

ANTIVIRUS
PLUS 2013



Bitdefender

Manuel d'utilisation

Bitdefender Antivirus Plus 2013

Bitdefender Antivirus Plus 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	14
5.4. Auto-Pilot	16
5.5. Mode Jeu et Mode Portable	16
5.5.1. Mode Jeu	17
5.5.2. Mode Portable	18
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	26
6.4. Widget Windows	27
6.4.1. Analyse des fichiers et des dossiers	29
6.4.2. Masquer / afficher le Widget Windows	29
7. Enregistrer Bitdefender	30
7.1. Saisie de votre clé de licence	30
7.2. Acheter ou renouveler des clés de licence	30
8. Compte MyBitdefender	32
8.1. Lier l'ordinateur à MyBitdefender	32
9. Maintenir Bitdefender à jour	35
9.1. Vérifier que Bitdefender est à jour	35
9.2. Mise à jour en cours	36
9.3. Activer ou désactiver la mise à jour automatique	36

9.4. Réglage des paramètres de mise à jour	37
Comment	39
10. Installation	40
10.1. Comment installer Bitdefender sur un deuxième ordinateur ?	40
10.2. Quand devrais-je réinstaller Bitdefender ?	40
10.3. Comment passer d'un produit Bitdefender 2013 à un autre ?	40
11. Enregistrement	42
11.1. Quel est le produit Bitdefender que j'utilise ?	42
11.2. Comment enregistrer une version d'essai ?	42
11.3. Quand ma protection Bitdefender expire-t-elle ?	42
11.4. Comment enregistrer Bitdefender sans connexion Internet ?	43
11.5. Comment renouveler ma protection Bitdefender ?	43
12. Analyser avec Bitdefender	45
12.1. Comment analyser un fichier ou un dossier ?	45
12.2. Comment analyser mon système ?	45
12.3. Comment créer une tâche d'analyse personnalisée ?	45
12.4. Comment exclure un dossier de l'analyse ?	46
12.5. Que faire lorsque Bitdefender a détecté un fichier sain comme étant infecté ?	47
12.6. Comment connaître les virus détectés par Bitdefender ?	48
13. Vie privée	49
13.1. Comment vérifier que ma transaction en ligne est sécurisée ?	49
13.2. Comment protéger mon compte Facebook ?	49
13.3. Comment supprimer définitivement un fichier avec Bitdefender ?	50
14. Informations Utiles	51
14.1. Comment éteindre automatiquement l'ordinateur une fois l'analyse terminée ?	51
14.2. Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?	51
14.3. Est-ce que j'utilise une version de Windows de 32 ou 64 bits ?	53
14.4. Comment afficher des objets masqués dans Windows ?	53
14.5. Comment supprimer les autres solutions de sécurité ?	54
14.6. Comment utiliser la Restauration du Système dans Windows ?	54
14.7. Comment redémarrer en mode sans échec ?	55
Gérer votre sécurité	57
15. Protection antivirus	58
15.1. Analyse à l'accès (protection en temps réel)	59
15.1.1. Activer ou désactiver la protection en temps réel	59
15.1.2. Régler le niveau de protection en temps réel	60
15.1.3. Configurer les paramètres de protection en temps réel	60
15.1.4. Restauration des paramètres par défaut	64
15.2. Analyse à la demande	64
15.2.1. Auto Scan	65

15.2.2. Rechercher des malwares dans un fichier ou un dossier	65
15.2.3. Exécuter une Analyse Rapide	65
15.2.4. Exécuter une Analyse du Système	66
15.2.5. Configurer une analyse personnalisée	66
15.2.6. Assistant d'analyse antivirus	69
15.2.7. Consulter les journaux d'analyse	72
15.3. Analyse automatique de supports amovibles	73
15.3.1. Comment cela fonctionne-t-il ?	73
15.3.2. Gérer l'analyse des supports amovibles	74
15.4. Configurer des exceptions d'analyse	75
15.4.1. Exclure de l'analyse des fichiers ou des dossiers	75
15.4.2. Exclure de l'analyse des extensions de fichiers	76
15.4.3. Gérer les exceptions d'analyse	77
15.5. Gérer les fichiers en quarantaine	77
15.6. Active Virus Control	78
15.6.1. Vérifier des applications détectées	78
15.6.2. Activer ou désactiver Active Virus Control	79
15.6.3. Régler la protection Active Virus Control	79
15.6.4. Gérer les processus exclus	80
15.7. Corriger les vulnérabilités du système	81
15.7.1. Analyser votre système à la recherche de vulnérabilités	81
15.7.2. Utiliser la surveillance des vulnérabilités automatique	82
16. Vie privée	85
16.1. Protection antiphishing	85
16.1.1. Protection Bitdefender dans le navigateur web	87
16.1.2. Alertes Bitdefender dans le navigateur	88
16.2. Cryptage de Messagerie Instantanée	88
16.3. Supprimer définitivement des fichiers	89
17. Transactions en ligne sécurisées par Safepay	91
17.1. Utiliser Bitdefender Safepay	91
17.2. Configuration des paramètres	92
17.3. Gérer les marque-pages	92
17.4. Protection hotspot pour les réseaux non sécurisés	93
18. Protection Safego pour réseaux sociaux	94
19. Bitdefender USB Immunizer	96
20. Gérer vos ordinateurs à distance	97
20.1. Accéder à MyBitdefender	97
20.2. Exécuter des tâches sur les ordinateurs	97
Résolution des problèmes	99
21. Résoudre les problèmes les plus fréquents	100
21.1. Mon système semble lent	100
21.2. L'analyse ne démarre pas	101
21.3. Je ne peux plus utiliser une application	101
21.4. Comment mettre à jour Bitdefender avec une connexion Internet lente ...	102

