bitdefender
ANTIVIRUS PRO 2011

Manuel d'utilisation

BitDefender Antivirus Pro 2011
Manuel d'utilisation

Publié le 2010.07.30

Notice Légale


bitdefender

Table des matières

Installation et désinstallation

1. Configuration requise

Vous pouvez installer BitDefender Antivirus Pro 2011 uniquement sur les ordinateurs fonctionnant avec les systèmes d'exploitation suivants :

- Windows XP avec Service Pack 3 (32 bits) / Windows XP avec Service Pack 2 (64 bits)
- Windows Vista avec Service Pack 1 ou supérieur (32/64 bits)
- Windows 7 (32/64 bits)

Avant d'installer le produit, vérifiez que le système remplit les conditions minimales suivantes :

Note

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

1.1. Configuration système minimale

- 1 Go d'espace disque disponible
- Processeur 800MHz
- Mémoire RAM :
  - 512 Mo pour Windows XP
  - 1 Go pour Windows Vista et Windows 7
- Internet Explorer 6.0
- .NET Framework 2 (également disponible dans le kit d'installation)
- Adobe Flash Player 10.0.45.2

1.2. Configuration système recommandée

- 1 Go d'espace disque disponible
- Intel CORE Duo (1,66 GHz) ou processeur équivalent
- Mémoire RAM :
  - 1 Go pour Windows XP et Windows 7
  - 1,5 Go pour Windows Vista
- Internet Explorer 7
- .NET Framework 2 (également disponible dans le kit d'installation)
- Adobe Flash Player 10.0.45.2

1.3. Logiciels

La protection antiphishing est seulement disponible pour :

- Internet Explorer 6.0 (ou version supérieure)
- Mozilla Firefox 3.x
- Yahoo! Messenger 8.1

- Microsoft Windows Live Messenger 8

Le cryptage des messageries instantanées est disponible seulement pour :

- Yahoo! Messenger 8.1
- Microsoft Windows Live Messenger 8

2. Préparation de l'Installation

Avant d'installer BitDefender Antivirus Pro 2011, 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. 2).
- Connectez-vous à l'ordinateur en utilisant un compte Administrateur.
- Désinstallez tous les logiciels de sécurité 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 par défaut avant le début de l'installation.

3. Installation de BitDefender

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

- Pour installer BitDefender à partir du CD, insérez le CD dans le lecteur. Un écran d'accueil s'affiche peu après. Suivez les instructions pour lancer l'installation.

  Note

  La fenêtre d'accueil dispose d'une option permettant de copier les fichiers d'installation du DVD vers un périphérique USB. Ceci est utile en particulier si vous avez besoin d'installer BitDefender sur un PC ne disposant pas de lecteur (Ex: Netbook).Branchez votre périphérique USB, puis cliquez sur **Copier vers un disque USB**.Ensuite, branchez votre disque USB sur votre PC ne disposant pas de lecteur DVD et double-cliquez sur `runsetup.exe` depuis le répertoire dans lequel vous avez mis le package d'installation.

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

- Pour installer BitDefender en utilisant le fichier d'installation téléchargé sur votre ordinateur, localisez le fichier et double-cliquez dessus.

Le programme d'installation vérifiera d'abord votre système pour valider l'installation. Si l'installation est validée, vous êtes invité à sélectionner une langue avant que l'assistant d'installation ne s'affiche.

L'assistant vous aidera à installer BitDefender sur votre ordinateur et vous permettra également de configurer les paramètres principaux et l'interface utilisateur.

3.1. Étape 1 - Introduction

Veuillez lire l'accord de licence et sélectionnez **En cochant cette case, j'accepte l'accord de licence de BitDefender**.Cliquez sur **Suivant** pour continuer.

Si vous être en désaccord avec les termes du contrat, cliquez sur **Annuler**. Le processus sera interrompu et vous quitterez l'installation.

3.2. Étape 2 - Préparation de l'installation

BitDefender analyse votre système et vérifie si un autre logiciel de sécurité est installé sur celui-ci.

Analyse Rapide

Une analyse rapide des zones critiques de votre système est effectuée afin de vérifier qu'aucun malware actif ne s'y trouve.

L'analyse ne devrait pas durer plus de quelques minutes. Vous pouvez l'annuler à tout moment à l'aide du bouton.

Important
Il est fortement recommandé de laisser l'analyse se terminer.
Des malwares actifs pourraient interrompre l'installation et même, la faire échouer.

Une fois l'analyse terminée, les résultats sont affichés. Si des menaces sont détectées, suivez les instructions pour les supprimer avant de continuer l'installation.

Cliquez sur **Suivant** pour continuer.

Désinstallation des Logiciels de Sécurité Existants

BitDefender Antivirus Pro 2011 vous prévient si d'autres produits de sécurité sont installés sur votre ordinateur.Cliquez sur le bouton correspondant pour lancer le processus de désinstallation et suivez les instructions pour supprimer tout produit détecté.

Avertissement
Il est fortement recommandé de désinstaller les autres antivirus avant d'installer BitDefender. Faire fonctionner plusieurs antivirus sur le même ordinateur le rend généralement inutilisable.

Si Windows Defender est activé, il est également recommandé d'autoriser BitDefender à le désactiver.

Cliquez sur **Suivant** pour continuer.

3.3. Étape 3 - Enregistrement

Le processus d'enregistrement de BitDefender consiste à enregistrer le produit avec une clé de licence et à activer des fonctions en ligne en créant un compte BitDefender.

Enregistrez Votre Produit

Procédez selon votre situation :

- **J'ai acheté BitDefender Antivirus Pro 2011 sur un CD ou en ligne**

  Dans ce cas, vous devez enregistrer le produit :

  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 d'activation BitDefender, cliquez sur le lien indiqué pour être dirigé vers la boutique en ligne BitDefender et en acheter une.

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

- **J'ai téléchargé BitDefender Antivirus Pro 2011 pour le tester**

  Dans ce cas, vous pouvez utiliser toutes les fonctionnalités du produit pendant une période de 30 jours. Pour commencer la période d'essai, sélectionnez **Je souhaite tester BitDefender Antivirus Pro 2011 pendant 30 jours** et cliquez sur **Suivant**.

Activer les Fonctionnalités en Ligne

Si vous avez acheté votre produit en ligne, vous devez créer un compte BitDefender afin de recevoir les mises à jour BitDefender.Le compte BitDefender vous donne accès au support technique gratuit, à des offres spéciales et à des promotions.Si vous perdez votre clé de licence BitDefender, vous pouvez la retrouver en vous connectant à votre compte à l'adresse https://myaccount.bitdefender.com/fr/MyAccount/login/.

Si vous ne souhaitez pas créer de compte BitDefender pour le moment, sélectionnez **Créer un compte plus tard** et cliquez sur **Suivant**.

Note

Si vous installez BitDefender Antivirus Pro 2011 pour l'évaluer, vous devez créer un compte BitDefender à ce stade.

Si vous avez acheté le produit, il est recommandé de créer un compte dans les 30 jours qui suivent l'installation.

Autrement, procédez selon votre situation actuelle :

- **Je n'ai pas de compte BitDefender**

  Pour créer un compte BitDefender, suivez ces étapes :

  1. Sélectionnez **Créer un nouveau compte**.
  2. Tapez les informations requises dans les champs correspondants. Les informations communiquées ici resteront confidentielles.

     - **Nom d'utilisateur** - saisissez votre adresse e-mail.

- **Mot de passe** - entrez un mot de passe pour votre compte BitDefender.Le mot de passe doit contenir entre 6 et 16 caractères.
- **Ressaisir le mot de passe** - confirmez le mot de passe que vous venez d'indiquer.

  Il n'est pas nécessaire de saisir à nouveau le mot de passe si vous avez choisi de ne pas masquer le mot de passe lorsque vous le tapez.

Note
Une fois le compte activé, 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. Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte.Cliquez sur **Afficher les Options de Contact** et sélectionnez l'une des options disponibles dans la fenêtre qui apparaît.
   - **M'envoyer tous les messages**
   - **Envoyer les messages importants**
   - **Ne pas m'envoyer de message**
4. Cliquez sur **Envoyer**.
5. Cliquez sur **Suivant** pour continuer.

Note
Vous devez activez votre compte avant de pouvoir l'utiliser.
Consultez votre messagerie et suivez les instructions données dans le message que vous a adressé le service d'enregistrement de BitDefender.

- **J'ai déjà un compte BitDefender**

  BitDefender détectera automatiquement si vous avez déjà un compte BitDefender actif sur cet ordinateur.Si c'est le cas, introduisez le mot de passe de votre compte, puis cliquez sur **Envoyer**.Cliquez sur **Suivant** pour continuer.

  Si vous avez déjà un compte actif, mais que BitDefender ne le détecte pas, suivez ces étapes pour enregistrer le produit avec ce compte :

  1. Sélectionnez **Se Connecter (Compte Existant)**.
  2. Tapez l'adresse e-mail et le mot de passe de votre compte dans les champs correspondants.

Note
Si vous ne souhaitez pas faire de modifications, cliquez sur **Terminer** pour fermer l'assistant.

3. Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte.Cliquez sur **Afficher les Options de Contact** et sélectionnez l'une des options disponibles dans la fenêtre qui apparaît.
   - **M'envoyer tous les messages**
   - **Envoyer les messages importants**
   - **Ne pas m'envoyer de message**
4. Cliquez sur **Envoyer**.
5. Cliquez sur **Suivant** pour continuer.

3.4. Étape 4 - Choix du Mode d'Affichage

C'est ici que vous choisissez le type d'installation à effectuer et le mode d'affichage de l'interface à utiliser.

Choisissez le Type d'Installation

Les options d'installation suivantes sont disponibles :

- **Installation Facile** - sélectionnez cette option si vous préférez une installation rapide et que vous n'avez pas l'intention de configurer les paramètres de BitDefender dans le détail.
- **Installation Personnalisée** - sélectionnez cette option si vous préférez personnaliser l'installation et les paramètres de BitDefender.

Pour voir un tutoriel vidéo qui vous aidera pour l'installation, cliquez sur **Obtenir de l'Aide**

Note
Pour installer BitDefender dans une configuration par défaut et vous rendre directement à la dernière étape de l'assistant d'installation, sélectionnez **Passer l'installation**.

Cliquez sur **Suivant** pour continuer.

Choisissez l'Emplacement d'Installation

Note
Cette étape n'apparaît que si vous avez choisi une **Installation personnalisée**.

Par défaut, BitDefender Antivirus Pro 2011 est installé dans `C:\Program Files\BitDefender\`.Si vous voulez choisir un autre répertoire, cliquez sur **Parcourir** et choisissez le répertoire d'installation.

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.

Cliquez sur **Suivant** pour continuer.

Choisissez l'Interface Utilisateur

Sélectionnez le mode d'affichage de l'interface utilisateur le plus adapté à vos besoins.BitDefender Antivirus Pro 2011 vous propose trois interfaces, chacune adaptée aux besoins d'un type d'utilisateur différent.

Mode STANDARD

Adapté aux débutants et aux personnes qui souhaitent que BitDefender protège leur ordinateur et données sans être dérangés. L'interface est simple à utiliser et requiert peu d'interaction de votre part.

Vous devez simplement corriger les problèmes rencontrés comme indiqué par BitDefender. Un assistant intuitif vous guidera pas à pas dans la résolution de ces problèmes.Vous pouvez également réaliser des tâches courantes comme la mise à jour des signatures de virus BitDefender et des fichiers du programme ou l'analyse de l'ordinateur.

Mode INTERMÉDIAIRE

Vous pouvez configurer les principaux paramètres de BitDefender, corriger des problèmes séparément, gérer les produits BitDefender installés sur les ordinateurs de votre foyer et choisir les problèmes à surveiller.

