

TOTAL
SECURITY 2013



Bitdefender®

Manuel d'utilisation

Bitdefender Total Security 2013

Bitdefender Total Security 2013 *Manuel d'utilisation*

Date de publication 10/07/2012

Copyright© 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 tests 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 l'élaboration de ce document, ses auteurs ne sauraient être tenus pour responsables envers toute personne ou entité des pertes ou dommages directs ou indirects consécutifs à l'utilisation des informations qu'il contient.

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 d'un 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.



Table des matières

Installation	1
1. Préparation de l'installation	2
2. Configuration requise	3
2.1. Configuration système minimale	3
2.2. Configuration système recommandée	3
2.3. Configuration logicielle requise	3
3. Scénarios d'installation	4
4. Installer votre produit Bitdefender	5
Introduction	11
5. Les fondamentaux	12
5.1. Ouverture de la fenêtre de Bitdefender	12
5.2. Correction des problèmes en cours	12
5.2.1. Assistant de Correction des Problèmes	13
5.2.2. Configurer les alertes d'état	14
5.3. Événements	15
5.4. Auto-Pilot	16
5.5. Mode Jeu et Mode Portable	17
5.5.1. Mode Jeu	17
5.5.2. Mode Portable	19
5.6. Paramètres Bitdefender de la protection par mot de passe	19
5.7. Rapports d'utilisation anonymes	20
6. Interface de Bitdefender	21
6.1. Icône de la zone de notification	21
6.2. Fenêtre principale	22
6.2.1. Barre d'outils supérieure	23
6.2.2. Panneaux	24
6.3. Fenêtre Aperçu des paramètres	28
6.4. Widget Windows	29
6.4.1. Analyse des fichiers et des dossiers	31
6.4.2. Masquer / afficher le Widget Windows	31
7. Enregistrer Bitdefender	32
7.1. Saisie de votre clé de licence	32
7.2. Acheter ou renouveler des clés de licence	32
8. Compte MyBitdefender	34
8.1. Lier l'ordinateur à MyBitdefender	35
9. Maintenir Bitdefender à jour	37
9.1. Vérifier que Bitdefender est à jour	37
9.2. Mise à jour en cours	38
9.3. Activer ou désactiver la mise à jour automatique	38

9.4. Réglage des paramètres de mise à jour	39
Comment	41
10. Installation	42
10.1. Comment installer Bitdefender sur un deuxième ordinateur ?	42
10.2. Quand devrais-je réinstaller Bitdefender ?	42
10.3. Comment passer d'un produit Bitdefender 2013 à un autre ?	42
11. Enregistrement	44
11.1. Quel est le produit Bitdefender que j'utilise ?	44
11.2. Comment enregistrer une version d'essai ?	44
11.3. Quand ma protection Bitdefender expire-t-elle ?	44
11.4. Comment enregistrer Bitdefender sans connexion Internet ?	45
11.5. Comment renouveler ma protection Bitdefender ?	45
12. Analyser avec Bitdefender	47
12.1. Comment analyser un fichier ou un dossier ?	47
12.2. Comment analyser mon système ?	47
12.3. Comment créer une tâche d'analyse personnalisée ?	47
12.4. Comment exclure un dossier de l'analyse ?	48
12.5. Que faire lorsque Bitdefender a détecté un fichier sain comme étant infecté ?	49
12.6. Comment connaître les virus détectés par Bitdefender ?	50
13. Contrôle Parental	51
13.1. Comment protéger mes enfants des menaces sur Internet ?	51
13.2. Comment limiter l'accès à Internet pour mon enfant ?	51
13.3. Comment empêcher mon enfant d'accéder à un site web ?	52
13.4. Comment empêcher mon enfant de jouer à un jeu ?	53
13.5. Comment créer des comptes utilisateurs Windows ?	53
14. Vie privée	55
14.1. Comment vérifier que ma transaction en ligne est sécurisée ?	55
14.2. Que faire si mon système a été volé ?	55
14.3. Comment protéger mon compte Facebook ?	56
14.4. Comment utiliser les coffres-forts ?	56
14.5. Comment supprimer définitivement un fichier avec Bitdefender ?	58
15. Optimisation	59
15.1. Comment améliorer les performances de mon système ?	59
15.1.1. Défragmentez votre disque dur	59
15.1.2. Nettoyez votre PC	59
15.1.3. Nettoyer le Registre Windows	60
15.1.4. Analysez votre système régulièrement	60
16. Sauvegarde en ligne de SafeBox	61
16.1. Comment accéder à mes fichiers sauvegardés depuis un autre ordinateur ?	61
16.2. Comment partager des fichiers avec mes amis ?	61
16.3. Où voir l'espace restant sur ma Safebox ?	61
16.4. Comment libérer de l'espace sur Safebox ?	62

17. Informations Utiles	63
17.1. Comment éteindre automatiquement l'ordinateur une fois l'analyse terminée ?	63
17.2. Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?	63
17.3. Est-ce que j'utilise une version de Windows de 32 ou 64 bits ?	65
17.4. Comment afficher des objets masqués dans Windows ?	65
17.5. Comment supprimer les autres solutions de sécurité ?	66
17.6. Comment utiliser la Restauration du Système dans Windows ?	66
17.7. Comment redémarrer en mode sans échec ?	67

Gérer votre sécurité

69

18. Protection antivirus	70
18.1. Analyse à l'accès (protection en temps réel)	71
18.1.1. Activer ou désactiver la protection en temps réel	71
18.1.2. Régler le niveau de protection en temps réel	72
18.1.3. Configurer les paramètres de protection en temps réel	72
18.1.4. Restauration des paramètres par défaut	76
18.2. Analyse à la demande	76
18.2.1. Auto Scan	77
18.2.2. Rechercher des malwares dans un fichier ou un dossier	77
18.2.3. Exécuter une Analyse Rapide	77
18.2.4. Exécuter une Analyse du Système	78
18.2.5. Configurer une analyse personnalisée	78
18.2.6. Assistant d'analyse antivirus	81
18.2.7. Consulter les journaux d'analyse	84
18.3. Analyse automatique de supports amovibles	85
18.3.1. Comment cela fonctionne-t-il ?	85
18.3.2. Gérer l'analyse des supports amovibles	86
18.4. Configurer des exceptions d'analyse	87
18.4.1. Exclure de l'analyse des fichiers ou des dossiers	87
18.4.2. Exclure de l'analyse des extensions de fichiers	88
18.4.3. Gérer les exceptions d'analyse	89
18.5. Gérer les fichiers en quarantaine	89
18.6. Active Virus Control	90
18.6.1. Vérifier des applications détectées	90
18.6.2. Activer ou désactiver Active Virus Control	91
18.6.3. Régler la protection Active Virus Control	91
18.6.4. Gérer les processus exclus	92
18.7. Corriger les vulnérabilités du système	93
18.7.1. Analyser votre système à la recherche de vulnérabilités	93
18.7.2. Utiliser la surveillance des vulnérabilités automatique	94
19. Antispam	97
19.1. Aperçu de l'antispam	98
19.1.1. Filtres AntiSpam	98
19.1.2. Fonctionnement de l'Antispam	99
19.1.3. Mises à jour de l'antispam	100
19.1.4. Clients et protocoles de messagerie pris en charge	100

19.2. Activer ou désactiver la protection antisпам	100
19.3. Utilisation de la barre d'outils Antisпам dans la fenêtre de votre client de messagerie	101
19.3.1. Indiquer des erreurs de détection	102
19.3.2. Indiquer les messages de spam non détectés	102
19.3.3. Configurer les paramètres de la barre d'outils	103
19.4. Configurer la liste d'amis	103
19.5. Configurer la liste des spammeurs	104
19.6. Régler le niveau de sensibilité	106
19.7. Configurer les filtres antisпам locaux	106
19.8. Configurer la détection "in-the-cloud"	107
20. Vie privée	108
20.1. Protection antiphishing	108
20.1.1. Protection Bitdefender dans le navigateur web	110
20.1.2. Alertes Bitdefender dans le navigateur	111
20.2. Cryptage de Messagerie Instantanée	111
20.3. Cryptage de fichiers	112
20.3.1. Gérer des coffres-forts à partir de l'interface de Bitdefender	112
20.3.2. Gérer les coffres-forts depuis Windows	117
20.4. Supprimer définitivement des fichiers	121
21. Pare-feu	123
21.1. Activer ou désactiver la protection pare-feu	124
21.2. Gérer les paramètres de connexion	124
21.3. Gérer les règles de pare-feu	125
21.3.1. Règles générales	125
21.3.2. Règles d'applications	126
21.3.3. Règles d'adaptateurs	129
21.4. Surveiller l'activité du réseau	130
21.5. Configurer l'intensité de l'alerte	131
21.6. Configurer les paramètres avancés	132
21.6.1. Système de détection d'intrusion	132
21.6.2. D'autres options	132
22. Transactions en ligne sécurisées par Safepay	134
22.1. Utiliser Bitdefender Safepay	134
22.2. Configuration des paramètres	135
22.3. Gérer les marque-pages	135
22.4. Protection hotspot pour les réseaux non sécurisés	136
23. Contrôle Parental	137
23.1. Accéder au tableau de bord du Contrôle Parental	137
23.2. Ajouter le profil de votre enfant	138
23.2.1. Surveiller les activités de l'enfant	138
23.2.2. Configurer les notifications par e-mail	139
23.3. Configuration du Contrôle Parental	139
23.3.1. Contrôle Web	140
23.3.2. Contrôle des Programmes	141
23.3.3. Protection Facebook	142
23.3.4. Contrôle des Messageries Instantanées	142

24. Protection Safego pour réseaux sociaux	144
25. Antivol de l'appareil	146
26. Bitdefender USB Immunizer	148
27. Gérer vos ordinateurs à distance	149
27.1. Accéder à MyBitdefender	149
27.2. Exécuter des tâches sur les ordinateurs	149
Optimisation et sauvegarde	151
28. Optimisation	152
28.1. Nettoyage de votre PC	152
28.2. Défragmenter des volumes de disque dur	153
28.3. Rechercher les doublons	154
28.4. Nettoyer le Registre Windows	155
28.5. Restauration du registre nettoyé	156
28.6. Analyseur de Performances	157
29. Sauvegarde et synchronisation en ligne de Safebox	158
29.1. Activation de Safebox	158
29.2. Gérer Safebox à partir de la fenêtre de Bitdefender	159
29.3. Gérer Safebox à partir de Windows	160
29.3.1. Ajouter des dossiers à Safebox	160
29.3.2. Supprimer des dossiers de la Safebox	160
29.3.3. Restauration des fichiers supprimés de SafeBox	160
29.4. Gérer Safebox depuis MyBitdefender	161
29.5. Synchroniser des fichiers entre vos ordinateurs	161
29.6. Mise à niveau de votre espace en ligne	162
29.7. Supprimer définitivement des fichiers	162
29.8. Limiter l'allocation de bande passante	163
Résolution des problèmes	164
30. Résoudre les problèmes les plus fréquents	165
30.1. Mon système semble lent	165
30.2. L'analyse ne démarre pas	166
30.3. Je ne peux plus utiliser une application	167
30.4. Je ne peux pas me connecter à Internet	168
30.5. Je ne peux pas accéder à un périphérique de mon réseau	168
30.6. Mon Internet est lent	170
30.7. Comment mettre à jour Bitdefender avec une connexion Internet lente ...	171
30.8. Mon ordinateur n'est pas connecté à Internet. Comment actualiser Bitdefender?	172
30.9. Le Services Bitdefender ne répondent pas	172
30.10. Le filtre antispam ne fonctionne pas correctement	173
30.10.1. Des messages légitimes sont signalés comme étant du [spam]	173
30.10.2. De nombreux messages de spam ne sont pas détectés	175
30.10.3. Le filtre antispam ne détecte aucun message de spam.	177
30.11. La désinstallation de Bitdefender a échoué	178

30.12. Mon système ne démarre pas après l'installation de Bitdefender	178
31. Suppression des malwares de votre système	181
31.1. Mode de Secours de Bitdefender	181
31.2. Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ?	183
31.3. Comment nettoyer un virus dans une archive ?	184
31.4. Comment nettoyer un virus dans une archive de messagerie ?	185
31.5. Que faire si je suspecte un fichier d'être dangereux ?	186
31.6. Comment nettoyer les fichiers infectés du System Volume Information ? ...	187
31.7. Que sont les fichiers protégés par mot de passe du journal d'analyse ?	188
31.8. Que sont les éléments ignorés du journal d'analyse ?	188
31.9. Que sont les fichiers ultra-compressés du journal d'analyse ?	189
31.10. Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?	189
Nous contacter	190
32. Demander de l'aide	191
32.1. Support Technique Editions Profil / Bitdefender	192
33. Ressources en ligne	195
33.1. Centre de Support de Bitdefender	195
33.2. Forum du Support Bitdefender	195
33.3. Portail Malware City	196
34. Nous contacter	197
34.1. Adresses Web	197
34.2. Distributeurs locaux	197
34.3. Bureaux de Bitdefender	197
Glossaire	200

Installation

1. Préparation de l'installation

Avant d'installer Bitdefender Total Security 2013, 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. 3).
- 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 des fichiers d'applications du package d'installation sont disponibles, Bitdefender peut les télécharger et les installer.

2. Configuration requise

Vous pouvez installer Bitdefender Total Security 2013 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
- Windows 8

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.

2.1. 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)

2.2. 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

2.3. 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 3.5 (automatiquement installé avec Bitdefender si manquant)

3. Scénarios d'installation

Nouvelle installation

Il n'y a pas de version antérieure de Bitdefender installée sur l'ordinateur. Dans ce cas, procédez selon les instructions fournies dans « *Installer votre produit Bitdefender* » (p. 5).

Mettre à niveau l'installation

Une version antérieure est déjà installée sur l'ordinateur et vous mettez à niveau vers Bitdefender 2013. Dans ce cas, la version antérieure doit être désinstallée avant l'installation.

Par exemple, pour désinstaller Bitdefender 2012 avant d'installer Bitdefender Total Security 2013 :

1. Suivez le chemin suivant à partir du menu démarrer de Windows : **Démarrer** → **Tous les programmes** → **Bitdefender 2012** → **Réparer ou Supprimer**.
2. Sélectionnez **Supprimer**.
3. Veuillez attendre que Bitdefender termine l'action que vous avez sélectionnée. Cela peut prendre quelques minutes.
4. Redémarrez l'ordinateur pour terminer le processus.

Si vous ne désinstallez pas la version antérieure avant de commencer l'installation de Bitdefender Total Security 2013, vous serez invité à le faire au début du processus d'installation. Suivez les instructions pour terminer la désinstallation de la version antérieure.

4. 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.fr/Downloads/>.

Si votre achat protège plus d'un ordinateur (si, par exemple, vous avez acheté Bitdefender Total Security 2013 pour 3 PC), répétez le processus d'installation et enregistrez votre produit avec la clé de licence sur chaque ordinateur.

- Pour installer Bitdefender à partir du disque d'installation, insérez le disque dans le lecteur optique. Un écran d'accueil s'affiche peu après. Suivez les instructions pour démarrer 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, utilisez l'Explorateur Windows pour aller 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.

Validation de l'installation

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

Le package d'installation de Bitdefender Total Security 2013 est constamment mis à jour. Si vous effectuez l'installation depuis un CD/DVD, Bitdefender peut télécharger

les dernières versions des fichiers pendant l'installation. Cliquez sur **Oui** lorsqu'on vous y invite afin de permettre à Bitdefender de télécharger les fichiers, ce qui vous garantit d'installer la dernière version du logiciel.



Note

Le téléchargement des fichiers d'installation peut prendre longtemps, en particulier sur des connexions Internet plus lentes.

Une fois l'installation validée, l'assistant de configuration apparaîtra. Suivez les étapes pour installer Bitdefender Total Security 2013.

Étape 1 - Bienvenue

L'écran d'accueil vous permet de choisir le type d'installation que vous souhaitez effectuer.

Pour une installation sans complications, cliquez simplement sur le bouton **Installer**. Bitdefender sera installé dans l'emplacement par défaut avec les paramètres par défaut et vous passerez directement à l'**Étape 3** de l'assistant.

Si vous souhaitez configurer les paramètres d'installation, sélectionnez **Je souhaite personnaliser mon installation** puis cliquez sur **Installer** pour passer à l'étape suivante.

Deux tâches supplémentaires peuvent être réalisées au cours de cette étape :

- Veuillez lire l'Accord de Licence Utilisateur Final avant de procéder à l'installation. L'Accord de Licence contient les termes et conditions d'utilisation de Bitdefender Total Security 2013.

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

- Activer l'envoi de **Rapports d'Utilisation Anonymes**. 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.

Étape 2 - Personnaliser les paramètres d'installation



Note

Cette étape apparaît uniquement si vous avez choisi de personnaliser l'installation lors de l'étape précédente.

Voici les options proposées :

Chemin d'installation

Par défaut, Bitdefender Total Security 2013 sera installé dans C:\Program Files\Bitdefender\Bitdefender 2013. Si vous souhaitez choisir un autre répertoire, cliquez sur **Modifier** et choisissez le répertoire d'installation de Bitdefender.

Définir Paramètres proxy

Bitdefender Total Security 2013 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.

Cliquez sur **Installer avec les paramètres personnalisés** pour confirmer vos préférences et commencer l'installation.

Étape 3 - Installation en cours

Patiencez 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 - Installation terminée

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.

Vous pouvez fermer la fenêtre, ou poursuivre la configuration initiale de votre logiciel en cliquant sur **Pour commencer**.

Étape 5 - Enregistrer votre produit



Note

Cette étape apparaît uniquement si vous avez sélectionné **Pour commencer** à l'étape précédente.

Pour terminer l'enregistrement de votre produit, vous devez saisir une clé de licence. 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 Bitdefender 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. 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 le produit**.

Cliquez sur **Suivant**.