21.5. Mon ordinateur n'est pas connecté à Internet. Comment actualiser Bitdefender?	103
21.6. Le Services Bitdefender ne répondent pas	103
21.7. La désinstallation de Bitdefender a échoué	104
21.8. Mon système ne démarre pas après l'installation de Bitdefender	105
22. Suppression des malwares de votre système	107
22.1. Mode de Secours de Bitdefender	107
22.2. Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ?	109
22.3. Comment nettoyer un virus dans une archive ?	110
22.4. Comment nettoyer un virus dans une archive de messagerie ?	111
22.5. Que faire si je suspecte un fichier d'être dangereux ?	112
22.6. Comment nettoyer les fichiers infectés du System Volume Information ? ...	113
22.7. Que sont les fichiers protégés par mot de passe du journal d'analyse ? ...	114
22.8. Que sont les éléments ignorés du journal d'analyse ?	114
22.9. Que sont les fichiers ultra-compressés du journal d'analyse ?	115
22.10. Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?	115
Nous contacter	116
23. Demander de l'aide	117
23.1. Support Technique Editions Profil / Bitdefender	118
24. Ressources en ligne	121
24.1. Centre de Support de Bitdefender	121
24.2. Forum du Support Bitdefender	121
24.3. Portail Malware City	122
25. Nous contacter	123
25.1. Adresses Web	123
25.2. Distributeurs locaux	123
25.3. Bureaux de Bitdefender	123
Glossaire	126

Installation

1. Préparation de l'installation

Avant d'installer Bitdefender Antivirus Plus 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.
- 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 Antivirus Plus 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
- .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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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

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

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

Étape 4 - 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. 18).

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.

Utilisez les boutons pour activer / désactiver :

- 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.

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. 32).

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 Antivirus Plus 2013 installé, votre ordinateur est protégé contre tous les types de malwares (tels que les virus, spywares et chevaux de Troie).

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. 14).

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. 30).

Pour utiliser les fonctionnalités en ligne de Bitdefender Antivirus Plus 2013, veillez à lier votre ordinateur à un compte MyBitdefender. Pour plus d'informations, reportez-vous à « **Compte MyBitdefender** » (p. 32).

Si vous rencontrez des problèmes lors de l'utilisation de Bitdefender, recherchez dans la section « **Résoudre les problèmes les plus fréquents** » (p. 100) des solutions possibles aux problèmes les plus courants. La section « **Comment** » (p. 39) 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 Antivirus Plus 2013, utilisez le menu Démarrer de Windows en suivant le chemin d'accès **Démarrer** → **Tous les programmes** → **Bitdefender 2013** → **Bitdefender Antivirus Plus 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 :

- 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**
- **Vie privée**
- **Mise à jour**
- **Safego**

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

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

Utilisation du Mode Jeu

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

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

- Faites un Clic-droit sur l'icône Bitdefender dans la barre d'état et sélectionnez **Activer le Mode Jeu**.
- 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 taper 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 et de Mise à jour 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 Antivirus Plus 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. 14).
- **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. 26).
- **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 **Analysier** 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. 58).

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.

- **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. 85).

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. 35).

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 Antivirus Plus 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. 94).

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.

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.

Mise à jour

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

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 Antivirus Plus 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'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.



Note

Le pare-feu n'est pas disponible dans Bitdefender Antivirus Plus 2013.

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 **1** pour un événement non lu, pour ouvrir la fenêtre Aperçu des événements. Pour plus d'informations, reportez-vous à « *Événements* » (p. 14).

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. 32).

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. 30). 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 2013 afin d'effectuer l'une des actions suivantes :

- Récupérez votre clé de licence, si jamais vous la perdez.
- Protégez vos comptes Facebook et Twitter avec **Safego**.
- Gérer Bitdefender Antivirus Plus 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.

8.1. Lier l'ordinateur à MyBitdefender

Pour lier votre ordinateur à un compte MyBitdefender, vous devez vous connecter à un compte depuis Bitdefender Antivirus Plus 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 Antivirus Plus 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. 51).
- 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. 103). 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. 102).
- 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. 36).

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. 117).

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. 69).

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. 53).
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. 46).
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. 117).

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. Vie privée

13.1. 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.

13.2. 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.

13.3. 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.

14. Informations Utiles

14.1. 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. 69).

14.2. 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.

14.3. 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.

14.4. 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**.

