanée

La page Alertes affiche les sites web, les applications et les contacts de messagerie instantanée ayant été bloqués par le Contrôle Parental. Pour supprimer une restriction, cliquez sur le bouton **Autoriser** correspondant. La restriction sera retirée de l'ordinateur de votre enfant après la prochaine synchronisation avec le site Web du Contrôle Parental à Distance (dans un intervalle de 10 minutes).

9. Pare-feu

Le pare-feu protège votre ordinateur contre les tentatives de connexions entrantes et sortantes non autorisées.Cela ressemble beaucoup à un garde à votre porte - il surveille les tentatives de connexion et détermine celles à autoriser et à bloquer.

Note
Un Firewall est essentiel si vous posséder une connexion à large bande comme l'ADSL.

Si votre ordinateur fonctionne sous Windows Vista ou Windows 7, Bitdefender attribue automatiquement un type de réseau à chaque nouvelle connexion réseau qu'il détecte. Sur les ordinateurs fonctionnant sous Windows XP, l'on vous demandera de sélectionner le type de réseau. Pour en savoir plus sur la configuration du pare-feu pour chaque type de réseau et sur comment modifier les paramètres réseau, veuillez vous reporter à « *Configurer les paramètres de connexion réseau* » (p. 113).

Le pare-feu Bitdefender utilise un ensemble de règles pour filtrer des données transmises vers et à partir de votre système. Les règles sont regroupées en 3 catégories :

Règles Générales
: Règles qui déterminent les protocoles sur lesquels la communication est autorisée.

  Un ensemble de règles par défaut fournissant une protection optimale est utilisé. Vous pouvez éditer les règles en autorisant ou refusant des connections sur certains protocoles.

Règles d'Applications
: Règles déterminant comment chaque application peut accéder aux ressources réseau et à Internet.

  Dans des conditions normales, Bitdefender crée automatiquement une règle lorsqu'une application essaie d'accéder à Internet. Vous pouvez également ajouter ou modifier manuellement des règles d'applications.

Règles d'Adaptateurs
: Règles déterminant si votre ordinateur peut communiquer avec d'autres ordinateurs.

  Vous devez créer des règles pour spécifiquement autoriser ou refuser le trafic.

Une protection supplémentaire est fournie par le Système de Détection d'Intrusion (IDS).Le Système de Détection d'Intrusion surveille les activités du réseau et du système à la recherche d'activités malveillantes et de violations de politiques. Peut détecter et bloquer les tentatives de modification de fichiers système critiques, de fichiers Bitdefender ou d'entrées de registre, l'installation de pilotes malveillants et les attaques réalisées par injection de code (injection de DLL).

9.1. Activer ou désactiver la protection pare-feu

Pour activer ou désactiver la protection pare-feu, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Pare-feu**.
3. Cliquez sur le bouton Pare-feu.

Avertissement

La désactivation du pare-feu exposant votre ordinateur à des connexions non autorisées, il devrait s'agir d'une mesure temporaire. Réactivez le pare-feu dès que possible.

9.2. Configurer les paramètres de connexion réseau

Pour afficher et éditer les paramètres de connexion réseau, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Pare-feu**.
3. Cliquez sur **Informations sur le réseau**.

Une nouvelle fenêtre s'affiche.Le graphique au-dessus de la fenêtre affiche des informations en temps réel concernant le trafic entrant et sortant.

Sous le graphique, les informations suivantes s'affichent pour chaque connexion réseau.

- **Type de Réseau** - le type de réseau auquel votre ordinateur est connecté. Bitdefender applique un ensemble de paramètres pare-feu de base en fonction du type de réseau auquel vous êtes connecté.

  Vous pouvez modifier le type de réseau en ouvrant le menu déroulant **Type de Réseau** et en sélectionnant l'un des types de réseau disponibles dans la liste.

Type de Réseau	Description
Confiance	Désactiver le Pare-feu pour l'adaptateur concerné.
Domicile/Bureau	Autoriser tout le trafic entre votre ordinateur et les ordinateurs du réseau local.
Public	Tout le trafic est filtré.
Non fiable	Bloquer complètement le trafic réseau et Internet via l'adaptateur respectif.

- **Mode Furtif** - si vous pouvez être détecté par d'autres ordinateurs.

Pour configurer le Mode Furtif, cliquez sur la flèche dans la colonne **Mode Furtif**, puis sélectionnez l'option de votre choix.

Option Furtif	Description
Activé	Le mode furtif est activé.Votre ordinateur n'est pas visible depuis le réseau local et Internet.
Désactivé	Le mode furtif est désactivé.N'importe qui sur le réseau local ou sur Internet peut détecter votre ordinateur (via la commande ping).
Distant	Votre ordinateur ne peut pas être détecté depuis Internet.Les utilisateurs du réseau local peuvent voir (Via la commande ping) et détecter votre ordinateur .

- **Générique** - si des règles génériques sont appliquées à cette connexion.

  Si l'adresse IP d'un adaptateur réseau est modifiée, Bitdefender modifie le type de réseau en conséquence.Si vous souhaitez conserver le même type, cliquez sur la flèche dans la colonne **Générique**, puis sélectionnez **Oui**.

9.3. Système de détection d'intrusion

Pour configurer le Système de Détection d'Intrusion, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Pare-feu** dans le menu de gauche puis sur l'onglet **Configuration**.
4. Pour activer le Système de Détection d'Intrusion, cliquez sur le bouton correspondant.
5. Déplacez le curseur sur l'échelle pour choisir le degré d'analyse approprié.Reportez-vous à la description à droite de l'échelle pour choisir le niveau le plus adapté à vos besoins de sécurité.

Vous pouvez vérifier les applications détectées par le Système de Détection d'Intrusion dans la fenêtre Événements.

Si vous avez confiance en certaines applications et ne souhaitez pas que le Système de Détection d'Intrusion les analyse, vous pouvez ajouter des règles d'exclusion pour elles. Pour exclure une application de l'analyse, suivez les étapes décrites dans la section « *Gérer des processus exclus* » (p. 64).

Note

Le fonctionnement du Système de Détection d'Intrusion est lié à celui d'Active Virus Control.Les règles d'exclusion de processus s'appliquent aux deux systèmes.

9.4. Configurer les paramètres du trafic

Pour configurer les paramètres du trafic, les étapes sont les suivantes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Pare-feu** dans le menu de gauche puis sur l'onglet **Configuration**.

Les fonctionnalités suivantes peuvent être activées ou désactivées dans la section **Trafic**.

- **Activer le support du partage de Connexion Internet (ICS)** - active le support du partage de connexion Internet (ICS).

  Note

  Cette option active uniquement le support de ce mode de partage qui doit par ailleurs être activé dans votre système d'exploitation.

- **Bloquer les analyses de ports** - détecte et bloque les démarches visant à détecter des ports ouverts sur un ordinateur.

  Les analyses de ports sont fréquemment utilisées par les pirates pour découvrir des ports ouverts sur votre ordinateur.Ils peuvent alors s'introduire dans votre ordinateur, s'ils découvrent un port vulnérable ou moins sécurisé.

- **Journaux plus détaillés** - améliore la précision du journal du pare-feu.

  Bitdefender dispose d'un journal d'événements concernant l'utilisation du module Pare-feu (activer/désactiver le pare-feu, bloquer le trafic, modifier les paramètres) ou des événements générés par les activités détectées par ce module (analyse des ports, bloquer les tentatives de connexion ou le trafic selon les règles).Il est possible d'accéder au journal à partir de la fenêtre **Activité du pare-feu** en cliquant sur **Afficher journal**.L'emplacement du fichier journal est `?\Program Files\Common Files\Bitdefender\Bitdefender Firewall\bdfirewall.txt`.

- **Afficher les notifications Wi-Fi** - si vous êtes connecté(e) à un réseau sans fil, affiche des fenêtres informatives concernant des événements réseau spécifiques (par exemple lorsqu'un nouvel ordinateur rejoint le réseau).

9.5. Règles générales

Quand des données sont transmises sur Internet, certains protocoles sont utilisés.

Les règles générales vous permettent de configurer les protocoles sur lesquels le trafic est autorisé. Pour modifier les règles, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Pare-feu** dans le menu de gauche puis sur l'onglet **Avancé**.
4. Sous Règles pare-feu, cliquez sur **Règles générales**.

Une nouvelle fenêtre s'affiche.Les règles actuelles s'affichent.

Pour éditer une règle, cliquez sur la flèche correspondante dans la colonne **Action** et sélectionnez **Autoriser** ou **Refuser**.

DNS sur UDP / TCP
Autoriser ou refuser DNS sur UDP et TCP.

Par défaut, ce type de connexion est autorisé.

ICMP / ICMPv6 entrants
Autoriser ou refuser les messages ICMP / ICMPv6.

Les messages ICMP sont souvent utilisés par des hackers pour perpétrer des attaques contre les réseaux informatiques. Par défaut, ce type de connexion est refusé.

Envoi d'e-mails
Autoriser ou refuser l'envoi d'e-mails sur SMTP.

Par défaut, ce type de connexion est autorisé.

HTTP navigation web
Autoriser ou refuser la navigation web HTTP.

Par défaut, ce type de connexion est autorisé.

Connexions Bureau à distance entrantes
Autoriser ou refuser l'accès à d'autres ordinateurs sur des Connexions Bureau à distance.

Par défaut, ce type de connexion est autorisé.

Trafic Windows Explorer sur HTTP / FTP
Autoriser ou refuser le trafic HTTP et FTP de Windows Explorer.

Par défaut, ce type de connexion est refusé.

9.6. Règles d'applications

Pour afficher et gérer les règles pare-feu contrôlant l'accès des applications aux ressources du réseau et à Internet, cliquez sur **Règles d'applications**.

1. Ouvrez la fenêtre de Bitdefender.

2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Pare-feu** dans le menu de gauche puis sur l'onglet **Avancé**.
4. Sous Règles pare-feu, cliquez sur **Règles d'Applications**.

Vous pouvez consulter dans le tableau les programmes (c'est-à-dire les processus) pour lesquels des règles pare-feu ont été créées.Pour consulter les règles créées pour une application spécifique, cliquez sur le signe + en regard de l'application concernée ou double-cliquez simplement dessus.

Les informations suivantes s'affichent pour chaque règle :

- **Types de Réseau/Processus** - le processus et les types d'adaptateur réseau auxquels la règle s'applique.Des règles sont créées automatiquement pour filtrer l'accès réseau ou Internet via n'importe quel adaptateur.Vous pouvez créer manuellement des règles ou éditer des règles existantes, afin de filtrer l'accès réseau ou Internet d'une application via un adaptateur spécifique (par exemple un adaptateur réseau sans fil).
- **Protocole** - le protocole IP auquel s'applique la règle.Vous verrez apparaître l'une des mentions suivantes :

Protocole	Description
Tous	Intègre tous les protocoles IP.
TCP	Transmission Control Protocol - TCP permet à deux PC d'établir une connexion et d'échanger des flux de données. TCP garantit la livraison des données et garantit également que les paquets seront livrés dans le même ordre que celui d'envoi.
UDP	User Datagram Protocol - UDP est un transport basé sur IP conçu pour de haute performance. Les jeux et des applications vidéo utilisent souvent UDP.
Un nombre	Désigne un protocole IP spécifique (autre que les protocoles TCP et UDP).Vous pouvez obtenir la liste complète des numéros de protocoles IP attribués à l'adresse http://www.iana.org/assignments/protocol-numbers.

- **Action** - si l'application est autorisée ou non à se connecter au réseau ou à Internet selon les circonstances spécifiées.

Pour gérer les règles, utilisez les boutons de la partie inférieure de la fenêtre :

- **Ajouter une règle** - ouvre la fenêtre Ajouter une règle d'application vous permettant de créer une nouvelle règle.
- **Éditer la règle** - ouvre la fenêtre Modifier une règle d'application où vous pouvez modifier les paramètres d'une règle sélectionnée.

- **Supprimer la règle** - supprime la règle sélectionnée.

Ajouter / éditer des règles d'applications

Pour ajouter ou éditer une règle d'application, cliquez sur le bouton correspondant.Une nouvelle fenêtre apparaîtra. Procédez comme suit :

- **Chemin du programme.** Cliquez sur **Parcourir** et sélectionnez l'application à laquelle s'applique la règle.
- **Adresse locale.** Spécifiez l'adresse IP locale et le port auxquels s'applique la règle en procédant comme suit :Si vous avez plus d'un adaptateur réseau, vous pouvez décocher la case **Tous** et entrer une adresse IP spécifique.
- **Adresse distante.** Spécifiez l'adresse IP distante et le port auxquels s'applique la règle en procédant comme suit :Pour filtrer le trafic entre votre ordinateur et un ordinateur spécifique, décochez la case **Tous** et entrer son adresse IP.
- **Type de Réseau.** Sélectionnez le type de réseau auquel s'applique la règle.
- **Événements.** En fonction du protocole sélectionné, choisissez les événements réseau auxquels la règle s'applique.Les événements suivants sont susceptibles d'être consignés :

Evénement	Description
Connexion	Échange préliminaire de messages standard, réalisé par les protocoles orientés connexion (tels que TCP) afin d'établir une connexion.Avec les protocoles orientés connexion, le trafic de données entre deux ordinateurs n'intervient qu'une fois qu'une connexion est établie.
Trafic	Flux de données entre deux ordinateurs.
Ecouter	État dans lequel une application surveille le réseau, dans l'attente de l'établissement d'une connexion ou de la réception d'informations provenant d'une application de même niveau.

- **Protocole.** Sélectionnez dans le menu le protocole IP auquel s'applique la règle.
  - Si vous voulez que la règle s'applique à tous les protocoles, sélectionnez **Toutes**.
  - Si vous souhaitez que la règle s'applique au protocole TCP, sélectionnez **TCP**.
  - Si vous souhaitez que la règle s'applique au protocole UDP, sélectionnez **UDP**.
  - Si vous voulez que la règle s'applique à un protocole spécifique, sélectionnez **Autre**.Un champ de saisie apparaît.Saisissez dans ce champ le numéro attribué au protocole que vous voulez filtrer.

Note

Les numéros des protocoles IP sont attribués par l'IANA (Internet Assigned Numbers Authority, l'organisation de gestion de l'adressage IP sur Internet).Vous pouvez obtenir la liste complète des numéros de protocoles IP attribués à l'adresse http://www.iana.org/assignments/protocol-numbers.

- **Direction.** Sélectionnez dans le menu la direction du trafic à laquelle s'applique la règle.

Direction	Description
Sortant	La règle s'applique seulement pour le trafic sortant.
Entrant	La règle s'applique seulement pour le trafic entrant.
Tous les deux	La règle s'applique dans les deux directions.

- **Version IP.** Sélectionnez dans le menu la version du protocole IP (IPv4, IPv6 ou autre) à laquelle s'applique la règle.
- **Permission.** Sélectionnez l'une des permissions disponibles :

Permission	Description
Autoriser	L'application spécifiée se verra autoriser l'accès réseau/Internet dans les circonstances spécifiées.
Refuser	L'application spécifiée se verra refuser l'accès réseau/Internet dans les circonstances spécifiées.

9.7. Règles d'adaptateurs

Pour chaque connexion réseau vous pouvez configurer des zones de confiance et des zones non fiables.

Une zone de confiance est un périphérique en lequel vous avez entièrement confiance, comme un ordinateur ou une imprimante. Tout le trafic entre votre ordinateur et un périphérique de confiance est autorisé.Pour partager des ressources avec des ordinateurs en particulier dans une réseau WiFi non sécurisé, ajoutez les comme étant des ordinateurs autorisés.

Une zone non fiable est un périphérique avec lequel vous n'autorisez aucune communication avec votre ordinateur.

Pour afficher et gérer les zones sur vos cartes réseau, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.

3. Cliquez sur **Pare-feu** dans le menu de gauche puis sur l'onglet **Avancé**.
4. Sous Règles pare-feu, cliquez sur **Règles d'adaptateurs**.