Étape 6 - Configurer le comportement du produit

Bitdefender peut être configuré pour gérer automatiquement votre sécurité en permanence ou dans certaines conditions. Utilisez les boutons pour activer ou désactiver **Auto-Pilot**, **Mode Portable automatique** et **Mode Jeu automatique**.

Activez l'Auto-Pilot pour une sécurité complètement silencieuse. Lorsqu'Auto-Pilot est activé, Bitdefender prend pour vous toutes les décisions liées à la sécurité et vous n'avez rien à configurer. Pour plus d'informations, reportez-vous à *« Auto-Pilot » (p. 16)*.

Si vous jouez régulièrement à des jeux, activez le Mode Jeu Automatique : ainsi, Bitdefender détectera les jeux que vous lancerez et entrera en Mode Jeu, en modifiant ses paramètres afin que son impact sur les performances de votre système demeure minime. Pour plus d'informations, reportez-vous à *« Mode Jeu » (p. 17)*.

Pour les utilisateurs d'ordinateurs portables, l'activation du Mode Portable Automatique fera passer Bitdefender en mode portable lorsqu'il détectera que votre ordinateur portable est alimenté par sa batterie, modifiant ses paramètres afin que l'impact sur la consommation de sa batterie soit minime. Pour plus d'informations, reportez-vous à « *Mode Portable* » (p. 19).

Cliquez sur **Suivant**.

Étape 7 - Configurer les filtres de connexion

Vous pouvez sélectionner ici les filtres de connexion à activer. Il s'agit des filtres qui veillent activement à ce que vous soyez protégé pendant vos activités en ligne et lorsque vous êtes connecté à des réseaux.

Utilisez les boutons pour activer / désactiver :

- Antispam
- Pare-feu
- Antimalware Web
- Antiphishing
- Antifraude
- Search Advisor

Vous pouvez activer ou désactiver les filtres à tout moment après l'installation depuis l'interface de Bitdefender. Pour obtenir le meilleur niveau de protection, nous vous recommandons d'activer tous les filtres.

Activez le filtre Antispam uniquement si vous utilisez un client de messagerie configuré pour recevoir des e-mails via le protocole POP3.

Cliquez sur **Suivant**.

Étape 8 - Connexion à MyBitdefender

Un compte MyBitdefender est nécessaire pour utiliser les fonctionnalités en ligne de votre produit. Pour plus d'informations, reportez-vous à « *Compte MyBitdefender* » (p. 34).

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.

- **E-mail** - indiquez votre adresse e-mail.
- **Nom d'utilisateur** - indiquez un nom d'utilisateur pour votre compte.
- **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.



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 <https://myaccount.bitdefender.com/fr/MyAccount/login/>.

3. Cliquez sur **Créer**.
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.

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. Sélectionnez le service que vous souhaitez utiliser. 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 demandera de saisir le mot de passe pour vous connecter à ce compte.

Si vous avez déjà un compte actif, mais que Bitdefender ne le détecte pas, ou si vous voulez simplement vous connecter à un compte différent, saisissez son adresse e-mail et son mot de passe et cliquez sur **Se connecter à MyBitdefender**.

Remettre à plus tard

Si vous souhaitez remettre cette tâche à plus tard, cliquez sur **Plus tard**. N'oubliez pas que vous devez vous connecter à un compte pour utiliser les fonctions en ligne du produit.

Introduction

5. Les fondamentaux

Une fois Bitdefender Total Security 2013 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).

Vous pouvez lancer l'**Auto-Pilot** pour bénéficier d'une sécurité complètement silencieuse 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. 15).

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, pensez à le faire avant la fin de la période d'essai. Pour plus d'informations, reportez-vous à « **Enregistrer Bitdefender** » (p. 32).

Pour utiliser les fonctionnalités en ligne de Bitdefender Total Security 2013, veuillez à lier votre ordinateur à un compte MyBitdefender. Pour plus d'informations, reportez-vous à « **Compte MyBitdefender** » (p. 34).

Si vous rencontrez des problèmes lors de l'utilisation de Bitdefender, recherchez dans la section « **Résoudre les problèmes les plus fréquents** » (p. 165) des solutions possibles aux problèmes les plus courants. La section « **Comment** » (p. 41) vous fournit des instructions pas à pas pour effectuer les tâches courantes.

5.1. Ouverture de la fenêtre de Bitdefender

Pour accéder à l'interface principale de Bitdefender Total Security 2013, utilisez le menu Démarrer de Windows en suivant le chemin d'accès **Démarrer** → **Tous les programmes** → **Bitdefender 2013** → **Bitdefender Total Security 2013** 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. 21).

5.2. 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 :

B Couleur rouge : Des problèmes critiques affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.

B Couleur 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.

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.

5.2.1. 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 **B** (indiquant des problèmes critiques) ou jaune **B** (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.

5.2.2. Configurer les alertes d'état

Bitdefender peut vous avertir lorsque des problèmes sont détectés lors du fonctionnement des composants de programmes suivants :

- Pare-feu
- Antispam
- Antivirus
- Mise à jour
- BitDefender Browser Security

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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Général**.
4. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Avancé**.
5. Cliquez sur le lien **Configurer les alertes d'état**.
6. Cliquez sur les boutons pour activer ou désactiver les alertes d'état en fonction de vos préférences.

5.3. Événements

Bitdefender tient un journal détaillé des événements concernant son activité sur votre ordinateur. Lorsqu'un événement concernant la sécurité de votre système ou de vos données a lieu, un nouveau message est ajouté aux Événements de Bitdefender, comme lorsqu'un nouvel e-mail arrive dans votre boîte de réception.

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 accéder au journal des Événements, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur les **Événements** sur la barre d'outils supérieure pour ouvrir la fenêtre **Aperçu des événements**.

Les messages sont regroupés en fonction du module Bitdefender dont ils sont liés à l'activité :

- **Antivirus**
- **Antispam**
- **Vie privée**
- **Pare-feu**
- **Optimisation**
- **Safebox**
- **Mise à jour**
- **Safego**
- **Cryptage de Fichiers**

Les **Compteurs d'événements** s'affichent dans l'interface de Bitdefender pour permettre d'identifier facilement les zones avec des événements importants. Il s'agit d'icônes apparaissant sur certains modules et indiquant le nombre d'événements critiques non lus liés à l'activité d'un module.

Par exemple, s'il y a un événement critique non lu lié à l'activité du module Mise à jour, l'icône  apparaît sur le panneau Mise à jour.

Un compteur indiquant le nombre total de messages non lus de l'ensemble des modules apparaît sur le bouton Événements de la fenêtre principale.

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 **Avertissement** signalent des problèmes non critiques. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
- Les événements **critiques** signalent 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.

5.4. Auto-Pilot

Pour les utilisateurs qui souhaitent que leur solution de sécurité les protège sans les interrompre, Bitdefender Total Security 2013 dispose d'un mode d'Auto-Pilot intégré.

En Auto-Pilot, 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 Auto-Pilot Bitdefender corrige automatiquement les problèmes critiques, active et gère silencieusement :

- 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.

Pour activer ou désactiver l'Auto-Pilot, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur le bouton **Mode Manuel / Auto-Pilot** sur la barre d'outils supérieure. Quand le bouton est sur la position Mode Manuel, l'Auto-Pilot est désactivé.

Tant que l'Auto-Pilot est activé, l'icône Bitdefender de la zone de notification est .



Important

Lorsque l'Auto-Pilot 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 l'Auto-Pilot était en cours, ouvrez la fenêtre **Événements**.

5.5. 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 2013 comprend deux modes de fonctionnement spéciaux :

- **Mode Jeu**
- **Mode Portable**

5.5.1. Mode Jeu

Le Mode Jeu modifie temporairement les paramètres de protection afin de minimiser leur impact sur les performances du système. Les paramètres suivants s'appliquent lorsque le Mode Jeu est activé :

- Toutes les alertes et fenêtres pop-up Bitdefender sont désactivées.
- L'**analyse à l'accès** est réglée sur le niveau de protection **Tolérant**.
- Auto Scan est désactivé. Auto Scan détecte et utilise les moments pendant lesquels la consommation des ressources du système passe sous un certain seuil pour effectuer des analyses régulières 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 de **Safebox** 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**.
- Activer à l'aide du **raccourci clavier** du 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.

Raccourci clavier du Mode Jeu

Pour définir et utiliser un raccourci clavier pour entrer en / quitter le Mode Jeu, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Général**.
4. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Général**.
5. Vérifiez que le bouton raccourci clavier du Mode Jeu est activé.
6. Configurez la combinaison souhaitée :

- a. La combinaison par défaut est Ctrl+Alt+Shift+G.

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 le raccourci, désactivez le bouton **Raccourci clavier du 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Général**.

4. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Général**.
5. Activez ou désactivez le mode jeu automatique en cliquant sur le bouton correspondant.

5.5.2. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Général**.
4. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Général**.
5. 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.

5.6. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Général**.
4. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Général**.
5. Activez la protection par mot de passe en cliquant sur le bouton.

6. Cliquez sur le lien **Changer de mot de passe**.
7. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Général**.
4. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Général**.
5. Désactivez la protection par mot de passe en cliquant sur le bouton. Entrez le mot de passe puis cliquez sur **OK**.

5.7. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Général**.
4. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Avancé**.
5. Cliquez sur le bouton pour désactiver les rapports d'utilisation anonymes.

6. Interface de Bitdefender

Bitdefender Total Security 2013 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 donne accès à d'importantes informations sur le produit, aux modules du programme et vous permet d'effectuer des tâches courantes. La fenêtre principale vous permet d'accéder à la **fenêtre paramètres** pour une configuration détaillée et des tâches d'administration avancée, et la fenêtre **Événements** permet d'accéder à un journal précis de l'activité de Bitdefender.

Si vous souhaitez garder en permanence un œil sur les informations de sécurité essentielles et disposer d'un accès rapide aux principaux paramètres, ajoutez le **Widget Window** à votre bureau.

6.1. 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.



Note

Si vous utilisez Windows Vista ou Windows 7, l'icône de Bitdefender ne sera peut-être pas visible en permanence. Pour que l'icône soit présente en permanence, procédez comme suit :

1. Cliquez sur la flèche  dans l'angle inférieur droit de l'écran.
2. Cliquez sur **Personnaliser...** pour ouvrir la fenêtre Icônes de la Zone de Notification.
3. Sélectionnez l'option **Afficher les icônes et les notifications** pour l'icône **Agent Bitdefender**.

Double-cliquez sur cette icône pour ouvrir Bitdefender. Un clic droit sur l'icône donne également accès à un menu contextuel qui vous permettra de rapidement administrer le produit Bitdefender.

- **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. 12).



- **Activer / désactiver le Mode Jeu** - active / désactive le **Mode Jeu**.
- **Afficher / Masquer le Widget Windows** - permet d'activer / de désactiver le **Widget Windows**.
- **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 :

B Des problèmes critiques affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.

B 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.

B Le produit fonctionne en **Mode jeu**.

B L'**Auto-Pilot** de Bitdefender est activé.

Si Bitdefender ne fonctionne pas, l'icône de la zone de notification apparaît sur un fond gris : **B**. 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.

6.2. 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 configurer le 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.

Le menu déroulant de **MyBitdefender** en haut de la fenêtre vous permet de gérer votre compte et d'accéder aux fonctionnalités en ligne de votre produit depuis le tableau de bord du compte.

Vous trouverez plusieurs liens utiles dans la partie inférieure de la fenêtre. Ces liens sont également accessibles dans les fenêtres **Événements** et **Paramètres**.

Lien	Description
Nombre de jours restants	Le temps restant avant l'expiration de votre licence actuelle est indiqué. Cliquez sur le lien pour ouvrir une fenêtre dans laquelle vous pouvez voir plus d'informations sur votre clé de licence ou enregistrer votre produit avec une nouvelle clé de licence.
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.
Aide et Support	Cliquez sur ce lien si vous avez besoin d'aide avec Bitdefender. Une nouvelle fenêtre apparaîtra vous permettant d'ouvrir l'aide du produit, d'aller dans le Centre de Support ou de contacter le support.
	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.

6.2.1. 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 la 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 **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. 12).

- **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. 15).
- **Configuration** vous permet d'accéder à une fenêtre où vous pouvez configurer les paramètres du produit. Pour plus d'informations, reportez-vous à « *Fenêtre Aperçu des paramètres* » (p. 28).
- **Auto-PilotMode Manuel** vous permet de lancer l'Auto-Pilot et de profiter d'une sécurité totalement silencieuse. Pour plus d'informations, reportez-vous à « *Auto-Pilot* » (p. 16).

6.2.2. Panneaux

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

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

Tous les panneaux du module contiennent les éléments suivants :

- Le nom du module et un message d'état.
- Une icône  est disponible dans l'angle supérieur droit de la plupart des panneaux. Cliquer dessus vous dirige directement vers la fenêtre des paramètres avancés de ce module.
- L'icône du module.

S'il y a des événements liés à l'activité d'un module que vous n'avez pas encore lus, un compteur d'événements s'affichera à côté de l'icône du module. Par exemple, s'il y a un événement non lu lié à l'activité du module Mise à jour, l'icône

 apparaît sur le panneau Mise à jour. Cliquez sur le compteur pour aller directement à la fenêtre Événements de ce module.

- 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.

Vous pouvez organiser les panneaux comme vous le souhaitez, en procédant comme suit :

1. Cliquez sur  à gauche du curseur sous les panneaux pour ouvrir la fenêtre Aperçu des Modules.
2. Faites glisser les panneaux de modules individuels et déposez-les à d'autres emplacements pour réorganiser la zone en fonction de vos besoins.
3. Cliquez sur  pour revenir à la fenêtre principale.

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 **Auto Scan** 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. 70).

Antispam

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

La protection Antispam n'est pas activée par défaut. Les composants du module sont installés la première fois que vous activez ce module avec le bouton Antispam.

Une fois le module activé, vous pouvez cliquer sur **Gérer** dans le panneau Antispam et sélectionner Amis ou Spammeurs dans le menu déroulant pour modifier la liste d'adresses correspondante.

Pour plus d'informations sur la configuration de la protection antispam, reportez-vous à « *Antispam* » (p. 97).

Confidentialité

Le module Protection 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 **Configurer** du panneau Protection Vie Privée et sélectionnez une tâche dans le menu déroulant :

- **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 « *Vie privée* » (p. 108).

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 **Activité du réseau** dans le panneau Pare-feu, vous pouvez configurer les paramètres généraux de connexion des cartes 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. 123).

Optimisation

Bitdefender Total Security 2013 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. 152).

Safebox

Safebox vous permet de sauvegarder vos fichiers importants sur des serveurs en ligne sécurisés, de les synchroniser entre vos appareils et de les partager avec vos amis.

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

- **Gérer les dossiers** - permet d'ajouter, de supprimer et de synchroniser les dossiers Safebox.
- **Gérer les fichiers partagés** - permet de partager des fichiers en les téléchargeant dans Safebox et en créant des liens accessibles de partout.
- **Aller au Tableau de bord** - permet de gérer vos sauvegardes Safebox directement à partir du tableau de bord MyBitdefender de votre navigateur web.

Le bouton Sync. Auto. vous permet d'activer ou de désactiver la synchronisation automatique des dossiers Safebox.

Pour plus d'informations, reportez-vous à « *Sauvegarde et synchronisation en ligne de Safebox* » (p. 158).

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 « *Maintenir Bitdefender à jour* » (p. 37).

Safego

Pour vous aider à profiter des réseaux sociaux en toute sécurité, vous pouvez accéder à Safego, la solution de sécurité Bitdefender pour réseaux sociaux, directement à partir de Bitdefender Total Security 2013.

Cliquez sur le bouton **Gérer** du panneau Safego et sélectionnez une tâche dans le menu déroulant :

- **Activer pour Facebook** dans votre compte MyBitdefender. Si Safego a déjà été activé, vous pouvez accéder à des statistiques sur son activité en cliquant sur **Rapports Facebook** dans le menu.
- **Activer pour Twitter** dans votre compte MyBitdefender. Si Safego a déjà été activé, vous pouvez accéder à des statistiques sur son activité en cliquant sur **Rapports Twitter** dans le menu.

Pour plus d'informations, reportez-vous à « *Protection Safego pour réseaux sociaux* » (p. 144).

Cryptage de Fichiers

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.

Cliquez sur le bouton **Coffre-fort** du panneau Cryptage de Fichiers et sélectionnez une tâche dans le menu déroulant :

- **Ajouter au coffre-fort** - lance un assistant vous permettant d'ajouter vos fichiers importants à un coffre-fort sécurisé, crypté.
- **Supprimer du coffre-fort** - lance un assistant qui vous permet de supprimer des fichiers d'un coffre-fort.
- **Afficher le coffre-fort** - lance un assistant qui vous permet d'afficher le contenu d'un coffre-fort.
- **Verrouiller le coffre-fort** - lance un assistant qui vous permet de verrouiller un coffre-fort.

6.3. Fenêtre Aperçu des paramètres

La fenêtre Aperçu des paramètres vous donne accès aux paramètres avancés de votre produit. Vous pouvez configurer ici Bitdefender en détail.

Sélectionnez un module pour configurer ses paramètres ou effectuer des tâches de sécurité ou 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.

Vie privée

Vous permet d'éviter les fuites de données et de protéger votre vie privée lorsque vous êtes en ligne. Configurez la protection de votre navigateur web, de vos logiciels de messagerie instantanée, créez des règles de 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.

Optimisation

Vous permet de surveiller les performances de votre ordinateur et de garder un œil sur la consommation de ressources.

Safebox

Vous permet de sauvegarder des données importantes sur des serveurs en ligne sécurisés, de synchroniser des fichiers entre vos appareils et de partager des fichiers avec vos amis.

Mise à jour

Vous permet de configurer en détail le processus de mise à jour.

Cryptage de Fichiers

Vous permet de créer et de gérer des disques cryptés où vous pouvez conserver des données sensibles en toute sécurité.

Pour revenir à la **fenêtre principale**, cliquez sur  dans l'angle supérieur gauche de la fenêtre.