Mode EXPERT

Ce mode, qui convient à des utilisateurs ayant plus de connaissances techniques, vous permet de configurer en détail chaque fonctionnalité de BitDefender.Vous pouvez également utiliser toutes les tâches fournies pour protéger votre ordinateur et vos données.

Faites votre sélection et cliquez sur **Suivant** pour continuer.

3.5. Étape 5 - Configurer

Vous pouvez personnaliser votre produit ici.

Configurer les Paramètres

Note
Cette étape n'apparaît que si vous avez réglé l'interface BitDefender sur **Mode Expert**.

Ici, vous pouvez activer et désactiver les fonctions de BitDefender organisées en deux catégories.Pour modifier l'état d'un paramètre, cliquez sur le bouton correspondant.

- **Paramètres de sécurité**

  Vous pouvez activer ou désactiver des paramètres du produit couvrant plusieurs aspects de la sécurité informatique et des données dans cette zone.

Paramètre	Description
Antivirus	La protection de fichiers en temps réel garantit que tous les fichiers sont analysés lorsque vous (ou une application exécutée sur ce système) y accédez.
Mise à jour automatique	La mise à jour automatique permet de télécharger et d'installer automatiquement et régulièrement les dernières versions du produit BitDefender et des fichiers de signatures.
Contrôle de vulnérabilité	La vérification automatique des vulnérabilités s'assure que les logiciels majeurs de votre ordinateur sont à jour.
Antiphishing	L'Antiphishing vous alerte en temps réel s'il détecte qu'une page Web est conçue pour voler des informations personnelles.
Contrôle d'identité	Le Contrôle d'Identité vous aide à empêcher que vos données personnelles ne soient transmises sur Internet sans votre accord. Il bloque tous les messages instantanés, e-mails ou formulaires Web transmettant vers des destinataires non autorisés des données que vous avez définies comme étant confidentielles.
Messagerie Inst.	Le cryptage de Messagerie Instantanée protège vos conversations via Yahoo! Messenger et Windows Live Messenger à condition que vos contacts de messagerie instantanée utilisent un produit BitDefender et un logiciel de messagerie instantanée compatibles.

Paramètres Généraux

Vous pouvez activer ou désactiver les paramètres qui affectent le fonctionnement du produit et son utilisation dans cette zone.

Paramètre	Description
Mode Jeu	Le Mode Jeu modifie temporairement les paramètres de protection afin de préserver les ressources de votre système pendant les jeux.
Détection du Mode Portable	Le Mode Portable modifie temporairement les paramètres de protection afin de préserver l'autonomie de la batterie de votre ordinateur portable.
Mot de passe paramètres	Cette option garantit que les paramètres BitDefender ne puissent être modifiés que par une personne connaissant ce mot de passe. Si vous activez cette option, on vous demandera de configurer le mot de passe des paramètres.Tapez le mot de passe souhaité dans les deux champs et cliquez sur **OK** pour définir le mot de passe.
BitDefender News	En activant cette option, vous serez informé par BitDefender de l'actualité de la société, des mises à jour de produits ou des nouvelles menaces de sécurité.
Alertes du produit	En activant cette option, vous recevrez des alertes d'information.
Barre de l'activité d'analyse	La Barre d'Activité d'Analyse est une petite fenêtre transparente indiquant la progression de l'activité d'analyse de BitDefender.Pour plus d'informations, reportez-vous à « *Barre de l'activité d'analyse* » (p. 20).
Envoyer rapports d'infection	En activant cette option, les rapports d'analyse virale sont envoyés aux laboratoires BitDefender pour être examinés. Notez que ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et qu'ils ne seront pas utilisés à des fins commerciales.
Outbreak Detection	En activant cette option, les rapports concernant les potentielles alertes virales sont envoyés aux laboratoires BitDefender pour être examinés. Notez que ces rapports ne comprendront aucune donnée

Paramètre	Description
	confidentielle, telle que votre nom ou votre adresse IP, et qu'ils ne seront pas utilisés à des fins commerciales.

Cliquez sur **Suivant** pour continuer.

Configurer Mes Outils

Note
Cette étape apparait uniquement si vous avez paramétré l'interface de BitDefender en mode **Standard** ou **Intermédiaire**.

Avec **Mes Outils**, vous pouvez personnaliser le tableau de bord en ajoutant des raccourcis vers les outils les plus importants pour vous. De cette façon, vous permettez un accès facile à ceux-ci.

À partir de cet écran, vous pouvez ajouter des raccourcis pour les outils suivants :

- Mode Jeu - configure BitDefender de façon à ce qu'il n'interfère pas dans votre pratique des jeux.
- Mode Portable - modifie de manière temporaire les paramètres de protection afin de minimiser leur impact sur la durée de vie de la batterie de votre ordinateur portable.
- Gestion du réseau domestique - gérez les produits BitDefender installés sur des ordinateurs du réseau domestique à partir d'un seul PC.
- Analyse Complète du Système - pour effectuer une analyse de l'ensemble du système.

Sélectionnez les outils que vous souhaitez ajouter et cliquez sur **Suivant** pour continuer.

Gestion du Réseau Domestique

Note
Cette étape n'apparaît que si vous avez ajouté la gestion du réseau domestique à Mes outils.

Vous pouvez sélectionner l'une de ces trois options :

- **Paramétrer cet ordinateur en tant que serveur**

  Sélectionnez cette option si vous prévoyez d'administrer des produits BitDefender sur d'autres ordinateurs du réseau domestique à partir de celui-ci.

Un mot de passe est requis pour rejoindre le réseau. Saisissez le mot de passe dans les zones de texte et cliquez sur **Envoyer**.

- **Configurer ce PC en tant que Client**

  Sélectionnez cette option si BitDefender sera géré par un autre ordinateur du réseau domestique exécutant également BitDefender.

  Un mot de passe est requis pour rejoindre le réseau. Saisissez le mot de passe dans les zones de texte et cliquez sur **Envoyer**.

- **Ignorer l'installation pour le moment**

  Sélectionnez cette option pour configurer cette fonction ultérieurement depuis la fenêtre BitDefender.

Cliquez sur **Suivant** pour continuer.

3.6. Etape 6 - Options d'assistance

C'est ici que vous pouvez personnaliser l'aide et les options de support :

- Activer / désactiver les **Astuces**.Les Astuces sont des messages personnalisés affichés dans le Tableau de bord BitDefender pour vous aider à améliorer les performances de votre ordinateur.
- Confirmez l'adresse e-mail que vous utiliserez si vous devez contacter le Service Client BitDefender. Si vous n'avez pas l'intention de contacter le Service Client par e-mail, cochez la case correspondante.

3.7. Étape 7 - Confirmation

Cette étape vous permet de vérifier la configuration sélectionnée.

Par défaut, deux tâches sont également programmées :

- Une analyse complète est planifiée immédiatement une fois l'installation terminée.

  Il est recommandé d'effectuer cette analyse approfondie qui permettra de détecter toute menace de malware présente sur votre système.

- Une analyse du système est programmée tous les dimanches à 14 h.

  Il est fortement recommandé d'analyser votre système au moins une fois par semaine.Sélectionnez un jour et une heure différents si la planification par défaut ne vous convient pas. Si l'ordinateur est éteint au moment prévu, l'analyse s'exécutera la prochaine fois que vous l'allumerez.

Cliquez sur **Terminer**.

3.8. Étape 8 - Terminer

L’installation est sur le point de se terminer. Les paramètres finaux sont appliqués et une mise à jour est réalisée.

L'assistant se fermera automatiquement une fois l'installation terminée. Si cette option était sélectionnée à l’étape précédente, une analyse complète est lancée.

Note

Il peut être nécessaire de redémarrer le système.

4. Mise à niveau depuis une ancienne version de BitDefender

Vous pouvez mettre à niveau vers BitDefender Antivirus Pro 2011 si vous utilisez la version bêta, 2008, 2009 ou 2010 de BitDefender Antivirus Pro 2011.

Il y a deux manières de réaliser la mise à niveau :

- Installez BitDefender Antivirus Pro 2011 directement sur la version plus ancienne.Si vous installez directement le produit via la version 2010, la quarantaine est automatiquement importée.
- Désinstallez la version la plus ancienne, puis redémarrez l'ordinateur et installez la nouvelle version comme expliqué dans le chapitre « *Installation de BitDefender* » (p. 5).Aucun paramètre du produit ne sera enregistré.Utilisez cette méthode de mise à niveau si l'autre échoue.

5. Réparer ou Désinstaller BitDefender

Si vous souhaitez réparer ou supprimer BitDefender Antivirus Pro 2011, suivez ce chemin à partir du menu Démarrer de Windows : **Démarrer → Tous les programmes → BitDefender 2011 → Réparer ou Supprimer**.

Un assistant apparaîtra pour vous aider à terminer la tâche souhaitée.

1. **Réparer ou supprimer**

   Sélectionnez l'action que vous voulez effectuer.

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

   Note

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

2. **Confirmer l'Action**

   Veillez à lire attentivement les informations affichées avant de cliquer sur **Suivant** pour confirmer l'action.

3. **Progression**

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

4. **Terminer**

   Les résultats sont affichés.

   Vous devez redémarrer l'ordinateur pour terminer le processus. Cliquez sur **Redémarrer** pour redémarrer votre ordinateur immédiatement, ou sur **Terminer** pour fermer la fenêtre et redémarrer ultérieurement.

Pour démarrer

6. Présentation

Une fois BitDefender Antivirus Pro 2011 installé, votre ordinateur est protégé contre tous les types de malwares (tels que les virus, spywares et chevaux de Troie).

Vous n'êtes pas tenu(e) de configurer des paramètres de BitDefender autres que ceux configurés pendant l'installation. Cependant, vous pouvez souhaiter profiter des paramètres de BitDefender pour ajuster et améliorer votre protection.

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 le souhaitez, vous pouvez configurer BitDefender de sorte qu'il ne vous alerte pas au sujet de problèmes spécifiques.

Si vous n'avez pas enregistré le produit (y compris si vous n'avez pas créé de compte BitDefender), pensez à le faire avant que ne se termine la période d'essai.Il est recommandé de créer un compte dans les 15 jours après l'installation de BitDefender.Dans le cas contraire, BitDefender ne se mettra plus à jour.Pour plus d'informations sur le processus d'enregistrement, reportez-vous à « *Enregistrement et Mon compte* » (p. 49).

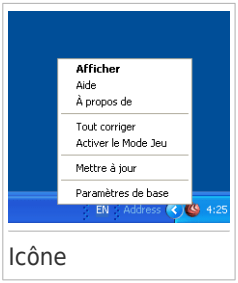
6.1. Ouverture de BitDefender

Pour accéder à l'interface principale de BitDefender Antivirus Pro 2011, utilisez le menu Démarrer de Windows en suivant le chemin d'accès **Démarrer → Tous les programmes → BitDefender 2010 → BitDefender Antivirus Pro 2011**ou, plus rapide, double-cliquez sur l'icône BitDefender dans la zone de notification.

Pour plus d'informations sur la principale fenêtre d'application, reportez-vous à « *Fenêtre principale de l'application* » (p. 24).

6.2. Icône de la zone de notification

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



Icône

- **Afficher** - ouvre l'interface principale BitDefender.
- **Aide** - ouvre le fichier d'aide, qui explique en détail comment configurer et utiliser BitDefender Antivirus Pro 2011.
- **A 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* » (p. 40).
- **Activer / désactiver le Mode Jeu** - active / désactive le Mode Jeu.
- **Mettre à jour** - effectue une mise à jour immédiate.Une nouvelle fenêtre apparaît affichant l'état de la mise à jour.
- **Paramètres de base** - ouvre une fenêtre où vous pouvez activer ou désactiver les principaux paramètres du produit et reconfigurer votre profil utilisateur. Pour plus d'informations, reportez-vous à « *Configuration des paramètres principaux* » (p. 43).