Une nouvelle fenêtre s'affiche.Les zones de réseau actuelles sont affichées par adaptateur.

Pour gérer les zones, utilisez les boutons de la partie supérieure de la fenêtre :

- **Ajouter une zone** - ouvre la fenêtre Ajouter une adresse IP qui vous permet de créer une nouvelle zone pour un adaptateur sélectionné.
- **Modifier Zone** - ouvre la fenêtre Modifier la règle où vous pouvez modifier les paramètres d'une zone sélectionnée.
- **Supprimer Zone** - supprime la zone sélectionnée.

Ajouter / modifier des zones

Pour ajouter ou éditer une zone, cliquez sur le bouton correspondant.Une nouvelle fenêtre affichant les adresses IP des périphériques connectés au réseau s'affichera. Procédez comme suit :

1. Sélectionnez l'adresse IP de l'ordinateur que vous souhaitez ajouter, ou tapez une adresse ou une plage d'adresses dans la zone de texte prévue à cet effet.
2. Sélectionnez l'action :
   - **Autoriser** - pour autoriser tout le trafic entre votre ordinateur et l'ordinateur sélectionné.
   - **Bloquer** - permet de bloquer tout le trafic entre votre ordinateur et l'ordinateur sélectionné.
3. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

9.8. Surveiller l'activité du réseau

Pour contrôler l'activité en cours du réseau/Internet (via TCP et UDP) triée par application et pour ouvrir le journal du pare-feu Bitdefender, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Pare-feu** dans le menu de gauche puis sur l'onglet **Avancé**.
4. Sous Activité des Réseaux, cliquez sur **Activité du pare-feu**.

Une nouvelle fenêtre s'affiche.Le trafic total répertorié par application s'affiche. Chaque application comporte des informations sur les connexions et les ports ouverts, des statistiques sur la vitesse du trafic entrant et sortant et le nombre total de données envoyées/reçues.

Une icône apparaît à côté de chaque connexion.La signification des icônes est la suivante :

- Indique une connexion sortante.
- Indique une connexion entrante.
- Indique un port ouvert sur votre ordinateur.

La fenêtre indique l'activité du réseau/Internet en temps réel. Lorsque des connexions ou des ports sont fermés, les statistiques correspondantes sont estompées et finissent par disparaître.Il en va de même pour toutes les statistiques correspondant à une application que vous fermez qui génère du trafic ou comporte des ports ouverts.

Pour obtenir une liste complète des événements concernant l'utilisation du module Pare-feu (activer/désactiver le pare-feu, bloquer le trafic, modifier les paramètres) ou des événements générés par les activités détectées par ce module (analyse des ports, bloquer les tentatives de connexion ou le trafic selon les règles paramétrées), visualisez le fichier journal du Pare-feu Bitdefender que vous trouverez en cliquant sur **Afficher le Journal**.

10. Optimisation

Bitdefender comporte un module Optimisation qui vous permet de préserver l'intégrité de votre système. Les outils de maintenance proposés sont essentiels pour améliorer la réactivité de votre système et pour gérer efficacement votre espace de disque dur.

Bitdefender vous propose les outils d'optimisation de PC suivants :

- Nettoyage du PC - supprime les fichiers Internet temporaires et les cookies, les fichiers système inutilisés et les raccourcis vers les documents récents.
- Défragmentation - réorganise physiquement les données sur le disque dur, de sorte que les différentes portions d'un fichier soient stockées les unes à la suite des autres, de façon continue.
- Détecteur de doublons - recherche et supprime les fichiers en double sur votre système.
- Le Nettoyage du Registre - identifie et supprime les références invalides ou expirées dans la base des registres Windows.Pour conserver une base de registre de Windows propre et parfaitement optimisée, nous vous recommandons d'exécuter l'outil de nettoyage des registres tous les mois.
- Restauration Registre - peut restaurer des clés de registre précédemment supprimées de la base de registre de Windows, en utilisant l'outil de nettoyage des registres de Bitdefender.
- L'Analyseur de Performances surveille votre configuration matérielle et logicielle système pour vous assurer une protection complète contre les malwares.

10.1. Nettoyage de votre PC

Chaque fois que vous vous rendez sur une page Web, un fichier Internet temporaire est créé pour vous permettre d'accéder plus rapidement à cette page la prochaine fois.

Lorsque vous vous rendez sur une page Web, des cookies sont également stockés sur votre ordinateur.

L'assistant de nettoyage du PC vous aide à libérer de l'espace disque et à protéger votre vie privée en supprimant les fichiers qui ne sont plus utiles.

- Fichiers Internet temporaires et cookies Internet Explorer.
- Fichiers Internet temporaires et cookies Mozilla Firefox.
- Fichiers système temporaires créés par Windows pendant son fonctionnement.
- Raccourcis vers les documents récents créés par Windows lorsque vous ouvrez un fichier.

Pour lancer l'assistant de Nettoyage du PC, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Optimisation**.
3. Cliquez sur **Optimiser** puis sélectionnez **Nettoyage du PC**.
4. Suivez cette procédure en trois étapes pour effectuer le nettoyage.Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.
   a. **Bienvenue**
   b. **Réaliser un Nettoyage**
   c. **Résultats**

Pour gérer les options de Nettoyage du PC, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Optimisation** dans le menu de gauche puis sur l'onglet **Configuration**.
4. Désactivez ou activez les options de Nettoyage du PC en cliquant sur les boutons correspondants :
   - Vider le cache Internet Explorer
   - Vider le cache Mozilla Firefox
   - Nettoyer les documents récents et les fichiers système temporaires

10.2. Défragmenter des volumes de disque dur

La fragmentation de fichiers intervient lors de la copie d'un fichier excédant le plus grand bloc d'espace libre du disque dur. Étant donné que l'espace libre est insuffisant pour y stocker l'intégralité du fichier en continu, celui-ci est stocké en plusieurs blocs. Les données du fichier fragmenté doivent être lues à partir de plusieurs emplacements différents.

Il est recommandé de défragmenter le disque dur pour:

- accéder aux fichiers plus rapidement ;
- améliorer la performance globale du système ;
- augmenter la durée de vie du disque dur.

Pour lancer l'assistant du Défragmenteur de Disques, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Optimisation**.
3. Cliquez sur **Optimiser** puis sélectionnez **Défragmentation**.

4. Suivez cette procédure en cinq étapes pour effectuer la défragmentation.Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.

   a. **Choisissez les disques à analyser**

      Sélectionnez les partitions dont vous souhaitez vérifier la fragmentation.

   b. **Analyser partition sélectionnée**

      Patientez jusqu'à ce que Bitdefender ait terminé l'analyse des partitions.

   c. **Sélectionner le disque**

      L'état de la fragmentation des partitions analysées est affiché. Sélectionnez les partitions que vous souhaitez défragmenter.

   d. **Défragmentation**

      Veuillez attendre que Bitdefender ait fini de défragmenter les partitions.

   e. **Résultats**

Note

La défragmentation peut prendre un certain temps sachant qu'elle implique de déplacer des parties de données stockées d'un emplacement du disque dur à un autre. Nous vous recommandons d'effectuer la défragmentation lorsque vous n'utilisez pas votre ordinateur.

10.3. Rechercher les doublons

Les doublons consomment beaucoup d'espace sur le disque dur. Imaginez le même fichier `.mp3` stocké à trois emplacements différents.

L'assistant du Détecteur de Doublons vous aidera à détecter et à supprimer les fichiers en double sur votre ordinateur.

Pour lancer le Détecteur de Doublons, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Optimisation**.
3. Cliquez sur **Optimiser** puis sélectionnez **Détecteur de Doublons**.
4. Suivez la procédure en quatre étapes pour identifier et supprimer les doublons. Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.

   a. **Sélectionner la cible**

      Ajoutez les dossiers où vous souhaitez rechercher les fichiers en double.

   b. **Rechercher les doublons**

      Patientez jusqu'à ce que Bitdefender ait terminé la recherche de doublons.

c. **Sélectionner les fichiers à supprimer**

Les fichiers identiques figurent dans des groupes. Vous pouvez choisir une action à mener sur tous les groupes ou séparément sur chaque groupe : conserver le plus récent, conserver le plus ancien ou ne rien faire.Vous pouvez aussi sélectionner des actions pour chaque fichier individuel.

Note
Si aucun doublon n'est détecté, cette étape sera ignorée.

d. **Résultats**

Pour gérer les options du Détecteur de Doublons, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Optimisation** dans le menu de gauche puis sur l'onglet **Configuration**.
4. Activez ou désactivez les options du Détecteur de Doublons en cliquant sur les boutons correspondants :
   - Ignorer les fichiers de 0 Ko
   - Ignorer les fichiers du programme Windows
   - Ignorer les éléments spécifiques à Windows
   - Afficher uniquement les groupes de plus de X Mo.

10.4. Nettoyer le Registre Windows

De nombreuses applications enregistrent des clés dans cette base au moment de leur installation. Lorsque ces applications sont supprimées, certaines de leurs clés associées peuvent ne pas être supprimées et demeurer dans la base de registre, ce qui ralentit le système et peut même provoquer son instabilité. Il en va de même lorsque vous supprimez des raccourcis vers certains fichiers d'applications installés dans votre système ou dans le cas de pilotes corrompus.

Pour lancer l'assistant de Nettoyage du Registre, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Optimisation**.
3. Cliquez sur **Optimiser** puis sélectionnez **Nettoyage du Registre**.
4. Suivez la procédure en quatre étapes pour nettoyer le registre. Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.

a. **Bienvenue**

b. **Effectuer l'analyse**

Patientez jusqu'à ce que Bitdefender ait terminé l'analyse du registre.

c. **Sélectionner les Clés**

Vous pouvez voir toutes les clés de registre non valides ou orphelines détectées. Chacune est accompagnée d'informations détaillées la concernant (nom, valeur, priorité, catégorie).

Les clés de registre sont regroupées selon leur emplacement dans le registre Windows :

Catégorie	Description
Répertoires de logiciels	Clés de registre contenant des informations sur les chemins des applications installées sur votre ordinateur. Les clés non valides sont indexées en priorité basse, ce qui signifie que vous pouvez les effacer en ne prenant quasiment aucun risque.
Commandes personnalisées	Clés de registre contenant des informations sur les extensions de fichiers enregistrées sur votre ordinateur.Ces clés de registre sont généralement utilisées pour conserver les associations de fichiers (pour s'assurer que le bon programme s'ouvre quand vous ouvrez un fichier en utilisant Windows Explorer).Par exemple, une telle clé de registre autorise Windows à ouvrir un fichier `.doc` dans Microsoft Word. Les clés non valides sont indexées en priorité basse, ce qui signifie que vous pouvez les effacer en ne prenant quasiment aucun risque.
Les DLL partagées	Clés de registre contenant des informations sur l'emplacement des DLLs partagés (Dynamic Link Libraries).Les fichiers DLLs intègrent des fonctions qui sont utilisées par les applications installées pour effectuer certaine taches. Elles peuvent être partagées par de multiples applications en vue de réduire la prise de ressource en mémoire ou en espace disque. Ces clés de registres deviennent non valides quand les DLL vers lesquelles elles pointent sont

Catégorie	Description
	déplacées dans un emplacement différent ou sont supprimées (c'est ce qui se produit généralement quand vous désinstallez un programme.) Les clés non valides sont indexées avec une Priorité Moyenne, ce qui veut dire que les effacer peut avoir des conséquences négatives sur le système.

Par défaut, toutes les clés sont sélectionnées pour être supprimées. Vous pouvez choisir de supprimer individuellement des clés non valides d'une catégorie sélectionnée.

Note
Vous pouvez récupérer les clés de registre supprimées à tout moment à l'aide de Restauration Registre.

d. **Résultats**

10.5. Restauration du registre nettoyé

Il est possible qu'après un nettoyage des registres, votre système ne fonctionne pas correctement ou que certaines applications présentent des dysfonctionnements dus à des clés de registre manquantes. Cela peut provenir de clés de registres partagées ayant été supprimées lors du nettoyage des registres ou d'autres clés supprimées. Pour résoudre ce problème, vous devez restaurer les registres nettoyés.

Pour lancer l'assistant de Récupération du Registre, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Optimisation**.
3. Cliquez sur **Optimiser** puis sélectionnez **Restauration Registre**.
4. Suivez cette procédure en deux étapes pour récupérer le registre nettoyé.Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.

   a. **Sélectionner le point de restauration**

   Vous pouvez voir une liste de moments spécifiques auxquels la base de registre de Windows a été nettoyée.Sélectionnez un moment spécifique pour appliquer la restauration de la base de registre de Windows.

Avertissement
Il se peut que la restauration des registres nettoyés écrase les clés de registre modifiées depuis le dernier nettoyage des registres.

b. **Résultats de la tâche**

10.6. Analyseur de Performances

Le module Analyseur de Performances surveille en permanence la charge du système, vous permettant ainsi de voir les applications en cours d'exécution et l'impact qu'elles ont sur le comportement général du système.

Voici ses fonctions principales :

- Pour afficher l'utilisation de la mémoire et du processeur du système à l'aide d'un ensemble d'indicateurs
- Pour déterminer l'utilisation des ressources des applications
- Pour vous aider à fermer toute application qui utilise une grande quantité de ressources et provoque un fonctionnement lent du système

Pour accéder aux options de l'Analyseur de Performances, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Optimisation** dans le menu de gauche puis sur l'onglet **Surveiller**.
4. Si vous rencontrez un problème de ralentissement, il se peut que celui-ci soit dû à des applications en cours d'exécution sur votre système. Pour résoudre ce problème, suivez ces étapes :
   a. Identifier l'application qui cause le problème.
   b. Cliquez sur le nom de l'application pour afficher un historique de l'utilisation du processeur et de la mémoire ainsi que le chemin d'installation.
   c. Fermez l'application à l'aide du bouton.

Avertissement
Si vous pensez que l'application (ou le processus) que vous souhaitez fermer fait partie du système d'exploitation Windows et que votre action peut avoir des répercussions sur le système, contactez le Service Client Bitdefender pour plus d'informations.

11. Mappage réseau

Le module Réseau vous permet de gérer les produits Bitdefender installés sur tous les ordinateurs de votre foyer à partir d'un seul et même ordinateur.

Vous devez suivre ces étapes pour pouvoir gérer les produits Bitdefender installés sur tous les ordinateurs de votre foyer :

1. Activer le réseau de Bitdefender sur votre ordinateur.Définissez votre ordinateur comme **Ordinateur serveur**.
2. Allumez chaque ordinateur que vous voulez gérer et rejoignez le réseau à partir de ceux-ci (en saisissant le mot de passe).Définissez chaque ordinateur comme **Ordinateur Standard**.
3. Revenez sur votre ordinateur et ajoutez les ordinateurs que vous voulez gérer.

11.1. Activation du réseau Bitdefender

Pour activer le réseau de Bitdefender, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Mappage réseau** dans le menu de gauche.
4. Cliquez sur **Activer le Réseau**.On vous demandera de configurer le mot de passe de gestion du mappage réseau.
5. Entrez le même mot de passe dans chacun des champs de saisie.
6. Définissez le rôle de l'ordinateur dans le mappage réseau de Bitdefender :
   - **Ordinateur serveur** - sélectionnez cette option sur l'ordinateur qui sera utilisé pour administrer tous les autres.
   - **Ordinateur standard** - sélectionnez cette option sur les ordinateurs qui seront gérés par l'ordinateur serveur.
7. Cliquez sur **OK**.

   Vous pouvez voir apparaître le nom de l'ordinateur sur la carte réseau.

   Le bouton **Désactiver la connexion** apparaît.

Note

Vous pouvez également activer le mappage réseau à partir de la fenêtre principale de Bitdefender :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Mappage réseau**.
3. Cliquez sur **Gérer** et sélectionnez **Activer le réseau** dans le menu déroulant.