6.4. Widget Windows

Le **Widget Windows** est une façon simple et rapide de surveiller et de contrôler Bitdefender Total Security 2013. Ajouter ce petit widget discret à votre bureau vous permet de voir des informations critiques et d'effectuer des tâches essentielles à tout moment :

- surveiller l'activité d'analyse en temps réel.
- surveiller l'activité du pare-feu en temps réel.
- surveiller l'état de sécurité de votre système et corriger tout problème existant.

- afficher des notifications et accéder aux derniers événements signalés par Bitdefender.
- accès à votre compte MyBitdefender en un clic.
- analyser des fichiers ou des dossiers en glissant-déposant un ou plusieurs éléments sur le widget.



Widget Windows

L'état de sécurité global de votre ordinateur s'affiche **au centre** du widget. L'état est indiqué par la couleur et la forme de l'icône qui s'affiche dans cette zone.



Des problèmes critiques affectent la sécurité de votre système.

Ils requièrent votre attention immédiate et doivent être réglés dès que possible. Cliquez sur l'icône d'état pour commencer à corriger les problèmes signalés.



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. Cliquez sur l'icône d'état pour commencer à corriger les problèmes signalés.



Votre système est protégé.



Lorsqu'une tâche d'analyse à la demande est en cours, cette icône animée apparaît.

Lorsque des problèmes sont signalés, cliquez sur l'icône d'état pour lancer l'assistant de correction des problèmes.

Le bouton **à gauche** du widget vous fournit un accès direct à la fenêtre des paramètres du Pare-feu, et présente également une représentation graphique en temps réel de l'activité du pare-feu. Lorsqu'une barre bleue apparaît sur ce bouton, cela signifie que le module pare-feu filtre activement les connexions réseau. Plus la barre bleue est haute, plus l'activité de ce module est intense.

La partie supérieure du widget affiche le compteur d'événements non lus (le nombre d'événements importants signalés par Bitdefender, s'il y en a). Cliquez sur le compteur d'événements, par exemple  pour un événement non lu, pour ouvrir

la fenêtre Aperçu des événements. Pour plus d'informations, reportez-vous à « *Événements* » (p. 15).

Le bouton **à droite** du widget vous fournit un accès direct à la fenêtre des paramètres Antivirus, et présente également une représentation graphique en temps réel de l'activité d'analyse. Quand une barre bleue apparaît sur ce bouton, elle indique qu'une activité d'analyse antivirus en temps réel est en cours. Plus la barre bleue est haute, plus l'activité de ce module est intense.

Le bouton **dans la partie inférieure** du widget lance le panneau de configuration de votre compte MyBitdefender dans une fenêtre de navigateur web. Pour plus d'informations, reportez-vous à « *Compte MyBitdefender* » (p. 34).

6.4.1. Analyse des fichiers et des dossiers

Vous pouvez utiliser le Widget Windows pour analyser rapidement des fichiers et des dossiers. Faites glisser tout fichier ou dossier que vous souhaitez analyser et déposez-le sur le **Widget Windows**.

L'**Assistant d'analyse antivirus** s'affichera et vous guidera au cours du processus d'analyse. Les options d'analyse sont déjà configurées pour que la détection soit la meilleure possible et ne peuvent pas être modifiées. Si des fichiers infectés sont détectés, Bitdefender essaiera de les désinfecter (de supprimer les codes malveillants). Si la désinfection échoue, l'Assistant d'analyse antivirus vous proposera d'indiquer d'autres moyens d'intervenir sur les fichiers infectés.

6.4.2. Masquer / afficher le Widget Windows

Lorsque vous ne souhaitez plus voir le widget, cliquez sur .

Pour restaurer le Widget Windows, procédez comme suit :

1. Faites un clic droit sur l'icône de Bitdefender dans la zone de notification.
2. Cliquez sur **Afficher le Widget Windows** dans le menu contextuel qui apparaît.

7. Enregistrer Bitdefender

Pour bénéficier de la protection de Bitdefender, vous devez enregistrer votre logiciel avec une clé de licence. 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. 32). 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.

7.1. 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.

Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender. Cliquez sur ce lien pour ouvrir la fenêtre d'enregistrement.

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 2013 :

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**.

Même après avoir acheté une clé de licence, tant que l'enregistrement du produit avec la clé ne sera pas terminé, Bitdefender Total Security 2013 continuera à apparaître comme une version d'évaluation.

7.2. 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 indiquant le nombre de jours restants à votre licence, situé en bas de la fenêtre Bitdefender, pour ouvrir la fenêtre d'enregistrement du produit.
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.

8. Compte MyBitdefender

Les fonctionnalités en ligne de votre produit et les services supplémentaires de Bitdefender sont disponibles exclusivement via MyBitdefender. Vous devez lier votre ordinateur à MyBitdefender en vous connectant à un compte depuis Bitdefender Total Security 2013 afin d'effectuer l'une des actions suivantes :

- Récupérez votre clé de licence, si jamais vous la perdez.
- Configurer les paramètres du **Contrôle Parental** pour les comptes Windows de vos enfants et surveiller leurs activités où que vous soyez.
- Sauvegardez et synchronisez vos fichiers importants sur des serveurs en ligne sécurisés à l'aide de **Safebox**.
- Protégez vos comptes Facebook et Twitter avec **Safego**.
- Protégez votre ordinateur et vos données contre le vol et la perte avec **Antivol**.
- Gérer Bitdefender Total Security 2013 **à distance**.

Plusieurs solutions de sécurité Bitdefender pour PC et d'autres plateformes s'intègrent à MyBitdefender. Vous pouvez gérer la sécurité de tous les appareils liés à votre compte depuis un seul tableau de bord centralisé.

Votre compte MyBitdefender est accessible depuis tout appareil connecté à Internet sur <https://myaccount.bitdefender.com/fr/MyAccount/login/>.

Vous pouvez également accéder à votre compte et le gérer directement depuis votre produit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur **MyBitdefender** en haut de la fenêtre et sélectionnez une option dans le menu déroulant :
 - **Paramètres du compte**
Se connecter à un compte, créer un nouveau compte, configurer le comportement de MyBitdefender.
 - **Tableau de bord**
Lancez le tableau de bord de MyBitdefender dans votre navigateur.
 - **Contrôle Parental**
Surveiller et contrôler l'utilisation de l'ordinateur faite par vos enfants.
 - **Anti-Theft**
Protégez votre ordinateur et vos données contre la perte et le vol.

8.1. Lier l'ordinateur à MyBitdefender

Pour lier votre ordinateur à un compte MyBitdefender, vous devez vous connecter à un compte depuis Bitdefender Total Security 2013. Tant que votre ordinateur ne sera pas lié à MyBitdefender, vous devrez vous connecter à MyBitdefender à chaque fois que vous souhaitez utiliser une fonctionnalité nécessitant un compte.

Pour ouvrir la fenêtre MyBitdefender à partir de laquelle vous pouvez créer ou vous connecter à un compte, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur **MyBitdefender** en haut de la fenêtre puis sélectionnez **Paramètres du compte** dans le menu déroulant.

Si vous êtes déjà connecté à un compte, le compte auquel vous êtes connecté s'affiche. Cliquez sur **Aller à MyBitdefender** pour aller dans votre tableau de bord. Pour changer le compte lié à l'ordinateur, choisissez de vous connecter à un autre compte.

Si vous ne vous êtes pas connecté à un compte, procédez en fonction de 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.
 - **E-mail** - indiquez votre adresse e-mail.
 - **Nom d'utilisateur** - indiquez un nom d'utilisateur pour votre compte.
 - **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.
3. Cliquez sur **Créer**.
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.

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 avez déjà un compte mais ne vous y êtes pas encore connecté, suivez les étapes suivantes pour vous y connecter :

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 **Se connecter à MyBitdefender**.

Une fois l'ordinateur lié à un compte, vous pouvez utiliser l'adresse e-mail et le mot de passe fournis pour vous connecter à <https://myaccount.bitdefender.com/fr/MyAccount/login/>.

Vous pouvez également accéder à votre compte directement à partir de Bitdefender Total Security 2013 à l'aide du menu déroulant en haut de la fenêtre.

9. Maintenir Bitdefender à jour

De nouveaux virus sont trouvés et identifiés chaque jour. 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. Par défaut, des mises à jour sont recherchées au démarrage de votre ordinateur puis toutes les **heures** après cela. 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. 63).
- 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 actualiser Bitdefender?* » (p. 172). 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. 171).
- 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. 38).

9.1. 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. Sur le panneau **Mise à jour**, recherchez l'heure de la dernière mise à jour 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. Dans la fenêtre **Aperçu des événements**, cliquez sur **Mise à jour**.

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.

9.2. 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 de Bitdefender et cliquez sur **Mettre à jour maintenant** dans le panneau **Mettre à jour**.
- 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. Il est recommandé de le faire dès que possible.

9.3. 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. Dans le panneau **Mise à jour**, cliquez sur le bouton **Automatique**.
3. Une fenêtre d'avertissement s'affiche. Vous devez confirmer votre choix en sélectionnant dans le menu pour combien de temps 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.

9.4. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Mise à jour**.
4. Dans la fenêtre **Paramètres des mises à jour**, ajustez 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).

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.

Comment

10. Installation

10.1. Comment installer Bitdefender sur un deuxième ordinateur ?

Si vous avez acheté une clé de licence pour plusieurs ordinateurs, vous pouvez utiliser la même clé de licence pour enregistrer un deuxième PC.

Pour installer Bitdefender correctement sur un second ordinateur, suivez les étapes suivantes :

1. Installez Bitdefender à partir du CD/DVD ou à l'aide du programme d'installation fourni dans l'e-mail d'achat en ligne et suivez les mêmes étapes d'installation.
2. Lorsque la fenêtre d'enregistrement apparaît, saisissez la clé de licence et cliquez sur **S'enregistrer**.
3. À l'étape suivante, vous avez la possibilité de vous connecter à votre compte MyBitdefender ou de créer un nouveau compte MyBitdefender.
Vous pouvez également choisir de créer un compte MyBitdefender ultérieurement.
4. Attendez la fin du processus d'installation et fermez la fenêtre.

10.2. 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://myaccount.bitdefender.com/fr/MyAccount/login/>. Tapez l'adresse e-mail et le mot de passe de votre compte dans les champs correspondants.

10.3. Comment passer d'un produit Bitdefender 2013 à un autre ?

Vous pouvez facilement passer d'un produit Bitdefender 2013 à un autre.

Les trois produits Bitdefender 2013 que vous pouvez installer sur votre système sont les suivants :

- Bitdefender Antivirus Plus 2013
- Bitdefender Internet Security 2013
- Bitdefender Total Security 2013

Si vous souhaitez installer sur votre système un autre produit Bitdefender 2013 que celui acheté, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender. Cliquez sur ce lien pour ouvrir la fenêtre d'enregistrement.
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 et suivez la procédure pour effectuer l'installation.

11. Enregistrement

11.1. 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 2013
 - Bitdefender Internet Security 2013
 - Bitdefender Total Security 2013

11.2. 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.

Pour enregistrer Bitdefender, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender. Cliquez sur ce lien pour ouvrir la fenêtre d'enregistrement.
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.

11.3. 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. Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender.
3. Pour des informations supplémentaires, cliquez sur le lien pour ouvrir la fenêtre d'enregistrement.
4. Dans la fenêtre **Enregistrement de votre produit**, vous pouvez :
 - Voir la clé de licence actuelle
 - Enregistrer avec une autre clé de licence

- Acheter une clé de licence

11.4. 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://myaccount.bitdefender.com/fr/MyAccount/login/> pour créer un compte MyBitdefender.
3. Vous connecter à votre compte.
4. Cliquez sur votre nom d'utilisateur en haut et sélectionnez **Produits** dans le menu déroulant.
5. Cliquez sur **Enregistrement hors ligne**.
6. Saisissez la clé de licence que vous avez achetée.
7. Cliquez sur **Soumettre** pour obtenir un code d'autorisation.



Important

Notez le code d'autorisation.

8. Retournez à votre PC avec le code d'autorisation.
9. Ouvrez la **fenêtre de Bitdefender**.
10. Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender. Cliquez sur ce lien pour ouvrir la fenêtre d'enregistrement.
11. Saisissez le code d'autorisation dans le champ correspondant et cliquez sur **S'enregistrer**.
12. Patientez jusqu'à la fin du processus d'enregistrement.

11.5. 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. Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender. Cliquez sur ce lien pour ouvrir la fenêtre d'enregistrement.
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. Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender. Cliquez sur ce lien pour ouvrir la fenêtre d'enregistrement.
 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 « *Demander de l'aide* » (p. 191).

12. Analyser avec Bitdefender

12.1. 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, à pointer sur Bitdefender et à sélectionner **Analyser avec Bitdefender** dans le menu. Pour terminer l'analyse, suivez l'assistant d'analyse antivirus. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés.

Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

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.

12.2. Comment analyser mon système ?

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

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Antivirus**, cliquez sur **Analyser maintenant** et sélectionnez **Analyse du Système** dans le menu déroulant.
3. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer. Pour plus d'informations, reportez-vous à « *Assistant d'analyse antivirus* » (p. 81).

12.3. Comment créer une tâche d'analyse personnalisée ?

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

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

1. Ouvrez la **fenêtre de Bitdefender**.

2. Dans le panneau **Antivirus**, cliquez sur **Analyser maintenant** et sélectionnez **Analyse personnalisée** dans le menu déroulant.
3. Cliquez sur **Ajouter cible** pour sélectionner les fichiers ou les dossiers à analyser.
4. Si vous souhaitez configurer les options d'analyse en détail, cliquez sur **Options d'analyse**.

Vous pouvez facilement configurer les options d'analyse en réglant le niveau d'analyse. Déplacez le curseur sur l'échelle pour choisir le niveau d'analyse souhaité.

Vous pouvez également choisir d'éteindre l'ordinateur une fois l'analyse terminée si aucune menace n'est détectée. N'oubliez pas qu'il s'agira du comportement par défaut à chaque fois que vous exécuterez cette tâche.

5. Cliquez sur **Démarrer l'analyse** et suivez l'**Assistant d'analyse antivirus** pour terminer l'analyse. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.
6. Si vous souhaitez enregistrer la tâche d'analyse pour l'utiliser par la suite, ouvrez de nouveau la fenêtre de configuration de l'analyse personnalisée.
7. Localisez l'analyse que vous venez d'exécuter dans la liste des **Analyses récentes**.
8. Placez le curseur de la souris sur le nom de l'analyse et cliquez sur l'icône ☆ pour ajouter l'analyse à la liste des Analyses favorites.
9. Indiquez un nom explicite pour l'analyse.

12.4. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Exclusions**.
5. Veillez à ce qu'**Exclusions pour les fichiers** soit activé en cliquant sur le bouton.
6. Cliquez sur le lien **Fichiers et dossiers exclus**.
7. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
8. Cliquez sur **Parcourir**, sélectionnez le dossier à exclure de l'analyse, puis cliquez sur **OK**.
9. Cliquez sur **Ajouter** puis sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

12.5. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
 - d. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Résident**.
 - e. 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. 65).
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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
 - d. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Quarantaine**.
 - e. 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. 48).
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. 191).

12.6. Comment connaître les virus détectés par Bitdefender ?

À chaque fois qu'une analyse est effectuée, un journal d'analyse est créé et Bitdefender enregistre les problèmes détectés.

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 ultérieurement un journal d'analyse ou toute infection détectée, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur le bouton **Événements** de la barre d'outils supérieure.
3. Dans la fenêtre **Aperçu des événements**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Événements Antivirus**, sélectionnez l'onglet **Analyse**. 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.
5. 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.
6. Pour ouvrir un journal d'analyse, cliquez sur **Afficher le journal**. Le journal d'analyse s'ouvrira dans une nouvelle fenêtre.

13. Contrôle Parental

13.1. 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.

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. 53).
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. Cliquez sur le bouton **MyBitdefender** en haut de la fenêtre et sélectionnez **Contrôle Parental** dans le menu déroulant.
 - c. Le tableau de bord du Contrôle Parental s'ouvrira dans une nouvelle fenêtre. Vous pouvez consulter et configurer ici les paramètres du Contrôle Parental.
 - d. Cliquez sur **Ajouter un enfant** sur le menu de gauche.
 - e. Indiquez le nom et l'âge de l'enfant dans l'onglet **Profil**. 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.

Vérifiez les activités de vos enfants et modifiez les paramètres du Contrôle Parental à l'aide de MyBitdefender depuis tout ordinateur ou appareil mobile connecté à Internet.

Pour des informations détaillées sur l'utilisation du Contrôle Parental, reportez-vous à « *Contrôle Parental* » (p. 137).

13.2. Comment limiter l'accès à Internet pour mon enfant ?

Une fois le Contrôle Parental configuré, vous pouvez facilement bloquer l'accès à Internet à des périodes bien définies.

Le Contrôle Parental de Bitdefender vous permet de contrôler l'utilisation d'Internet de vos enfants même lorsque vous n'êtes pas chez vous.

Pour limiter l'accès à Internet à certaines heures de la journée, suivez ces étapes :

1. Sur tout périphérique avec un accès à Internet, ouvrez un navigateur web.
2. Allez à : <https://myaccount.bitdefender.com/fr/MyAccount/login/>
3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
5. Sélectionnez le profil de votre enfant dans le menu de gauche.
6. Cliquez  sur le panneau **Web** pour accéder à la fenêtre **Activité Web**.
7. Cliquez sur **Planifier**.
8. 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 commencer une nouvelle sélection, cliquez sur **Réinitialiser**.
9. Cliquez sur **OK**.



Note

Bitdefender effectuera des mises à jour toutes les heures même si l'accès à Internet est bloqué.

13.3. Comment empêcher mon enfant d'accéder à un site web ?

Le Contrôle Parental de Bitdefender vous permet de contrôler le contenu auquel accède votre enfant lorsqu'il utilise l'ordinateur et de bloquer l'accès à un site web même lorsque vous n'êtes pas chez vous.