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 :

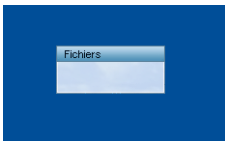
Triangle rouge avec un point d'exclamation : D'importants problèmes affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.
Lettre G: Le produit fonctionne en Mode jeu.

Si BitDefender ne fonctionne pas, l'icône de la zone de notification est grisée .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.

6.3. Barre de l'activité d'analyse

La **Barre d'analyse d'activité** est une visualisation graphique de l'analyse d'activité de votre système.Cette petite fenêtre est disponible par défaut uniquement en Mode Expert.

Les barres grises (la **Fichiers**) montrent le nombre de fichiers analysés par seconde, sur une échelle de 0 à 50.



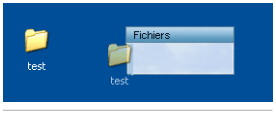
Barre de l'activité d'analyse

Note
La barre d'analyse d'activité vous prévient lorsque la protection en temps réel est désactivée en affichant une croix rouge au-dessus du **fichier**.

6.3.1. Analyser Fichiers et Dossiers

Vous pouvez utiliser la barre d'activité d'analyse pour analyser rapidement des fichiers et des dossiers. Glissez le fichier ou répertoire que vous voulez analyser et déposez-le sur la **Barre d'analyse de l'activité**, comme sur l'image ci-dessous.

Glisser le fichier



Déposer le fichier

L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse.

Options d'analyse. 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 (suppression du code du malware). Si la désinfection échoue, l'assistant d'analyse antivirus vous proposera d'indiquer d'autres moyens d'intervenir sur les fichiers infectés.Les options d'analyse sont standard et vous ne pouvez pas les modifier.

6.3.2. Désactiver/Restaurer la Barre d'Activité d'Analyse

Si vous ne souhaitez plus voir cette barre, il vous suffit de faire un clic-droit dessus et de choisir **Cacher**.Pour restaurer la barre d'activité d'analyse, suivez ces étapes :

1. Lancer BitDefender.

2. Cliquez sur le bouton **Options** dans l'angle supérieur droit de la fenêtre et sélectionnez **Préférences**.
3. Dans la catégorie Paramètres Généraux, utilisez le bouton correspondant à **Barre d'activité d'analyse** pour l'activer.
4. Cliquez sur **OK** pour enregistrer et appliquer les modifications.

6.4. Détection automatique de périphérique

BitDefender détecte automatiquement la connexion d'un périphérique de stockage amovible à votre ordinateur et vous propose de l'analyser avant que vous accédiez à ses fichiers.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

Lorsqu'un tel périphérique est détecté, une fenêtre d'alerte s'affiche.

Pour analyser le périphérique de stockage, cliquez simplement sur **Oui**.L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse.

Si vous ne souhaitez pas analyser le périphérique, cliquez sur **Non**. Dans ce cas, il se peut que l'une des options suivantes vous semble utile :

- **Ne plus me demander pour ce type de périphérique** - BitDefender ne proposera plus d'analyser ce type de périphériques de stockage lorsqu'ils seront connectés à votre ordinateur.
- **Désactiver la détection automatique de périphérique** - On ne vous proposera plus d'analyser les nouveaux périphériques de stockage lorsqu'ils seront connectés à l'ordinateur.

Si vous avez désactivé par erreur la détection automatique de périphérique et que vous voulez l'activer, ou si vous souhaitez configurer ses paramètres, procédez comme suit :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Antivirus>Analyse Antivirus**.
3. Dans la liste des tâches d'analyse, repérez la tâche **Analyse des périphériques**.
4. Faites un clic droit sur la tâche, puis sélectionnez **Propriétés**.Une nouvelle fenêtre s'affiche.

5. Dans l'onglet **Présentation**, configurez les options d'analyse selon vos besoins.Pour plus d'informations, reportez-vous à « *Configuration des paramètres d'analyse* » (p. 75).
6. Dans l'onglet **Détection**, sélectionnez les types de périphériques de stockage à détecter.
7. Cliquez sur **OK** pour enregistrer et appliquer les modifications.

7. Fenêtre principale de l’application

BitDefender Antivirus Pro 2011 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.

Vous pouvez choisir d'afficher l'interface utilisateur avec l'un des trois modes, en fonction de vos compétences en informatique et de votre connaissance de BitDefender.

Mode STANDARD

Convient aux débutants en informatique et aux personnes qui souhaitent que BitDefender protège leur ordinateur et leurs données sans être interrompues. Ce mode est facile à utiliser et ne requiert de votre part que très peu d'interventions.

Vous devez simplement corriger les problèmes rencontrés comme indiqué par BitDefender. Un assistant intuitif vous guidera pas à pas dans la résolution de ces problèmes.Vous pouvez également réaliser des tâches courantes comme la mise à jour des signatures de virus BitDefender et des fichiers du programme ou l'analyse de l'ordinateur.

Mode INTERMÉDIAIRE

Destinée aux utilisateurs disposant de compétences informatiques intermédiaires, cette interface vous permet d’aller un peu plus loin qu’en Mode Standard.

Vous pouvez corriger les problèmes séparément et choisir les éléments à surveiller.De plus, vous pouvez gérer à distance les produits BitDefender installés sur les ordinateurs de votre foyer.

Mode EXPERT

Ce mode, qui convient à des utilisateurs ayant plus de connaissances techniques, vous permet de configurer en détail chaque fonctionnalité de BitDefender.Vous pouvez également utiliser toutes les tâches fournies pour protéger votre ordinateur et vos données.

Le mode d'affichage est sélectionné au cours de l'installation.

Pour modifier le mode d'affichage :

1. Lancer BitDefender.
2. Cliquez sur le bouton **Options** dans l’angle supérieur droit de la fenêtre.
3. Sélectionnez le mode d’affichage souhaité dans le menu.

7.1. Mode STANDARD

Si vous êtes débutant en informatique, l'affichage de l'interface utilisateur en Mode Standard est probablement le choix le approprié pour vous.Ce mode est simple à utiliser et ne requiert que très peu d'interventions de votre part.

La fenêtre est organisée en trois catégories :

Zone d'état
: Des informations sur l'état se trouvent dans la partie de gauche de la fenêtre.

Zone Protection de Votre PC
: C'est à partir d'ici que vous pouvez mener les actions nécessaires pour gérer votre protection.

Zone d'Aide
: C'est ici que vous pouvez obtenir des informations sur l'utilisation de BitDefender Antivirus Pro 2011 et obtenir de l'aide.

Le bouton **Options** dans l'angle supérieur droit de la fenêtre vous permet de modifier le mode d'affichage de l'interface utilisateur et de configurer les principaux paramètres du programme.

Dans l'angle inférieur droit de la fenêtre, vous trouverez plusieurs liens utiles.

Lien	Description
Informations de Licence	Ouvre une fenêtre où vous pouvez voir des informations sur la clé de licence actuelle et enregistrer votre produit avec une nouvelle clé de licence.
Journaux	Vous permet d'afficher un historique détaillé de toutes les tâches exécutées par BitDefender sur votre système.
Aide et Support	Cliquez sur ce lien si vous avez besoin d'aide avec BitDefender.
	Vous donne accès à un fichier d'aide qui vous montrera comment utiliser BitDefender.

7.1.1. Zone d'état

Des informations sur l'état se trouvent dans la partie de gauche de la fenêtre.

- L'**État de Sécurité** vous avertit si des problèmes affectent la sécurité de votre ordinateur et vous aide à les corriger.Si vous cliquez sur **Tout corriger**, un assistant vous aidera à supprimer facilement toutes les menaces affectant votre ordinateur et la sécurité de vos données.Pour plus d'informations, reportez-vous à « *Correction des problèmes* » (p. 40).

- L'**État de la licence** indique le nombre de jours restants avant l'expiration de la licence.Si vous utilisez une version d'essai ou si votre licence va arriver à expiration, vous pouvez cliquer sur **Acheter** pour acheter une clé de licence.Pour plus d'informations, reportez-vous à « *Enregistrement et Mon compte* » (p. 49).

7.1.2. Zone Protection de Votre PC

C'est à partir d'ici que vous pouvez mener les actions nécessaires pour gérer votre protection.

Trois boutons sont disponibles:

- **Sécurité** vous fournit des raccourcis vers des tâches et des paramètres de sécurité.
- L'icône **Mettre à jour** vous aide à mettre à jour les signatures de virus et les fichiers du produit BitDefender.Une nouvelle fenêtre apparaît affichant l'état de la mise à jour.Si des mises à jour sont détectées, elles sont automatiquement téléchargées et installées sur votre ordinateur.
- **Mes Outils** vous permet de créer des raccourcis vers vos tâches et paramètres favoris. Un menu apparait.

Pour effectuer une tâche ou configurer des paramètres, cliquez sur le bouton correspondant et choisissez l'outil souhaité dans le menu. Pour ajouter ou supprimer des raccourcis, cliquez sur le bouton correspondant et choisissez **Plus d'Options**.Pour plus d'informations, reportez-vous à « *Mes Outils* » (p. 32).

7.1.3. Zone d'Aide

C'est ici que vous pouvez obtenir des informations sur l'utilisation de BitDefender Antivirus Pro 2011 et obtenir de l'aide.

Les **Astuces** sont une manière amusante et simple de découvrir les meilleures pratiques de sécurité informatique et comment utiliser BitDefender Antivirus Pro 2011.

Si vous avez besoin d'aide, tapez un mot ou une question dans le champ **Aide et Support**, puis cliquez sur **Rechercher**.

7.2. Mode INTERMÉDIAIRE

Conçu pour des utilisateurs ayant des compétences informatiques moyennes, le Mode Intermédiaire est une interface simple qui vous donne accès à tous les modules à un niveau basique. Vous devrez prêter attention aux avertissements et aux alertes critiques et corriger les problèmes indésirables.

La fenêtre Mode Intermédiaire est organisée en plusieurs onglets.

Tableau de bord
: Le tableau de bord vous permet de surveiller et de gérer facilement votre protection.

Sécurité
: Affiche l'état des paramètres de sécurité et vous aide à corriger les problèmes détectés.Vous pouvez exécuter des tâches de sécurité ou configurer les paramètres de sécurité.

Réseau
: Affiche la structure du réseau domestique BitDefender.Vous pouvez effectuer ici plusieurs actions pour configurer et gérer les produits BitDefender installés sur votre réseau domestique.De cette façon, vous pouvez gérer la sécurité de votre réseau domestique à partir d'un seul ordinateur.

Le bouton **Options** dans l'angle supérieur droit de la fenêtre vous permet de modifier le mode d'affichage de l'interface utilisateur et de configurer les principaux paramètres du programme.

Dans l'angle inférieur droit de la fenêtre, vous trouverez plusieurs liens utiles.

Lien	Description
Informations de Licence	Ouvre une fenêtre où vous pouvez voir des informations sur la clé de licence actuelle et enregistrer votre produit avec une nouvelle clé de licence.
Journaux	Vous permet d'afficher un historique détaillé de toutes les tâches exécutées par BitDefender sur votre système.
Acheter/Renouveler	Vous aide à acheter une clé de licence pour votre produit BitDefender Antivirus Pro 2011.
Aide et Support	Cliquez sur ce lien si vous avez besoin d'aide avec BitDefender.
	Vous donne accès à un fichier d'aide qui vous montrera comment utiliser BitDefender.

7.2.1. Tableau de bord

Le tableau de bord vous permet de surveiller et de gérer facilement votre protection.

Le tableau de bord se compose des sections suivantes :

- Les **Détails sur l'état** indiquent l'état de chacun des modules à l'aide de phrases explicites et l'une des icônes suivantes :

  Cercle vert coché : Aucun problème n'affecte l'état de sécurité.Votre ordinateur et vos données sont protégés.