11.2. Ajouter des ordinateurs au réseau de Bitdefender

Tout ordinateur sera ajouté automatiquement au réseau s'il répond aux critères suivants :

- le mappage réseau de Bitdefender a été activé sur celui-ci.
- le rôle a été défini sur Ordinateur Standard.
- le mot de passe défini lors de l'activation du réseau est le même que celui de l'Ordinateur Serveur.

Note

Vous pouvez analyser le mappage réseau à la recherche d'ordinateurs correspondant aux critères à tout moment en cliquant sur le bouton **Auto détect.**.

Pour ajouter manuellement un ordinateur au mappage réseau de Bitdefender, à partir de l'ordinateur serveur, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Mappage réseau** dans le menu de gauche.
4. Cliquez sur **Ajouter un PC**.
5. Tapez le mot de passe de gestion et cliquez sur **OK**.Une nouvelle fenêtre s'affiche.

   Vous pouvez voir à l'écran la liste des ordinateurs rattachés au réseau.La signification des icônes est la suivante :

   Indique un ordinateur en ligne sans aucun produit Bitdefender installé.

   Indique un ordinateur en ligne avec Bitdefender installé.

   Indique un ordinateur hors connexion avec Bitdefender installé.
6. Choisissez l'une des possibilités suivantes :
   - Sélectionnez dans la liste le nom de l'ordinateur à ajouter.
   - Tapez l'adresse IP ou le nom de l'ordinateur à ajouter dans le champ correspondant.
7. Cliquez sur **Ajouter**.
8. Tapez le mot de passe de gestion défini sur l'ordinateur concerné.
9. Cliquez sur **OK**.Si vous avez spécifié le bon mot de passe, le nom de l'ordinateur sélectionné apparaît sur la carte réseau.

11.3. Gérer le réseau Bitdefender

Une fois votre mappage réseau Bitdefender créé, vous pouvez gérer l'ensemble des produits Bitdefender à partir de l'ordinateur serveur.

Pour exécuter plusieurs tâches sur tous les ordinateurs gérés, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Mappage réseau**.
3. Cliquez sur **Gérer** et sélectionnez les boutons correspondants dans le menu déroulant :
   - **Désactiver la connexion** - vous permet de désactiver le réseau.
   - **Tout analyser** - vous permet d'analyser en une seule opération l'ensemble des ordinateurs administrés.
   - **Tout mettre à jour** vous permet de mettre à jour en une seule opération l'ensemble des ordinateurs gérés.

Avant de lancer une tâche sur un ordinateur spécifique, vous serez invité à saisir le mot de passe de gestion locale.Tapez le mot de passe de gestion et cliquez sur **OK**.

Pour voir le mappage réseau et accéder à toutes les tâches d'administration, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Mappage réseau** dans le menu de gauche.

Si vous déplacez le curseur sur un ordinateur de la carte réseau, vous pouvez consulter quelques informations le concernant (adresse IP, nombre de problèmes affectant la sécurité du système, état d'enregistrement de Bitdefender).

En cliquant sur le nom d'un ordinateur sur la carte du réseau, vous pouvez voir toutes les tâches administratives que vous pouvez lancer sur cet ordinateur distant.

Enregistrer le produit
Vous permet d'enregistrer Bitdefender sur cet ordinateur en entrant une clé de licence.

Configurer le mot de passe des paramètres du produit
Vous permet de créer un mot de passe pour limiter l'accès aux paramètres de Bitdefender sur ce PC.

Exécuter une tâche d'analyse à la demande
Vous permet de lancer une analyse à la demande sur un ordinateur distant. Vous pouvez réaliser l'une des tâches d'analyse suivantes : Analyse Rapide, ou Analyse Complète du Système.

Tout corriger
Vous permet de corriger les problèmes qui affectent la sécurité de cet ordinateur à l'aide de l'assistant Tout corriger.

Afficher les événements
Vous permet d'accéder au module **Événements** du produit Bitdefender installé sur cet ordinateur.

Mettre à jour maintenant
Lance le processus de Mise à jour du produit Bitdefender installé sur cet ordinateur.

Configurer le profil du Contrôle Parental
Permet de définir la catégorie d'âge devant être utilisée par le filtre Web de contrôle parental sur cet ordinateur.

Exécuter une tâche d'optimisation
Vous permet de lancer une tâche d'optimisation sur le PC distant. Vous pouvez réaliser l'une des tâches suivantes : défragmenter les disques ou nettoyer les fichiers temporaires Internet.

Définir comme serveur de mise à jour pour ce réseau
Vous permet de définir cet ordinateur comme serveur de mise à jour pour tous les produits Bitdefender installés sur les ordinateurs de ce réseau.Utiliser cette option réduira le trafic Internet car seul un ordinateur du réseau se connectera à Internet pour télécharger des mises à jour.

Supprimer le PC du mappage réseau
Vous permet de retirer un PC du réseau.

Note

Si vous prévoyez de lancer plusieurs tâches, il peut s'avérer utile de sélectionner l'option **Ne plus afficher ce message durant cette session**.En sélectionnant cette option, vous n'aurez plus à saisir le mot de passe pour la session en cours.

12. Mise à jour

Chaque jour, de nouveaux codes malveillants sont détectés et identifiés. C'est pourquoi il est très important que Bitdefender soit à jour dans les signatures de codes malveillants.

Si vous êtes connecté à Internet par câble ou DSL, Bitdefender s'en occupera automatiquement. Il lance la procédure de mise à jour de la base virale à chaque fois que vous démarrez votre ordinateur puis toutes les **heures**.Si une mise à jour est détectée, elle est automatiquement téléchargée et installée sur votre ordinateur.

Le processus de mise à jour est exécuté à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, le processus de mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.

Important
Pour être protégé contre les dernières menaces, maintenez la mise à jour automatique activée.

Votre intervention peut être nécessaire, dans certains cas, pour maintenir la protection de Bitdefender à jour :

- Si votre ordinateur se connecte à Internet via un serveur proxy, vous devez configurer les paramètres du proxy comme indiqué dans « *Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?* » (p. 42).
- Si vous n'avez pas de connexion Internet, vous pouvez mettre à jour Bitdefender manuellement comme indiqué dans « *Mon ordinateur n'est pas connecté à Internet. Comment puis-je mettre à jour Bitdefender ?* » (p. 149).Le fichier de mise à jour manuelle est publié une fois par semaine.
- Des erreurs peuvent se produire lors du téléchargement de mises à jour avec une connexion à Internet lente. Pour savoir comment éviter ces erreurs, veuillez vous reporter à « *Comment mettre à jour Bitdefender avec une connexion Internet lente* » (p. 148).
- Si vous êtes connecté à Internet via une connexion RTC (ou RNIS), nous vous conseillons de prendre l'habitude d'utiliser régulièrement les mises à jour à la demande.Pour plus d'informations, reportez-vous à « *Mise à jour en cours* » (p. 134).

12.1. Vérifier que Bitdefender est à jour

Pour vérifier que la protection de Bitdefender est à jour, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Mise à jour**.

3. L'heure de la dernière mise à jour s'affiche juste en-dessous du nom du panneau.

Pour des informations détaillées sur les dernières mises à jour, vérifiez les événements de mise à jour :

1. Dans la fenêtre principale, cliquez sur **Événements** dans la barre d'outils supérieure.
2. Cliquez sur **Mise à jour** dans le menu de gauche.

Vous pouvez savoir quand des mises à jour ont été lancées et obtenir des informations à leur sujet (si elles ont été ou non réussies, si elles nécessitent un redémarrage pour que leur installation se termine).Si nécessaire, redémarrez le système dès que possible.

12.2. Mise à jour en cours

Pour effectuer des mises à jour, une connexion à Internet est requise.

Pour lancer une mise à jour, choisissez l'une des options suivantes :

- Ouvrez la fenêtre Bitdefender, allez dans le panneau **Mise à jour** et cliquez sur **Mettre à jour maintenant**.
- Faites un clic droit sur l'icône de Bitdefender de la zone de notification et sélectionnez **Mettre à jour maintenant**.

Le module de Mise à jour se connectera au serveur de mise à jour de Bitdefender et recherchera des mises à jour. Si une mise à jour est détectée, elle sera installée automatiquement ou il vous sera demandé de confirmer son installation, selon les paramètres de mise à jour.

Important
Il peut être nécessaire de redémarrer votre PC lorsque vous avez terminé une mise à jour. Nous vous recommandons de le faire dès que possible.

12.3. Activer ou désactiver la mise à jour automatique

Pour activer ou désactiver la mise à jour automatique, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Mise à jour**.
3. Cliquez sur le bouton pour activer ou désactiver la mise à jour automatique.
4. Si vous tentez de désactiver la mise à jour automatique, une fenêtre d'avertissement apparaît.Vous devez confirmer votre choix en sélectionnant dans le menu la durée pendant laquelle vous souhaitez désactiver la mise à jour automatique. Vous pouvez désactiver la mise à jour automatique pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.

Avertissement

Cela peut poser un problème de sécurité important. Nous vous recommandons de désactiver la mise à jour automatique pendant le moins de temps possible. Si Bitdefender n'est pas régulièrement mis à jour, il ne pourra pas vous protéger contre les dernières menaces.

12.4. Réglage des paramètres de mise à jour

Les mises à jour peuvent être réalisées depuis le réseau local, depuis Internet, directement ou à travers un serveur proxy.Par défaut, Bitdefender recherche les mises à jour chaque heure sur Internet et installe celles qui sont disponibles sans vous en avertir.

Les paramètres de mise à jour par défaut sont adaptés à la plupart des utilisateurs et vous n'avez normalement pas besoin de les modifier.

Pour régler les paramètres de mise à jour, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Mise à jour** dans le menu de gauche.
4. Réglez les paramètres en fonction de vos préférences.

Emplacement de mise à jour

Bitdefender est configuré pour se mettre à jour à partir des serveurs de mise à jour de Bitdefender sur Internet. L'emplacement de mise à jour est `http://upgrade.bitdefender.com`, une adresse Internet générique qui est automatiquement redirigée vers le serveur de mise à jour Bitdefender le plus proche de votre région.

Ne modifiez pas l'emplacement de mise à jour sauf sur demande d'un représentant de Bitdefender ou de votre administrateur réseau (si vous êtes connecté à un réseau d'entreprise).

Si vous avez installé Bitdefender sur plusieurs ordinateurs de votre foyer, vous pouvez configurer un réseau domestique Bitdefender et choisir l'un de vos ordinateurs comme serveur de mise à jour. Des informations détaillées sont disponibles dans « *Mappage réseau* » (p. 129).Le programme Bitdefender installé sur le serveur de mise à jour choisi se mettra à jour à partir d'Internet. Les programmes Bitdefender des autres ordinateurs obtiendront leurs mises à jour à partir du serveur local de mise à jour (leur emplacement de mise à jour est automatiquement modifié en conséquence.)Cette configuration est conçue pour réduire le trafic Internet et optimiser les mises à jour.

Vous pouvez revenir à l'emplacement de mise à jour Internet générique en cliquant sur **Par défaut**.

Règles de traitement

Vous disposez de trois façons de télécharger et d'installer des mises à jour :

- **Mise à jour silencieuse** - Bitdefender télécharge et implémente automatiquement la mise à jour.
- **Demander avant de télécharger les mises à jour** - à chaque fois qu'une mise à jour sera disponible, le système demandera votre autorisation avant de la télécharger.
- **Demander avant l'installation** - à chaque fois qu'une mise à jour est téléchargée, le système demande votre autorisation avant de l'installer.

Certaines mises à jour nécessitent un redémarrage pour terminer l'installation. Par défaut, si une mise à jour nécessite un redémarrage, Bitdefender continuera à fonctionner avec les anciens fichiers jusqu'à ce que l'utilisateur redémarre volontairement l'ordinateur. Cela évite que le processus de mise à jour de Bitdefender interfère avec le travail de l'utilisateur.

Si vous souhaitez être averti lorsqu'une mise à jour nécessite un redémarrage, désactivez l'option **Reporter le redémarrage** en cliquant sur le bouton correspondant.

Mises à jour P2P

Outre le mécanisme de mise à jour normal, Bitdefender utilise également un système de partage de mise à jour intelligent basé sur le protocole peer-to-peer (P2P) pour distribuer des mises à jour de signatures de malwares entre utilisateurs de Bitdefender.

Vous pouvez activer ou désactiver les options de mise à jour P2P à l'aide des boutons correspondants.

Utiliser le système de mise à jour P2P

Activez cette option pour télécharger les mises à jour de signatures de malwares auprès d'autres utilisateurs de Bitdefender utilisant le système de mise à jour P2P.Bitdefender utilise les ports 8880 – 8889 pour la mise à jour peer-to-peer.

Distribuer les fichiers Bitdefender

Activez cette option pour partager les dernières signatures de malwares disponibles sur votre ordinateur avec d'autres utilisateurs de Bitdefender.

13. Sauvegarde en ligne de SafeBox

SafeBox est la solution Bitdefender qui vous permet de sauvegarder vos données importantes sur nos serveurs sécurisés en ligne.

Note
Un compte MyBitdefender est nécessaire pour utiliser cette fonctionnalité.
Pour plus d'informations, reportez-vous à « *Enregistrement du Produit* » (p. 8).

Avec SafeBox :

- Vous obtenez 2 Go d'espace libre en ligne pour vos sauvegardes.
- Vous pouvez gérer vos sauvegardes directement à partir de Windows Explorer. Pour plus d'informations, reportez-vous à Gérer les sauvegardes SafeBox à partir de Windows.
- Vous pouvez synchroniser des sauvegardes entre plusieurs ordinateurs exécutant Bitdefender Total Security 2012.
- Les fichiers sauvegardés ayant été supprimés peuvent être restaurés.
- Les modifications apportées à vos fichiers sont enregistrées afin que vous puissiez restaurer des versions antérieures.

Un raccourci vers le dossier de sauvegarde par défaut est placé sur votre bureau.

Pour sauvegarder facilement vos données sur les serveurs de Bitdefender, utilisez la synchronisation automatique. Pour activer ou désactiver la synchronisation automatique, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **SafeBox**.
3. Cliquez sur le bouton **Sync. auto.**.

Les sauvegardes de SafeBox peuvent être administrées par la fenêtre Bitdefender ou en utilisant le menu contextuel de Windows.

13.1. Gérer les sauvegardes de SafeBox à partir de la fenêtre Bitdefender

Pour gérer vos sauvegardes SafeBox à partir de l'interface de Bitdefender, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Allez dans **SafeBox**.

Deux liens sont disponibles.

Gérer les dossiers SafeBox

Cliquez sur ce lien pour ouvrir une nouvelle fenêtre affichant les dossiers ajoutés à SafeBox.Vous pouvez voir pour chaque dossier le dossier local, le dossier distant vers lequel il est lié et le moment de la dernière synchronisation.

Gérez les dossiers à l'aide des boutons :

- **Ajouter un dossier** - ouvre une fenêtre vous permettant de sélectionner un nouveau dossier local à ajouter à SafeBox. Pour utiliser un autre dossier distant que celui sélectionné automatiquement, décochez la case correspondante et entrez un nouveau nom ou sélectionnez un autre dossier dans le champ **Dossier distant**.
- **Modifier le dossier** - ouvre une fenêtre vous permettant de modifier la façon dont les dossiers locaux et distants sont liés.
- **Supprimer le dossier** - supprime le dossier sélectionné de SafeBox.

Note

Supprimer un dossier de SafeBox ne supprime pas le dossier distant, cela supprime uniquement le lien entre le dossier local et le dossier distant.

Restaurer les fichiers supprimés

Cliquez sur ce lien pour ouvrir une nouvelle fenêtre affichant les dossiers ajoutés à SafeBox.Pour restaurer les fichiers supprimés d'un dossier, cochez la case à ses côtés et cliquez sur le bouton **Restaurer**.

13.2. Gérer les sauvegardes SafeBox à partir de Windows

Lorsque vous faites un clic droit sur un dossier ou à l'intérieur d'un dossier, le menu contextuel Windows vous permet d'accéder rapidement à toutes les opérations disponibles de la SafeBox.