Le Contrôle Parental de Bitdefender vous permet de contrôler l'utilisation d'Internet de vos enfants même lorsque vous n'êtes pas chez vous.

Pour bloquer l'accès à un site web, procédez comme suit :

1. Sur tout périphérique avec un accès à Internet, ouvrez un navigateur web.
2. Allez à : <https://myaccount.bitdefender.com/fr/MyAccount/login/>
3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
5. Sélectionnez le profil de votre enfant dans le menu de gauche.
6. Cliquez  sur le panneau **Web** pour accéder à la fenêtre **Activité Web**.

7. Cliquez sur **Liste noire**.
8. Indiquez l'adresse du site web dans le champ correspondant et cliquez sur **Ajouter**.
9. Le site web a été ajouté à la liste des sites web bloqués.

13.4. Comment empêcher mon enfant de jouer à un jeu ?

Le Contrôle Parental de Bitdefender vous permet de contrôler le contenu auquel votre enfant accède lorsqu'il utilise l'ordinateur.

Si vous avez besoin de limiter l'accès à un jeu ou à une application, vous pouvez utiliser le Contrôle Parental de Bitdefender même lorsque vous n'êtes pas chez vous.

Pour bloquer l'accès à un jeu ou à une application, suivez ces étapes :

1. Sur tout périphérique avec un accès à Internet, ouvrez un navigateur web.
2. Allez à :<https://myaccount.bitdefender.com/fr/MyAccount/login/>
3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
5. Sélectionnez le profil de votre enfant dans le menu de gauche.
6. Cliquez sur le panneau  **Applications** pour accéder à la fenêtre **Activité des Applications**.
7. Cliquez sur **Liste noire**.
8. Tapez (ou copiez-collez) le chemin vers l'exécutable dans le champ correspondant.
9. Cliquez sur **Ajouter** pour ajouter l'application aux **Applications de la Liste Noire**.

13.5. 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 surnom. Cliquez ensuite sur Suivant.
 5. Pour 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 ni 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 surnom. Cliquez ensuite sur Suivant.
 5. Pour le type de compte, cliquez sur Standard puis sur Créer un compte. Les comptes limités sont adaptés aux enfants car ils ne peuvent pas faire de modification globale dans 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.

14. Vie privée

14.1. Comment vérifier que ma transaction en ligne est sécurisée ?

Pour assurer la confidentialité de vos opérations en ligne, vous pouvez utiliser le navigateur fourni par Bitdefender pour protéger vos transactions et applications bancaires.

Bitdefender Safepay est un navigateur sécurisé conçu pour protéger vos informations bancaires, votre numéro de compte et toutes les autres données confidentielles que vous pouvez saisir lorsque vous accédez à différents sites en ligne.

Pour assurer la sécurité et la confidentialité de vos activités en ligne, procédez comme suit :

1. Double-cliquez sur l'icône Bitdefender Safepay de votre bureau.

La navigateur Bitdefender Safepay apparaîtra.

2. Cliquez sur le bouton  pour accéder au **Clavier virtuel**.
3. Utilisez le **Clavier virtuel** lorsque vous tapez des informations confidentielles telles que des mots de passe.

14.2. Que faire si mon système a été volé ?

Le vol d'ordinateurs portables est l'un des principaux problèmes actuels affectant les particuliers et les entreprises dans le monde entier.

Bitdefender Anti-Theft vous permet de localiser et de verrouiller l'ordinateur portable volé, mais également d'effacer toutes ses données afin d'empêcher que celles-ci ne soient utilisées par le voleur.

Pour accéder aux fonctionnalités antivols à partir de votre compte, procédez comme suit :

1. Allez dans <https://myaccount.bitdefender.com/fr/MyAccount/login/> et connectez-vous à votre compte.
2. Cliquez sur **Anti-Theft**.
3. Sélectionnez votre ordinateur dans la liste de périphériques.
4. Sélectionnez la fonctionnalité que vous souhaitez utiliser :

-  **Localiser** - permet d'afficher la localisation de votre appareil sur Google Maps.

-  **Effacer** - permet d'effacer toutes les données de votre ordinateur.



Important

Une fois les données d'un appareil effacées, toutes les fonctionnalités Antivols cessent de fonctionner.

-  **Verrouiller** - permet de verrouiller votre ordinateur et de spécifier un code PIN numérique pour le déverrouiller.

14.3. Comment protéger mon compte Facebook ?

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.

Pour accéder à Safego à partir de votre produit Bitdefender, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Safego**, cliquez sur **Gérer** et sélectionnez **Activer pour Facebook** dans le menu déroulant. Vous serez dirigé vers votre compte.

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

3. Utilisez vos informations de connexion Facebook pour vous connecter à l'application Safego.
4. Autoriser Safego à accéder à votre compte Facebook.

14.4. 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 s'affiche. 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 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 et Ouvrir**.



Note

Quand vous ouvrez le coffre, 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 coffre-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. 112).

14.5. Comment supprimer définitivement un fichier avec Bitdefender ?

Si vous souhaitez supprimer définitivement un fichier de votre système, vous avez besoin de supprimer physiquement les données de votre disque dur.

Le Destructeur de fichiers Bitdefender vous aidera à 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, pointez sur Bitdefender 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.

15. Optimisation

15.1. 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. 59)
- « *Nettoyez votre PC* » (p. 59)
- « *Nettoyer le Registre Windows* » (p. 60)
- « *Analysez votre système régulièrement* » (p. 60)

15.1.1. 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. Dans le panneau **Optimisation**, cliquez sur **Optimiser** et sélectionnez **Défragmenteur de disque** dans le menu déroulant.
3. Suivez les étapes de l'assistant.

15.1.2. 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. Dans le panneau **Optimisation**, cliquez sur **Optimiser** et sélectionnez **Nettoyage du PC** dans le menu déroulant.
3. Suivez les étapes de l'assistant.

15.1.3. 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. Dans le panneau **Optimisation**, cliquez sur **Optimiser** et sélectionnez **Nettoyage du registre** dans le menu déroulant.
3. Suivez les étapes de l'assistant.

15.1.4. 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. Dans le panneau **Antivirus**, cliquez sur **Analyser maintenant** et sélectionnez **Analyse du Système** dans le menu déroulant.
3. Suivez les étapes de l'assistant.

16. Sauvegarde en ligne de SafeBox

16.1. Comment accéder à mes fichiers sauvegardés depuis un autre ordinateur ?

Bitdefender vous permet d'accéder aux fichiers que vous avez sauvegardés avec Safebox de partout, même si vous n'êtes pas chez vous.

Il vous suffit d'un ordinateur avec accès Internet et d'un navigateur web.

Pour accéder à vos fichiers, vous avez besoin de vous connecter à MyBitdefender :

1. Sur tout périphérique avec un accès à Internet, ouvrez un navigateur web.
2. Allez à : <https://myaccount.bitdefender.com/fr/MyAccount/login/>
3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Cliquez sur **Safebox** pour accéder au tableau de bord de Safebox.

16.2. Comment partager des fichiers avec mes amis ?

Bitdefender Total Security 2013 est la solution qui vous permet de partager des photos, de la musique, des vidéos ou des documents avec vos amis.

Pour partager un fichier avec Bitdefender Total Security 2013, procédez de l'une des façons suivantes :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Safebox**, cliquez sur **Gérer** et sélectionnez **Gérer les fichiers partagés** dans le menu déroulant.
3. Faites glisser le fichier et déposez-le dans la fenêtre **Gérer le partage**.
4. Sélectionnez le fichier et cliquez sur **Partager le lien**.
5. Cliquez sur le lien indiqué pour copier le lien dans le presse-papiers.
6. Pour permettre l'accès au fichier partagé, envoyez le lien à la personne avec laquelle vous souhaitez partager le fichier.

16.3. Où voir l'espace restant sur ma Safebox ?

Pour connaître l'espace restant sur votre Safebox, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Safebox**.

4. La section **Espace utilisé** vous permet de connaître l'espace restant.

Si vous avez une grande quantité de données avec de la musique, des films ou d'importants fichiers, l'espace gratuit en ligne peut ne pas être suffisant.

Pour mettre à niveau votre espace en ligne, cliquez sur **Mettre à niveau Safebox**.

La page MyBitdefender s'ouvrira dans votre navigateur web. Suivez les instructions pour finaliser l'achat.

16.4. Comment libérer de l'espace sur Safebox ?

Bitdefender vous offre 2 Go d'espace gratuit en ligne pour vos données.

Si vous avez une grande quantité de données avec de la musique, des films ou d'importants fichiers, l'espace gratuit en ligne peut ne pas être suffisant.

Pour libérer de l'espace sur Safebox, procédez comme suit :

1. Sur tout périphérique avec un accès à Internet, ouvrez un navigateur web.
2. Allez à : <https://myaccount.bitdefender.com/fr/MyAccount/login/>
3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Cliquez sur **Safebox** pour accéder au tableau de bord de Safebox.
5. Sélectionnez l'onglet **Corbeille**.
6. Cochez la case correspondant au fichier que vous souhaitez supprimer.
7. Cliquez sur **Actions** et sélectionnez **Supprimer** dans le menu déroulant.
8. Une fenêtre de confirmation s'affichera. Cliquez sur **OK** pour valider.

17. Informations Utiles

17.1. Comment éteindre automatiquement l'ordinateur une fois l'analyse terminée ?

Bitdefender propose plusieurs tâches d'analyse que vous pouvez utiliser pour vérifier que votre système n'est pas infecté par des malwares. L'analyse de l'ensemble de l'ordinateur peut prendre plus de temps en fonction de la configuration matérielle et logicielle de votre système.

C'est pourquoi Bitdefender vous permet de configurer Bitdefender pour éteindre votre système dès que l'analyse est terminée.

Prenons l'exemple suivant : vous avez terminé d'utiliser l'ordinateur et souhaitez aller dormir. Vous aimeriez que l'ensemble de votre système fasse l'objet d'une analyse antimalware par Bitdefender.

Voici comment configurer Bitdefender pour éteindre votre système à la fin de l'analyse :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Antivirus**, cliquez sur **Analyser maintenant** et sélectionnez **Analyse personnalisée** dans le menu déroulant.
3. Cliquez sur **Ajouter cible** pour sélectionner les fichiers ou les dossiers à analyser.
4. Si vous souhaitez configurer les options d'analyse en détail, cliquez sur **Options d'analyse**.
5. Choisissez d'éteindre l'ordinateur une fois l'analyse terminée si aucune menace n'est détectée.
6. Cliquez sur **Démarrer l'analyse**.

Si aucune menace n'est détectée, l'ordinateur sera éteint.

Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer. Pour plus d'informations, reportez-vous à « **Assistant d'analyse antivirus** » (p. 81).

17.2. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Général**.
4. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Avancé**.
5. Activez l'utilisation du proxy en cliquant sur le bouton.
6. Cliquez sur le lien **Gérer Proxy**.
7. 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.
8. 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.

17.3. 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.

17.4. 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**.

17.5. 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 2013 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.

17.6. 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.

17.7. 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.

Gérer votre sécurité

18. 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 - à la demande.

Lorsqu'**Auto Scan** est activé, il est inutile de lancer manuellement des analyses antimalwares. Auto Scan analysera votre ordinateur encore et encore, et adoptera les mesures appropriées lorsque des malwares seront détectés. Auto Scan 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. 85).

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 « **Configurer des exceptions d'analyse** » (p. 87).

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. 89).

Si votre ordinateur a été infecté par des malwares, veuillez vous référer à « **Suppression des malwares de votre système** » (p. 181). 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. 90).

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. 93).

18.1. 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.

18.1.1. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Résident**.
5. Cliquez sur le bouton pour activer ou désactiver l'analyse à l'accès.

6. 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 pour combien de temps 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.

18.1.2. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Résident**.
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.

18.1.3. Configurer les paramètres de protection en temps réel

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 configurer les paramètres de la protection en temps réel, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Résident**.
5. Cliquez sur **Personnaliser**.

6. Configurez les paramètres d'analyse selon vos besoins.
7. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

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.
- **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.

Par défaut, les dossiers locaux et les partages réseau sont sujets à l'analyse à l'accès. Pour de meilleures performances du système, vous pouvez exclure certains emplacements du réseau de l'analyse à l'accès.

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; fpx; 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; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Analyser 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 sans 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

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 d'amorçage.** 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.
- **Rechercher les keyloggers.** Sélectionnez cette option pour analyser votre système à la recherche de keyloggers. Les keyloggers enregistrent ce que vous tapez sur votre clavier et envoient des rapports sur Internet à une personne malveillante (un hacker). Le pirate peut récupérer des informations sensibles à partir des données volées, comme vos numéros de comptes bancaires ou vos mots de passe pour les utiliser à son propre profit.

Actions appliquées à l'encontre des malwares détectés

Vous pouvez configurer les actions appliquées par la protection en temps réel.

Pour configurer les actions, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Résident**.
5. Cliquez sur **Personnaliser**.
6. Configurez les paramètres d'analyse selon vos besoins.
7. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Les actions suivantes peuvent être appliquées par la protection en temps réel dans Bitdefender :

Action automatique

Bitdefender appliquera les actions recommandées en fonction du type de fichier détecté :

- **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 tentera de supprimer automatiquement le code malveillant du fichier infecté et de reconstituer 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. 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. 89).



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.

- **Fichiers suspects**. Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique.Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible. Ils seront placés en quarantaine afin d'éviter 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.

● Archives contenant des fichiers infectés.

- ▶ Les archives contenant uniquement des fichiers infectés sont automatiquement supprimées.
- ▶ Si une archive contient à la fois des fichiers infectés et des fichiers sains, Bitdefender tentera de supprimer les fichiers infectés s'il peut reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Tout déplacer en quarantaine

Déplace les fichiers détectés 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. 89).

Refuser l'accès

Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.

18.1.4. 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**.

18.2. Analyse à la demande

L'objectif principal de Bitdefender est de conserver votre PC sans virus. Cela se fait 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 il est encore plus prudent d'analyser régulièrement votre ordinateur contre les virus.

L'analyse à la demande est fondée 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.

18.2.1. Auto Scan

Auto Scan 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. Auto Scan détecte et utilise les moments pendant lesquels la consommation des ressources du système passe sous un certain seuil pour effectuer des analyses régulières de l'ensemble du système.

Les avantages de l'utilisation d'Auto Scan :

- 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 Auto Scan, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Antivirus**, cliquez sur le bouton pour activer ou désactiver **Auto Scan**.

18.2.2. 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, pointez sur **Bitdefender** et sélectionnez **Analyser avec Bitdefender**. L'**Assistant d'analyse antivirus** s'affichera et vous guidera au cours du processus d'analyse. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.

18.2.3. 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. Dans le panneau **Antivirus**, cliquez sur **Analyser maintenant** et sélectionnez **Analyse rapide** dans le menu déroulant.
3. Suivez les indications de l'**Assistant d'analyse antivirus** pour terminer l'analyse. Bitdefender appliquera automatiquement les actions recommandées.

aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

18.2.4. Exécuter une Analyse du Système

La tâche d'Analyse 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 **Auto Scan**, nous vous recommandons d'exécuter une Analyse du Système au moins une fois par semaine.



Note

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

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

- Vérifiez que Bitdefender dispose de signatures de malwares à jour. Analyser votre ordinateur en utilisant une base de données de signatures non à jour peut empêcher Bitdefender de détecter le nouveau malware identifié depuis la mise à jour précédente. Pour plus d'informations, reportez-vous à « *Maintenir Bitdefender à jour* » (p. 37).
- 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 une analyse personnalisée* » (p. 78).

Pour exécuter une Analyse du Système, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Antivirus**, cliquez sur **Analyser maintenant** et sélectionnez **Analyse du Système** dans le menu déroulant.
3. Suivez les indications de l'**Assistant d'analyse antivirus** pour terminer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

18.2.5. Configurer une analyse personnalisée

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

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Antivirus**, cliquez sur **Analyser maintenant** et sélectionnez **Analyse personnalisée** dans le menu déroulant.

3. Vous pouvez si vous le souhaitez exécuter de nouveau rapidement une analyse personnalisée antérieure en cliquant sur l'entrée correspondante dans la liste des **Analyses récentes** ou des **Analyses favorites**.
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 choisir 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 la section.
 - b. Vous pouvez aussi configurer ces options générales :
 - **Exécuter la tâche en priorité basse** . Diminue la priorité du processus d'analyse. Vous allez permettre aux autres logiciels de s'exécuter à une vitesse supérieure en augmentant le temps nécessaire pour que l'analyse soit finie.
 - **Réduire l'assistant d'analyse dans la zone de notification** . Réduit la fenêtre d'analyse dans la **zone de notification**. Double-cliquez sur l'icône de Bitdefender pour l'ouvrir.
 - Spécifiez l'action à mener si aucune menace n'a été trouvée.
 - c. 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. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.

Enregistrer une analyse personnalisée dans les analyses favorites

Lorsque vous configurez et exécutez une analyse personnalisée, elle est automatiquement ajoutée à une liste limitée d'analyses récentes. Si vous pensez réutiliser une analyse personnalisée ultérieurement, vous pouvez choisir de l'enregistrer dans la liste des analyses favorites.

Pour enregistrer une analyse personnalisée exécutée récemment dans la liste des analyses favorites, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'analyse personnalisée.

- a. Ouvrez la **fenêtre de Bitdefender**.
 - b. Dans le panneau **Antivirus**, cliquez sur **Analyser maintenant** et sélectionnez **Analyse personnalisée** dans le menu déroulant.
2. Localisez l'analyse souhaitée dans la liste des **Analyses récentes**.
 3. Placez le curseur de la souris sur le nom de l'analyse et cliquez sur l'icône ★ pour ajouter l'analyse à la liste des analyses favorites.

Les analyses enregistrées en tant que favorites sont signalées à l'aide de l'icône ★. Si vous cliquez sur cette icône, l'analyse sera retirée de la liste des analyses favorites.