Cercle rouge avec un point d'exclamation : Des problèmes affectent la sécurité de votre système.D'importants problèmes requièrent votre attention immédiate. Des problèmes non critiques devraient également être réglés dès que possible.

Cercle gris avec un point d'exclamation : L'activité des composants de ce module n'est pas surveillée. Il n'y a donc pas d'informations disponibles au sujet de leur état de sécurité.Il peut y avoir des problèmes spécifiques liés à ce module.

Cliquez sur le nom d'un module pour afficher plus de détails sur son état et configurer les paramètres de contrôle pour ses composants.

- L'**État de la licence** indique le nombre de jours restants avant l'expiration de la licence.Si vous utilisez une version d'essai ou si votre licence va arriver à expiration, vous pouvez cliquer sur **Acheter** pour acheter une clé de licence.Pour plus d'informations, reportez-vous à « *Enregistrement et Mon compte* » (p. 49).
- **Mes Outils** vous permet de créer des raccourcis vers vos tâches et paramètres favoris. Un menu apparait. Pour plus d'informations, reportez-vous à « *Mes Outils* » (p. 32).
- Les **Astuces** sont une manière amusante et simple de découvrir les meilleures pratiques de sécurité informatique et comment utiliser BitDefender Antivirus Pro 2011.

7.2.2. Sécurité

L'onglet Sécurité vous permet de gérer la sécurité de votre ordinateur et de vos données.

Zone d'état

La zone d'état affiche la liste complète des composants de sécurité surveillés et leur état actuel.En surveillant chaque module de sécurité, BitDefender vous avertira lorsque vous configurerez des paramètres pouvant affecter la sécurité de votre ordinateur, mais aussi si vous oubliez d'effectuer des tâches importantes.

L'état actuel d'un composant est indiqué en utilisant des phrases explicites et l'une des icônes suivantes :

Cercle vert coché : Aucun problème n'affecte le composant.

Cercle rouge avec un point d'exclamation : Problèmes affectent le composant.

Cliquez simplement sur le bouton **Corriger** correspondant à une phrase pour corriger le problème signalé.Si un problème de sécurité n'a pas pu être directement résolu, suivez les instructions de l'assistant.

Pour configurer quels composants doivent être surveillés :

1. Cliquez sur **Modifier la Liste**.
2. Pour activer ou désactiver la surveillance d'un élément particulier, utilisez le bouton correspondant.
3. Cliquez sur **Fermer** pour sauvegarder les modifications et fermer la fenêtre.

Important
Pour assurer une protection complète à votre système, activez le contrôle pour tous les composants et corrigez tous les problèmes signalés.

Tâches Rapides

Vous trouverez ici des liens vers les tâches de sécurité les plus importantes :

- **Mettre à jour** - effectue une mise à jour immédiate.
- **Analyse Complète du Système** - lance une analyse standard de votre ordinateur (hors archives). Pour des tâches d'analyse à la demande supplémentaires, cliquez sur la flèche de ce bouton et sélectionnez une tâche d'analyse différente.
- **Analyse Personnalisée** - lance un assistant qui vous permet de créer et d'exécuter une tâche d'analyse personnalisée.
- **Analyse de Vulnérabilité** -lance un assistant qui recherche les vulnérabilités de votre système et vous aide à les corriger.

7.2.3. Réseau

Vous pouvez effectuer ici plusieurs actions pour configurer et gérer les produits BitDefender installés sur votre réseau domestique.De cette façon, vous pouvez gérer la sécurité de votre réseau domestique à partir d'un seul ordinateur.

Pour plus d'informations, reportez-vous à « *Réseau Domestique* » (p. 110).

7.3. Mode EXPERT

L'Interface Expert vous donne accès à chaque composant de BitDefender. Vous pouvez y configurer BitDefender en détail.

Note
Le Mode Expert est destiné aux utilisateurs disposant de compétences informatiques avancées, qui connaissant le type de menaces auxquelles un ordinateur est exposé et comment les programmes de sécurité fonctionnent.

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

module.For detailed information, please refer to the « Configuration et administration » (p. 53) part of this user guide.

Général
: Vous permet d'accéder aux paramètres généraux ou de consulter le tableau de bord et des informations détaillées sur le système.

Antivirus
: Vous permet de configurer en détail votre antivirus et les opérations d'analyse, de définir les exceptions et de configurer le module Quarantaine.C'est ici que vous pouvez également configurer la protection antiphishing et Search Advisor.

Contrôle Vie Privée
: Vous permet d'éviter le vol de données sur votre ordinateur et de protéger votre vie privée lorsque vous êtes en ligne.

Vulnérabilité
: Vous permet de maintenir à jour les logiciels majeurs de votre ordinateur.

Cryptage
: Vous permet de crypter les communications Yahoo et Windows Live (MSN) Messenger.

Modes spéciaux
: Vous permet de reporter les tâches BitDefender programmées si votre ordinateur portable fonctionne sur batterie, ainsi que de désactiver toutes les alertes et fenêtres pop-up lorsqu'un jeu vidéo est lancé.

Réseau Domestique
: Vous permet de configurer et de gérer les différents ordinateurs présents dans votre foyer.

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

Enregistrement
: Vous permet d'enregistrer BitDefender Antivirus Pro 2011, de modifier la clé de licence ou de créer un compte BitDefender.

Le bouton **Options** dans l'angle supérieur droit de la fenêtre vous permet de modifier le mode d'affichage de l'interface utilisateur et de configurer les principaux paramètres du programme.

Dans l'angle inférieur droit de la fenêtre, vous trouverez plusieurs liens utiles.

Lien	Description
Informations de Licence	Ouvre une fenêtre où vous pouvez voir des informations sur la clé de licence actuelle et enregistrer votre produit avec une nouvelle clé de licence.

Lien	Description
Journaux	Vous permet d'afficher un historique détaillé de toutes les tâches exécutées par BitDefender sur votre système.
Acheter/Renouveler	Vous aide à acheter une clé de licence pour votre produit BitDefender Antivirus Pro 2011.
Aide et Support	Cliquez sur ce lien si vous avez besoin d'aide avec BitDefender.
	Vous donne accès à un fichier d'aide qui vous montrera comment utiliser BitDefender.

8. Mes Outils

Lorsque vous utilisez BitDefender en Mode Standard ou Intermédiaire, vous pouvez personnaliser votre tableau de bord en ajoutant des raccourcis vers les tâches et les paramètres qui vous semblent importants.De cette façon, vous pouvez accéder facilement aux fonctionnalités que vous utilisez régulièrement et aux paramètres avancés sans avoir à passer à un mode d'affichage de l'interface plus avancé.

En fonction du mode d'affichage de l'interface utilisateur que vous utilisez, les raccourcis ajoutés à Mes Outils sont disponibles comme suit :

Mode STANDARD
: Dans la zone Protection de votre PC, cliquez sur Mes Outils. Un menu s'affichera.Cliquez sur un raccourci pour lancer l'outil correspondant.

Mode INTERMÉDIAIRE
: Les raccourcis apparaissent sous Mes Outils.Cliquez sur un raccourci pour lancer l'outil correspondant.

Pour ouvrir la fenêtre à partir de laquelle vous pouvez sélectionner les raccourcis qui apparaîtront dans Mes Outils, procédez comme suit :

Mode STANDARD
: Dans la zone Protection de votre PC, cliquez sur Mes Outils et choisissez **Plus d'Options**.

Mode INTERMÉDIAIRE
: Cliquez sur l'un des boutons dans Mes Outils ou sur le lien **Configurer Mes Outils**.

Utilisez les boutons pour sélectionner les outils à ajouter à Mes Outils. Vous pouvez sélectionner l'une des catégories d'outils suivantes.

- **Tâches d'analyse**

  Ajoutez des tâches que vous utilisez régulièrement pour analyser votre système et rechercher les menaces de sécurité.

Tâche d'analyse	Description
Analyse Approfondie	Analyse l'ensemble du système.La configuration par défaut permet d'analyser tous les types de codes malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse Complète	Analyse l'ensemble du système, mis à part les archives.Dans la configuration par défaut, l'analyse recherche tous les types de malwares à l'exception des rootkits.

Tâche d'analyse	Description
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.
Analyse personnalisée	Lance un assistant qui vous permet de créer une tâche d'analyse personnalisée.
Analyse de Mes documents	Utilisez-la pour analyser les dossiers importants de l'utilisateur actuel: `Mes documents`, `Bureau` et `Démarrage`. Cela vous permet d'assurer la sécurité de vos documents, un espace de travail sécurisé et d'exécuter des applications saines au démarrage.
Planifier Mes Analyses	Vous dirige vers la fenêtre des paramètres Antivirus où vous pouvez personnaliser les tâches d'analyse à la demande.

Pour plus d'informations sur les tâches d'analyse, reportez-vous à« *Gestion des tâches d'analyse existantes* » (p. 72)

- **Configuration**

  Ajoutez des raccourcis vers les paramètres de BitDefender que vous voulez configurer :

Configuration	Description
Paramètres antivirus	Configurez le module Antivirus. Pour plus d'informations, reportez-vous à« *Protection Antivirus* » (p. 59)
Mode Jeu	Basculer en Mode Jeu. Pour plus d'informations, reportez-vous à« *Mode Jeu* » (p. 104)
Mode Portable	Basculez en Mode Portable. Pour plus d'informations, reportez-vous à« *Mode Portable* » (p. 107)
Mettre à jour	Réalisez une mise à jour de BitDefender. Pour plus d'informations, reportez-vous à« *Mise à jour* » (p. 114)
Voir & Corriger tous les problèmes	Ouvrez un assistant qui vous aidera à résoudre tous les problèmes de sécurité qui affectent votre système. Pour plus d'informations, reportez-vous à« *Correction des problèmes* » (p. 40)

- **Aide & Support**

  Entrez dans la section support. Pour plus d'informations, reportez-vous à« Contactez-Nous Directement à partir de Votre Produit BitDefender » (p. 148)

9. Alertes et Fenêtres pop-up

BitDefender utilise des notes et des alertes pour vous informer de son fonctionnement et des événements qui peuvent vous intéresser et vous invite à mener des actions, le cas échéant.Ce chapitre présente les notes et les alertes de BitDefender que vous pouvez rencontrer.

Les fenêtres pop-up sont de petites fenêtres qui s'affichent pour vous informer d'événements BitDefender divers : analyse du courrier électronique, nouvel ordinateur connecté au réseau sans fil, ajout d'une nouvelle règle concernant le pare-feu, etc.Quand des fenêtres pop-up s'afficheront, vous devrez cliquez sur un bouton **OK** ou sur un lien.

Les alertes sont des fenêtres de plus grande taille qui vous invitent à mener une action ou vous informent sur un événement important (par exemple, un virus qui a été détecté).En plus des fenêtres d'alerte, vous pouvez recevoir des alertes par e-mail, messagerie instantanée ou page web.

Les alertes et les notes de BitDefender incluent :

- Alertes Antivirus
- Alertes Active Virus Control
- Alertes de Détection de Périphérique
- Pages Web d'alerte antiphishing
- Alertes du Contrôle Vie privée

9.1. Alertes Antivirus

BitDefender vous protège contre différents types de logiciels malveillants comme les virus, les spywares ou les rootkits.Lorsqu'il détecte un virus ou un autre malware, BitDefender mène des actions spécifiques sur le fichier infecté et vous en informe via une fenêtre d'alerte.

Vous pouvez voir le nom du virus, le chemin d'accès au fichier infecté et la mesure prise par BitDefender.

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

Important

Lorsqu'un virus est détecté, il est recommandé d'analyser la totalité de l'ordinateur pour s'assurer qu'il n'y a pas d'autres virus.Pour plus d'informations, reportez-vous à « *Comment analyser des fichiers et des dossiers ?* » (p. 119).
Si le virus n'a pas été bloqué, reportez-vous à « *Suppression de malwares depuis votre système* » (p. 137).