13.2.1. Ajouter des dossiers à SafeBox

Pour ajouter un dossier à SafeBox, faites un clic droit sur son icône ou ailleurs dans le dossier et sélectionnez **Ajouter à SafeBox**.

Un dossier distant portant le même nom est créé sur les serveurs Bitdefender. Vous pouvez éditer les dossiers comme indiqué dans la section « *Gérer les sauvegardes de SafeBox à partir de la fenêtre Bitdefender* » (p. 137).

Bitdefender commencera à transférer le contenu du dossier entier vers les serveurs en ligne. Lorsque la synchronisation du dossier sera terminée, l'icône de Bitdefender

apparaîtra sur l'icône du dossier.

Les icônes des fichiers et dossiers du dossier SafeBox changeront en fonction de l'état de leur synchronisation avec le dossier distant :

Le fichier / dossier est synchronisé.

Le fichier / dossier n'est pas synchronisé.

Le fichier / dossier est en cours de synchronisation.

Une fois un dossier ajouté à SafeBox et tant que la Synchronisation Automatique est activée, les contenus du dossier sont automatiquement synchronisés avec le dossier (distant) en ligne.

13.2.2. Suppression de dossiers de la SafeBox

Pour retirer un dossier de SafeBox, faites un clic droit sur son icône, pointez sur **Bitdefender SafeBox** et sélectionnez **Retirer de Bitdefender SafeBox**.Une fenêtre de confirmation apparaîtra. Cliquez sur **Oui** pour empêcher SafeBox de gérer le dossier.

Note
Supprimer un dossier de SafeBox ne supprime pas le dossier distant, cela supprime uniquement le lien entre le dossier local et le dossier distant.

13.2.3. Restauration des fichiers supprimés de SafeBox

Lorsqu'un dossier est ajouté à SafeBox, Bitdefender surveille toutes les modifications apportées à ce dossier. Cela vous permet de restaurer des fichiers supprimés d'un dossier local SafeBox et de récupérer les versions antérieures de fichiers que vous avez modifiés.

Pour restaurer les fichiers supprimés d'un dossier SafeBox, faites un clic droit sur l'icône du dossier ou ailleurs dans le dossier, pointez sur **Bitdefender SafeBox** et sélectionnez **Restaurer les fichiers supprimés**.Cela restaurera les dernières versions de tous les fichiers supprimés du dossier.

Pour restaurer un fichier vers une certaine version, suivez ces étapes :

1. Faites un clic droit sur le fichier.
2. Pointez vers **Bitdefender SafeBox** et sélectionnez **Afficher les versions antérieures**.
3. Une liste de moments où le fichier a été modifié s'affiche. Sélectionnez la version que vous souhaitez restaurer.
4. Cliquez sur **Restaurer dans...**.
5. Sélectionnez le dossier où vous souhaitez restaurer le fichier et cliquez sur **OK**.

13.3. Synchroniser des fichiers entre vos ordinateurs

La synchronisation de fichiers entre 2 ordinateurs ou plus fonctionne lorsque les conditions suivantes sont remplies :

- Bitdefender Total Security 2012 est installé sur les ordinateurs entre lesquels vous souhaitez synchroniser les fichiers.
- Vous êtes connecté avec le même compte MyBitdefender sur chaque ordinateur.
- Des dossiers locaux ont été liés au même dossier distant sur chaque ordinateur.

Si les conditions sont remplies, les contenus de dossiers ajoutés à SafeBox sur un ordinateur seront synchronisés avec ceux liés aux mêmes dossiers distants sur les autres ordinateurs.

Note

Pour la synchronisation automatique, vérifiez que la **Synchronisation Automatique** de SafeBox est activée sur chaque ordinateur.

14. Protection Safego pour réseaux sociaux

Vous faites confiance à vos amis en ligne. Mais avez-vous confiance en leurs ordinateurs ?Utilisez la protection Safego pour réseaux sociaux afin de protéger votre compte et vos amis des menaces en ligne.

Safego est une application Facebook développée par Bitdefender pour protéger votre compte de réseau social. Son rôle consiste à analyser les liens que vous recevez de la part de vos amis sur Facebook et à surveiller les paramètres de confidentialité de votre compte.

Note

Un compte MyBitdefender est nécessaire pour utiliser cette fonctionnalité.
Pour plus d'informations, reportez-vous à « *Enregistrement du Produit* » (p. 8).

Voici ses fonctions principales :

- analyse automatiquement les publications de votre fil d'actualité à la recherche de liens malveillants.
- protège votre compte des menaces en ligne.

  Lorsqu'une publication ou un commentaire sera détecté comme étant du spam, une tentative de phishing ou un malware, vous recevrez un message d'avertissement.
- avertit vos amis des liens suspects publiés sur leurs fils d'actualité.
- vous aide à construire un réseau d'amis sûr à l'aide de la fonctionnalité **Friend'O'Meter**.
- vérifier l'état de sécurité du système grâce à Bitdefender QuickScan.

Pour accéder à Safego à partir de votre produit Bitdefender, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Safego**.
3. Cliquez sur **Activer**.Vous serez dirigé vers votre compte.

   Si vous avez déjà activé Safego, vous aurez accès à des statistiques sur son activité en cliquant sur le bouton **Afficher les rapports**.
4. Utilisez vos informations de connexion Facebook pour vous connecter à l'application Safego.
5. Autoriser Safego à accéder à votre compte Facebook.

15. Résolution des problèmes

Ce chapitre présente certains problèmes que vous pouvez rencontrer lorsque vous utilisez Bitdefender et vous fournit des solutions possibles à ces problèmes.La plupart de ces problèmes peuvent être résolus via la configuration appropriée des paramètres du produit.

- « *Mon système semble lent* » (p. 142)
- « *L'analyse ne démarre pas* » (p. 143)
- « *Je ne peux plus utiliser une application* » (p. 144)
- « *Je ne peux pas me connecter à Internet* » (p. 145)
- « *Je ne peux pas accéder à un périphérique de mon réseau* » (p. 145)
- « *Mon Internet est lent* » (p. 147)
- « *Comment mettre à jour Bitdefender avec une connexion Internet lente* » (p. 148)
- « *Mon ordinateur n'est pas connecté à Internet. Comment puis-je mettre à jour Bitdefender ?* » (p. 149)
- « *Le Services Bitdefender ne répondent pas* » (p. 149)
- « *Le filtre antispam ne fonctionne pas correctement* » (p. 150)
- « *La désinstallation de Bitdefender a échoué* » (p. 155)
- « *Mon système ne démarre pas après l'installation de Bitdefender* » (p. 155)

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du support technique Bitdefender comme indiqué dans le chapitre « *Support* » (p. 166).

15.1. Mon système semble lent

Généralement, après l'installation d'un logiciel de sécurité, on assiste à un léger ralentissement du système, qui est normal dans une certaine mesure.

Si vous remarquez un ralentissement important, ce problème peut apparaître pour les raisons suivantes :

- **Bitdefender n'est pas le seul logiciel de sécurité installé sur le système.**

  Bien que Bitdefender recherche et supprime les programmes de sécurité trouvés pendant l'installation, il est recommandé de supprimer tout programme antivirus que vous utilisiez avant d'installer Bitdefender.Pour plus d'informations, reportez-vous à « *Comment supprimer les autres solutions de sécurité ?* » (p. 174).

- **Vous ne disposez pas de la configuration système minimale pour l'exécution de Bitdefender.**

Si votre machine ne dispose pas de la Configuration Système Minimale, l'ordinateur deviendra lent, notamment lorsque plusieurs applications s'exécuteront simultanément. Pour plus d'informations, reportez-vous à « *Configuration système minimale* » (p. 1).

- **Il reste trop de clés de registre non valides dans votre Registre Windows.**

  Nettoyer le Registre Windows peut améliorer les performances de votre système. Pour plus d'informations, reportez-vous à « *Nettoyer le Registre Windows* » (p. 125).

- **Vos disques durs sont trop fragmentés.**

  La fragmentation de fichiers ralentit l'accès aux fichiers et fait diminuer les performances système.

  L'exécution du défragmenteur de disque peut améliorer les performances de votre système.Pour plus d'informations, reportez-vous à « *Défragmenter des volumes de disque dur* » (p. 123).

- **Les applications en cours d'exécution sur votre système consomment trop de ressources.**

  L'Analyseur de performances Bitdefender vous permet de déterminer l'impact des applications exécutées sur votre système en termes de charge de processeur, d'utilisation de mémoire et de disque dur.

  Vous devriez pouvoir localiser les applications qui ralentissent votre système, les surveiller ou les fermer.Pour plus d'informations, reportez-vous à « *Analyseur de Performances* » (p. 128).

15.2. L'analyse ne démarre pas

Ce type de problème peut avoir deux causes principales :

- **Une installation précédente de Bitdefender qui n'a pas été complètement supprimée ou une installation défectueuse de Bitdefender**.

  Dans ce cas, procédez comme suit :

  1. Désinstaller complètement Bitdefender du système :
     a. Sur http://www.bitdefender.com/uninstall téléchargez l'outil de désinstallation sur votre ordinateur.
     b. Lancez l'outil de désinstallation avec les privilèges administrateur.
     c. Redémarrez votre ordinateur.
  2. Réinstallez Bitdefender sur le système.

- **Bitdefender n'est pas la seule solution de sécurité installée sur votre système**.

Dans ce cas, procédez comme suit :

1. Supprimer l'autre solution de sécurité. Pour plus d'informations, reportez-vous à « *Comment supprimer les autres solutions de sécurité ?* » (p. 174).
2. Désinstaller complètement Bitdefender du système :
   a. Sur http://www.bitdefender.com/uninstall téléchargez l'outil de désinstallation sur votre ordinateur.
   b. Lancez l'outil de désinstallation avec les privilèges administrateur.
   c. Redémarrez votre ordinateur.
3. Réinstallez Bitdefender sur le système.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 167).

15.3. Je ne peux plus utiliser une application

Ce problème se produit lorsque vous essayez d'utiliser un programme qui fonctionnait normalement avant d'installer Bitdefender.

Vous pouvez rencontrer l'une des situations suivantes :

- Vous pourriez recevoir un message de Bitdefender indiquant que le programme essaie d'apporter une modification au système.
- Il est possible que vous receviez un message d'erreur du programme que vous tentez d'utiliser.

Ce type de situation se produit lorsque le module Active Virus Control détecte à tort que certaines applications sont malveillantes.

Active Virus Control est un module Bitdefender qui surveille en permanence les applications s'exécutant sur votre système et signale celles au comportement potentiellement malveillant.Étant donné que la fonction est basée sur un système heuristique, des applications légitimes peuvent, dans certains cas, être signalées par Active Virus Control.

Lorsque cette situation se produit, vous pouvez empêcher l'application correspondante d'être surveillée par Active Virus Control.

Pour ajouter le programme à la liste d'exceptions, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Exclusions**.
4. Cliquez sur le lien **Processus Exclus**.Dans la fenêtre qui apparaît, vous pouvez gérer les exclusions de processus Active Virus Control.

5. Ajoutez des exclusions en suivant ces étapes :
   a. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
   b. Cliquez sur **Parcourir**, sélectionnez l'application que vous souhaitez exclure, puis cliquez sur **OK**.
   c. Gardez l'option **Autoriser** sélectionnée pour empêcher Active Virus Control de bloquer l'application.
   d. Cliquez sur **Ajouter**.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 167).

15.4. Je ne peux pas me connecter à Internet

Vous remarquerez peut-être qu'un programme ou un navigateur web ne peut plus se connecter à Internet ou accéder aux services réseau après avoir installé Bitdefender.

Dans ce cas, la meilleure solution est de configurer Bitdefender afin qu'il autorise automatiquement les connexions de et vers l'application logicielle en question :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Pare-feu** dans le menu de gauche puis sur l'onglet **Avancé**.
4. Sous Règles pare-feu, cliquez sur **Règles d'Applications**.
5. Pour ajouter une règle d'application, cliquez sur le bouton correspondant.
6. Cliquez sur **Parcourir** et sélectionnez l'application à laquelle s'applique la règle.
7. Sélectionnez tous les types de réseau disponibles.
8. Allez dans **Permission** et sélectionnez **Autoriser**.

Fermez Bitdefender, ouvrez l'application logicielle et réessayez de vous connecter à Internet.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 167).

15.5. Je ne peux pas accéder à un périphérique de mon réseau

En fonction du réseau auquel vous êtes connecté, le pare-feu Bitdefender peut bloquer la connexion entre votre système et un autre périphérique (tel qu'un ordinateur ou une imprimante).Vous ne pouvez donc plus partager ou imprimer des fichiers.

Dans ce cas, la meilleure solution est de configurer Bitdefender afin qu'il autorise automatiquement les connexions de et vers le périphérique en question.Pour chaque connexion réseau vous pouvez configurer une zone spéciale de confiance.

Une zone de confiance est un périphérique auquel vous faites entièrement confiance.Tout le trafic entre votre ordinateur et le périphérique de confiance est autorisé.Pour partager des ressources avec des périphériques spécifiques, tels que des ordinateurs ou des imprimantes, ajoutez-les comme zones de confiance.

Pour ajouter une zone de confiance sur vos cartes réseau, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Pare-feu** dans le menu de gauche puis sur l'onglet **Avancé**.
4. Sous Règles pare-feu, cliquez sur **Règles d'adaptateurs**.
5. Pour ajouter une zone, cliquez sur le bouton correspondant.Une nouvelle fenêtre affichant les adresses IP des périphériques connectés au réseau s'affichera.
6. Sélectionnez l'adresse IP de l'ordinateur ou de l'imprimante que vous souhaitez ajouter, ou tapez une adresse ou une plage d'adresses dans la zone de texte prévue à cet effet.
7. Allez dans **Permission** et sélectionnez **Autoriser**.

Si vous ne pouvez toujours pas vous connecter au périphérique, le problème n'est peut-être pas causé par Bitdefender.

Vérifiez d'autres causes possibles, telles que les suivantes :

- Le pare-feu de l'autre ordinateur peut bloquer le partage de fichiers et d'imprimantes avec celui-ci.
  - Si le Pare-Feu Windows est utilisé, il peut être configuré pour autoriser le partage de fichiers et d'imprimantes comme suit : ouvrez la fenêtre de configuration du Pare-Feu Windows, l'onglet **Exceptions** et cochez la case **Partage de fichiers et d'imprimantes**
  - Si un autre programme pare-feu est utilisé, veuillez vous reporter à sa documentation ou au fichier d'aide.
- Conditions générales pouvant empêcher d'utiliser ou de se connecter à une imprimante partagée :
  - Il se peut que vous ayez besoin de vous connecter à un compte Windows administrateur pour avoir accès à l'imprimante partagée.
  - L'imprimante partagée est configurée pour autoriser l'accès uniquement à certains ordinateurs et utilisateurs. Si vous partagez votre imprimante, vérifiez que l'imprimante autorise l'accès à l'utilisateur de l'autre ordinateur. Si vous

essayez de vous connecter à une imprimante partagée, vérifiez avec l'utilisateur de l'autre ordinateur que vous êtes autorisé(e) à vous connecter à l'imprimante.

- L'imprimante connectée à votre ordinateur ou à l'autre ordinateur n'est pas partagée.
- L'imprimante partagée n'a pas été ajoutée à l'ordinateur.

Note
Pour apprendre à gérer le partage d'imprimante (partager une imprimante, définir ou supprimer des permissions pour une imprimante, se connecter à l'imprimante d'un réseau ou à une imprimante partagée) consultez le Centre d'aide et de support de Windows (dans le menu Démarrer, cliquez sur **Aide et Support**).

- L'accès à une imprimante réseau peut être limité à des ordinateurs et des utilisateurs spécifiques uniquement. Consultez l'administrateur réseau pour savoir si vous avez l'autorisation de vous connecter à cette imprimante.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 167).