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; xls; 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 sans 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 d'amorçage.** 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 la mémoire.** Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire de votre système.
- **Analyser 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.
- **Analyser 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.
- **Analyser les rootkits.** Sélectionnez cette option pour rechercher des **rootkits** et des objets masqués à l'aide de ce logiciel.

18.2.6. Assistant d'analyse antivirus

À chaque fois que vous lancerez une analyse à la demande (par exemple en faisant un clic droit sur un dossier, en pointant sur Bitdefender et en sélectionnant **Analyser avec Bitdefender**), l'assistant de l'analyse antivirus Bitdefender 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 **zone de notification**. Vous pouvez cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

Étape 1 - Effectuer l'analyse

Bitdefender commence à analyser les objets sélectionnés. Vous pouvez voir des informations en temps réel sur l'état et les statistiques de l'analyse (y compris le temps écoulé, une estimation du temps restant et le nombre de menaces détectées). Pour plus d'informations, cliquez sur le lien **Plus de statistiques**.

Patiencez jusqu'à ce que Bitdefender ait terminé l'analyse. L'analyse peut durer un certain temps, suivant sa complexité.

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**.

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 :

- **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.

Sélectionnez l'option souhaitée et cliquez sur **OK** pour poursuivre l'analyse.

Étape 2 - Sélectionner des actions

À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.



Note

Si vous lancez une analyse rapide ou une analyse complète du système, Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés pendant

l'analyse. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

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 :

Action automatique

Bitdefender appliquera les actions recommandées en fonction du type de fichier détecté :

- **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 tentera de supprimer automatiquement le code malveillant du fichier infecté et de reconstituer 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. 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. 89).



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.

- **Fichiers suspects**. Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible. Ils seront placés en quarantaine afin d'éviter 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.

- **Archives contenant des fichiers infectés.**

- ▶ Les archives contenant uniquement des fichiers infectés sont automatiquement supprimées.
- ▶ Si une archive contient à la fois des fichiers infectés et des fichiers sains, Bitdefender tentera de supprimer les fichiers infectés s'il peut reconstituer

l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Supprimer

Supprime du disque les fichiers détectés.

Si des fichiers infectés sont contenus dans une archive avec des fichiers sains, Bitdefender tentera de supprimer les fichiers infectés et de reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Ignorer

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.

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

Étape 3 - Récapitulatif

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.

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



Important

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. Si cela est nécessaire, il vous sera demandé de redémarrer votre système pour terminer le processus d'installation. 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. 181).

18.2.7. Consulter les journaux d'analyse

À chaque fois qu'une analyse est effectuée, un journal d'analyse est créé et Bitdefender enregistre les problèmes détectés dans la fenêtre Présentation de l'Antivirus. 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 ultérieurement un journal d'analyse ou toute infection détectée, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur le bouton **Événements** de la barre d'outils supérieure.
3. Dans la fenêtre **Aperçu des événements**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Événements Antivirus**, sélectionnez l'onglet **Analyse**. 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.
5. 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.
6. Pour ouvrir le journal d'analyse, cliquez sur **Journal**. Le journal d'analyse s'affichera dans votre navigateur Internet par défaut.

18.3. 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.

18.3.1. 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 l'Auto-Pilot 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 l'Auto-Pilot 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. 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

Veillez 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.

3. 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. 181).

18.3.2. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Exclusions**.

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.

18.4. Configurer des exceptions d'analyse

Bitdefender vous 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 accédez.



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**.

18.4.1. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Exclusions**.
5. Activez les exceptions d'analyse pour les fichiers à l'aide du bouton correspondant.
6. 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.
7. 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**.

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

18.4.2. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Exclusions**.
5. Activez les exceptions d'analyse pour les fichiers à l'aide du bouton correspondant.
6. Cliquez sur le lien **Extensions exclues**. La fenêtre qui s'affiche vous permet de gérer les extensions de fichiers exclues de l'analyse.
7. 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**.
8. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

18.4.3. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Exclusions**. Utilisez les options de la section **Fichiers et dossiers** pour gérer les exceptions d'analyse.
5. 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**.
6. Pour désactiver les exceptions d'analyse, cliquez sur le bouton correspondant.

18.5. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.

4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Quarantaine**.
5. 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 suspects de la quarantaine pour analyse

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.

6. 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**.

18.6. 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 un score global est calculé 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 l'Auto-Pilot 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**.

18.6.1. 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. Dans la fenêtre **Aperçu des événements**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Événements Antivirus**, sélectionnez l'onglet **Active Virus Control**.
5. Cliquez sur un événement pour afficher des informations à son sujet.
6. 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 les activités suspectes d'une application exclue sont détectées, l'événement sera simplement enregistré et signalé au Cloud Bitdefender comme erreur de détection.

18.6.2. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Résident**.
5. Cliquez sur le bouton pour activer ou désactiver Active Virus Control.

18.6.3. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Résident**.
5. Vérifiez qu'Active Virus Control est activé.
6. 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).

18.6.4. Gérer les 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 les activités suspectes d'une application exclue sont détectées, 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Exclusions**.
5. 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.

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 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**.
7. Pour supprimer ou éditer des exclusions, procédez comme suit :
 - Pour effacer un objet de la liste, sélectionnez le et cliquez sur le bouton **Effacer**.
 - 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**.

8. Enregistrer les modifications et fermer la fenêtre.

18.7. 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.

18.7.1. 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. Dans le panneau **Antivirus**, cliquez sur **Analyser maintenant** et sélectionnez **Vulnérabilité** dans le menu déroulant.
3. 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**

Patiencez 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 indiqué 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.

18.7.2. 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. Dans la fenêtre **Aperçu des événements**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Événements Antivirus**, sélectionnez l'onglet **Vulnérabilité**.
5. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Événements Antivirus**, sélectionnez l'onglet **Vulnérabilité**.
5. 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.

6. 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.

19. Antispam

Le spam est un terme utilisé pour décrire les e-mails non sollicités. Le spam est un problème croissant, à la fois pour les particuliers et les entreprises. Vous ne voudriez pas que vos enfants tombent sur certains e-mails, 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 empêcher les gens d'en envoyer. L'idéal serait de pouvoir arrêter de les recevoir. Malheureusement, le spam revêt 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. 98).

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 signalés comme étant du [spam] par Bitdefender vers un dossier de quarantaine personnalisé.

19.1. Aperçu de l'antispam

19.1.1. 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 d'entreprises et d'organismes d'un même domaine. En utilisant **les listes amis/spammeurs**, vous pouvez déterminer aisément de quelles personnes vous voulez recevoir des e-mails quel que soit leur contenu (amis) et de quelles personnes vous ne voulez plus en recevoir (spammeurs).



Note

Nous vous suggérons d'ajouter les noms de vos amis et leurs adresses mail à la **Liste d'Amis**. Bitdefenderne bloquera aucun de leurs messages; l'ajout des amis à la liste assure la transmission des messages légitimes.

Filtre jeu de caractères

De nombreux messages de spam sont rédigés en caractères cyrilliques et/ou asiatiques. Le filtre de caractères détecte ce type de messages et les signale comme étant du 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 recherche toutes les URL d'un message dans sa base de données. En cas de concordance, le message est signalé comme étant du 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 antisпам.

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'antisпам. Pour plus d'informations, reportez-vous à « *Régler le niveau de sensibilité* » (p. 106).

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 antisпам efficace et toujours à jour.

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

19.1.2. Fonctionnement de l'Antisпам

Le Moteur de Bitdefender Antisпам utilise tous les filtres antisпам 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 d'amis/Liste des spammeurs**. Si l'adresse de l'expéditeur est identifiée dans la **Liste d'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'e-mail est rédigé en caractères cyrilliques ou asiatiques. Si tel est le cas, le message sera marqué comme étant du 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. Lorsqu'il y a correspondance, l'e-mail sera considéré comme 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. 106).

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.

19.1.3. 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.

19.1.4. 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

19.2. Activer ou désactiver la protection antispam

La protection Antispam n'est pas activée par défaut. Pour activer le module antispam, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.

2. Dans le panneau **Antispam**, cliquez sur le bouton pour activer ou désactiver l'**Antispam**.
3. Attendez que Bitdefender installe les composants du module.

19.3. 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. 100).

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 « *Configurer la liste des spammeurs* » (p. 104).

 **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 « *Configurer la liste d'amis* » (p. 103).

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

19.3.1. 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 considérablement l'efficacité du filtrage 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.

19.3.2. 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). Ils sont immédiatement signalés comme étant du [spam] et déplacés vers le dossier du courrier indésirable.

19.3.3. Configurer les 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.

19.4. Configurer la liste d'amis

La **liste d'amis** est une liste de toutes les adresses e-mail de la part desquelles vous voulez toujours recevoir les messages, quel que soit leur contenu. Les messages de vos amis ne seront jamais considérés comme étant du spam, même si leur contenu ressemble à du 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. Dans le panneau **Antispam**, cliquez sur **Gérer** et sélectionnez **Gérer les amis** dans le menu déroulant.

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'utiliser sur 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.

19.5. Configurer la liste des spammeurs

La **liste des spammeurs** est une liste de toutes les adresses e-mail de la part desquelles vous ne voulez recevoir aucun message, quel que soit leur 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. Dans le panneau **Antispam**, cliquez sur **Gérer** et sélectionnez **Gérer les spammeurs** dans le menu déroulant.
 3. Allez dans le panneau **Antispam**.
 4. 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 webmail légitimes (tels que Yahoo, Gmail, Hotmail ou d'autres) à la liste des 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 pouvoir l'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.

19.6. 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. 173) 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antispam**.
4. Dans la fenêtre **Paramètres Antispam**, sélectionnez l'onglet **Paramètres**.
5. 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.

19.7. Configurer les filtres antispam locaux

Comme cela est décrit dans « *Aperçu de l'antispam* » (p. 98), 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antispam**.
4. Dans la fenêtre **Paramètres Antispam**, sélectionnez l'onglet **Paramètres**.
5. 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**.

19.8. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antispam**.
4. Dans la fenêtre **Paramètres Antispam**, sélectionnez l'onglet **Cloud**.
5. Cliquez sur le bouton pour activer ou désactiver la détection "in-the-cloud".
6. Des échantillons d'e-mails de spam ou légitimes peuvent être envoyés au Cloud Bitdefender lorsque vous signalez 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**.

20. 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.

La Protection 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.
- **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.

20.1. 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

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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Vie privée**.

4. Dans la fenêtre **Paramètres de la Protection Vie Privée**, sélectionnez l'onglet **Antiphishing**.

Cliquez sur les boutons pour activer ou désactiver :

- Affichage de la **barre d'outils Bitdefender** dans le navigateur web.



Note

La barre d'outils du navigateur Bitdefender n'est pas activée par défaut.

- Search advisor, un composant qui évalue les résultats de vos requêtes sur les moteurs de recherche et les liens postés sur les sites web de réseaux sociaux en plaçant une icône à côté de chaque résultat :

- Nous vous déconseillons de consulter cette page web.

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

- Cette page peut être consultée en toute sécurité.

Search Advisor évalue les résultats de recherche des moteurs de recherche web suivants :

- ▶ Google
- ▶ Yahoo!
- ▶ Bing
- ▶ Baidu

Search Advisor évalue les liens postés sur les sites de réseaux sociaux suivants :

- ▶ Facebook
- ▶ Twitter

- 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 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.

20.1.1. 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 "Page non sûre" apparaît sur un fond rouge - nous vous recommandons de quitter immédiatement la page web. Pour plus d'informations sur cette menace, cliquez sur le symbole + sur le résultat de la page.
- 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.

Les fenêtres du navigateur ouvertes dans Sandbox seront facilement identifiables grâce à leur contour modifié et à l'icône Sandbox ajoutée au centre de la barre de titre.



Note

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

Paramètres

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

- Filtre Antiphishing
- Filtre Web 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.

20.1.2. 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. Voici les options proposées :

- Quittez la page web en cliquant sur **Retour en toute sécurité**.
- Désactivez le blocage des pages de phishing en cliquant sur **Désactiver le filtre antiphishing**.
- Désactivez le blocage des pages contenant des malwares en cliquant sur **Désactiver le filtre Antimalware**.
- 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.
- Pour vous rendre sur le site web, malgré l'avertissement, cliquez sur **Je comprends les risques, je souhaite quand même consulter cette page**.

20.2. Cryptage de Messagerie Instantanée

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 ait installé sur son ordinateur une version de Bitdefender qui prenne en charge le cryptage de messagerie instantanée et que ce dernier soit activé pour l'application de messagerie instantanée utilisée pour converser.

- Vous et votre interlocuteur utilisez Yahoo! Messenger.



Important

Bitdefender ne cryptera pas la conversation si l'un des participants utilise une application de messagerie web instantanée telle que Meebo.

Une fois les prérequis remplis, Bitdefender vous informera de l'état du cryptage de votre session de messagerie instantanée par des messages affichés dans la fenêtre de chat.

Pour activer ou désactiver le cryptage des messageries instantanées, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Vie privée**.
4. Dans la fenêtre **Paramètres de la Protection Vie Privée**, cliquez sur le bouton pour activer ou désactiver le cryptage des messageries instantanées. Le cryptage est activé par défaut.

20.3. 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 courants 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.

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.

20.3.1. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Cryptage de Fichiers**.
4. Dans la fenêtre **Cryptage de Fichiers**, sélectionnez 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 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 un coffre-fort** 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.

Ajouter des fichiers aux coffres-forts

Pour lancer un assistant qui vous permettra d'ajouter des fichiers à un coffre-fort, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Cryptage de Fichiers**, cliquez sur **Cryptage** et sélectionnez **Ajouter 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, reportez-vous à « **Créer des coffres-forts** » (p. 113)

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 contenues dans le coffre est donc complètement bloqué.

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

Pour lancer un assistant qui vous permettra de verrouiller un coffre-fort, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Cryptage de Fichiers**, cliquez sur **Coffre-fort** et 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 supprimer des fichiers d'un coffre-fort, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Cryptage de Fichiers**, cliquez sur **Cryptage** et sélectionnez **Supprimer 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 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, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Cryptage de Fichiers**, cliquez sur **Coffre-fort** et sélectionnez **Afficher 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 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. 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 @).

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.

20.3.2. 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 **Bitdefender > 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. 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.

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.

Ajouter des 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 contenues dans le coffre 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.

20.4. 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.
2. Sélectionnez **Bitdefender > Destructeur de fichiers** dans le menu contextuel qui apparaît.
3. Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour lancer l'assistant du Destructeur de Fichiers.
4. Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.
5. 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. Dans le panneau **Confidentialité**, cliquez sur **Sécurisé** et sélectionnez **Destructeur de fichiers** dans le menu déroulant.
3. 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 des 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.

21. Pare-feu

Le Pare-feu protège votre ordinateur contre les tentatives de connexion non autorisées entrantes et sortantes, à la fois sur les réseaux locaux et sur Internet. Cela ressemble beaucoup à un garde à votre porte - il surveille les tentatives de connexion et détermine celles à autoriser et à bloquer.

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 connexions 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 connectés au même réseau.

Vous devez créer des règles pour autoriser ou refuser spécifiquement le trafic entre votre ordinateur et d'autres ordinateurs.

Si votre ordinateur fonctionne sous Windows Vista ou Windows 7, Bitdefender attribue automatiquement un type de réseau à chaque connexion réseau qu'il détecte. En fonction du type de réseau, la protection pare-feu est définie pour le niveau approprié de chaque connexion.

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 « *Gérer les paramètres de connexion* » (p. 124).

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).

Bitdefender est configuré par défaut pour appliquer automatiquement les actions recommandées pour votre protection, sans vous interrompre. Si vous souhaitez être informé et choisir la meilleure action à prendre lorsqu'une application demande un accès à Internet ou a un comportement suspect, vous devez activer le **Mode paranoïaque**.

21.1. 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. Dans le panneau **Pare-feu**, 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.

21.2. Gérer les paramètres de connexion

Pour afficher et éditer les paramètres de connexion réseau, suivez ces étapes :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Pare-feu**, cliquez sur **Activité du 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, sélectionnez l'option souhaitée dans le menu déroulant correspondant.

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 de réseau, sélectionnez **Oui** dans le menu déroulant correspondant.

21.3. Gérer les règles de pare-feu

21.3.1. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Pare-feu**.
4. Dans la fenêtre **Paramètres du pare-feu**, sélectionnez l'onglet **Paramètres**.
5. 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.

21.3.2. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Pare-feu**.
4. Dans la fenêtre **Paramètres du pare-feu**, sélectionnez l'onglet **Paramètres**.
5. 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 ordinateurs 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 hautes performances. Les jeux et les 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 s'affiche. 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. 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. Pour filtrer le trafic entre votre ordinateur et un ordinateur spécifique, décochez la case **Tous** et entrez 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 :

Événement	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.

Direction	Description
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.

21.3.3. 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 un 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Pare-feu**.
4. Dans la fenêtre **Paramètres du pare-feu**, sélectionnez l'onglet **Paramètres**.
5. Sous Règles pare-feu, cliquez sur **Règles d'adaptateurs**.

Une nouvelle fenêtre apparaîtra indiquant les cartes réseau avec des connexions actives et les zones actuelles, le cas échéant.

Pour gérer les zones, utilisez les boutons de la partie inférieure 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.

21.4. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Pare-feu**.
4. Dans la fenêtre **Paramètres du Pare-feu**, sélectionnez l'onglet **Avancé**.
5. Sous **Activité des réseaux**, cliquez sur **Activité du réseau**.

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**. L'emplacement du fichier journal est ?\Program Files\Common Files\Bitdefender\Bitdefender Firewall\bdfirewall.txt.

21.5. Configurer l'intensité de l'alerte

Bitdefender Total Security 2013 est conçu pour être aussi discret que possible. Dans des conditions normales, vous n'avez pas à prendre de décisions pour autoriser ou non des connexions ou des actions tentées par des applications en cours d'exécution sur votre système. Bitdefender prend toutes les décisions pour vous.