9.2. Alertes Active Virus Control

Active Virus Control peut être configuré pour vous prévenir et vous demander quelle action entreprendre lorsqu'une application essaie de réaliser une action potentiellement malveillante.

Si vous utilisez l'Interface Standard ou Intermédiaire, une fenêtre pop-up vous informera lorsqu'Active Virus Control bloquera une application potentiellement malveillante. Si vous utilisez l'Interface Expert, on vous demandera de choisir une action, via une fenêtre d'alertes, lorsqu'une application présentera un comportement suspect.

Si vous connaissez l'application et la savez de confiance, cliquez sur **Autoriser**.

Si vous voulez fermer immédiatement cette application, cliquez sur **OK**.

Cochez la case **Retenir cette action pour cette application** avant de faire votre choix et BitDefender réalisera la même action pour l'application détectée par la suite.La règle ainsi créée apparaîtra dans la fenêtre de configuration d'Active Virus Control.

9.3. Alertes de Détection de Périphérique

BitDefender détecte automatiquement la connexion d'un périphérique de stockage amovible à votre ordinateur et vous propose de l'analyser avant que vous accédiez à ses fichiers.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

Lorsqu'un tel périphérique est détecté, une fenêtre d'alerte s'affiche.

Pour analyser le périphérique de stockage, cliquez simplement sur **Oui**.L'Assistant d'Analyse Antivirus apparaîtra et vous guidera tout au long du processus d'analyse.

Si vous ne souhaitez pas analyser le périphérique, cliquez sur **Non**. Dans ce cas, il se peut que l'une des options suivantes vous semble utile :

- **Ne plus me demander pour ce type de périphérique** - BitDefender ne proposera plus d'analyser ce type de périphériques de stockage lorsqu'ils seront connectés à votre ordinateur.
- **Désactiver la détection automatique de périphérique** - On ne vous proposera plus d'analyser les nouveaux périphériques de stockage lorsqu'ils seront connectés à l'ordinateur.

Si vous avez désactivé par erreur la détection automatique de périphérique et que vous voulez l'activer, ou si vous souhaitez configurer ses paramètres, procédez comme suit :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Antivirus>Analyse Antivirus**.
3. Dans la liste des tâches d'analyse, localisez la tâche **Analyse des périphériques détectés**.
4. Faites un clic droit sur la tâche et sélectionnez **Ouvrir**.Une nouvelle fenêtre s'affiche.
5. Dans l'onglet **Présentation**, configurez les options d'analyse selon vos besoins.Pour plus d'informations, reportez-vous à « *Configuration des paramètres d'analyse* » (p. 75).
6. Dans l'onglet **Détection**, sélectionnez les types de périphériques de stockage à détecter.
7. Cliquez sur **OK** pour enregistrer et appliquer les modifications.

9.4. Alertes Antiphishing

Lorsque la protection antiphishing est activée, BitDefender vous alerte quand vous tentez d'accéder à des pages Web conçues pour dérober des informations personnelles.Avant de pouvoir accéder à cette page Web, BitDefender la bloque et affiche une page Web d'alerte générique.

Examinez l'adresse de la page Web dans la barre d'adresse de votre navigateur.Cherchez des indices qui pourraient indiquer que la page Web est destinée au phishing.Si la page Web est suspecte, il vous est recommandé de ne pas l'ouvrir.

Voici quelques astuces dont vous pourrez apprécier l'utilité :

- Si vous avez entré l'adresse d'un site Web légitime, vérifiez que l'adresse est correcte. Si ce n'est pas le cas, tapez-la de nouveau et retournez sur la page.
- Si vous avez cliqué sur un lien dans un e-mail ou dans un message instantané, regardez qui vous l'a envoyé. Si l'expéditeur vous est inconnu, il s'agit probablement d'une tentative de phishing. Si vous connaissez l'expéditeur, vérifiez que c'est bien lui qui vous a envoyé ce lien.
- Si vous avez atteint cette page en naviguant sur Internet, vérifiez la page Web où vous avez trouvé le lien (cliquez sur le bouton Retour de votre navigateur)

Si vous voulez voir la page Web, cliquez sur le lien correspondant pour prendre une des mesures qui suivent :

- **Afficher la page Web cette fois-ci seulement.** C'est sans risque tant que vous n'entrez aucune information sur la page Web.Si la page web est légitime, vous pouvez l'ajouter à la Liste Blanche (cliquez sur la barre d'outils Antiphishing BitDefender et sélectionnez **Ajouter à la Liste Blanche**).
- **Ajouter la page Web à la Liste blanche.** La page Web s'affichera immédiatement et BitDefender ne vous alertera plus à son sujet.

Important

N'ajoutez à la Liste blanche que les pages auxquelles vous faites totalement confiance (par exemple l'adresse du site de votre banque, les boutiques en ligne connues, etc.).BitDefender n'effectue pas de vérification antiphishing des pages Web de la Liste blanche.

Vous pouvez gérer la protection antiphishing et la Liste blanche au moyen de la barre d'outils BitDefender de votre navigateur web.Pour plus d'informations, reportez-vous à « *Gestion de la Protection Antiphishing BitDefender dans Internet Explorer et Firefox* » (p. 86).

9.5. Alertes du Contrôle Vie privée

Le contrôle de la vie privée fournit aux utilisateurs avancés des fonctions supplémentaires pour protéger leur vie privée.On vous demandera de choisir une action via des fenêtres d'alertes spécifiques si vous choisissez d'activer l'un de ces composants :

- Contrôle du Registre - demande votre autorisation dès lors qu'un programme tente de modifier une entrée de registre afin de s'exécuter au démarrage de Windows.
- Contrôle des cookies - demande votre autorisation dès lors qu'un nouveau site Web tente de créer un cookie sur votre ordinateur.
- Contrôle des Scripts - demande votre autorisation dès lors qu'un site Web tente d'exécuter un script ou un autre contenu actif.

9.5.1. Alertes registre

Si vous activez le Contrôle du Registre, on demandera votre autorisation lorsqu'un nouveau programme tentera de modifier une entrée du registre pour être exécuté au démarrage de Windows.

Vous pouvez voir le programme essayant de modifier le registre Windows.

Note

BitDefender vous alertera à l'installation de nouveaux logiciels nécessitant d'être lancés après le prochain démarrage de votre ordinateur. Ces programmes sont généralement légitimes et fiables.

Si vous ne reconnaissez pas le programme et qu'il vous semble suspect, cliquez sur **Bloquer** pour l'empêcher de modifier le registre Windows.Autrement, cliquez sur **Autoriser** pour permettre la modification.

Une règle est créée et ajoutée au tableau des règles à partir de votre réponse.La même action est appliquée à chaque fois que ce programme tente de modifier une entrée de la base registre.

Pour plus d'informations, reportez-vous à « *Contrôle du Registre* » (p. 94).

9.5.2. Alertes de scripts

Si vous activez le Contrôle des Scripts, il vous demandera l'autorisation lorsqu'un nouveau site essaiera d'exécuter un script ou un autre contenu actif.

Vous pouvez voir le nom de la ressource.

Cliquez sur **Oui** ou sur **Non** et une règle sera créée, appliquée, et ajoutée au tableau des règles.La même action sera automatiquement appliquée à chaque fois que le site concerné essaiera d'exécuter du contenu actif.

Note
Certaines pages Web peuvent ne pas s'afficher correctement si vous bloquez le contenu actif.

Pour plus d'informations, reportez-vous à « *Contrôle des Scripts* » (p. 97).

9.5.3. Alertes de cookies

Si vous activez le contrôle des cookies, on vous demandera votre autorisation lorsqu'un nouveau site essaiera de créer ou d'utiliser un cookie.

Vous pouvez voir le nom de l'application qui tente de transmettre le fichier de type cookie.

Cliquez sur **Oui** ou sur **Non** et une règle sera créée, appliquée, et ajoutée au tableau des règles.La même action sera appliquée automatiquement chaque fois que vous vous connecterez au site en question.

Pour plus d'informations, reportez-vous à « *Contrôle des cookies* » (p. 95).

10. Correction des problèmes

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).

Voici comment les problèmes en attente sont signalés :

- Un symbole spécial apparaît sur l'icône de BitDefender dans la zone de notification pour signaler la présence de problèmes en attente.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 BitDefender, la zone d'État de Sécurité indique le nombre de problèmes affectant votre système.
  - En Mode Standard, l'état de sécurité est affiché dans la partie gauche de la fenêtre.
  - En Mode Expert, allez à **Général > Tableau de bord**, pour vérifier l'état de la sécurité.

10.1. Assistant de correction des problèmes

La manière la plus facile de corriger les problèmes existants est de suivre l'**Assistant de correction des problèmes**.Pour ouvrir l'assistant, procédez comme indiqué :

- Faites un clic droit sur l'icône de BitDefender dans la zone de notification et sélectionnez **Tout corriger**.
- Ouvrez BitDefender et, en fonction du mode d'affichage de l'interface utilisateur, procédez comme suit :
  - En Mode Standard, cliquez sur **Voir tous les problèmes**.
  - En Mode Expert, allez dans **Général > Tableau de bord** et cliquez sur **Voir tous les problèmes**.

Note
Vous pouvez également ajouter un raccourci à Mes Outils.

Une liste des menaces de sécurité présentes sur votre ordinateur s'affiche.

Tous les problèmes présents sont sélectionnés pour être corrigés. Si vous ne voulez pas corriger un problème, décochez simplement la case correspondante. Son état passera alors à **Ignorer**.

Note
Si vous ne voulez pas être informé(e) de la présence de certains problèmes, vous devez configurer le système d'alerte en conséquence, comme décrit dans la section suivante.

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 exemple de ce type de tâches est l'analyse de votre ordinateur. Nous vous recommandons d'analyser votre ordinateur au moins une fois par semaine. En général, BitDefender réalisera cette analyse pour vous de façon automatique. Mais si vous avez modifié la planification de l'analyse ou si la planification n'a pas été réalisée, ce problème vous sera signalé.

  Un assistant vous aide à corriger ces problèmes.
- **Vulnérabilités du Système.** BitDefender recherche automatiquement les vulnérabilités de votre système et vous les signale.Les vulnérabilités du Système peuvent être :
  - des mots de passe non sécurisés de comptes utilisateurs Windows
  - la présence sur votre ordinateur de logiciels non à jour
  - des mises à jour Windows manquantes
  - les mises à jour automatiques de Windows sont désactivées

  Lorsque de tels problèmes doivent être corrigés, l'assistant de l'analyse de vulnérabilité est lancé. Cet assistant vous aide à corriger les vulnérabilités du système qui ont été détectées.For detailed information, please refer to section « *Rechercher des vulnérabilités* » (p. 99).

10.2. Configuration des alertes d'état

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

Vous pouvez configurer le système d'alertes afin de répondre au mieux à vos besoins de sécurité en choisissant des problèmes spécifiques sur lesquels vous souhaitez être informé.Vous pouvez le faire en Mode Intermédiaire ou Expert.

- En Mode Intermédiaire, le système d'alerte peut être configuré à partir de différents endroits.Suivez ces étapes :
  1. Allez à l'onglet **Sécurité**.
  2. Cliquez sur le lien **Modifier la Liste** dans la zone d'état.
  3. Utilisez le bouton correspondant à un élément pour modifier son état d'alerte.
- En Mode Expert, le système d'alerte peut être configuré à partir d'un emplacement central.Suivez ces étapes :
  1. Allez à **Général > Tableau de bord**.
  2. Cliquez sur **Ajouter/Modifier des Alertes**.
  3. Utilisez le bouton correspondant à un élément pour modifier son état d'alerte.