15.6. Mon Internet est lent

Cette situation peut se produire après l'installation de Bitdefender.Le problème pourrait être causé par des erreurs dans la configuration du pare-feu de Bitdefender.

Pour régler cette situation, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Pare-feu** et cliquez sur le bouton pour le désactiver.
3. Vérifiez si votre connexion Internet s'est améliorée avec le pare-feu Bitdefender désactivé.
   - Si votre connexion à Internet est lente, il est possible que le problème ne soit pas causé par Bitdefender. Nous vous recommandons de contacter votre fournisseur d'accès à Internet afin de vérifier que la connexion fonctionne de son côté.

     Si vous recevez la confirmation de votre fournisseur d'accès à Internet que la connexion est opérationnelle de leur côté et que le problème persiste, contactez Bitdefender comme cela est décrit dans la section « *Demander de l'aide* » (p. 167).
   - Si la connexion Internet s'est améliorée après la désactivation du pare-feu Bitdefender, suivez ces étapes :
     a. Ouvrez la fenêtre de Bitdefender.
     b. Allez dans le panneau **Pare-feu** et cliquez sur le bouton pour l'activer.

c. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.

d. Cliquez sur **Pare-feu** dans le menu de gauche puis sur l'onglet **Configuration**.

e. Allez dans **Partage de connexion Internet** et cliquez sur le bouton pour l'activer.

f. Allez dans **Bloquer les analyses de ports** et cliquez sur le bouton pour le désactiver.

g. Cliquez sur le bouton **Domicile** de la barre d'outils supérieure.

h. Allez dans le panneau **Pare-feu** et cliquez sur **Informations sur le réseau**.

i. Allez dans **Type de Réseau** et sélectionnez **Domicile/Bureau**.

j. Allez dans **Mode Furtif** et réglez-le sur **Distant**. Réglez **Générique** sur **Oui**.

k. Fermez Bitdefender, redémarrez le système et vérifiez la vitesse de la connexion à Internet.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 167).

15.7. Comment mettre à jour Bitdefender avec une connexion Internet lente

Si votre connexion Internet est lente (RTC ou RNIS, par exemple), des erreurs peuvent se produire pendant le processus de mise à jour.

Pour maintenir votre système à jour avec les dernières signatures de malwares Bitdefender, suivez les étapes suivantes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Mise à jour** dans le menu de gauche puis sur l'onglet **Mise à jour**.
4. Sous **Règles de traitement des mises à jour**, sélectionnez **Demander avant le téléchargement**.
5. Cliquez sur le bouton **Domicile** de la barre d'outils supérieure.
6. Allez dans l'onglet **Mise à jour**, et cliquez sur **Mettre à jour maintenant**.
7. Sélectionnez uniquement **Mises à jour de signatures**, puis cliquez sur **OK**.
8. Bitdefender ne téléchargera et n'installera que les mises à jour des signatures de malwares.

15.8. Mon ordinateur n'est pas connecté à Internet. Comment puis-je mettre à jour Bitdefender ?

Si votre ordinateur n'est pas connecté à Internet, vous devez télécharger manuellement les mises à jour sur un ordinateur avec accès Internet, puis les transférer sur votre ordinateur à l'aide d'un dispositif amovible comme une clé USB.

Suivez ces étapes :

1. Sur un ordinateur connecté à Internet, ouvrez le navigateur Web et allez sur :

   http://www.bitdefender.fr/site/view/Desktop-Products-Updates.html

2. Dans la colonne **Mise à jour Manuelle**, cliquez sur le lien correspondant à votre produit et à votre architecture système. Si vous ignorez si votre version de Windows est de 32 ou 64 bits, reportez-vous à « *Est-ce que j'utilise une version de Windows de 32 ou 64 bits ?* » (p. 175).

3. Enregistrez le fichier nommé `weekly.exe` dans le système.

4. Transférez le fichier téléchargé sur un support amovible comme une clé USB, puis sur votre ordinateur.

5. Double-cliquez sur le fichier, puis suivez les étapes de l'assistant.

15.9. Le Services Bitdefender ne répondent pas

Cet article vous aide à régler l'erreur **Les Services Bitdefender ne répondent pas**.Vous pouvez rencontrer cette erreur de la façon suivante :

- L'icône Bitdefender de la zone de notification est grisée et vous informe que les services Bitdefender ne répondent pas.
- La fenêtre Bitdefender indique que les services Bitdefender ne répondent pas.

L'erreur peut être causée par :

- une mise à jour importante est en cours d'installation.
- erreurs de communication temporaires entre les services Bitdefender.
- certains services Bitdefender sont interrompus.
- d'autres solutions de sécurité sont en cours d'exécution sur votre ordinateur en même temps que Bitdefender.

Pour régler cette erreur, essayez ces solutions :

1. Attendez quelques instants et voyez si quelque chose change. L'erreur peut être temporaire.
2. Redémarrez l'ordinateur et attendez quelques instants jusqu'à ce que Bitdefender soit chargé. Ouvrez Bitdefender pour voir si l'erreur persiste.Redémarrer l'ordinateur règle habituellement le problème.

3. Vérifiez que vous n'avez pas d'autre solution de sécurité installée car cela pourrait affecter le fonctionnement normal de Bitdefender. Si c'est le cas, nous vous recommandons de supprimer toutes les autres solutions de sécurité et de réinstaller ensuite Bitdefender.

   Pour plus d'informations, reportez-vous à « *Comment supprimer les autres solutions de sécurité ?* » (p. 174).

Si l'erreur persiste, veuillez contacter les représentants de notre support technique pour obtenir de l'aide, comme indiqué dans la section « *Demander de l'aide* » (p. 167).

15.10. Le filtre antispam ne fonctionne pas correctement

Cet article aide à régler les problèmes suivants avec le filtrage Antispam Bitdefender :

- Certains e-mails légitimes sont signalés comme étant du [spam].
- De nombreux messages de spam ne sont pas signalés comme tels par le filtre antispam.
- Le filtre antispam ne détecte aucun message de spam.

15.10.1. Des messages légitimes sont signalés comme étant du [spam]

Des messages légitimes sont signalés comme étant du [spam] car ils ressemblent à du spam pour le filtre antispam de Bitdefender.Vous pouvez normalement régler ce problème en configurant le filtre Antispam de façon adaptée.

Bitdefender ajoute automatiquement les destinataires de vos e-mails à une Liste d'Amis.Les e-mails que vous recevez des contacts de la Liste d'Amis sont considérés comme légitimes. Ils ne sont pas vérifiés par le filtre antispam et ne sont donc jamais signalés comme étant du [spam].

La configuration automatique de la liste d'Amis n'empêche pas les erreurs de détection pouvant se produire dans les situations suivantes :

- Vous recevez de nombreux e-mails commerciaux sollicités après vous être inscrit(e) sur plusieurs sites Internet.Dans ce cas, la solution est de ne pas ajouter les adresses e-mail des expéditeurs de ces messages à la liste d'Amis.
- Une part importante des e-mails légitimes que vous recevez provient de personnes auxquelles vous n'avez jamais envoyé d'e-mail auparavant, telles que des clients, des partenaires commerciaux potentiels etc.D'autres solutions sont requises dans ce cas.

  1. Si vous utilisez l'un des clients de messagerie dans lesquels Bitdefender s'intègre, indiquez les erreurs de détection.

Note

Bitdefender s'intègre dans la plupart des clients de messagerie via une barre d'outils antispam facile à utiliser.Pour une liste complète des clients de messagerie pris en charge, veuillez vous référer à « *Clients et protocoles de messagerie pris en charge* » (p. 72).

2. Diminuer le niveau de protection de l'antispam. Si vous diminuez le niveau de protection, le filtre antispam aura besoin de plus d'indications pour considérer qu'un e-mail est du spam. Essayez cette solution seulement si de nombreux messages légitimes (y compris des messages commerciaux sollicités) sont détectés à tort comme étant du spam.

Ajouter des contacts à la Liste d'amis

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement ajouter les expéditeurs d'e-mails légitimes à la liste d'Amis. Suivez ces étapes :

1. Dans votre client de messagerie, sélectionnez un e-mail provenant de l'expéditeur que vous voulez ajouter à la liste d'Amis.
2. Cliquez sur le bouton **Ajouter un ami** de la barre d'outils antispam Bitdefender.
3. Il se peut qu'on vous demande de valider les adresses ajoutées à la liste d'Amis. Sélectionnez **Ne plus afficher ce message** et cliquez sur **OK**.

Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.

Si vous utilisez un client de messagerie différent, vous pouvez ajouter des contacts à la liste d'Amis à partir de l'interface de Bitdefender.Suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Antispam**.
3. Cliquez sur **Gérer** et sélectionnez **Amis** dans le menu. Une fenêtre de configuration s'affichera.
4. Tapez l'adresse e-mail à partir de laquelle vous souhaitez toujours recevoir les messages d'e-mail puis cliquez sur **Ajouter**.Vous pouvez ajouter autant d'adresses e-mail que vous le souhaitez.
5. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Indiquer des erreurs de détection

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement corriger le filtre antispam (en indiquant quels e-mails n'auraient pas dû être signalés comme étant du `[spam]`). Cela contribue à améliorer l'efficacité du filtre antispam.Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans le dossier de courrier indésirable dans lequel les messages de spam sont placés.
3. Sélectionnez le message légitime considéré à tort comme étant du [spam] par Bitdefender.
4. Cliquez sur le bouton **Ajouter un ami** de la barre d'outils antispam Bitdefender pour ajouter l'expéditeur à la liste d'Amis.Il se peut que vous ayez besoin de cliquer sur **OK** pour valider.Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.
5. Cliquez sur le bouton **Pas Spam** de la barre d'outils antispam de Bitdefender (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Le message d'e-mail sera placé dans la boîte de réception.

Diminuer le niveau de protection de l'antispam

Pour diminuer le niveau de protection de l'antispam, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Allez dans **Antispam** dans le menu de gauche.
4. Descendez le curseur sur l'échelle.

15.10.2. De nombreux messages de spam ne sont pas détectés

Si vous recevez de nombreux messages de spam qui ne sont pas signalés comme étant du [spam], vous devez configurer le filtre antispam de Bitdefender pour améliorer son efficacité.

Essayez les solutions suivantes :

1. Si vous utilisez l'un des clients de messagerie dans lesquels Bitdefender s'intègre, indiquez les messages de spam non détectés.

   Note

   Bitdefender s'intègre dans la plupart des clients de messagerie via une barre d'outils antispam facile à utiliser.Pour une liste complète des clients de messagerie pris en charge, veuillez vous référer à « *Clients et protocoles de messagerie pris en charge* » (p. 72).

2. Ajouter des spammeurs à la liste des Spammeurs Les messages provenant d'adresses qui figurent dans la liste de Spammeurs seront automatiquement considérés comme étant du [spam].

3. Augmenter le niveau de protection de l'antispam. Si vous augmentez le niveau de protection, le filtre antispam aura besoin de moins d'indications pour considérer qu'un e-mail est du spam.

Indiquer les messages de spam non détectés

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement indiquer quels e-mails auraient dû être détectés comme étant du spam. Cela contribue à améliorer considérablement l'efficacité du filtrage antispam.Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans la boîte de Réception.
3. Sélectionnez les messages de spam non détectés.
4. Cliquez sur le bouton **Spam** de la barre d'outils antispam de Bitdefender(généralement située dans la partie supérieure de la fenêtre du client de messagerie). Les messages sont immédiatement signalés comme étant du `[spam]` et son placés dans le dossier de courrier indésirable.

Ajouter des spammeurs à la Liste des Spammeurs

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement ajouter les expéditeurs de spam à la liste de Spammeurs. Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans le dossier de courrier indésirable dans lequel les messages de spam sont placés.
3. Sélectionnez les messages signalés comme étant du `[spam]` par Bitdefender.
4. Cliquez sur le bouton **Ajouter Spammeur** de la barre d'outils antispam Bitdefender.
5. Il se peut qu'on vous demande de valider les adresses ajoutées à la liste de Spammeurs. Sélectionnez **Ne plus afficher ce message** et cliquez sur **OK**.

Si vous utilisez un client de messagerie différent, vous pouvez ajouter manuellement des spammeurs à la liste de Spammeurs à partir de l'interface de Bitdefender. Cela s'avère utile lorsque vous avez reçu plusieurs e-mails de spam provenant de la même adresse e-mail.Suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Allez dans le panneau **Antispam**.
3. Cliquez sur **Gérer** et sélectionnez **Spammeurs** dans le menu. Une fenêtre de configuration s'affichera.

4. Tapez l'adresse e-mail du spammeur puis cliquez sur **Ajouter**.Vous pouvez ajouter autant d'adresses e-mail que vous le souhaitez.
5. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Augmenter le niveau de protection de l'antispam

Pour augmenter le niveau de protection de l'antispam, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Cliquez sur **Antispam** dans le menu de gauche.
4. Élevez le curseur sur l'échelle.

15.10.3. Le filtre antispam ne détecte aucun message de spam.

Si aucun message de spam n'est signalé comme étant du `[spam]`, il se peut qu'il y ait un problème avec le filtre Antispam de Bitdefender.Avant d'essayer de régler ce problème, assurez-vous qu'il n'est pas causé par l'une des situations suivantes :

- La protection antispam pourrait être désactivée. Pour vérifier l'état de la protection antispam, ouvrez la fenêtre Bitdefender et rendez-vous dans le panneau **Antispam**.

  Si l'Antispam est désactivé, il s'agit de la cause de votre problème.Cliquez sur le bouton pour activer votre protection antispam.

- La protection Bitdefender Antispam est disponible seulement pour les clients de messagerie configurés pour recevoir des e-mails via le protocole POP3.Cela signifie que :

  - Les e-mails reçus via des services de webmail (tels que Yahoo, Gmail, Hotmail ou d'autres) ne font pas l'objet d'une analyse antispam de la part de Bitdefender.
  - Si votre client de messagerie est configuré pour recevoir des e-mails en utilisant un protocole autre que POP3 (par exemple IMAP4), vos e-mails ne seront pas analysés par Bitdefender Antispam.

  Note

  POP3 est l'un des protocoles les plus utilisés pour télécharger des e-mails à partir d'un serveur de messagerie. Si vous ne connaissez pas le protocole que votre client de messagerie utilise pour télécharger des e-mails, posez la question à la personne ayant configuré votre client de messagerie.

- Bitdefender Total Security 2012 n'analyse pas le trafic POP3 de Lotus Notes.

Une solution possible consiste à réparer ou réinstaller le produit. Il est toutefois recommandé de contacter Bitdefender pour obtenir de l'assistance, comme cela est décrit dans la section « *Support* » (p. 166).

15.11. La désinstallation de Bitdefender a échoué

Cet article vous aide à régler les erreurs pouvant se produire lors de la désinstallation de Bitdefender.Deux situations sont possibles :

- Pendant la désinstallation, un écran d'erreur s'affiche. L'écran comporte un bouton permettant de lancer un outil de désinstallation pour nettoyer le système.
- La désinstallation s'interrompt et, éventuellement, votre système se bloque. Cliquez sur **Annuler** pour abandonner la désinstallation. Si cela ne fonctionne pas, redémarrez le système.

Si la désinstallation échoue, certaines clés de registre et fichiers Bitdefender peuvent demeurer sur votre système. De tels restes peuvent empêcher une nouvelle installation de Bitdefender. Ils peuvent aussi affecter la performance du système et sa stabilité.

Afin de désinstaller complètement Bitdefender de votre système, procédez comme suit :

1. Sur http://www.bitdefender.com/uninstall téléchargez l'outil de désinstallation sur votre ordinateur.
2. Lancez l'outil de désinstallation avec les privilèges administrateur.
3. Redémarrez votre ordinateur.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 167).

15.12. Mon système ne démarre pas après l'installation de Bitdefender

Si vous venez d'installer Bitdefender et ne pouvez plus redémarrer votre système en mode normal, il peut y avoir plusieurs raisons à ce problème.