14.5. 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 Antivirus Plus 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.

14.6. 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.

14.7. 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

15. 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. 73).

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. 75).

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. 77).

Si votre ordinateur a été infecté par des malwares, veuillez vous référer à « **Suppression des malwares de votre système** » (p. 107). 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. 78).

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. 81).

15.1. 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.

15.1.1. 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.

15.1.2. 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.

15.1.3. 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. 77).



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. 77).

Refuser l'accès

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

15.1.4. 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**.

15.2. 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.

15.2.1. 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**.

15.2.2. 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.

15.2.3. 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.

15.2.4. 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. 35).
- 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. 66).

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.

15.2.5. 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.

15.2.6. 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. 77).



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. 107).

15.2.7. 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.

15.3. 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.

15.3.1. 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. 107).

15.3.2. 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.

15.4. 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**.

15.4.1. 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.

15.4.2. 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.

15.4.3. 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.

15.5. 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**.

15.6. 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**.

15.6.1. 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.

15.6.2. 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.

15.6.3. 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).

15.6.4. 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.
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.

15.7. 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.

15.7.1. 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.

15.7.2. 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.

16. 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.
- **Destructeur de fichiers** - efface définitivement des fichiers et toute trace de ceux-ci sur votre ordinateur.

16.1. 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 correspondant 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.

16.1.1. 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.

16.1.2. 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**.

16.2. 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.

16.3. 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**

Patiencez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.

c. **Résultats**

Les résultats sont affichés. Cliquez sur **Fermer** pour quitter l'assistant.

17. 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

17.1. 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  respectivement.
- 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 .

17.2. 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.

17.3. 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**.

17.4. 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 Antivirus Plus 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.

18. 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. 32).

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.

19. 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. 82).

20. 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

20.1. 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.

20.2. 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.

Résolution des problèmes

21. 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. 100)
- « *L'analyse ne démarre pas* » (p. 101)
- « *Je ne peux plus utiliser une application* » (p. 101)
- « *Comment mettre à jour Bitdefender avec une connexion Internet lente* » (p. 102)
- « *Mon ordinateur n'est pas connecté à Internet. Comment actualiser Bitdefender?* » (p. 103)
- « *Le Services Bitdefender ne répondent pas* » (p. 103)
- « *La désinstallation de Bitdefender a échoué* » (p. 104)
- « *Mon système ne démarre pas après l'installation de Bitdefender* » (p. 105)

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. 117).

21.1. 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. 54).

- **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).

- **Vos disques durs sont trop fragmentés.**

La fragmentation de fichiers ralentit l'accès aux fichiers et fait diminuer les performances système.

Pour défragmenter votre disque en utilisant votre système d'exploitation Windows, suivez ce chemin à partir du menu démarrer de Windows : **Démarrer** → **Tous les programmes** → **Accessoires** → **Outils système** → **Défragmenteur de disque**.

21.2. 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. 54).
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. 117).

21.3. 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. 117).

21.4. 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.

21.5. 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. 53).
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.

21.6. 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. 54).

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. 117).

21.7. 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. 117).

21.8. 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. 55).
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. 55).
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. 55).
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. 54).
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. 117).

22. 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. 107)
- « *Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ?* » (p. 109)
- « *Comment nettoyer un virus dans une archive ?* » (p. 110)
- « *Comment nettoyer un virus dans une archive de messagerie ?* » (p. 111)
- « *Que faire si je suspecte un fichier d'être dangereux ?* » (p. 112)
- « *Comment nettoyer les fichiers infectés du System Volume Information ?* » (p. 113)
- « *Que sont les fichiers protégés par mot de passe du journal d'analyse ?* » (p. 114)
- « *Que sont les éléments ignorés du journal d'analyse ?* » (p. 114)
- « *Que sont les fichiers ultra-compressés du journal d'analyse ?* » (p. 115)
- « *Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?* » (p. 115)

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. 117).

22.1. 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 Antivirus Plus 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. 107).
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.

22.2. 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. 53).
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. 55).
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. 117).

22.3. 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. 117).

22.4. 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. 117).

22.5. 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. 45).
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. 117).

22.6. 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. 117).

22.7. 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.

22.8. 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.

22.9. Que sont les fichiers ultra-compressés du journal d'analyse ?

Les éléments ultra-compressés sont des éléments qui n'ont pas pu être extraits par le moteur d'analyse ou des éléments dont le temps de décryptage aurait été trop long et aurait rendu le système instable.

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

22.10. 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

23. 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. 100) 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. 117)
- « **Contactez-nous via notre Centre de Support en ligne** » (p. 118)



Important

Pour contacter le Service Client de Bitdefender, vous devez enregistrer votre produit Bitdefender. Pour plus d'informations, reportez-vous à « *Enregistrer Bitdefender* » (p. 30).

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.

23.1. 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.

24. 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.

24.1. 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>.

24.2. 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.

24.3. 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>.

25. 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.

25.1. 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>

25.2. 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.

25.3. 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.

Bitdefender Antivirus Plus 2013

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 (plugins) pour certains formats.

Non-heuristique

Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut 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.