11. Configuration des paramètres principaux

Vous pouvez configurer les principaux paramètres du produit (y compris reconfigurer le profil d'utilisation) à partir de la fenêtre Préférences. Pour l'ouvrir, utilisez l'une des méthodes suivantes :

- Ouvrez BitDefender, cliquez sur **Options** dans le coin supérieur droit de la fenêtre, puis choisissez **Préférences**.
- Faites un clic droit sur l'icône BitDefender dans la zone de notification, puis sélectionnez **Préférences**.

Note

Pour configurer les paramètres du produit en détail, utilisez le Mode Expert de l'interface.For detailed information, please refer to the « Configuration et administration » (p. 53) part of this user guide.

Les paramètres sont regroupés en trois catégories :

- Paramètres de sécurité
- Paramètres des Alertes
- Paramètres Généraux

Pour activer ou désactiver un paramètre, cliquez sur le bouton correspondant.

Pour appliquer et enregistrer les modifications de configuration que vous faites, cliquez sur **OK**. Pour fermer la fenêtre sans enregistrer les modifications, cliquez sur **Annuler**.

Le lien **Reconfigurer le profil** situé dans le coin supérieur droit de la fenêtre vous permet de reconfigurer le profil utilisé.Pour plus d'informations, reportez-vous à « *Reconfiguration du Profil d'Utilisation* » (p. 46).

11.1. Paramètres de sécurité

Vous pouvez activer ou désactiver des paramètres du produit couvrant plusieurs aspects de la sécurité informatique et des données dans cette zone. Pour activer ou désactiver un paramètre, cliquez sur le bouton correspondant.

Avertissement

Soyez prudent(e) lorsque vous désactivez la protection antivirus en temps réel ou la mise à jour automatique.Désactiver ces fonctionnalités peut compromettre la sécurité de votre ordinateur. Si vous avez réellement besoin de les désactiver, pensez à les réactiver dès que possible.

Vous avez le choix entre :

Antivirus
La protection de fichiers en temps réel garantit que tous les fichiers sont analysés lorsque vous (ou une application exécutée sur ce système) y accédez.

Mise à jour automatique
La mise à jour automatique permet de télécharger et d'installer automatiquement et régulièrement les dernières versions du produit BitDefender et des fichiers de signatures.Les mises à jour sont réalisées toutes les heures par défaut.

Vulnérabilité
L'Analyse de Vulnérabilité Automatique vous informe des vulnérabilités de votre système pouvant affecter sa sécurité et vous aide à les corriger. Ces vulnérabilités comprennent les logiciels non à jour, les mots de passe non sécurisés de comptes utilisateur et les mises à jour Windows manquantes.

Antiphishing
L'Antiphishing vous alerte en temps réel s'il détecte qu'une page Web est conçue pour voler des informations personnelles.

Search Advisor
Search Advisor analyse les liens des résultats de vos recherches et vous indique lesquels sont sûrs et lesquels ne le sont pas.

Contrôle d'identité
Le Contrôle d'Identité vous aide à empêcher que vos données personnelles ne soient transmises sur Internet sans votre accord. Il bloque tous les messages instantanés, e-mails ou formulaires Web transmettant vers des destinataires non autorisés des données que vous avez définies comme étant confidentielles.

Messagerie Inst.
Le cryptage de Messagerie Instantanée protège vos conversations via Yahoo! Messenger et Windows Live Messenger à condition que vos contacts de messagerie instantanée utilisent un produit BitDefender et un logiciel de messagerie instantanée compatibles.

L'état de certains de ces paramètres peut être surveillé par le système de contrôle de BitDefender.Si vous désactivez un paramètre surveillé, BitDefender le signalera comme un problème à corriger.

Si vous ne souhaitez pas qu'un paramètre surveillé que vous avez désactivé apparaisse comme un problème, vous devez configurer le système de contrôle en conséquence. Vous pouvez le faire en Mode Intermédiaire ou Expert.Pour plus d'informations, reportez-vous à « *Configuration des alertes d'état* » (p. 41).

11.2. Paramètres des Alertes

Vous pouvez désactiver les alertes et fenêtres pop-up BitDefender dans cette zone.BitDefender utilise des alertes pour vous demander quelle action entreprendre

et des fenêtres pop-up pour vous informer au sujet des actions prises automatiquement ou sur d'autres événements. Pour activer ou désactiver une catégorie d'alertes, cliquez sur le bouton correspondant.

Important
La plupart de ces alertes et de ces notes doivent rester activées afin d'éviter des problèmes potentiels.

Vous avez le choix entre :

Alertes Antivirus
Des alertes antivirus vous informent lorsque BitDefender détecte et bloque un virus. Lorsqu'un virus est détecté, il est recommandé d'analyser la totalité de l'ordinateur pour s'assurer qu'il n'y a pas d'autres virus.

Messages d'Active Virus Control
Si vous utilisez l'Interface Standard ou Intermédiaire, une fenêtre pop-up vous informera lorsqu'Active Virus Control bloquera une application potentiellement malveillante. Si vous utilisez l'Interface Expert, on vous demandera de choisir une action, via une fenêtre d'alertes, lorsqu'une application présentera un comportement suspect.

Messages d'analyse des e-mails
Ces notes sont affichées pour vous informer que BitDefender est en cours d'analyse des e-mails à la recherche de malwares.

Alertes de la Gestion du Réseau Domestique
Ces alertes informent l'utilisateur lorsque des actions administratives sont effectuées à distance.

Alertes de la Quarantaine
Les alertes de la quarantaine vous informent lorsque d'anciens fichiers de la quarantaine ont été supprimés.

Messages d'enregistrement
Les messages d'enregistrement sont utilisés pour vous rappeler que vous avez besoin d'enregistrer BitDefender ou pour vous signaler que la clé de licence est sur le point d'expirer ou a déjà expiré.

11.3. Paramètres Généraux

Vous pouvez activer ou désactiver les paramètres qui affectent le fonctionnement du produit et son utilisation dans cette zone. Pour activer ou désactiver un paramètre, cliquez sur le bouton correspondant.

Vous avez le choix entre :

Mode Jeu
Le Mode Jeu modifie temporairement les paramètres de protection afin de préserver les ressources de votre système pendant les jeux.

Détection du Mode Portable

Le Mode Portable modifie temporairement les paramètres de protection afin de préserver l'autonomie de la batterie de votre ordinateur portable.

Mot de passe paramètres

Pour empêcher que quelqu'un d'autre ne modifie les paramètres de BitDefender, vous pouvez les protéger avec un mot de passe.Si vous activez cette option, on vous demandera de configurer le mot de passe des paramètres.Tapez le mot de passe souhaité dans les deux champs et cliquez sur **OK** pour définir le mot de passe.

BitDefender News

En activant cette option, vous serez informé par BitDefender de l'actualité de la société, des mises à jour de produits ou des nouvelles menaces de sécurité.

Alertes du produit

En activant cette option, vous recevrez des alertes d'information.

Barre de l'activité d'analyse

La Barre d'Activité d'Analyse est une petite fenêtre transparente indiquant la progression de l'activité d'analyse de BitDefender.

Envoyer rapports d'infection

En activant cette option, les rapports d'analyse virale sont envoyés aux laboratoires BitDefender pour être examinés. Notez que ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et qu'ils ne seront pas utilisés à des fins commerciales.

Outbreak Detection

En activant cette option, les rapports concernant les potentielles alertes virales sont envoyés aux laboratoires BitDefender pour être examinés. Notez que ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et qu'ils ne seront pas utilisés à des fins commerciales.

11.4. Reconfiguration du Profil d'Utilisation

Pendant l'installation, vous pouvez configurer un profil d'utilisation.Le profil d'utilisation reflète les principales activités réalisées avec l'ordinateur. L'interface du produit s'adapte à votre profil d'utilisation pour vous permettre d'accéder facilement à vos tâches favorites.

Pour reconfigurer le profil d'utilisation, cliquez sur **Reconfigurer le profil** et suivez l'assistant de configuration. Vous pouvez naviguer dans l'assistant à l'aide des boutons **Suivant** et **Retour**. Pour quitter l'assistant, cliquez sur **Annuler**.

1. **Choisir votre Mode d'Affichage**

   Choisissez votre vue favorite de l'interface utilisateur.

2. **Configurer Mes Outils**

Si vous avez sélectionné le Mode Standard ou Intermédiaire, choisissez les fonctionnalités vers lesquelles vous aimeriez créer des raccourcis sur le Bureau.

3. **Configurer les Paramètres**

   Si vous avez sélectionné le Mode Expert, configurez les paramètres de BitDefender selon vos besoins. Pour activer ou désactiver un paramètre, cliquez sur le bouton correspondant.

4. **Gestion du Réseau Domestique**

   Note
   Cette étape n'apparaît que si vous avez ajouté la gestion du réseau domestique à Mes outils.

   Vous pouvez sélectionner l'une de ces trois options :

   - **Configurer ce PC en tant que "Serveur"**

     Sélectionnez cette option si vous prévoyez d'administrer des produits BitDefender sur d'autres ordinateurs du réseau domestique à partir de celui-ci.

     Un mot de passe est requis pour rejoindre le réseau. Saisissez le mot de passe dans les zones de texte et cliquez sur **Envoyer**.

   - **Configurer ce PC en tant que "Client"**

     Sélectionnez cette option si BitDefender sera géré par un autre ordinateur du réseau domestique exécutant également BitDefender.

     Un mot de passe est requis pour rejoindre le réseau. Saisissez le mot de passe dans les zones de texte et cliquez sur **Envoyer**.

   - **Ignorer l'installation pour le moment**

     Sélectionnez cette option pour configurer cette fonction ultérieurement depuis la fenêtre BitDefender.

5. **Installation terminée**

   Cliquez sur **Terminer**.

12. Historique et Événements

Le lien **Afficher les Journaux** situé en bas de la fenêtre principale de BitDefender ouvre une autre fenêtre contenant l'historique et les événements de BitDefender. Cette fenêtre vous présente les événements liés à la sécurité.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.

Les catégories suivantes, présentées à gauche, permettent de filtrer l'historique et les événements BitDefender:

- **Tableau de bord**
- **Antivirus**
- **Contrôle Vie Privée**
- **Vulnérabilité**
- **Cryptage de Messagerie Instantanée**
- **Modes spéciaux**
- **Réseau Domestique**
- **Mise à jour**
- **Enregistrement**

Une liste d'événements est proposée pour chaque catégorie. Chaque événement comporte les informations suivantes : une courte description de l'événement, l'action menée par BitDefender, la date et l'heure de l'événement. Pour obtenir plus d'informations sur un événement de la liste en particulier, double-cliquez sur cet événement.

Cliquez sur **Effacer tous les journaux** si vous voulez supprimer les anciens journaux ou sur **Actualiser** pour vous assurer que les journaux les plus récents sont affichés.

13. Enregistrement et Mon compte

L'enregistrement se fait en deux étapes :

1. **Activation du produit (enregistrement d'un compte BitDefender).** Si vous avez acheté votre produit en ligne, vous devez créer un compte BitDefender afin de recevoir les mises à jour et d'avoir accès au support technique gratuit.Si vous avez déjà un compte BitDefender, enregistrez votre produit BitDefender avec ce compte.Si vous avez besoin d'activer votre produit, BitDefender vous le signalera et vous aidera à régler ce problème.

   Important

   Il est recommandé de créer un compte dans les 15 jours qui suivent l'installation de BitDefender.Dans le cas contraire, BitDefender ne se mettra plus à jour.

2. **Enregistrement 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.

Si vous avez acheté BitDefender Antivirus Pro 2011 sur un CD/DVD ou en ligne, on vous a demandé d'enregistrer votre produit avec une clé de licence pendant l'installation.