Cela est sans doute dû à une installation précédente de Bitdefender qui n'a pas été désinstallée correctement ou à une autre solution de sécurité toujours présente sur le système.

Voici comment faire face à chaque situation :

- **Vous aviez Bitdefender et vous ne l'avez pas désinstallé correctement.**

  Pour résoudre cela, suivez ces étapes :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, reportez-vous à « *Comment redémarrer en mode sans échec ?* » (p. 175).
2. Désinstallez Bitdefender de votre système :
   a. Sur http://www.bitdefender.com/uninstall téléchargez l'outil de désinstallation sur votre ordinateur.
   b. Lancez l'outil de désinstallation avec les privilèges administrateur.
   c. Redémarrez votre ordinateur.
3. Redémarrez votre système en mode normal et réinstallez Bitdefender.

- **Vous aviez une autre solution de sécurité auparavant et vous ne l'avez pas désinstallée correctement.**

  Pour résoudre cela, suivez ces étapes :

  1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, reportez-vous à « *Comment redémarrer en mode sans échec ?* » (p. 175).
  2. Désinstallez Bitdefender de votre système :
     a. Sur http://www.bitdefender.com/uninstall téléchargez l'outil de désinstallation sur votre ordinateur.
     b. Lancez l'outil de désinstallation avec les privilèges administrateur.
     c. Redémarrez votre ordinateur.
  3. Afin de désinstaller correctement les autres logiciels, allez sur leur site Internet et exécutez leur outil de désinstallation, ou contactez-les directement afin qu'ils vous indiquent la procédure de désinstallation.
  4. Redémarrez votre système en mode normal et réinstallez Bitdefender.

Vous avez déjà suivi les étapes ci-dessus et la situation n'est pas résolue.

Pour résoudre cela, suivez ces étapes :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, reportez-vous à « *Comment redémarrer en mode sans échec ?* » (p. 175).
2. Utilisez l'option Restauration du Système de Windows pour restaurer l'ordinateur à une date antérieure à l'installation du produit Bitdefender.Pour savoir comment faire cela, reportez-vous à « *Comment utiliser la Restauration du Système dans Windows ?* » (p. 176).
3. Redémarrez le système en mode normal et contactez les représentants de notre support technique pour obtenir de l'aide, comme indiqué dans la section « *Demander de l'aide* » (p. 167).

16. Suppression des malwares de votre système

Les malwares peuvent affecter votre système de nombreuses manières et l'approche de Bitdefender dépend du type d'attaque de malware.Les virus changeant souvent de comportement, il est difficile de définir leur comportement et leurs actions.

Il s'agit des situations où Bitdefender ne peut supprimer automatiquement l'infection de malwares de votre système. Dans ce cas, votre intervention est nécessaire.

- « *Mode de Secours de Bitdefender* » (p. 157)
- « *Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ?* » (p. 159)
- « *Comment nettoyer un virus dans une archive ?* » (p. 160)
- « *Comment nettoyer un virus dans une archive de messagerie ?* » (p. 161)
- « *Que faire si je suspecte un fichier d'être dangereux ?* » (p. 162)
- « *Comment nettoyer les fichiers infectés du System Volume Information ?* » (p. 163)
- « *Que sont les fichiers protégés par mot de passe du journal d'analyse ?* » (p. 164)
- « *Que sont les éléments ignorés du journal d'analyse ?* » (p. 164)
- « *Que sont les fichiers ultra-compressés du journal d'analyse ?* » (p. 165)
- « *Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?* » (p. 165)

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du support technique Bitdefender comme indiqué dans le chapitre « *Support* » (p. 166).

16.1. Mode de Secours de Bitdefender

Le **Mode de secours** est une fonctionnalité de Bitdefender qui vous permet d'analyser et de désinfecter toutes les partitions de votre disque dur hors de votre système d'exploitation.

Une fois Bitdefender Total Security 2012 installé, le Mode de Secours peut être utilisé même si vous ne pouvez plus démarrer sous Windows.

Démarrer votre système en Mode de Secours

Vous pouvez entrer en Mode de Secours de l'une des deux façons suivantes :

À partir de la fenêtre de Bitdefender

Pour entrer en Mode de Secours directement à partir de Bitdefender, suivez ces étapes :

1. Allez dans le panneau **Antivirus**.

2. Cliquez sur **Analyser** et sélectionnez **Mode de secours** dans le menu déroulant.

   Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour redémarrer votre ordinateur.

3. Après le redémarrage de l'ordinateur, un menu apparaîtra vous demandant de sélectionner un système d'exploitation. Sélectionnez **Image de Secours de Bitdefender** et appuyez sur la touche **Entrée** pour démarrer dans un environnement Bitdefender vous permettant de nettoyer votre partition Windows.

4. Si cela vous est demandé, cliquez sur **Entrée** et sélectionnez la résolution d'écran la plus proche de celle que vous utilisez habituellement. Puis, cliquez de nouveau sur **Entrée**.

   Le Mode de Secours de Bitdefender se chargera dans quelques instants.

Démarrez votre ordinateur directement en Mode de secours

Si Windows ne démarre plus, vous pouvez démarrer directement votre ordinateur en Mode de Secours Bitdefender en suivant les étapes ci-dessous.

Note

Cette méthode n'est pas disponible pour les ordinateurs fonctionnant sous Windows XP.

1. Démarrez / redémarrez votre ordinateur et appuyez sur la touche **espace** de votre clavier avant que n'apparaisse le logo Windows.

2. Un menu apparaîtra vous demandant de sélectionner un système d'exploitation à démarrer. Cliquez sur **ONGLET** pour vous rendre dans la zone d'outils.Sélectionnez **Image de Secours de Bitdefender** et appuyez sur la touche **Entrée** pour démarrer dans un environnement Bitdefender vous permettant de nettoyer votre partition Windows.

3. Si cela vous est demandé, cliquez sur **Entrée** et sélectionnez la résolution d'écran la plus proche de celle que vous utilisez habituellement. Puis, cliquez de nouveau sur **Entrée**.

   Le Mode de Secours de Bitdefender se chargera dans quelques instants.

Analyser votre système en Mode de Secours

Pour analyser votre système en Mode de Secours, procédez comme suit :

1. Entrez en Mode de Secours, comme indiqué dans « Démarrer votre système en Mode de Secours » (p. 157).

2. Le logo Bitdefender apparaîtra et les moteurs antivirus commenceront à être copiés.

3. Une fenêtre d'accueil apparaîtra. Cliquez sur **Continuer**.
4. Une mise à jour des signatures antivirus a démarré.
5. Une fois la mise à jour terminée, la fenêtre du Scanner Antivirus à la demande Bitdefender s'affiche.
6. Cliquez sur **Analyser**, sélectionnez la cible de l'analyse dans la fenêtre qui s'affiche et cliquez sur **Ouvrir** pour lancer l'analyse.

   Nous vous recommandons l'analyse de la totalité de votre partition Windows.

   Note

   En Mode de Secours, les noms de partitions sont de type Linux. Des partitions de disque apparaîtront, `sda1` correspondant probablement à la partition de type Windows `(C:)`, `sda2` correspondant à `(D:)`, etc.

7. Patientez jusqu'à la fin de l'analyse. Si un malware est détecté, suivez les instructions pour supprimer la menace.
8. Pour quitter le Mode de Secours, faites un clic droit sur une zone vide du Bureau, sélectionnez **Déconnexion** dans le menu qui apparaît puis choisissez de redémarrer ou d'éteindre l'ordinateur.

16.2. Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ?

Il est possible que vous découvriez qu'un virus se trouve sur votre ordinateur de l'une des manières suivantes :

- Vous avez analysé votre ordinateur et Bitdefender y a détecté des éléments infectés.
- Une alerte de virus vous informe que Bitdefender a bloqué un ou plusieurs virus sur votre ordinateur.

Dans de telles situations, mettez à niveau Bitdefender pour vous assurer de disposer des dernières signatures de malwares, puis exécutez une analyse complète du système.

Dès que l'analyse complète est terminée, sélectionnez l'action souhaitée à appliquer aux éléments infectés (Désinfecter, Supprimer, Quarantaine).

Avertissement

Si vous pensez que le fichier fait partie du système d'exploitation Windows ou qu'il ne s'agit pas d'un fichier infecté, ne suivez pas ces étapes et contactez le Service Client de Bitdefender dès que possible.

Si l'action sélectionnée ne peut être appliquée et que le journal d'analyse révèle une infection qui ne peut être supprimée, vous devez supprimer le(s) fichier(s) manuellement :

La première méthode peut être utilisée en mode normal :

1. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Ouvrez la fenêtre de Bitdefender.
   b. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
   c. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Résident**.
   d. Cliquez sur le bouton pour désactiver **l'analyse à l'accès**.
2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, reportez-vous à « *Comment afficher des objets masqués dans Windows ?* » (p. 177).
3. Accédez à l'emplacement du fichier infecté (consultez le journal d'analyse), puis supprimez-le.
4. Activez la protection antivirus en temps réel de Bitdefender.

Si la première méthode ne parvient pas à supprimer l'infection, suivez ces étapes :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, reportez-vous à « *Comment redémarrer en mode sans échec ?* » (p. 175).
2. Afficher les objets masqués dans Windows.
3. Accédez à l'emplacement du fichier infecté (consultez le journal d'analyse), puis supprimez-le.
4. Redémarrez votre système et entrez en mode normal.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 167).

16.3. Comment nettoyer un virus dans une archive ?

Une archive est un fichier ou un ensemble de fichiers compressés sous un format spécial pour réduire l'espace nécessaire sur le disque pour stocker les fichiers.

Certains de ces formats sont des formats ouverts, permettant ainsi à Bitdefender de les analyser, puis de mener les actions appropriées pour les supprimer.

D'autres formats d'archive sont fermés partiellement ou totalement, et Bitdefender peut uniquement détecter la présence de virus dans ceux-ci, mais n'est pas capable de mener d'autres actions.

Si Bitdefender indique qu'un virus a été détecté dans une archive et qu'aucune action n'est disponible, cela signifie qu'il n'est pas possible de supprimer le virus en raison de restrictions sur les paramètres d'autorisation de l'archive.

Voici comment nettoyer un virus stocké dans une archive :

1. Identifiez l'archive où se trouve le virus en réalisant une analyse complète du système.
2. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Ouvrez la fenêtre de Bitdefender.
   b. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
   c. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Résident**.
   d. Cliquez sur le bouton pour désactiver **l'analyse à l'accès**.
3. Rendez-vous à l'emplacement de l'archive et décompressez-la à l'aide d'une application d'archivage, comme WinZip.
4. Identifier le fichier infecté et le supprimer.
5. Supprimez l'archive d'origine afin de vous assurer que l'infection est totalement supprimée.
6. Recompressez les fichiers dans une nouvelle archive à l'aide d'une application d'archivage, comme WinZip.
7. Activez la protection antivirus en temps réel de Bitdefender et exécutez une analyse complète du système afin de vous assurer qu'aucune autre infection n'est présente sur le système.

Note
Il est important de noter qu'un virus contenu dans une archive ne représente pas de menace immédiate pour votre système, puisque, pour infecter votre système, le virus doit être décompressé et exécuté.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 167).

16.4. Comment nettoyer un virus dans une archive de messagerie ?

Bitdefender permet également de repérer les virus dans les bases de données d'e-mails et les archives d'e-mails stockées sur le disque.

Il est parfois nécessaire d'identifier le message infecté à l'aide des informations du rapport d'analyse, et de le supprimer manuellement.

Voici comment nettoyer un virus stocké dans une archive de messagerie électronique :

1. Analysez la base de données des e-mails avec Bitdefender.
2. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Ouvrez la fenêtre de Bitdefender.
   b. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
   c. Cliquez sur **Antivirus** dans le menu de gauche puis sur l'onglet **Résident**.
   d. Cliquez sur le bouton pour désactiver **l'analyse à l'accès**.
3. Ouvrez le rapport d'analyse et utilisez les informations d'identification (Sujet, Expéditeur, Destinataire) des messages infectés pour les localiser dans le client de messagerie.
4. Supprimez les messages infectés.La plupart des clients de messagerie placent les messages supprimés dans un dossier de récupération permettant de les restaurer.Il est recommandé de vous assurer que le message a été supprimé également dans ce dossier de récupération.
5. Compactez le dossier contenant le message infecté.
   - Dans Outlook Express :Dans le menu Fichier, cliquez sur Dossier, puis sur Compacter tous les dossiers.
   - Dans Microsoft Outlook :Dans le menu Fichier, cliquez sur Gestion des fichiers de données.Sélectionnez les dossiers de fichiers personnels (.pst) que vous souhaitez compresser, puis cliquez sur Configuration.Cliquez sur Compacter.
6. Activez la protection antivirus en temps réel de Bitdefender.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 167).

16.5. Que faire si je suspecte un fichier d'être dangereux ?

Vous pouvez suspecter qu'un fichier de votre système est dangereux, même si votre produit Bitdefender ne l'a pas détecté.

Pour vérifier que votre système est protégé, suivez ces étapes :

1. Exécutez une **Analyse complète du système** avec Bitdefender.Pour savoir comment faire cela, reportez-vous à « *Comment analyser mon système ?* » (p. 35).
2. Si le résultat de l'analyse n'indique pas d'infection, mais que vous avez encore des doutes et souhaitez vérifier le fichier, contactez les représentants de notre support technique afin que nous puissions vous aider.

   Pour savoir comment faire cela, reportez-vous à « *Demander de l'aide* » (p. 167).

16.6. Comment nettoyer les fichiers infectés du System Volume Information ?

Le dossier System Volume Information est une zone du disque dur créée par le système d'exploitation et utilisée par Windows pour stocker des informations critiques relatives à la configuration du système.

Les moteurs de Bitdefender permettent de détecter tout fichier infecté stocké par le System Volume Information mais, étant donné que c'est une zone protégée, il est possible qu'il ne puisse pas les supprimer.

Les fichiers infectés détectés dans les dossiers Restauration du Système apparaîtront dans le journal d'analyse comme suit :

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

Pour supprimer complètement et immédiatement le ou les fichiers infectés dans la banque de données, désactivez, puis réactivez la fonction Restauration du Système.

Lorsque la Restauration du Système est désactivée, tous les points de restauration sont supprimés.

Lorsque la Restauration du Système est réactivée, de nouveaux points de restauration sont créés en fonction des besoins de la planification et des événements.

Pour désactiver la restauration du système, procédez comme suit :

- **Pour Windows XP :**
  1. Suivez ce chemin : **Démarrer** → **Tous les programmes** → **Accessoires** → **Outils système** → **Restauration du système**
  2. Cliquez sur **Paramètres de restauration du système** situé à gauche de la fenêtre.
  3. Cochez la case **Désactiver la Restauration du Système** sur tous les lecteurs et cliquez sur **Appliquer**.
  4. Lorsque l'on vous informe que tous les Points de Restauration existants seront supprimés, cliquez sur **Oui** pour continuer.
  5. Pour activer la Restauration du Système, décochez la case **Désactiver la Restauration du Système** sur tous les lecteurs, et cliquez sur **Appliquer**.
- **Pour Windows Vista :**
  1. Suivez ce chemin : **Démarrer** → **Panneau de configuration** → **Système et maintenance** → **Système**
  2. Dans le volet gauche, cliquez sur **Protection du système**.

     Si l'on vous demande un mot de passe administrateur ou une confirmation, saisissez le mot de passe ou confirmez-le.

3. Pour désactiver la Restauration du Système, décochez les cases correspondant à chaque lecteur et cliquez sur **Ok**.
4. Pour activer la Restauration du Système, cochez les cases correspondant à chaque lecteur et cliquez sur **Ok**.

- **Pour Windows 7 :**

1. Cliquez sur **Démarrer**, faites un clic droit sur **Ordinateur**, puis cliquez sur **Propriétés**.
2. Cliquez sur le lien **Protection du système** dans le volet gauche.
3. Dans les options **Protection du système**, sélectionnez chaque lettre des lecteurs, puis cliquez sur **Configurer**.
4. Sélectionnez **Désactiver la protection du système** et cliquez sur **Appliquer**.
5. Cliquez sur **Supprimer**, puis sur **Continuer** lorsqu'on vous le demande et enfin sur **OK**.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 167).