Si vous souhaitez contrôler entièrement la prise de décision, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Pare-feu**.
4. Dans la fenêtre **Paramètres du pare-feu**, sélectionnez l'onglet **Paramètres**.
5. Activez le **Mode Paranoïaque** en cliquant sur le bouton correspondant.



Note

Quand le Mode Paranoïaque est activé, l'**Auto-Pilot** est automatiquement désactivé.

Tant que le Mode Paranoïaque est activé, une alerte s'affichera vous demandant de sélectionner l'action à appliquer à chaque fois que l'une des situations suivantes se produit :

- Une application essaie de se connecter à Internet.
- Une application essaie de réaliser une action considérée comme suspecte par le **système de détection d'intrusion** ou par **Active Virus Control**.

L'alerte contient des informations détaillées au sujet de l'application et du comportement détecté. Vous devez sélectionner l'action **Autoriser** ou **Refuser** à l'aide du bouton correspondant.

21.6. Configurer les paramètres avancés

Pour configurer les paramètres avancés du pare-feu, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Pare-feu**.
4. Dans la fenêtre **Paramètres du Pare-feu**, sélectionnez l'onglet **Avancé**.

21.6.1. Système de détection d'intrusion

Pour configurer le Système de Détection d'Intrusion, procédez comme suit :

1. Pour activer le Système de Détection d'Intrusion, cliquez sur le bouton correspondant.
2. 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 les processus exclus* » (p. 92).



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.

21.6.2. D'autres options

Les fonctionnalités suivantes peuvent être activées ou désactivées.

- **Partage de Connexion Internet** - active le support du partage de connexion Internet.



Note

Cette option n'active pas automatiquement le **Partage de connexion Internet** sur votre système, mais permet uniquement ce type de connexion si vous l'activez 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**.

- **Surveiller les connexions Wi-Fi** - si vous êtes connecté(e) à des réseaux sans fil, des informations s'affichent au sujet d'événements réseau spécifiques (par exemple lorsqu'un nouvel ordinateur rejoint le réseau).

22. Transactions en ligne sécurisées par Safepay

L'ordinateur devient rapidement indispensable pour les achats et les transactions bancaires. Payer vos factures, virer de l'argent, et acheter quasiment tout ce que vous pouvez imaginer n'a jamais été aussi rapide ni aussi simple.

Cela implique l'envoi sur Internet d'informations personnelles, de données de comptes et de cartes bancaires, de mots de passe et d'autres types d'informations confidentielles, en d'autres termes exactement le type d'informations qui intéressent tout particulièrement les cybercriminels. Les pirates ne sont pas avares d'efforts lorsqu'il s'agit de voler ces informations, et vous n'êtes donc jamais trop prudent pour ce qui est de la sécurisation des transactions en ligne.

Bitdefender Safepay propose une solution unique aux différentes compromissions possibles de vos données confidentielles. Il s'agit d'un navigateur protégé, un environnement sécurisé conçu pour assurer la confidentialité et la sécurité des opérations bancaires, achats en ligne et autres types de transactions sur Internet. Vous pouvez lancer Bitdefender Safepay quand vous le souhaitez pour envoyer des informations sensibles sur Internet, ou le configurer afin qu'il se lance automatiquement lorsque vous consultez certains sites web.

Bitdefender Safepay dispose des fonctions suivantes :

- Il bloque l'accès à votre bureau et toute tentative de prise d'instantanés de votre écran.
- Il est accompagné d'un clavier virtuel, qui, lorsqu'il est utilisé, empêche les pirates de lire vos frappes au clavier.
- Il est complètement indépendant de vos autres navigateurs.
- Il contient une protection hotspot intégrée à utiliser lorsque votre ordinateur est connecté à des réseaux Wifi non sécurisés.
- Il supporte les marque-pages et vous permet de consulter vos sites bancaires et boutiques en ligne préférés.
- Il ne se limite pas aux sites bancaires et boutiques en ligne. Tout site web peut être ouvert dans Bitdefender Safepay

22.1. Utiliser Bitdefender Safepay

Par défaut, Bitdefender détecte lorsque vous naviguez sur un site bancaire ou une boutique en ligne dans tout navigateur sur votre ordinateur et vous invite à le lancer dans Bitdefender Safepay.

Pour ouvrir Bitdefender Safepay manuellement, suivez ce chemin : **Démarrer** → **Tous les programmes** → **Bitdefender 2013** → **Bitdefender Safepay** ou, plus rapide, double-cliquez sur le raccourci de Bitdefender Safepay sur votre bureau.

Si vous êtes habitués aux navigateurs web, vous n'aurez pas de problème pour utiliser Bitdefender Safepay - il ressemble et se comporte comme un navigateur standard :

- saisissez les URL que vous souhaitez consulter dans la barre d'adresses.
- ajoutez des onglets pour visiter plusieurs sites web dans la fenêtre de Bitdefender Safepay en cliquant sur .
- naviguez d'une page à l'autre et actualisez les pages à l'aide de .
- accédez aux **paramètres** Bitdefender Safepay en cliquant sur .
- gérez vos **marque-pages** en cliquant sur  à côté de la barre d'adresses.
- ouvrez le clavier virtuel en cliquant sur .

22.2. Configuration des paramètres

Cliquez sur  pour configurer les paramètres suivants :

Comportement général de Bitdefender Safepay

Choisissez ce qui se passera lorsque vous accéderez à une boutique ou à un site bancaire en ligne dans un navigateur web standard :

- Ouvrir automatiquement dans Bitdefender Safepay.
- Faire en sorte que Bitdefender vous consulte pour l'action à chaque fois.
- Ne jamais utiliser Bitdefender Safepay pour les pages consultées dans un navigateur standard.

Liste des domaines

Choisissez comment Bitdefender Safepay se comportera lorsque vous consulterez les sites web de certains domaines dans votre navigateur web standard en les ajoutant à la liste de domaines et en sélectionnant son comportement pour chacun d'entre eux :

- Ouvrir automatiquement dans Bitdefender Safepay.
- Faire en sorte que Bitdefender vous consulte pour l'action à chaque fois.
- Ne jamais utiliser Bitdefender Safepay lors de la consultation d'une page de ce domaine dans un navigateur standard.

22.3. Gérer les marque-pages

Si vous avez désactivé la détection automatique de certains ou de tous les sites web, ou si Bitdefender ne détecte simplement pas certains sites web, vous pouvez

ajouter des marque-pages à Bitdefender Safepay afin de pouvoir lancer facilement vos sites web favoris à l'avenir.

Suivez ces étapes pour ajouter une URL aux marque-pages de Bitdefender Safepay :

1. Cliquez sur  à côté de la barre d'adresses pour ouvrir la page Marque-pages.



Note

La page Marque-pages s'ouvre par défaut lorsque vous lancez Bitdefender Safepay.

2. Cliquez sur le bouton **+** pour ajouter un nouveau marque-pages.
3. Indiquez l'URL et le titre du marque-pages et cliquez sur **Créer**. L'URL est également ajoutée à la Liste de domaines sur la page **paramètres**.

22.4. Protection hotspot pour les réseaux non sécurisés

Lorsque vous utilisez Bitdefender Safepay en étant connecté à des réseaux Wifi non sécurisés (par exemple, à un point d'accès public), un niveau de sécurité supplémentaire est fourni par la fonctionnalité Protection Hotspot. Ce service chiffre la communication Internet sur des connexions non sécurisées, vous aidant à assurer la protection de votre vie privée quel que soit le réseau auquel vous êtes connecté.

Les prérequis suivants doivent être remplis pour que la protection hotspot fonctionne :

- Vous êtes connecté à un compte MyBitdefender depuis Bitdefender Total Security 2013.
- Votre ordinateur est connecté à un réseau non sécurisé.

Une fois les prérequis remplis, Bitdefender vous demandera automatiquement d'utiliser la connexion sécurisée lorsque vous ouvrirez Bitdefender Safepay. Saisissez simplement vos identifiants MyBitdefender lorsque vous y êtes invité.

La connexion sécurisée sera initialisée et un message s'affichera dans la fenêtre Bitdefender Safepay lorsque la connexion sera établie. Le symbole  apparaît en face de l'URL dans la barre d'adresses pour vous aider à identifier facilement les connexions sécurisées.

23. Contrôle Parental

Le module de contrôle parental de vous permet de contrôler l'accès à Internet et à des applications spécifiques pour chaque utilisateur disposant d'un compte utilisateur sur le système.

Une fois le Contrôle Parental configuré, il est facile pour vous de connaître les activités de votre enfant sur l'ordinateur.

Il vous suffit d'un ordinateur avec accès Internet et d'un navigateur web.

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 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.

Vérifiez les activités de vos enfants et modifiez les paramètres du Contrôle Parental à l'aide de MyBitdefender depuis tout ordinateur ou appareil mobile connecté à Internet.

23.1. Accéder au tableau de bord du Contrôle Parental

Le tableau de bord du Contrôle Parental est organisé en modules qui vous permettent de surveiller les activités de l'enfant sur l'ordinateur.

Bitdefender vous permet de contrôler l'accès de vos enfants à Internet et à certaines applications. Il vous permet également de surveiller l'activité de leur compte Facebook.

Bitdefender vous permet d'accéder aux paramètres du Contrôle Parental depuis un compte MyBitdefender sur tout ordinateur ou appareil mobile connecté à Internet.

Accédez à votre compte en ligne :

- Sur tout appareil avec un accès à Internet :
 1. Ouvrez un navigateur web.
 2. Allez à : <https://myaccount.bitdefender.com/fr/MyAccount/login/>
 3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
 4. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
- Depuis votre interface Bitdefender 2013 :

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 **MyBitdefender** en haut de la fenêtre et sélectionnez **Contrôle Parental** dans le menu déroulant.
4. Le tableau de bord du Contrôle Parental s'ouvrira dans une nouvelle fenêtre. Vous pouvez vérifier et configurer ici les paramètres du Contrôle Parental de chaque compte utilisateur Windows.

23.2. Ajouter le profil de votre enfant

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. 53).

Pour ajouter le profil de votre enfant au Contrôle Parental :

1. Accédez au tableau de bord du Contrôle Parental depuis votre compte MyBitdefender.
2. Cliquez sur **Ajouter un enfant** sur le menu de gauche.
3. Indiquez le nom et l'âge de l'enfant dans l'onglet **Profil**. 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.
4. Sélectionnez l'onglet **Appareils**.

L'onglet Périphériques vous permet de voir les ordinateurs et les appareils mobiles liés à votre compte MyBitdefender.

5. Sélectionnez l'ordinateur et le compte Windows de votre enfant.
6. Cliquez sur **Enregistrer**.

L'ordinateur et le compte Windows de votre enfant sont désormais liés à votre compte MyBitdefender.

23.2.1. Surveiller les activités de l'enfant

Bitdefender vous aide à surveiller l'activité de vos enfants sur l'ordinateur.

Vous pouvez de cette façon toujours savoir exactement quels sites web ils ont consultés, quelles applications ils ont utilisées et les activités bloquées par le Contrôle Parental.

Les rapports contiennent des informations détaillées pour chaque événement, comme :

- L'état de l'événement.
- Le nom du site web bloqué.
- Le nom de l'application bloquée.
- Le nom de l'appareil.
- La date et l'heure auxquelles l'événement a eu lieu.
- Les actions appliquées par Bitdefender.

Pour surveiller le trafic Internet, les applications auxquelles a accédé votre enfant et ses activités, procédez comme suit :

1. Accédez au tableau de bord du Contrôle Parental depuis votre compte MyBitdefender.
2. Cliquez sur  pour accéder à la fenêtre d'activité du module correspondant.

23.2.2. Configurer les notifications par e-mail

Lorsque le Contrôle Parental est activé, les activités de vos enfants sont enregistrées par défaut.

Pour recevoir des notifications par email, procédez comme suit :

1. Accédez au tableau de bord du Contrôle Parental depuis votre compte MyBitdefender.
2. Cliquez sur l'icône **Paramètres généraux**  dans l'angle supérieur droit.
3. Saisissez l'adresse e-mail pour recevoir les notifications par e-mail.
4. Cliquez sur le bouton à côté de **Mise à jour** pour ajuster la fréquence : quotidienne, hebdomadaire, ou mensuelle.

23.3. Configuration du Contrôle Parental

Le tableau de bord du Contrôle Parental vous permet de gérer directement les modules du Contrôle Parental.

Chaque module contient les éléments suivants : le nom du module, un message d'état, l'icône du module et un bouton  qui vous permet d'effectuer d'importantes tâches liées au module.

Cliquez sur un onglet pour configurer la fonction de contrôle parental correspondante pour l'ordinateur :

- **Web** - permet de filtrer la navigation Web et de définir des restrictions horaires pour l'accès à Internet.
- **Applications** - permet de bloquer ou de limiter l'accès à certaines applications.
- **Facebook** - permet de protéger le compte Facebook de votre enfant.
- **Messagerie Instantanée** - permet d'autoriser ou de bloquer les conversations avec certains contacts de messagerie instantanée.

Vous pouvez accéder aux modules suivants pour surveiller l'activité de votre enfant sur l'appareil mobile :

- **Localisation** - permet de situer l'appareil de votre enfant sur Google Maps.
- **SMS** - permet de bloquer les messages de texte provenant d'un numéro de téléphone spécifique.
- **Appels** - permet de bloquer les appels provenant d'un numéro de téléphone spécifique.

Pour plus d'informations sur ces modules, accédez à votre compte MyBitdefender.

23.3.1. Contrôle Web

Le Contrôle Web vous aide à bloquer les sites web au contenu inapproprié et à définir des restrictions horaires pour l'accès à Internet.

Pour configurer le Contrôle Web pour un compte utilisateur spécifique :

1. Cliquez  sur le panneau **Web** pour accéder à la fenêtre **Activité Web**.
2. Utilisez le bouton pour activer l'**Activité Web**.

Bloquer un site web

Pour bloquer l'accès à un site web, procédez comme suit :

1. Cliquez sur le bouton **Liste noire**.
2. Indiquez le site web dans le champ correspondant.
3. Cliquez sur **Ajouter**. Le site web sera ajouté à la liste des sites web bloqués. Si vous changez d'avis, cliquez sur le bouton **Supprimer** correspondant.

Contrôle par Mots-clés

Le Contrôle par mots-clés vous aide à bloquer l'accès des utilisateurs aux messages instantanés et aux pages web contenant certains mots. Le Contrôle par mots-clés vous permet d'empêcher que vos enfants ne voient des mots ou des expressions inappropriés lorsqu'ils sont en ligne. 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.

Pour configurer le Contrôle par mots-clés pour un compte utilisateur spécifique, procédez comme suit :

1. Cliquez sur le bouton **Mots-clés**.
2. Indiquez le mot-clé dans le champ correspondant.
3. Cliquez sur **Ajouter**. Si vous changez d'avis, cliquez sur le bouton **Supprimer** correspondant.

Filtrage par Catégories

Le Filtrage par catégories filtre de façon dynamique l'accès aux sites web en fonction de leur contenu. Lorsque vous définissez l'âge de votre enfant, le filtre est automatiquement configuré pour bloquer les catégories de sites web considérées comme inappropriées à l'âge de votre enfant. Cette configuration convient à la plupart des cas.

Si vous souhaitez mieux contrôler le contenu Internet auquel votre enfant est exposé, vous pouvez choisir les catégories de sites web à bloquer avec le Filtrage par Catégories.

Pour configurer en détail l'accès aux paramètres du Filtrage par catégories pour un compte utilisateur spécifique, procédez comme suit :

1. Cliquez sur le bouton **Catégories**.
2. Vous pouvez vérifier les catégories Web bloquées/restreintes automatiquement pour les âges sélectionnés. Si vous n'êtes pas satisfait des paramètres par défaut, vous pouvez les configurer selon vos besoins.
3. Cliquez sur **Enregistrer**.

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 du **Planificateur Web** dans la fenêtre **Activité Web**.

Pour configurer en détail l'accès à Internet pour un compte utilisateur spécifique, procédez comme suit :

1. Cliquez sur le bouton **Planifier**.
2. Sélectionnez dans la grille les intervalles de temps pendant lesquels l'accès à Internet est bloqué.
3. Cliquez sur **OK**.

23.3.2. Contrôle des Programmes

Le Contrôle des Programmes vous aide à bloquer l'exécution de tout programme. Les logiciels de jeux, pour médias et de messagerie, ainsi que d'autres catégories de logiciels et de malwares peuvent être bloqués de cette manière.

Pour configurer le Contrôle des Programmes pour un compte utilisateur spécifique, procédez comme suit :

1. Cliquez sur le panneau  **Applications** pour accéder à la fenêtre **Activité des Applications**.
2. Utilisez le bouton pour activer l'**Activité des Applications**.
3. Cliquez sur le bouton **Liste noire**.
4. Cliquez sur **Ajouter** pour ajouter l'application aux **Applications de la Liste Blanche** ou aux **Applications de la Liste Noire**.

23.3.3. Protection Facebook

Le Contrôle Parental surveille le compte Facebook de votre enfant et signale ses principales activités.

Ces activités en ligne sont vérifiées et vous êtes averti si elles constituent une menace pour la confidentialité de votre compte.

Les éléments surveillés du compte en ligne comprennent :

- le nombre d'amis
- les commentaires de l'enfant ou de ses amis sur ses photos ou publications
- messages
- les publications du mur
- les photos et vidéos téléchargées
- les paramètres de confidentialité du compte

Pour configurer la protection Facebook pour un compte utilisateur spécifique :

1. Allez dans l'onglet **Facebook**.
2. Cliquez sur **Connecter le profil de l'enfant** dans le panneau **Facebook**.
3. Pour protéger le compte Facebook de l'enfant, installez l'application à l'aide du lien correspondant.

23.3.4. Contrôle des Messageries Instantanées

Le Contrôle des Messageries Instantanées (MI) vous permet de spécifier les contacts de MI avec lesquels vos enfants sont autorisés à discuter et de bloquer l'accès aux messages instantanés contenant certains mots.



Note

Le Contrôle des MI est disponible uniquement pour Yahoo! Messenger et Windows Live Messenger (MSN).