Si vous avez téléchargé BitDefender Antivirus Pro 2011 en mode d'évaluation, vous devez enregistrer le produit avec une clé de licence pour continuer à l'utiliser après les 30 jours de la période d'essai.Pendant la période d'essai, toutes les fonctionnalités du programme sont disponibles et vous pouvez donc tester le produit pour voir s'il répond à vos attentes.

13.1. Enregistrement de BitDefender Antivirus Pro 2011

Si vous souhaitez enregistrer le produit avec une clé de licence ou modifier la clé de licence actuelle, cliquez sur le lien **Informations de Licence** situé en bas de la fenêtre de BitDefender.La fenêtre d'enregistrement du produit s'affichera.

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 Pro 2011 :

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 indiqué pour lancer un assistant qui vous aidera à en acheter une.

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

13.2. Activation de BitDefender

Pour activer BitDefender, vous devez créer un compte BitDefender ou vous connecter à un compte existant.Si vous n'avez pas enregistré de compte BitDefender pendant l'assistant d'installation, vous pouvez procéder comme suit :

Mode STANDARD
: Cliquez sur **Voir tous les problèmes**.L'assistant vous aidera à corriger les problèmes en attente, y compris l'activation du produit.

Mode INTERMÉDIAIRE
: Allez à l'onglet **Sécurité**, puis cliquez sur le bouton **Voir & Corriger** correspondant au problème concernant la mise à jour du produit.Cliquez sur **Démarrer** dans la fenêtre de l'assistant pour activer le produit.

Mode EXPERT
: Allez dans **Enregistrement** et cliquez sur le bouton **Activer le produit**.

Une fenêtre d'enregistrement du compte s'ouvrira.C'est là que vous pouvez créer un compte BitDefender ou vous connecter à un compte existant pour activer votre produit.

Si vous ne souhaitez pas créer immédiatement un compte BitDefender, sélectionnez **Créer un compte plus tard** et cliquez sur **Terminer**.Autrement, procédez selon votre situation actuelle :

- « Je n'ai pas de compte BitDefender » (p. 50)
- « J'ai déjà un compte BitDefender » (p. 51)

Important

Il est recommandé de créer un compte dans les 15 jours qui suivent l'installation de BitDefender.Dans le cas contraire, BitDefender ne se mettra plus à jour.

Je n'ai pas de compte BitDefender

Pour créer un compte BitDefender, suivez ces étapes :

1. Sélectionnez **Créer un nouveau compte**.
2. Tapez les informations requises dans les champs correspondants. Les informations communiquées ici resteront confidentielles.

- **Nom d'utilisateur** - saisissez votre adresse e-mail.
- **Mot de passe** - entrez un mot de passe pour votre compte BitDefender.Le mot de passe doit contenir entre 6 et 16 caractères.
- **Ressaisir le mot de passe** - confirmez le mot de passe que vous venez d'indiquer.

  Il n'est pas nécessaire de saisir à nouveau le mot de passe si vous avez choisi de ne pas masquer le mot de passe lorsque vous le tapez.
- **Indice du mot de passe** - saisissez un mot ou une phrase qui vous aidera à vous souvenir du mot de passe en cas d'oubli.

Note

Une fois le compte activé, 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. Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte.Cliquez sur **Afficher les Options de Contact** et sélectionnez l'une des options disponibles dans la fenêtre qui apparaît.
   - **M'envoyer tous les messages**
   - **Envoyer les messages importants**
   - **Ne pas m'envoyer de message**
4. Cliquez sur **Envoyer**.
5. Cliquez sur **Terminer** pour fermer la fenêtre.

Note

Vous devez activez votre compte avant de pouvoir l'utiliser.
Consultez votre messagerie et suivez les instructions données dans le message que vous a adressé le service d'enregistrement de BitDefender.

J'ai déjà un compte BitDefender

BitDefender détectera automatiquement si vous avez déjà un compte BitDefender actif sur cet ordinateur.Si c'est le cas, introduisez le mot de passe de votre compte, puis cliquez sur **Envoyer**.Cliquez sur **Terminer** pour fermer la fenêtre.

Si vous avez déjà un compte actif, mais que BitDefender ne le détecte pas, suivez ces étapes pour enregistrer le produit avec ce compte :

1. Sélectionnez **Se Connecter (Compte Existant)**.
2. Tapez l'adresse e-mail et le mot de passe de votre compte dans les champs correspondants.

Note
Si vous ne souhaitez pas faire de modifications, cliquez sur **Terminer** pour fermer l'assistant.

3. Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte.Cliquez sur **Afficher les Options de Contact** et sélectionnez l'une des options disponibles dans la fenêtre qui apparaît.
   - **M'envoyer tous les messages**
   - **Envoyer les messages importants**
   - **Ne pas m'envoyer de message**
4. Cliquez sur **Envoyer**.
5. Cliquez sur **Terminer** pour fermer la fenêtre.

13.3. Achat ou renouvellement de 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.En tant que client BitDefender, vous avez droit à une réduction lorsque vous renouvelez la licence de votre produit BitDefender. Vous pouvez également mettre à niveau votre produit vers la version actuelle à un tarif spécial ou gratuitement.

Pour commencer une procédure simple et sûre en quatre étapes qui vous permettra d'acheter une nouvelle clé ou d'en renouveler une existante, ouvrez BitDefender en Mode Intermédiaire ou Expert, puis cliquez sur le lien **Acheter** ou **Renouveler**, situé en bas de la fenêtre.

Configuration et administration

14. Paramètres Généraux

Le module Général donne des informations sur l'activité de BitDefender et sur le système.Vous pouvez également modifier le comportement global de BitDefender.

Pour configurer les paramètres généraux :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Général > Configuration**.

- **Activer la protection par mot de passe pour les paramètres du produit** - permet de choisir un mot de passe afin de protéger la configuration de BitDefender.

  Note

  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.

  Entrez le mot de passe dans le champ **Mot de passe**, re-saisissez le dans le champ **Resaisir le mot de passe** et cliquez sur **OK**.

  Une fois le mot de passe paramétré, il vous sera demandé dès que vous voudrez modifier les paramètres de BitDefender.Les autres administrateurs du système, s'il y en a, auront également à fournir le mot de passe pour changer les paramètres de BitDefender.

  Important

  Si vous avez oublié votre mot de passe vous devrez réinstaller partiellement le produit pour modifier la configuration de BitDefender.

- **Afficher BitDefender News (notifications liées à la sécurité)** - communique de temps en temps les notifications de sécurité relatives aux irruptions de virus envoyées par le serveur BitDefender.
- **Afficher des notes sur l'écran** - affiche des fenêtres de notifications sur l'état de votre produit.Vous pouvez configurer BitDefender afin qu'il affiche des notes uniquement lorsque l'interface se trouve en Mode Standard/Intermédiaire ou Expert.
- **Activer la barre d'analyse de l'activité (graphique de l'activité du produit)** - affiche la barre d'analyse de l'activité à chaque fois que vous démarrez Windows..Décochez cette case si vous ne voulez plus que la barre d'analyse de l'activité s'affiche.

Note

Seul le compte utilisateur Windows actuel peut configurer cette option.La barre d'activité d'analyse est disponible uniquement lorsque l'interface est en Mode Expert.

Paramètres du rapport antivirus

- **Envoyer des rapports d'infection** - envoie au laboratoire BitDefender des rapports concernant les virus identifiés sur vote PC. Les informations envoyées contiendront seulement le nom des virus et seront utilisées pour créer des rapports statistiques.

  Le rapport ne contiendra aucune donnée confidentielle, comme votre nom, votre adresse IP ou autre et ne sera pas utilisé à des fins commerciales. Les informations envoyées contiendront seulement le nom des virus et seront utilisées pour créer des rapports statistiques.

- **Activer l'Outbreak Detection de BitDefender** - envoie des rapports aux BitDefender Labs à propos d'apparitions éventuelles de virus.

  Le rapport ne contiendra aucune donnée confidentielle, comme votre nom, votre adresse IP ou autre et ne sera pas utilisé à des fins commerciales. Les informations envoyées contiendront uniquement les virus potentiels et seront utilisées dans le seul but de créer des rapports statistiques.

Paramètres de connexion

Plusieurs composants de BitDefender (le Pare-feu, LiveUpdate, les modules Real Time Virus Reporting et Real-Time Spam Reporting) nécessitent un accès à Internet. BitDefender inclut un gestionnaire de proxy qui vous permet de configurer depuis un emplacement les paramètres du proxy utilisés par les composants de BitDefender pour accéder à Internet.

Si votre entreprise utilise un serveur proxy pour se connecter à Internet, vous devez spécifier les paramètres du proxy afin que BitDefender puisse se mettre à jour. Sinon, BitDefender utilisera les paramètres du proxy de l'administrateur qui a installé le produit ou du navigateur par défaut de l'utilisateur actuel, le cas échéant.Pour plus d'informations, reportez-vous à « *Comment connaître mes paramètres de proxy ?* » (p. 157).

Note

Les paramètres du proxy peuvent être configurés uniquement par les utilisateurs possédant des droits d'administrateur ou par des utilisateurs privilégiés (des utilisateurs qui connaissent le mot de passe pour accéder aux paramètres du produit).

Pour gérer les paramètres du proxy, cliquez sur **Paramètres proxy**.

Il existe trois catégories de paramètres de proxy :

- **Proxy détecté lors de l'installation** - paramètres proxy détectés sur le compte de l'administrateur lors de l'installation et ne pouvant être configurés que si vous êtes connecté à ce compte. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, vous devez les indiquer dans les champs correspondants.
- **Proxy du Navigateur par défaut** - paramètres proxy de l'utilisateur acteur, extraits du navigateur par défaut. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, vous devez les spécifier dans les champs correspondants.

Note

Les navigateurs Web pris en charge sont Internet Explorer, Mozilla Firefox et Opera. Si vous utilisez un autre navigateur par défaut, BitDefender ne pourra pas obtenir les paramètres du proxy de l'utilisateur actuel.

- **Proxy Personnalisé** - paramètres proxy que vous pouvez configurer si vous êtes connecté(e) en tant qu'administrateur.

  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** - entrez le 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.

BitDefender utilisera les ensembles de paramètres de proxy dans l'ordre suivant jusqu'à ce qu'il parvienne à se connecter à Internet :

1. les paramètres de proxy spécifiés.
2. les paramètres du proxy détectés lors de l'installation.
3. les paramètres proxy de l'utilisateur actuel.

Lors de la tentative de connexion à Internet, chaque catégorie de paramètres de proxy est testée, jusqu'à ce que BitDefender parvienne à se connecter.

Tout d'abord, la catégorie contenant vos propres paramètres de proxy est utilisée pour la connexion Internet. Si elle ne fonctionne pas, ce sont alors les paramètres de proxy détectés lors de l'installation qui sont utilisés. Finalement, s'ils ne fonctionnent pas non plus, les paramètres du proxy de l'utilisateur actuel sont pris sur le navigateur par défaut et utilisés pour la connexion Internet.

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

Cliquez sur **Appliquer** pour enregistrer les modifications ou cliquez sur **Défaut** pour charger les paramètres par défaut.

Informations système

BitDefender vous permet d'afficher, à partir d'un emplacement unique, tous les paramètres du système ainsi que les applications enregistrées pour être exécutées au démarrage. Vous pouvez ainsi contrôler l'activité du système et des applications installées et identifier d'éventuelles infections.

Pour obtenir des informations sur le système :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Général > Informations Système**.

La liste contient tous les objets chargés au démarrage du système ainsi que les objets chargés par différentes applications.

Trois boutons sont disponibles:

- **Restaurer** - modifie une association de fichiers actuelle vers le niveau par défaut.Disponible pour les paramètres d' **associations de fichiers** uniquement !
- **Aller à** - ouvre une fenêtre où l'objet a été placé (la **Base de Registres** par exemple).