16.7. Que sont les fichiers protégés par mot de passe du journal d'analyse ?

Il ne s'agit que d'une notification qui indique que Bitdefender a détecté que ces fichiers sont soit protégés par un mot de passe soit par une forme de cryptage.

Les éléments protégés par un mot de passe sont généralement :

- Fichiers appartenant à une autre solution de sécurité.
- Fichiers appartenant au système d'exploitation.

Afin que le contenu soit analysé, ces fichiers auront besoin d'être extraits ou décryptés.

Si ce contenu était extrait, le moteur d'analyse en temps réel de Bitdefender l'analyserait automatiquement pour que votre ordinateur reste protégé.Si vous souhaitez analyser ces fichiers avec Bitdefender, vous devez contacter le fabricant du produit afin d'obtenir plus d'informations sur ces fichiers.

Nous vous recommandons d'ignorer ces fichiers car ils ne constituent pas une menace pour votre système.

16.8. Que sont les éléments ignorés du journal d'analyse ?

Tous les fichiers apparaissant comme Ignorés dans le rapport d'analyse sont sains.

Pour de meilleures performances, Bitdefender n'analyse pas les fichiers n'ayant pas été modifiés depuis la dernière analyse.

16.9. Que sont les fichiers ultra-compressés du journal d'analyse ?

Les éléments ultra-compressés sont des éléments qui n’ont pas pu être extraits par le moteur d’analyse ou des éléments dont le temps de décryptage aurait été trop long et aurait rendu le système instable.

Surcompressé signifie que Bitdefender a ignoré l'analyse dans cette archive car sa décompression consommait trop de ressources système. Son contenu sera analysé à l'accès en temps réel si nécessaire.

16.10. Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?

Si un fichier infecté est détecté, Bitdefender tente automatiquement de le désinfecter.Si la désinfection échoue, le fichier est placé en quarantaine afin de contenir l’infection.

Pour certains types de malware, la désinfection n’est pas possible car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

C’est généralement le cas avec les fichiers d’installation qui sont téléchargés depuis des sites non fiables.Si vous vous trouvez dans une telle situation, téléchargez le fichier d'installation sur le site web du fabricant ou sur un autre site de confiance.

17. Obtenir de l'aide

17.1. Support

Bitdefender fait le maximum pour apporter à ses clients une aide hors pair, rapide et efficace.Si vous rencontrez le moindre problème ou si vous avez des questions sur le produit Bitdefender, vous pouvez utiliser plusieurs ressources en ligne pour trouver rapidement une solution ou une réponse.Si vous le préférez, vous pouvez également contacter l'équipe du Service Client de Bitdefender. Nos membres du support technique répondront à vos questions aussi rapidement que possible et vous fourniront l'assistance dont vous avez besoin.

17.1.1. Ressources en ligne

De nombreuses ressources en ligne sont disponibles pour vous aider à résoudre vos questions et problèmes liés à Bitdefender.

- Centre de Support de Bitdefender :http://www.bitdefender.fr/site/KnowledgeBase/supportCenter/
- Forum du Support Bitdefender :http://forum.bitdefender.com
- le portail de sécurité informatique Malware City :http://www.malwarecity.com/fr

Vous pouvez également utiliser votre moteur de recherche favori pour obtenir plus d'informations sur la sécurité informatique, les produits et l'entreprise Bitdefender.

Centre de Support de Bitdefender

Le Centre de Support de Bitdefender est une base en ligne d'informations concernant les produits Bitdefender.Il contient, dans un format facilement accessible, les rapports d'incidents survenus et constatés par le support technique, les équipes de réparation des bugs de Bitdefender. Ainsi que des articles généraux sur la prévention antivirus, la gestion des solutions Bitdefender, des informations détaillées et beaucoup d'autres articles.

Le Centre de Support de Bitdefender est accessible au public et consultable gratuitement.Cet ensemble d'informations est une autre manière de fournir aux clients de Bitdefender les informations techniques dont ils ont besoin.Toutes les requêtes valides d'informations ou de rapports de bugs provenant de clients Bitdefender trouvent une réponse dans le Centre de Support Bitdefender, comme les rapports de corrections de bugs, les solutions de rechange, ou les articles d'informations venant compléter les fichiers d'aide des produits.

Le Centre de Support de Bitdefender est disponible en permanence sur http://www.bitdefender.fr/site/KnowledgeBase/supportCenter/.

Forum du Support Bitdefender

Le Forum du Support Bitdefender fournit aux utilisateurs de Bitdefender une manière simple d'obtenir de l'aide et d'aider les autres.

Si votre produit Bitdefender ne fonctionne pas correctement, s'il ne peut pas supprimer certains virus de votre ordinateur ou si vous avez des questions sur son mode de fonctionnement, exposez votre problème ou posez vos questions sur le forum.

Les techniciens du support Bitdefender surveillent le forum à la recherche de nouveaux messages afin de vous aider. Vous pouvez aussi obtenir une réponse ou une solution grâce à un utilisateur de Bitdefender plus expérimenté.

Avant de publier un problème ou une question, recherchez s'il existe une rubrique similaire ou connexe dans le forum.

Le forum de support de Bitdefender est disponible à http://forum.bitdefender.com, dans 5 langues différentes : français, anglais, allemand, espagnol et roumain.Cliquez sur le lien **Protection des indépendants & des petites entreprises** pour accéder à la section dédiée aux produits de consommation.

Portail Malware City

Le portail Malware City est une riche source d'informations sur la sécurité informatique. Vous y trouverez des articles sur les différentes menaces auxquelles votre ordinateur est exposé lorsqu'il est connecté à Internet (malwares, phishing, spam, cybercriminels).Un dictionnaire vous aide à comprendre les termes de sécurité informatique que vous ne connaissez pas.

De nouveaux articles sont régulièrement publiés pour vous tenir au courant des dernières menaces découvertes, des tendances actuelles en matière de sécurité et vous fournir encore d'autres informations sur le secteur de la sécurité informatique.

La page Web de Malware City est http://www.malwarecity.com/fr.

17.1.2. Demander de l'aide

La section **Résolution des problèmes** vous fournit les informations nécessaires concernant les problèmes les plus fréquents que vous pouvez rencontrer lors de l'utilisation de ce produit.

Si vous ne trouvez pas de solution à votre problème dans les ressources fournies, vous pouvez nous contacter directement :

- « Contactez-nous directement à partir de votre produit Bitdefender » (p. 168)
- « Contactez-nous via notre Centre de Support en ligne » (p. 168)

Important

Pour contacter le Service Client de Bitdefender, vous devez enregistrer votre produit Bitdefender. Pour plus d'informations, reportez-vous à « *Enregistrement du Produit* » (p. 8).

Contactez-nous directement à partir de votre produit Bitdefender

Si vous disposez d'une connexion Internet, vous pouvez contacter l'assistance de Bitdefender directement à partir de l'interface du produit.

Suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le lien **Aide et Support**, situé dans le coin inférieur droit de la fenêtre.
3. Vous disposez des options suivantes :
   - Consultez les articles et les documents pertinents et essayez les solutions proposées.
   - Lancez une recherche dans notre base de données pour trouver les informations qui vous intéressent.
   - Utilisez le bouton **Contacter le support** pour lancer l'Outil Support et contacter le Support Client. Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.
     a. Cochez la case d'accord et cliquez sur **Suivant**.
     b. Compléter le formulaire de soumission avec les données nécessaires :
        i. Saisissez votre adresse e-mail.
        ii. Indiquez votre nom complet.
        iii. Sélectionnez votre pays dans le menu correspondant.
        iv. Décrivez le problème que vous avez rencontré.
     c. Veuillez patienter pendant quelques minutes pendant que Bitdefender recueille les informations sur le produit. Ces informations aideront nos ingénieurs à trouver une solution à votre problème.
     d. Cliquez sur **Terminer** pour envoyer les informations au Service Client de Bitdefender. Nous vous contacterons dès que possible.

Contactez-nous via notre Centre de Support en ligne

Si vous ne parvenez pas à accéder aux informations nécessaires à l'aide du produit Bitdefender, consultez notre Centre de Support en ligne :

1. Allez à http://www.bitdefender.fr/site/KnowledgeBase/supportCenter.Le Centre de Support de Bitdefender contient de nombreux articles apportant des solutions aux problèmes liés à Bitdefender.
2. Sélectionnez votre produit dans la colonne de gauche et recherchez dans le Centre de Support de Bitdefender les articles susceptibles de contenir une solution à votre problème.
3. Consultez les articles et les documents pertinents et essayez les solutions proposées.
4. Si la solution ne permet pas de corriger le problème, utilisez le lien dans l'article pour contacter le Service Client de Bitdefender.
5. Contactez le support technique de Bitdefender par e-mail, par chat ou par téléphone.

17.1.3. Support Technique Editions Profil / Bitdefender

Centre d'Assistance des Laboratoires Technologiques et Scientifiques

Les Laboratoires d'Editions Profil et de Bitdefender assurent un niveau d'assistance sur tous les produits maintenus par l'équipe de développement. La résolution d'un problème peut nous amener à vous proposer de mettre gratuitement à niveau la version de votre produit.

Ce service offre une assistance pour les questions ou problèmes liés à des applications courantes pour l'utilisateur final ou les entreprises, telles que :

- Des configurations personnalisées des produits Bitdefender.
- Des conseils de prise en main en monoposte ou en relation avec des réseaux simples.
- Des problèmes techniques après l'installation des produits Bitdefender.
- Des aides afin de contrer les activités de codes malicieux présents sur un système.
- L'accès à notre site internet de maintenance personnalisée et de FAQ en ligne 24h/24 et 7j/7 : http://www.bitdefender.fr/site/KnowledgeBase/supportCenter/.
- L'accès aux informations des centres de support internationaux, qui permettent de gérer les situations par chat online – Accessible 7j/7 – 365j/an. Pour y accéder, veuillez saisir l'adresse ci-dessous dans votre navigateur : http://www.bitdefender.fr/site/KnowledgeBase/getSupport/. Attention : ce module est un service international, assuré majoritairement en Anglais.

Assistance téléphonique :

Les Laboratoires Editions Profil et Bitdefender mettent en oeuvre tous les efforts commercialement envisageables pour maintenir l'accès à l'assistance téléphonique de ce service, pendant les heures ouvrées locales du lundi au vendredi, sauf pendant les jours fériés.

Accès téléphoniques aux Laboratoires Editions Profil et Bitdefender :

- **Pour la France et les DOM-TOM** : 0892 561 161 (0.34 euros / minute)
- **Pour la Belgique** : 070 35 83 04
- **Pour la Suisse** : 0900 000 118 (0,60 FS / minute)

Avant de nous appeler, munissez-vous :

- du numéro de licence du produit Bitdefender. Communiquez le à un de nos analystes afin qu'il vérifie votre niveau d'assistance.
- de la version actuelle du système d'exploitation.
- des informations sur les marques et modèles de tous les périphériques et des logiciels chargés en mémoire ou utilisés.

En cas d'infection, l'analyste pourra demander une liste d'informations techniques à fournir ainsi que certains fichiers, qui pourront être nécessaires à son diagnostic.

Lorsqu'un analyste vous le demande, précisez les messages d'erreurs reçus et le moment où ils apparaissent, les activités qui ont précédées le message d'erreur et les démarches déjà entreprises pour résoudre le problème.

L'analyste suivra une procédure de dépannage stricte afin de tenter de diagnostiquer le problème.

Le Service n'inclut pas les éléments suivants :

- Ce service d'assistance ne comprend pas les applications, les installations, la désinstallation, le transfert, la maintenance préventive, la formation, l'administration à distance ou configurations logicielles autres que celles spécifiquement notifiées par l'analyste des Laboratoires Editions Profil et Bitdefender lors de l'intervention.
- L'installation, le paramétrage, l'optimisation et la configuration en réseau ou à distance d'applications n'entrant pas dans le cadre de l'assistance actuelle.
- Sauvegarde des logiciels/données. Il incombe au Client d'effectuer une sauvegarde de toutes les données, des logiciels et des programmes existants sur les systèmes d'information pris en charge avant toute prestation de service par Editions Profil et de Bitdefender.

Edtions Profil ou Bitdefender NE PEUVENT ÊTRE TENUS RESPONSABLE DE LA PERTE OU DE LA RÉCUPÉRATION DE DONNÉES, DE PROGRAMMES, OU DE LA PRIVATION DE JOUISSANCE DES SYSTÈME(S) OU DU RÉSEAU.

Les conseils sont strictement limités aux questions demandées et basées sur les informations fournies par le client. Les problèmes et les solutions peuvent dépendre de la nature de l'environnement du système et d'une variété d'autres paramètres qui sont inconnus à Editions Profil ou Bitdefender. Par conséquent, Editions Profil ou Bitdefender ne peuvent en aucun cas être tenus responsable de dommages résultant de l'utilisation de ces informations.

Il est possible que l'état du système sur lequel les produits Bitdefender doivent être installés soit instable (infection préalable, installation d'antivirus ou solutions de sécurité multiples, etc.). Dans ces cas précis, il est possible que l'analyste vous propose une prestation de maintenance auprès de votre revendeur avant de pouvoir régler votre problème.

Les informations techniques peuvent changer lorsque des nouvelles données deviennent disponibles, par conséquent, Editions Profil et Bitdefender recommandent que vous consultiez régulièrement notre site "Produits" à l'adresse suivante : http://www.bitdefender.fr pour des mises à jour, ou notre site internet de FAQ à l'adresse http://www.bitdefender.fr/site/KnowledgeBase/supportCenter/.

Tout dommage direct, indirect, spécial, accidentel ou conséquent en relation avec l'usage des informations fournies ne peuvent pas être imputés à Editions Profil et Bitdefender.

Si une intervention sur site est nécessaire, l'analyste vous donnera de plus amples instructions concernant votre revendeur le plus proche.

17.2. Nous contacter

Une communication efficace est la clé d'une relation réussie. Au cours des dix dernières années, BITDEFENDER s'est bâti une réputation incontestable dans sa recherche constante d'amélioration de la communication pour dépasser les attentes de ses clients et de ses partenaires. N'hésitez pas à nous contacter pour toute question que vous pourriez avoir.

17.2.1. Adresses Web

Ventes : bitdefender@editions-profil.eu
Centre de support :http://www.bitdefender.fr/site/KnowledgeBase/supportCenter/
Documentation : documentation@bitdefender.com
Distributeurs locaux : http://www.bitdefender.fr/partners/
Programme de partenariat : partners@bitdefender.com
Relations médias : pr@bitdefender.com
Emplois : jobs@bitdefender.com
Soumissions de virus : virus_submission@bitdefender.com
Envoi de spams : spam_submission@bitdefender.com
Signaler un abus : abuse@bitdefender.com
Site Web : http://www.bitdefender.com

17.2.2. Distributeurs locaux

Les distributeurs locaux Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux.

Pour trouver un distributeur Bitdefender dans votre pays :

1. Allez à http://www.bitdefender.fr/partners/.
2. Les coordonnées des distributeurs locaux de Bitdefender devraient s'afficher automatiquement. Si ce n'est pas le cas, sélectionnez votre pays de résidence pour afficher ces informations.
3. Si vous ne trouvez pas de distributeur Bitdefender dans votre pays, n'hésitez pas à nous contacter par e-mail à l'adresse bitdefender@editions-profil.eu.Merci de nous contacter par email pour optimiser le traitement de votre demande.

17.2.3. Bureaux de Bitdefender

Les bureaux de Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux. Leur adresse respective et contacts sont listés ci-dessous.