Pour configurer le Contrôle des Messageries Instantanées pour un compte utilisateur spécifique, procédez comme suit :

1. Allez dans l'onglet **Messagerie Instantanée**.
2. Cliquez  sur le panneau **Messagerie Instantanée** pour accéder à la fenêtre **Activité Messageries Instantanées**.
3. Utilisez le bouton pour activer l'**Activité Messageries Instantanées**.

Limitez l'accès à la **Messagerie Instantanée** à l'aide de l'une des options disponibles :

- Le bouton **liste noire** pour saisir un identifiant de messagerie instantanée.
- Le bouton **Mots-clés** pour bloquer l'accès aux messages instantanés contenant certains mots.

24. Protection Safego pour réseaux sociaux

Vous faites confiance à vos amis en ligne, mais faites-vous confiance à 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 Bitdefender développée pour assurer la sécurité de vos comptes Facebook et Twitter. Son rôle consiste à analyser les liens que vous recevez de la part de vos amis 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 « *Compte MyBitdefender* » (p. 34).

Protection Safego pour Facebook

Les principales fonctionnalités disponibles pour votre compte Facebook sont les suivantes :

- 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 pour Facebook à partir de votre produit Bitdefender, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Safego**, cliquez sur **Gérer** et sélectionnez **Activer pour Facebook** dans le menu déroulant. Vous serez dirigé vers votre compte.
Si vous avez déjà activé Safego pour Facebook, vous aurez accès à des statistiques sur son activité en cliquant sur le bouton **Afficher les rapports pour Facebook**.
3. Utilisez vos informations de connexion Facebook pour vous connecter à l'application Safego.
4. Autoriser Safego à accéder à votre compte Facebook.

Protection Safego pour Twitter

Les principales fonctionnalités disponibles pour votre compte Twitter sont les suivantes :

- analyse en permanence votre compte en tâche de fond.
- quand une menace est détectée, vous êtes averti via un message direct afin que vous puissiez adopter les actions nécessaires à sa neutralisation.
- envoie un message direct depuis votre compte aux personnes de votre liste d'abonnements pour lesquelles des problèmes de compte ont été détectés.
- analyse vos messages privés à la recherche de spam, de phishing et de malwares.
- publie automatiquement des statistiques de sécurité hebdomadaires sur l'activité de votre compte.

Pour accéder à Safego pour Twitter à partir de votre produit Bitdefender, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Safego**, cliquez sur **Gérer** et sélectionnez **Activer pour Twitter** dans le menu déroulant. Vous serez dirigé vers votre compte.
Si vous avez déjà activé Safego pour Twitter, vous aurez accès à des statistiques sur son activité en cliquant sur le bouton **Afficher les rapports pour Twitter**.
3. Utilisez vos informations de connexion Twitter pour vous connecter à l'application Safego.
4. Autoriser Safego à accéder à votre compte Twitter.

25. Antivol de l'appareil

La vol d'ordinateurs portables est un problème important qui touche à la fois les particuliers et les entreprises. Plus que la perte du matériel en lui-même, la perte des données qui l'accompagne peut causer d'importants dommages, à la fois financiers et émotionnels.

Pourtant, peu de personnes prennent les mesures adaptées pour protéger leurs données personnelles, commerciales et financières importantes en cas de perte ou de vol.

Bitdefender Anti-Theft vous aide à mieux vous préparer à un tel événement en vous permettant de localiser ou de verrouiller à distance votre ordinateur, et même, d'effacer toutes ses données, si jamais vous en étiez séparé contre votre gré.

Pour utiliser les fonctionnalités Antivol, les configurations requises suivantes doivent être remplies :

- Vous devez lier votre ordinateur à un compte MyBitdefender en vous connectant à un compte depuis Bitdefender Total Security 2013.
- Les commandes peuvent uniquement être envoyées depuis le compte MyBitdefender auquel votre ordinateur est lié.
- L'ordinateur doit être connecté à Internet pour recevoir les commandes.

Les fonctionnalités Antivol fonctionnent de la manière suivante :

Localisation à distance

Afficher l'endroit où se trouve votre appareil sur Google Maps.

La précision de la localisation dépend de la façon dont Bitdefender est capable de la déterminer. L'emplacement est déterminé avec une précision de dix mètres si le Wifi est activé sur votre ordinateur et s'il y a des réseaux sans fil à sa portée.

Si l'ordinateur est connecté à un réseau local câblé sans emplacement Wifi disponible, son emplacement sera déterminé en fonction de l'adresse IP, ce qui est bien moins précis.

Verrouillage à distance

Verrouillez votre ordinateur et spécifiez un code PIN à 4 chiffres pour le déverrouiller. Lorsque vous envoyez la commande Verrouiller, l'ordinateur redémarre et se reconnecter à Windows est possible uniquement après avoir saisi le code PIN que vous avez défini.

Effacement des données à distance

Effacer toutes les données de votre ordinateur. Lorsque vous envoyez la commande Effacer, l'ordinateur redémarre et les données sur toutes les partitions du disque dur sont effacées.

Anti-Theft est activé après l'installation et est accessible uniquement via votre compte MyBitdefender à partir de tout appareil connecté à Internet, où que vous soyez.

Utiliser les fonctionnalités Antivol depuis MyBitdefender

Pour accéder aux fonctionnalités antivol à partir de votre compte, procédez comme suit :

1. Allez dans <https://myaccount.bitdefender.com/fr/MyAccount/login/> et connectez-vous à votre compte.
2. Cliquez sur **Anti-Theft**.
3. Sélectionnez votre ordinateur dans la liste de périphériques.
4. Sélectionnez la fonctionnalité que vous souhaitez utiliser :



Localiser - permet d'afficher la localisation de votre appareil sur Google Maps.



Effacer - permet d'effacer toutes les données de votre ordinateur.



Important

Une fois les données d'un appareil effacées, toutes les fonctionnalités Antivol cessent de fonctionner.



Verrouiller - permet de verrouiller votre ordinateur et de spécifier un code PIN pour le déverrouiller.

26. Bitdefender USB Immunizer

La fonction Autorun intégrée aux systèmes d'exploitation Windows est très utile car elle permet aux ordinateurs d'exécuter automatiquement un fichier depuis un support qui y est connecté. Par exemple, les installations de logiciels peuvent démarrer automatiquement lorsqu'un CD est inséré dans le lecteur optique.

Malheureusement, cette fonctionnalité peut également être utilisée par des malwares pour se lancer automatiquement et infiltrer votre ordinateur depuis des supports réinscriptibles tels que des lecteurs flash USB et des cartes mémoire connectés via des lecteurs de cartes. De nombreuses attaques exploitant la fonctionnalité Autorun ont été créées ces dernières années.

Avec USB Immunizer, vous pouvez empêcher tout lecteur flash formaté en NTFS, FAT32 ou FAT d'exécuter des malwares. Lorsqu'un périphérique USB est immunisé, les malwares ne peuvent plus le configurer pour qu'il exécute une application spécifique lorsqu'il est connecté à un ordinateur fonctionnant sous Windows.

Pour immuniser un périphérique USB, procédez comme suit :

1. Connectez le lecteur flash à votre ordinateur.
2. Localisez sur votre ordinateur le périphérique de stockage amovible et faites un clic droit sur son icône.
3. Dans le menu contextuel, pointez sur **Bitdefender** et sélectionnez **Immuniser ce lecteur**.



Note

Si le lecteur a déjà été immunisé, le message **Le périphérique USB est protégé contre les malwares autorun** s'affichera au lieu de l'option Immuniser.

Pour empêcher que votre ordinateur ne lance des malwares depuis des lecteurs USB non immunisés, désactivez la fonction Exécution automatique des médias. Pour plus d'informations, reportez-vous à « *Utiliser la surveillance des vulnérabilités automatique* » (p. 94).

27. Gérer vos ordinateurs à distance

Votre compte MyBitdefender vous permet de gérer les produits Bitdefender installés sur vos ordinateurs à distance.

Utilisez MyBitdefender pour créer et appliquer à distance des tâches à vos ordinateurs.

Tout ordinateur sera géré depuis un compte MyBitdefender s'il remplit les conditions suivantes :

- vous avez installé un produit Bitdefender 2013 sur l'ordinateur
- vous avez lié le produit Bitdefender au compte MyBitdefender.
- l'ordinateur est connecté à Internet

27.1. Accéder à MyBitdefender

Bitdefender vous permet de contrôler la sécurité de vos ordinateurs en ajoutant des tâches à vos produits Bitdefender.

Bitdefender vous permet d'accéder à votre compte MyBitdefender sur tout ordinateur ou appareil mobile connecté à Internet.

Accédez à MyBitdefender :

- Sur tout appareil avec un accès à Internet :
 1. Ouvrez un navigateur web.
 2. Allez à : <https://myaccount.bitdefender.com/fr/MyAccount/login/>
 3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
- Depuis votre interface Bitdefender 2013 :
 1. Ouvrez la **fenêtre de Bitdefender**.
 2. Cliquez sur le bouton **MyBitdefender** en haut de la fenêtre et sélectionnez **Tableau de bord** dans le menu déroulant.

27.2. Exécuter des tâches sur les ordinateurs

Pour exécuter une tâche sur l'un de vos ordinateurs, accédez à votre compte MyBitdefender.

En cliquant sur l'icône d'un ordinateur en bas de la fenêtre, vous pouvez voir toutes les tâches administratives que vous pouvez lancer sur cet ordinateur distant.

Enregistrement du Produit

Vous permet d'enregistrer Bitdefender sur l'ordinateur distant en entrant une clé de licence.

Effectuer une analyse complète de votre PC

Vous permet de lancer une analyse complète sur l'ordinateur distant.

Analyser les zones critiques pour détecter les malwares actifs

Vous permet de lancer une analyse rapide sur l'ordinateur distant.

Corriger les problèmes critiques

Vous permet de corriger les problèmes affectant la sécurité de l'ordinateur distant.

Mise à jour du produit

Lance le processus de mise à jour du produit Bitdefender installé sur cet ordinateur.

Optimisation et sauvegarde

28. 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 l'espace sur le 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.

28.1. 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. Dans le panneau **Optimisation**, cliquez sur **Optimiser** et sélectionnez **Nettoyage du PC** dans le menu déroulant.
3. 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**

Activez ou désactivez les options de Nettoyage du PC en cliquant sur **Nettoyage Personnalisé** :

- Vider le cache Internet Explorer
- Vider le cache Mozilla Firefox
- Nettoyer les documents récents et les fichiers système temporaires

b. **Réaliser un Nettoyage**

c. **Résultats**

28.2. 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. Dans le panneau **Optimisation**, cliquez sur **Optimiser** et sélectionnez **Défragmenteur de disque** dans le menu déroulant.
3. 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

Patiencez 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

Veillez 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.

28.3. 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. Dans le panneau **Optimisation**, cliquez sur **Optimiser** et sélectionnez **Détecteur de doublons** dans le menu déroulant.
3. 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

Patiencez jusqu'à ce que Bitdefender ait terminé la recherche de doublons.

c. 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

28.4. 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. Dans le panneau **Optimisation**, cliquez sur **Optimiser** et sélectionnez **Nettoyage du registre** dans le menu déroulant.
3. 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

Patiencez 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 :

- **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 DLL intègrent des fonctions qui sont utilisées par les applications installées pour effectuer certaines tâches. Elles peuvent être partagées par de multiples applications pour 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 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.

d. Résultats

28.5. 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 registre 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. Dans le panneau **Optimisation**, cliquez sur **Optimiser** et sélectionnez **Restauration du registre** dans le menu déroulant.
3. 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 un point de contrôle

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

28.6. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Optimisation**.
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 support de Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 191).

29. Sauvegarde et synchronisation en ligne de Safebox

Safebox est le service Bitdefender qui vous permet de sauvegarder vos données importantes sur des serveurs en ligne sécurisés, de les partager avec vos amis et de les synchroniser entre vos appareils.



Note

Un compte MyBitdefender est nécessaire pour utiliser cette fonctionnalité. Pour plus d'informations, reportez-vous à « *Compte MyBitdefender* » (p. 34).

Avec Safebox :

- Vous obtenez 2 Go d'espace gratuit 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**.
- 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.
- Vous pouvez synchroniser des fichiers entre plusieurs appareils sur lesquels sont installés Bitdefender Total Security 2013 ou l'application autonome Safebox. Les applications Safebox sont disponibles pour Windows PC, iOS et Android.

Pour plus d'informations, consultez <http://www.bitdefender.com/solutions/safebox.html>.

- Vous pouvez accéder à vos fichiers même sur des appareils sur lesquels Bitdefender Total Security 2013 et Bitdefender Safebox ne sont pas installés en accédant simplement à votre compte MyBitdefender directement à partir du navigateur de tout ordinateur ou appareil mobile connecté à Internet.

29.1. Activation de Safebox

Pour activer Safebox, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Safebox**, cliquez sur le bouton **Sync. auto.**

Un raccourci vers le dossier Safebox par défaut est placé sur votre bureau.

Pour sauvegarder facilement vos données sur les serveurs de Bitdefender, maintenez la synchronisation automatique activée.

Les sauvegardes de Safebox peuvent être gérées à partir de la fenêtre de Bitdefender, de Windows Explorer et d'autres gestionnaires de fichiers à l'aide du menu contextuel de Windows, ou en ligne à partir du compte MyBitdefender.

29.2. Gérer Safebox à partir de la fenêtre de Bitdefender

Pour gérer vos sauvegardes Safebox à partir de Bitdefender, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Dans le panneau **Safebox**, cliquez sur **Gérer** et sélectionnez une option dans le menu déroulant.

Gérer les dossiers

Une nouvelle fenêtre apparaîtra listant les dossiers ajoutés à Safebox depuis cet ordinateur, ainsi que depuis d'autres ordinateurs et depuis MyBitdefender.

- Pour ajouter un nouveau dossier à la synchronisation de Safebox, localisez-le sur votre ordinateur puis glissez-déposez-le dans la fenêtre Gérer les dossiers.

Ajoutez des dossiers à la synchronisation de Safebox et activez la Synchronisation Automatique de Safebox pour qu'elle synchronise automatiquement leur contenu avec les serveurs Safebox en ligne accessibles à partir de MyBitdefender.

- Pour supprimer un dossier de la synchronisation de Safebox, sélectionnez-le et cliquez sur le bouton **Désync.**



Note

Supprimer un dossier de la synchronisation de SafeBox ne supprime pas le dossier en ligne, cela supprime uniquement le lien entre le dossier local et le dossier en ligne.

- Les dossiers de Safebox ajoutés depuis d'autres ordinateurs ou depuis MyBitdefender apparaissent dans la liste mais ne sont pas synchronisés par défaut (l'icône  apparaît à côté d'eux).

Pour ajouter l'un de ces dossiers aux dossiers synchronisés sur cet ordinateur, sélectionnez-le et cliquez sur **Sync.** Une nouvelle fenêtre apparaîtra vous demandant de sélectionner l'emplacement du dossier local. Cliquez sur **Oui** pour utiliser l'emplacement par défaut, ou sur **Non** pour sélectionner un autre emplacement.

Pour supprimer un dossier non synchronisé ajouté depuis un autre ordinateur de la liste, sélectionnez-le et cliquez sur **Supprimer.**

Gérer les fichiers partagés

Une nouvelle fenêtre apparaîtra listant les fichiers ajoutés au partage Safebox depuis cet ordinateur, ainsi que depuis d'autres ordinateurs et depuis MyBitdefender.

- Pour ajouter un nouveau fichier au partage Safebox, localisez-le sur votre ordinateur puis glissez-déposez-le dans la fenêtre Gérer le partage. Une nouvelle fenêtre apparaîtra indiquant la progression du téléchargement. Une

fois le téléchargement terminé, copiez le lien public dans le presse-papiers en cliquant sur le message correspondant.

- Pour copier le lien d'un fichier d'une liste vers le presse-papiers, cliquez sur le bouton **Partager le lien** puis sur le message correspondant.
- Pour supprimer un fichier du partage Safebox, sélectionnez-le et cliquez sur **Supprimer le lien**.

29.3. Gérer 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.

29.3.1. 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 est créé sur les serveurs Bitdefender et le contenu de l'ensemble du dossier y est téléchargé. 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.

29.3.2. Supprimer des dossiers de la Safebox

Pour retirer un dossier de la synchronisation de Safebox, faites un clic droit dessus, pointez sur **Bitdefender Safebox** et sélectionnez **Retirer de Bitdefender Safebox**. Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour empêcher que Safebox ne synchronise le dossier.

29.3.3. 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 sur **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**.

29.4. Gérer Safebox depuis MyBitdefender

Vous pouvez accéder à vos dossiers de Safebox via votre compte MyBitdefender à partir de tout ordinateur ou appareil mobile connecté à Internet. Les mêmes opérations peuvent être effectuées depuis votre compte à partir de Bitdefender Total Security 2013.

Pour accéder à Safebox depuis MyBitdefender :

- Depuis tout ordinateur ou appareil mobile, connectez-vous à votre compte sur <https://myaccount.bitdefender.com/fr/MyAccount/login/> puis cliquez sur l'icône de Safebox.
- Depuis Bitdefender Total Security 2013 :
 1. Ouvrez la **fenêtre de Bitdefender**.
 2. Dans le panneau **Safebox**, cliquez sur **Gérer** et sélectionnez **Aller au Tableau de bord** dans le menu déroulant.

29.5. 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 2013 ou l'application autonome de Safebox est installé sur les ordinateurs entre lesquels vous souhaitez synchroniser les fichiers.
- Vous êtes connecté avec le même compte MyBitdefender sur chaque ordinateur.

- Les dossiers locaux liés au même dossier en ligne ont été ajoutés à la synchronisation de Safebox sur chaque ordinateur.
- Pour la synchronisation automatique, vérifiez que la **Synchronisation Automatique** de Safebox est activée sur tous les ordinateurs.

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.

29.6. Mise à niveau de votre espace en ligne

Safebox vous offre 2 Go d'espace gratuit en ligne pour vos sauvegardes.

Si vous avez une grande quantité de données avec de la musique, des films ou d'importants fichiers ayant besoin d'être protégés, les 2 Go d'espace gratuit en ligne peuvent ne pas être suffisants.

Pour augmenter votre espace Safebox, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Safebox**.
4. Dans la fenêtre **Paramètres de Safebox**, cliquez sur **Mettre à niveau Safebox**.
5. La page MyBitdefender s'ouvrira dans votre navigateur web. Suivez les instructions pour acheter de l'espace supplémentaire.

29.7. Supprimer définitivement des fichiers

Pour supprimer complètement un fichier de Safebox, vous devez non seulement le supprimer du dossier Safebox de votre ordinateur, mais également du dossier en ligne. Suivez ces étapes :

1. Allez dans <https://myaccount.bitdefender.com/fr/MyAccount/login/> et connectez-vous à votre compte.
2. Cliquez sur l'icône de Safebox.
3. Dans l'onglet **Fichiers et dossiers**, sélectionnez le fichier puis **Supprimer** dans le menu déroulant Actions. Le fichier sera placé dans la Corbeille de Safebox.
4. Dans l'onglet **Corbeille**, sélectionnez le fichier puis **Supprimer** dans le menu déroulant Actions. Cliquez sur **Oui** dans la fenêtre de confirmation pour supprimer complètement le fichier.

Une fois un fichier complètement supprimé de Safebox, vous ne pouvez plus le restaurer ni récupérer de versions antérieures.

29.8. Limiter l'allocation de bande passante

La sauvegarde de vos fichiers peut ralentir votre connexion à Internet, en particulier lorsque vous transférez de grandes quantités de données.

Afin de ne pas interférer avec d'autres activités en ligne, vous pouvez limiter la quantité de bande passante allouée aux transferts de Safebox.

Pour limiter la bande passante de Safebox à 50 Ko/s, procédez comme suit :

1. Ouvrez la **fenêtre de Bitdefender**.
2. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
3. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Safebox**.
4. Dans la fenêtre **Paramètres de Safebox**, cliquez sur le bouton **limiter la bande passante**.

Résolution des problèmes

30. Résoudre les problèmes les plus fréquents

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. 165)
- « *L'analyse ne démarre pas* » (p. 166)
- « *Je ne peux plus utiliser une application* » (p. 167)
- « *Je ne peux pas me connecter à Internet* » (p. 168)
- « *Je ne peux pas accéder à un périphérique de mon réseau* » (p. 168)
- « *Mon Internet est lent* » (p. 170)
- « *Comment mettre à jour Bitdefender avec une connexion Internet lente* » (p. 171)
- « *Mon ordinateur n'est pas connecté à Internet. Comment actualiser Bitdefender?* » (p. 172)
- « *Le Services Bitdefender ne répondent pas* » (p. 172)
- « *Le filtre antispam ne fonctionne pas correctement* » (p. 173)
- « *La désinstallation de Bitdefender a échoué* » (p. 178)
- « *Mon système ne démarre pas après l'installation de Bitdefender* » (p. 178)

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 « *Demander de l'aide* » (p. 191).

30.1. 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. 66).

● **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. 3).

- **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. 155).

- **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. 153).

- **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. 157).

30.2. 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. 66).
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. 191).

30.3. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antivirus**.
4. Dans la fenêtre **Paramètres Antivirus**, sélectionnez l'onglet **Exclusions**.

5. Cliquez sur le lien **Processus Exclus**. Dans la fenêtre qui apparaît, vous pouvez gérer les exclusions de processus Active Virus Control.
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 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. 191).

30.4. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Pare-feu**.
4. Dans la fenêtre **Paramètres du pare-feu**, sélectionnez l'onglet **Paramètres**.
5. Sous Règles pare-feu, cliquez sur **Règles d'Applications**.
6. Pour ajouter une règle d'application, cliquez sur le bouton correspondant.
7. Cliquez sur **Parcourir** et sélectionnez l'application à laquelle s'applique la règle.
8. Sélectionnez tous les types de réseau disponibles.
9. 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. 191).

30.5. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Pare-feu**.
4. Dans la fenêtre **Paramètres du pare-feu**, sélectionnez l'onglet **Paramètres**.
5. Sous Règles pare-feu, cliquez sur **Règles d'adaptateurs**.
6. Pour ajouter une zone, cliquez sur le bouton correspondant. Une nouvelle fenêtre affichant les adresses IP des périphériques connectés au réseau s'affichera.
7. 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.
8. 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. 191).

30.6. 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. Dans le panneau **Pare-feu**, cliquez sur le bouton pour désactiver le **Pare-feu**.
3. Vérifiez si votre connexion Internet s'est améliorée avec le pare-feu Bitdefender désactivé.

- Si votre connexion à Internet est toujours lente, le problème n'est peut-être pas causé par Bitdefender. Nous vous recommandons de contacter votre fournisseur d'accès à Internet afin de vérifier si la connexion est opérationnelle 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. 191).

- Si la connexion Internet s'est améliorée après la désactivation du pare-feu Bitdefender, suivez ces étapes :

- a. Ouvrez la **fenêtre de Bitdefender**.
- b. Dans le panneau **Pare-feu**, cliquez sur le bouton pour activer le **Pare-feu**.
- c. Cliquez sur le bouton **Configuration** de la barre d'outils supérieure.
- d. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Pare-feu**.
- e. Dans la fenêtre **Paramètres du Pare-feu**, sélectionnez l'onglet **Avancé**.
- f. Allez dans **Partage de connexion Internet** et cliquez sur le bouton pour l'activer.
- g. Allez dans **Bloquer les analyses de ports** et cliquez sur le bouton pour le désactiver.
- h. Cliquez sur  pour revenir à la fenêtre principale.
- i. Dans le panneau **Pare-feu**, cliquez sur **Activité du réseau**.
- j. Allez dans **Type de Réseau** et sélectionnez **Domicile/Bureau**.
- k. Allez dans **Mode Furtif** et réglez-le sur **Distant**. Réglez **Générique** sur **Oui**.
- l. 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. 191).

30.7. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Mise à jour**.
4. Dans la fenêtre **Paramètres des mises à jour**, sélectionnez l'onglet **Mise à jour**.
5. Sous **Règles de traitement des mises à jour**, sélectionnez **Demander avant le téléchargement**.
6. Cliquez sur  pour revenir à la fenêtre principale.

7. Allez dans l'onglet **Mise à jour**, et cliquez sur **Mettre à jour maintenant**.
8. Sélectionnez uniquement **Mises à jour de signatures**, puis cliquez sur **OK**.
9. Bitdefender ne téléchargera et n'installera que les mises à jour des signatures de malwares.

30.8. Mon ordinateur n'est pas connecté à Internet. Comment actualiser 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. 65).
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.

30.9. 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. 66).

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. 191).

30.10. 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.

30.10.1. 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. 100).

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. Dans le panneau **Antispam**, cliquez sur **Gérer** et sélectionnez **Amis** dans le menu déroulant.

Une fenêtre de configuration s'affichera.

3. 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.
4. 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 considérablement l'efficacité du filtrage 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antispam**.
4. Dans la fenêtre **Paramètres Antispam**, sélectionnez l'onglet **Paramètres**.
5. Descendez le curseur sur l'échelle.

30.10.2. 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. 100).

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). Ils sont immédiatement signalés comme étant du [spam] et déplacés vers le dossier du 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 autre client de messagerie, vous pouvez ajouter manuellement des spammeurs à la liste des 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. Dans le panneau **Antispam**, cliquez sur **Gérer** et sélectionnez **Spammeurs** dans le menu déroulant.
Une fenêtre de configuration s'affichera.
3. Tapez l'adresse e-mail du spammeur puis cliquez sur **Ajouter**. Vous pouvez ajouter autant d'adresses e-mail que vous le souhaitez.
4. 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. Dans la fenêtre **Aperçu des paramètres**, sélectionnez **Antispam**.
4. Dans la fenêtre **Paramètres Antispam**, sélectionnez l'onglet **Paramètres**.
5. Élevez le curseur sur l'échelle.

30.10.3. 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 2013 n'analyse pas le trafic POP3 de Lotus Notes.

Une solution possible consiste à réparer ou à réinstaller le produit. Il est toutefois recommandé de contacter Bitdefender pour obtenir de l'assistance, comme cela est décrit dans la section « *Demander de l'aide* » (p. 191).

30.11. 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 de 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. 191).

30.12. 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. 67).
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. 67).
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. 67).

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. 66).
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. 191).

31. 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. 181)
- « *Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ?* » (p. 183)
- « *Comment nettoyer un virus dans une archive ?* » (p. 184)
- « *Comment nettoyer un virus dans une archive de messagerie ?* » (p. 185)
- « *Que faire si je suspecte un fichier d'être dangereux ?* » (p. 186)
- « *Comment nettoyer les fichiers infectés du System Volume Information ?* » (p. 187)
- « *Que sont les fichiers protégés par mot de passe du journal d'analyse ?* » (p. 188)
- « *Que sont les éléments ignorés du journal d'analyse ?* » (p. 188)
- « *Que sont les fichiers ultra-compressés du journal d'analyse ?* » (p. 189)
- « *Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?* » (p. 189)

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 « *Demander de l'aide* » (p. 191).

31.1. 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 2013 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. Ouvrez la **fenêtre de Bitdefender**.

2. Dans le panneau **Antivirus**, 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. 181).
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.

31.2. 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. Sélectionnez **Antivirus**.
 - d. Cliquez sur l'onglet **Résident** dans la fenêtre **Paramètres Antivirus**.
 - e. 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. 65).
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. 67).
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. 191).

31.3. 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 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. Sélectionnez **Antivirus**.
 - d. Cliquez sur l'onglet **Résident** dans la fenêtre **Paramètres Antivirus**.
 - e. 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. Recompresser 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. 191).

31.4. 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. Sélectionnez **Antivirus**.
 - d. Cliquez sur l'onglet **Résident** dans la fenêtre **Paramètres Antivirus**.
 - e. 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. Compactionnez 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. 191).

31.5. 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. Exécuter une **Analyse du Système** avec Bitdefender. Pour savoir comment faire cela, reportez-vous à « **Comment analyser mon système ?** » (p. 47).
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. 191).

31.6. 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. 191).

31.7. 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.

31.8. 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.

31.9. 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.

Surcomprimé signifie que Bitdefender a ignoré l'analyse dans cette archive car sa décompression consommait trop de ressources système. Le contenu sera analysé à l'accès en temps réel si nécessaire.

31.10. 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.

Nous contacter

32. Demander de l'aide

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 Clients de Bitdefender. Nos membres du support technique répondront à vos questions aussi rapidement que possible et vous fourniront l'assistance dont vous avez besoin.

La section « *Résoudre les problèmes les plus fréquents* » (p. 165) 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. 191)
- « **Contactez-nous via notre Centre de Support en ligne** » (p. 192)



Important

Pour contacter le Service Client de Bitdefender, vous devez enregistrer votre produit Bitdefender. Pour plus d'informations, reportez-vous à « *Enregistrer Bitdefender* » (p. 32).

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 :
 - **Aide de Bitdefender.**
Parcourez les articles de la documentation Bitdefender et essayez les solutions proposées.
 - **Centre de Support**
Accédez à notre base de données et recherchez les informations nécessaires.
 - **Contacteur le Support**

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/support/consumer.html>. Le Centre de Support de Bitdefender contient de nombreux articles apportant des solutions aux problèmes liés à Bitdefender.
2. Sélectionnez votre produit et recherchez dans le Centre de Support de Bitdefender les articles susceptibles de fournir une solution à votre problème.
3. Consultez les articles et les documents pertinents et essayez les solutions proposées.
4. Si la solution ne règle pas votre problème, allez dans <http://www.bitdefender.fr/site/Main/nousContacter/> et contactez nos représentants du support.

32.1. 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.

33. 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/support/consumer.html>
- Forum du Support Bitdefender : <http://forum.bitdefender.com>
- le portail de sécurité informatique Malware City : <http://www.malwarecity.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.

33.1. 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 à tout moment sur <http://www.bitdefender.fr/support/consumer.html>.

33.2. 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 nouvelles publications afin de vous aider. Vous pouvez également obtenir une réponse ou une solution d'un utilisateur 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.

33.3. Portail Malware City

Le portail Malware City comprend de nombreuses informations sur la sécurité informatique. Vous pouvez découvrir ici 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.fr>.

34. 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.

34.1. 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.fr>

34.2. 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/#Trouver%20un%20partenaire>.
2. Les informations de contact des distributeurs locaux de Bitdefender devraient s'afficher automatiquement. Si ce n'est pas le cas, sélectionnez votre pays de résidence pour afficher les 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.

34.3. 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.com/help>

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, 1^o 1^a
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 Internet : <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 Internet : <http://www.bitdefender.ro>

Émirats arabes unis

Dubai Internet City

Building 17, Office # 160
Dubai, UAE
Téléphone du service commercial : 00971-4-4588935 / 00971-4-4589186
Email du service commercial : sales@bitdefender.com
Support technique : <http://www.bitdefender.com/suport>
Site Internet : <http://www.bitdefender.com/world>

Glossaire

ActiveX

ActiveX est un modèle pour écrire des programmes afin 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 poser ou répondre à des questions, utiliser des boutons et interagir de multiples 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 mais exigeant leur acceptation par l'utilisateur. Ces adwares étant généralement installés une fois 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 contrariants 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.

Applet Java

Il s'agit d'un programme Java conçu pour s'exécuter uniquement 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 laissée en place par des développeurs ou des personnes chargées de la maintenance. Les intentions ne sont pas toujours malveillantes ; quelques systèmes d'exploitation, par exemple, permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Chemin

Directions exactes vers un fichier d'un ordinateur. Ces directions sont généralement décrites 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 arme à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent car vous voyez seulement les annonces vous intéressant. Mais cela implique également le "pistage" et le "suivi" des sites que vous consultez et de ce sur quoi vous cliquez. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "numéro SKU" (le code barres se trouvant au dos des produits). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

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 le manque de 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 anciens OS n'en 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)

Fichier qui enregistre les actions ayant eu lieu. 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 basée sur des règles 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 les 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 les cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion ou 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

Zones de stockage internes dans l'ordinateur. Le terme mémoire définit le stockage de données sous la forme de composants électroniques, le mot stockage étant utilisé pour définir le stockage de données sur bande magnétique ou disques amovibles. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

Mise à jour

Nouvelle version d'un logiciel ou d'un produit hardware, destinée à remplacer une version antérieure du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, et si ce n'est pas le cas, 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 (plug-ins) 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 sembler être un virus et ne génère donc pas de fausses alertes.

Objets menu démarrage

Tous les fichiers placés dans ce dossier s'ouvrent au démarrage de l'ordinateur. Par exemple, un écran de démarrage, un fichier son pour le démarrage de l'ordinateur, un calendrier, des programmes, peuvent être placés dans ce dossier. C'est généralement un raccourci vers le fichier qui est placé 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 de l'e-mail. Cet e-mail oriente 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 sur un ordinateur auquel vous pouvez connecter un appareil. Les ordinateurs comportent plusieurs sortes de ports. Il existe plusieurs ports internes permettant de connecter des lecteurs de disques, des écrans et des claviers. A l'extérieur, les ordinateurs 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

Fichier dans un format compressé. Beaucoup de systèmes d'exploitation et d'applications contiennent des commandes vous permettant de compresser un fichier afin qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide" à la suite. Normalement, cela nécessite 10 octets.

Pourtant, un logiciel qui compresse des fichiers remplace la série d'espaces par un caractère spécial pour les séries 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 un accès de niveau administrateur à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX et se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs système.

Le principal rôle des rootkits est de masquer des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseau ou des périphériques, s'ils incluent les logiciels appropriés.

Les rootkits ne sont pas nécessairement malveillants. 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, modifier des fichiers et des logs et passer inaperçus.

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

Secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, du cluster, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge le système d'exploitation.

Signature de virus

La "signature" binaire du virus, utilisé par l'antivirus pour la détection et l'élimination du virus.

Spam

Messages électroniques ou messages de groupes de discussion indésirables. Souvent répertoriés comme des emails non sollicités.

Spyware

Tout type de logiciel récupérant les informations des utilisateurs via leur connexion Internet à leur insu, généralement à des fins publicitaires. Les spywares sont généralement cachés dans des logiciels sharewares ou freewares pouvant être téléchargés sur Internet. Notons toutefois que la plupart des applications sharewares ou freewares ne comportent pas de spywares. Une fois installé, le spyware surveille l'activité de l'utilisateur sur Internet et transmet discrètement ces 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 le fait que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une des manières les plus classiques d'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 les ressources de l'ordinateur de l'utilisateur en utilisant sa bande passante lors de l'envoi d'informations à leur base via la connexion Internet. En raison 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 - Ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux

interconnectés d'ordinateurs avec diverses architectures matérielles et divers systèmes d'exploitation. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Télécharger

Copie des données (généralement un fichier entier) d'une source principale vers 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)

Programme destructeur qui prétend être une application normale. Contrairement aux virus, les chevaux de Troie ne se répliquent pas, mais ils peuvent être tout aussi destructeurs. Un des types de chevaux de Troie les plus insidieux est un logiciel qui prétend désinfecter votre PC mais qui au lieu de cela l'infecte.

Le terme provient de la fameuse histoire de l'Illiade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Troyens, 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

Programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure de sa propagation. Il ne peut pas se joindre à d'autres programmes.

Virus

Programme ou morceau de code chargé dans votre ordinateur à votre insu et qui fonctionne contre votre gré. La plupart des virus peuvent également se répliquer. Tous les virus informatiques sont créés par des personnes. Un virus simple peut se copier très rapidement et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est par exemple capable de se transmettre via un réseau et de déjouer les systèmes de sécurité.

Virus de boot

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

Type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent de puissants 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

Virus qui change de forme avec chaque fichier qu'il infecte. Ces virus n'ayant pas de forme unique bien définie, ils 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.