France

Editions Profil
49, Rue de la Vanne
92120 Montrouge
Téléphone : +33 (0)1 47 35 72 73
Ventes : bitdefender@editions-profil.eu
Support technique : http://www.bitdefender.fr/site/Main/nousContacter
Site Web : http://www.bitdefender.fr

U.S.A

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Téléphone (services administratif et commercial) : 1-954-776-6262
Ventes : sales@bitdefender.com
Support technique : http://www.bitdefender.com/help/
Site Web : http://www.bitdefender.com

Royaume-Uni et Irlande

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
E-mail : info@bitdefender.co.uk
Téléphone : +44 (0) 8451-305096
Ventes : sales@bitdefender.co.uk
Support technique : http://www.bitdefender.co.uk/site/KnowledgeBase/supportCenter
Site Web : http://www.bitdefender.co.uk

Allemagne

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Service administratif : +49 2301 91 84 0
Ventes : vertrieb@bitdefender.de
Support technique : http://kb.bitdefender.de
Site Web : http://www.bitdefender.de

Espagne

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Fax : +34 93 217 91 28
Téléphone : +34 902 19 07 65
Ventes : comercial@bitdefender.es
Support technique : http://www.bitdefender.es/ayuda
Site Web : http://www.bitdefender.es

Roumanie

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax : +40 21 2641799
Téléphone du service commercial : +40 21 2063470
Email du service commercial : sales@bitdefender.ro
Support technique : http://www.bitdefender.ro/suport
Site Web : http://www.bitdefender.ro

18. Informations utiles

Ce chapitre présente certaines des procédures les plus importantes à connaître avant de commencer à résoudre un problème technique.

Le dépannage d'un problème technique dans Bitdefender nécessite quelques notions de Windows, c'est pourquoi les prochaines étapes concernent principalement le système d'exploitation Windows.

- « *Comment supprimer les autres solutions de sécurité ?* » (p. 174)
- « *Comment redémarrer en mode sans échec ?* » (p. 175)
- « *Est-ce que j'utilise une version de Windows de 32 ou 64 bits ?* » (p. 175)
- « *Comment utiliser la Restauration du Système dans Windows ?* » (p. 176)
- « *Comment afficher des objets masqués dans Windows ?* » (p. 177)

18.1. Comment supprimer les autres solutions de sécurité ?

La principale raison à l'utilisation d'une solution de sécurité est d'assurer la protection et la sécurité de vos données. Mais qu'arrive-t-il quand vous avez plus d'un produit de sécurité sur le même système ?

Lorsque vous utilisez plusieurs solutions de sécurité sur le même ordinateur, le système devient instable. Le programme de désinstallation de Bitdefender Total Security 2012 détecte d'autres programmes de sécurité et vous permet de les désinstaller.

Si vous n'avez pas supprimé les autres solutions de sécurité au cours de l'installation initiale, suivez ces étapes :

- Pour **Windows XP** :
  1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Ajout/Suppression de programmes**.
  2. Patientez quelques instants jusqu'à ce que la liste des logiciels installés s'affiche.
  3. Trouvez le nom du programme que vous souhaitez supprimer, puis sélectionnez **Supprimer**.
  4. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
- Pour **Windows Vista** et **Windows 7** :
  1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
  2. Patientez quelques instants jusqu'à ce que la liste des logiciels installés s'affiche.

3. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
4. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

Si vous ne parvenez pas à supprimer l'autre solution de sécurité de votre système, obtenez l'outil de désinstallation sur le site web de l'éditeur ou contactez-les directement afin qu'ils vous indiquent la procédure de désinstallation.

18.2. Comment redémarrer en mode sans échec ?

Le mode sans échec est un mode de fonctionnement de diagnostic, utilisé principalement pour résoudre des problèmes affectant le fonctionnement normal de Windows. Ce type de problèmes peut intervenir lors de conflits de drivers et de virus empêchant Windows de démarrer normalement.En Mode sans échec, seules quelques applications fonctionnent et Windows ne charge que les pilotes de base et un minimum de composants du système d'exploitation.C'est pourquoi la plupart des virus sont inactifs lorsque Windows est en Mode sans échec et qu'ils peuvent être supprimés facilement.

Pour démarrer Windows en Mode sans échec :

1. Redémarrer votre système.
2. Appuyez plusieurs fois sur la touche **F8** avant que Windows ne démarre afin d'accéder au menu de démarrage.
3. Sélectionnez **Mode sans échec** dans le menu de démarrage ou **Mode sans échec avec prise en charge réseau** si vous souhaitez avoir accès à Internet.
4. Cliquez sur **Entrée** et patientez pendant que Windows se charge en Mode sans échec.
5. Ce processus se termine avec un message de confirmation. Cliquez sur **OK** pour valider.
6. Pour démarrer Windows normalement, il suffit de redémarrer le système.

18.3. Est-ce que j'utilise une version de Windows de 32 ou 64 bits ?

Pour savoir si vous disposez d'un système d'exploitation de 32 ou de 64 bits, suivez les étapes suivantes :

- Pour **Windows XP** :
  1. Cliquez sur **Démarrer**.
  2. Recherchez **Poste de travail** dans le menu **Démarrer**.
  3. Faites un clic droit sur **Poste de Travail**, puis sélectionnez **Propriétés**.

4. Si **Edition x64** est indiqué sous **Système**, c'est que vous exécutez la version 64 bits de Windows XP.

   Si **Edition x64** ne s'affiche pas, c'est que vous utilisez une version 32 bits de Windows XP.

- Pour **Windows Vista** et **Windows 7** :

  1. Cliquez sur **Démarrer**.
  2. Repérez **Ordinateur** dans le menu **Démarrer**.
  3. Faites un clic droit sur **Ordinateur** et sélectionnez **Propriétés**.
  4. Reportez-vous à ce qui est indiqué sous **Système** afin de vérifier les informations concernant votre système.

18.4. Comment utiliser la Restauration du Système dans Windows ?

Si vous ne pouvez pas démarrer l'ordinateur en mode normal, lancez le Mode sans échec et utilisez la Restauration du système pour restaurer un moment où vous pouviez démarrer l'ordinateur sans erreurs.

Pour effectuer la Restauration du Système, vous devez être connecté à Windows en tant qu'administrateur.

Pour utiliser la restauration du système, suivez ces étapes :

- Dans Windows XP :

  1. Se connecter à Windows en Mode sans échec.
  2. Suivez le chemin suivant à partir du menu démarrer de Windows : **Démarrer → Tous les programmes → Outils système → Restauration du système**.
  3. Sur la page **Bienvenue dans la Restauration du système**, cliquez pour sélectionner l'option **Restaurer mon ordinateur à une date antérieure**, puis cliquez sur Suivant.
  4. Suivez les étapes de l'assistant et vous devriez pouvoir démarrer le système en mode normal.

- Pour Windows Vista et Windows 7 :

  1. Se connecter à Windows en Mode sans échec.
  2. Suivez le chemin suivant à partir du menu démarrer de Windows : **Tous les programmes → Accessoires → Outils système → Restauration du système**.
  3. Suivez les étapes de l'assistant et vous devriez pouvoir démarrer le système en mode normal.

18.5. Comment afficher des objets masqués dans Windows ?

Ces étapes sont utiles en cas de malwares, si vous avez besoin de détecter et de supprimer les fichiers infectés, qui peuvent être cachés.

Suivez ces étapes pour afficher les objets cachés dans Windows :

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et sélectionnez **Options des dossiers**.
2. Allez dans l'onglet **Afficher**.
3. Sélectionnez **Afficher le contenu des dossiers système** (pour Windows XP uniquement).
4. Sélectionnez **Afficher les fichiers et les dossiers cachés**.
5. Effacez **Masquer les extensions de fichier pour les types de fichier connus**.
6. Décochez **Masquer les fichiers protégés du système d'exploitation**.
7. Cliquez sur **Appliquer** puis sur **Ok**.

Glossaire

ActiveX

ActiveX est un modèle pour écrire des programmes tels que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour faire des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent demander ou répondre à des questions, utiliser des boutons et interagir d'autres façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic.

Active X est connu pour son manque total de commandes de sécurité ; les experts en sécurité informatique déconseillent son utilisation sur Internet.

Adware

Les adwares sont souvent associés à des applications gratuites ce qui implique leur acceptation par l'utilisateur. Ces adwares étant généralement installés après que l'utilisateur en a accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant les « pop up » publicitaires peuvent devenir contrariant et dans certains cas dégrader les performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui ne s'étaient pas complètement rendu compte des termes de l'accord de licence.

Applette Java

Il s'agit d'un programme Java conçu pour s'exécuter seulement dans une page Web. Pour utiliser un applet dans une page Web, vous devez spécifier le nom de l'applet et la taille (la longueur et la largeur - en pixels) qu'il peut utiliser. Lors d'un accès à la page Web, le navigateur télécharge l'applet depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applets diffèrent des applications par le fait qu'ils sont régis par un protocole de sécurité strict.

Par exemple, bien que les applets s'exécutent sur le client, ils ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les applets sont également limités pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.

Archive

Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés.

Un fichier qui contient un ou plusieurs fichiers dans un format compressé.

Backdoor

Il s'agit d'une faille dans la sécurité d'un système délibérément laissé en place par des développeurs ou mainteneurs. La motivation n'est pas toujours négative ; quelques logiciels permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Chemin

Les directions exactes vers un fichier. Ces directions sont décrites d'habitude par arborescence, de haut en bas.

La connexion entre deux points, telle le canal de communication entre deux ordinateurs.

Client de messagerie

Un client de messagerie est un logiciel qui vous permet d'envoyer et recevoir des messages (e-mails).

Cookies

Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une épée à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent (vous voyez seulement des annonces vous intéressant) mais d'autre part, cela implique en réalité "le pistage" et "le suivi" d'où vous allez et de ce sur quoi vous cliquez sur Internet. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple " numéro SKU " (vous savez, le code barres à l'arrière des produits). Bien que ce point de vue puisse paraître extrême, dans certains cas cette perception est justifiée.

Disk drive

C'est une appareil qui lit et écrit des données sur un disque.

Une unité de disque dur lit et écrit sur un disque dur.

Un lecteur de disquette accède à des disquettes.

Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).

E-mail

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

Événements

Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme l'analyse de la mémoire.

Extension de fichier

La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier.

De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS Dos. Elles comportent communément une à trois lettres (certains vieux OS ne supportent pas plus de trois). Exemples : "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

Fausse alerte

Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.

Fichier journal (Log)

Un fichier qui enregistre les actions qui surviennent. Bitdefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.

Heuristique

Méthode permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique est de pouvoir détecter des variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

IP

Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP chargé de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Keylogger

Application qui enregistre tout ce qui est tapé.

Les keyloggers ne sont pas nécessairement malveillants. Ils peuvent être utilisés à des fins légitimes, comme pour surveiller les activités d'employés ou d'enfants. Ils sont toutefois de plus en plus utilisés par des cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion et des numéros de sécurité sociale).

Ligne de commande

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

Mémoire

Zone de stockage interne dans votre ordinateur. Le terme mémoire regarde le stockage des données dans les "chips" (composants), et le terme stockage regarde les disques. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

Mise à jour

Une nouvelle version du logiciel ou d'un produit hardware, destinée à remplacer une ancienne version du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, sinon la mise à jour ne se fait pas.

Bitdefender a son propre module de mise à jour permettant à l'utilisateur de vérifier manuellement les mises à jour ou de les programmer automatiquement.

Navigateur

Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les deux navigateurs les plus populaires sont Netscape Navigator et Microsoft Internet Explorer. Les deux sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plugins) pour certains formats.

Non-heuristique

Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut paraître un virus et ne génère donc pas de fausses alertes.

Objets menu démarrage

Tous les fichiers placés dans ce dossier s'ouvrent au démarrage. Par exemple, un écran de démarrage, un fichier son pour quand l'ordinateur démarre, un calendrier, des programmes, peuvent être placées dans ce dossier. D'habitude c'est un raccourci vers le fichier qui est mis dans le dossier, et pas le fichier.

Phishing

Action d'envoyer un e-mail à un utilisateur en prétendant être une entreprise connue dans le but d'obtenir frauduleusement des informations privées qui permettront d'utiliser l'identité du destinataire du mail. Cet e-mail dirige l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables

entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

Port

Une interface de l'ordinateur à laquelle vous pouvez connecter un périphérique. Les PCs comportent plusieurs sortes de ports. A l'intérieur, il y a quelques ports pour la connexion des disques, cartes vidéo. A l'extérieur, les PCs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Programmes empaquetés

Un fichier comprimé. Beaucoup de plates-formes et applications contiennent des commandes vous permettant de comprimer un fichier pour qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide". Normalement, cela nécessite 10 octets.

Pourtant, un logiciel qui comprime les fichiers remplace la série d'espaces par un caractère spécial série d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. C'est juste une technique de compression, il y en a une multitude.

Rootkit

Un rootkit est un ensemble d'outils logiciels permettant aux administrateurs d'accéder à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs systèmes.

Le principale rôle des rootkits est de cacher des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseaux, s'ils incluent les logiciels appropriés.

Les Rootkits ne sont pas malveillants par nature. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler des codes malveillants ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des codes malveillants, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, corrompre des fichiers et des logs et éviter leur détection.

Scripts

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

Secteur de boot

Un secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge la plate-forme.

Signature de virus

La "signature" binaire du virus, utilisé par l'antivirus pour la détection et l'élimination du virus.

Spam

Message électronique ou envoi de messages souvent répertoriés comme des emails « non sollicités ».

Spyware

Tout type de logiciel qui récupère secrètement les informations des utilisateurs au travers de leur connexion Internet sans les avertir, généralement à des fins publicitaires. Les spywares sont généralement cachés dans des logiciels shareware ou freeware qui peuvent être téléchargés sur Internet. Cependant, la majorité des applications shareware ou freeware ne comportent pas de spyware. Après son installation, le spyware surveille l'activité de l'utilisateur sur Internet et transmet discrètement des informations à une tierce personne. Les spywares peuvent également récupérer des informations sur les adresses mail, les mots de passe ou même les numéros de cartes de crédit.

Leur point commun avec les Chevaux de Troie est que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une de manière les plus classique pour être victime de spywares est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d'éthique et de respect de la vie privée, les spywares volent aussi les ressources de l'ordinateur de l'utilisateur en utilisant de la bande passante lors de l'envoi d'information au travers de sa connexion Internet. A cause de cette utilisation de la mémoire et des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu'à entraîner des plantages ou provoquer une instabilité globale du système.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés avec divers architectures hardware et diverses plates-formes. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Télécharger

Copier des données (généralement un fichier entier) d'une source principale à un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.

Trojan (Cheval de Troie)

Un programme destructif qui prétend être une application normale. Les Trojans ne sont pas des virus et ne se repliquent pas, mais peuvent être tout aussi destructifs. Un des types les plus répandu de Trojans est un logiciel prétendant désinfecter votre PC (mais au lieu de faire cela il l'infecte).

Le terme provient de la fameuse histoire de l'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Trojans, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Ver

Un programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure qu'il se propage. Il ne peut pas s'attacher aux autres programmes.

Virus

Programme ou morceau de code qui est chargé dans votre ordinateur sans que vous le sachiez et fonctionne contre votre gré. La plupart des virus peuvent se répliquer. Tous les virus sont créés par des personnes. Un virus simple capable de se copier continuellement est relativement facile à créer. Même un virus simple de ce type est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est capable de se transmettre via un réseau et d'échapper aux systèmes de sécurité.

Virus de boot

Un virus qui infecte le secteur de boot d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus de boot rendra le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.

Virus Macro

Un type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent des langages macro.

Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.

Virus polymorphique

Un virus qui change de forme avec chaque fichier qu'il infecte. Comme ils n'ont pas une forme unique bien définie, ces virus sont plus difficiles à identifier.

Zone de notification

Introduite avec Windows 95, la zone de notification se situe dans la barre de tâches Windows (en général, à côté de l'horloge) et contient des icônes miniatures permettant d'accéder facilement aux fonctions système : fax, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.