Note
Suivant l'objet sélectionné, le bouton **Aller vers** peut ne pas apparaître.

- **Actualiser** - re-ouvre la section **Informations Système**.

Optimization

The Optimization tab is useful when you wish to run an on-demand scan without being disturbed from your work.

For example, if you want to run a Deep System Scan this may take some time if you have many items on your hard disk or if your system configuration doesn't meet the recommended requirements.

To access the Optimization tab:

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Go to **General > Optimization**.

System load is constantly being monitored.When the system enters an idle state BitDefender can launch:

- **Analyse Approfondie**

- **Analyse Rapide**
- **Analyse Complète**
- **Analyse de Mes documents**

Note

Select **Update product before running this task** check box to make sure you have the latest virus definitions.

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:

- Protection en temps réel - 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.

  À propos de la protection en temps réel, on parle aussi d'analyse à l'accès – les fichiers sont analysés quand l'utilisateur veut les ouvrir.

  Important
  Pour prévenir l'infection de votre ordinateur par des virus, laissez la **protection en temps réel** activée.

- Analyse à la demande - permet de détecter et de supprimer les codes malveillants déjà présents dans le système.C'est l'analyse classique antivirus déclenchée par l'utilisateur – vous choisissez le lecteur, dossier ou fichier que BitDefender doit analyser et BitDefender le fait – A la demande.Les tâches d'analyse permettent de créer des programmes d'analyse personnalisés qui peuvent être planifiés pour être exécutés régulièrement.

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 « *Zone de quarantaine* » (p. 82).

Si votre ordinateur a été infecté par des malwares, veuillez vous référer à « *Suppression de malwares depuis votre système* » (p. 137).

Les utilisateurs avancés peuvent configurer des exceptions d'analyse s'ils ne souhaitent pas que certains fichiers soient analysés. Pour plus d'informations, reportez-vous à « *Configuration des exclusions d'analyse* » (p. 79).

15.1. 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.

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

- « *Réglage du Niveau de Protection en Temps Réel* » (p. 60)
- « *Création d'un niveau de protection personnalisé* » (p. 61)
- « *Modification des actions menées sur les fichiers détectés* » (p. 62)
- « *Restauration des paramètres par défaut* » (p. 64)

Pour vous protéger contre les applications malveillantes inconnues, BitDefender utilise une technologie heuristique avancée (Active Virus Control) et un Système de Détection d'Intrusion qui surveillent votre système en permanence. Pour en savoir plus, reportez-vous à ces sujets :

- « *Configuration d'Active Virus Control* » (p. 64)
- « *Configuration du système de détection d'intrusion* » (p. 66)

15.1.1. Réglage du 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 :

1. Lancer BitDefender.
2. Procédez comme suit, en fonction du mode d'affichage de l'interface utilisateur :

   Mode INTERMÉDIAIRE

   Allez à l'onglet **Sécurité**, puis cliquez sur **Configuration Antivirus** dans la zone Tâches rapides située dans la partie gauche de la fenêtre.

   Allez dans l'onglet **Résident**.

   Mode EXPERT

   Allez dans **Antivirus > Résident**.

Note

En Mode Standard et Intermédiaire, vous pouvez configurer un raccourci afin d'accéder à ces paramètres depuis votre tableau de bord.Pour plus d'informations, reportez-vous à « *Mes Outils* » (p. 32).

3. 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.

15.1.2. Création d'un niveau de protection personnalisé

Les utilisateurs avancés peuvent utiliser les paramètres d'analyse proposés par BitDefender. Le moteur d'analyse peut être configuré pour analyser uniquement des extensions de fichiers spécifiques, pour rechercher des menaces de codes malveillants spécifiques ou pour passer les archives. Cela peut permettre de réduire considérablement la durée d'une analyse et d'améliorer la réactivité de votre ordinateur lors de l'analyse.

Vous pouvez configurer les paramètres de protection en temps réel en détail en créant un niveau de protection personnalisé. Pour créer un niveau de protection personnalisé :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Antivirus > Résident**.
3. Cliquez sur **Personnaliser**.
4. Configurez les paramètres d'analyse selon vos besoins. Pour savoir ce qu'une option provoque, placez le curseur dessus et lisez la description affichée au bas de la fenêtre.
5. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Ces informations peuvent vous être utiles :

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

  Les applications (ou les fichiers du programme) sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers.Cette catégorie comprend les extensions de fichiers suivantes : `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

Si vous optez pour **Analyser les extensions définies par l'utilisateur**, il est recommandé d'inclure toutes les extensions d'application en plus des extensions de fichier que vous considérez comme dangereuses.

- **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.
- **Analyse dans les archives.** L'analyse à l'intérieur des archives est un processus lent et consommant beaucoup de ressources, qui n'est donc pas recommandé pour une protection en temps réel. Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système.Les malwares peuvent affecter votre système uniquement si le fichier infecté est extrait de l'archive et exécuté dans que la protection en temps réel ne soit activée.
- **Options d'action.** Si vous envisagez de modifier les actions appliquées aux fichiers détectés, consultez les astuces dans « *Modification des actions menées sur les fichiers détectés* » (p. 62).
- **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
  - trafic Web
  - fichiers reçus via Yahoo! Messenger et Windows Live Messenger

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

  Bien que ce ne soit pas recommandé, vous pouvez désactiver l'analyse antivirus du trafic Internet, de la messagerie électronique et de la messagerie instantanée pour améliorer les performances du système.Si vous désactivez les options d'analyse correspondantes, les e-mails et les fichiers reçus ou téléchargés sur Internet ne seront pas analysés, ce qui permettra aux fichiers infectés d'être enregistrés sur votre ordinateur. Ce n'est pas une menace majeure car la protection en temps réel bloquera le malware lorsque vous tenterez d'accéder (ouvrir, déplacer, copier ou exécuter) aux fichiers infectés.

15.1.3. Modification des actions menées sur les fichiers détectés

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

- **Fichiers infectés .** Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants BitDefender.BitDefender peut généralement supprimer le code

malveillant d'un fichier infecté et reconstruire le fichier d'origine. Cette opération est appelée désinfection.

Note

Les signatures de malwares sont des fragments de codes extraits à partir de malwares réels. Elles sont utilisées par les programmes antivirus pour rechercher certaines caractéristiques et détecter les malwares.

La base de données de signatures de malwares BitDefender rassemble des signatures de malwares mises à jour toutes les heures par les chercheurs de malwares BitDefender.

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

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

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

Important

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

- Si un fichier suspect est détecté, l'accès à ce fichier est refusé pour éviter une infection potentielle.

Vous ne devez pas modifier les actions par défaut menées sur les fichiers détectés à moins d'avoir une raison valable.

Pour modifier les actions appliquées par défaut aux fichiers infectés ou suspects détectés :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Antivirus > Résident**.
3. Cliquez sur **Personnaliser**.
4. Configurez les actions à appliquer à chaque catégorie de fichiers détectés, selon vos besoins. La deuxième action est menée si la première échoue (par exemple, la désinfection n'est pas possible et le fichier infecté est placé en quarantaine).

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 :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Antivirus > Résident**.
3. Cliquez sur **Niveau par défaut**.

15.1.5. Configuration d'Active Virus Control

BitDefender Active Virus Control détecte les applications potentiellement dangereuses en fonction de leur comportement.

Active Virus Control surveille en permanence les applications en cours d'exécution sur l'ordinateur, à la recherche d'actions ressemblant à celles des malwares. Chacune de ces actions est notée et une note globale est calculée pour chaque processus. Lorsque le score global d'un processus atteint un certain seuil, le processus est considéré comme malveillant. En fonction des paramètres du programme, le processus est bloqué automatiquement ou vous pouvez être invité(e) à spécifier l'action à appliquer.

Active Virus Control peut être configuré pour vous prévenir et vous demander quelle action entreprendre lorsqu'une application essaie de réaliser une action potentiellement malveillante.

Si vous connaissez l'application et la savez de confiance, cliquez sur **Autoriser**.

Si vous voulez fermer immédiatement cette application, cliquez sur **OK**.

Cochez la case **Retenir cette action pour cette application** avant de faire votre choix et BitDefender réalisera la même action pour l'application détectée par la suite.La règle ainsi créée apparaîtra dans la fenêtre de configuration d'Active Virus Control.

Pour configurer Active Virus Control :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Antivirus > Résident**.
3. Cliquez sur **Paramètres Avancés**.
4. Allez à l'onglet **BD AVC**.
5. Cochez la case correspondante pour activer Active Virus Control.

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.

Réglage du Niveau de Protection

Pour configurer le niveau de protection d'Active Virus Control :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Antivirus > Résident**.
3. Cliquez sur **Paramètres Avancés**.
4. Allez à l'onglet **BD AVC**.
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.

Configuration de la réponse aux comportements malveillants

Si une application présente un comportement malveillant, vous serez invité à l'autoriser ou à la bloquer.

Pour configurer la réponse à un comportement malveillant :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Antivirus > Résident**.
3. Cliquez sur **Paramètres Avancés**.
4. Allez à l'onglet **BD AVC**.
5. Si vous souhaitez que l'on vous demande de choisir une action lorsqu'Active Virus Control détecte une application potentiellement malveillante, cochez la case **M'alerter avant d'appliquer une action**.Pour bloquer automatiquement une application présentant un comportement malveillant (sans afficher de fenêtre d'alerte), décochez cette case.

Gestion de la liste des Applications de confiance / non fiables

Vous pouvez ajouter à la Liste des applications de confiance des applications que vous connaissez et en lesquelles vous avez confiance. Ces applications ne seront plus contrôlées par BitDefender Active Virus Control et seront automatiquement autorisées.

Pour gérer les applications qui ne sont pas surveillées par Active Virus Control :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Antivirus > Résident**.
3. Cliquez sur **Paramètres Avancés**.
4. Allez à l'onglet **BD AVC**.
5. Cliquez sur l'onglet **Exclusions**.

Les applications pour lesquelles des règles ont été créées apparaissent dans le tableau **Exclusions**.Le chemin vers l'application et l'action que vous avez définie pour celle-ci (Autorisée ou Bloquée) sont indiqués pour chaque règle.

Pour modifier l'action pour une application, cliquez sur l'action actuelle et sélectionnez l'autre action à partir du menu.

Pour gérer la liste, utilisez les boutons placés au-dessus du tableau :

Ajouter - ajoute une nouvelle application à la liste.
Supprimer - supprime une application de la liste.
Éditer - permet de modifier une règle d'application.

15.1.6. Configuration du système de détection d'intrusion

Le Système de Détection d'Intrusion de BitDefender surveille les activités du réseau et du système à la recherche d'activités malveillantes ou de violations de politique.

Pour configurer le système de détection d'intrusion :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Antivirus > Résident**.
3. Cliquez sur **Paramètres Avancés**.
4. Allez à l'onglet **IDS**.
5. Cochez la case correspondante pour activer le système de détection d'intrusion.
6. Déplacez le curseur sur l'échelle pour choisir le degré d'analyse approprié.Reportez-vous à la description à droite de l'échelle pour choisir le niveau de protection le plus adapté à vos besoins de sécurité.

15.2. Analyse à la demande

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

Il y a cependant un risque qu'un virus soit déjà logé dans votre système, avant même l'installation de BitDefender. C'est pourquoi il est prudent d'analyser votre

ordinateur après l'installation de BitDefender. Et c'est encore plus prudent d'analyser régulièrement votre ordinateur contre les virus.

L'analyse sur demande est basée sur les tâches d'analyse. Les tâches d'analyse permettent de spécifier les options d'analyse et les objets à analyser.Vous pouvez analyser votre ordinateur à tout moment en exécutant les tâches par défaut ou vos propres tâches d'analyse (tâches définies par l'utilisateur). Vous pouvez aussi les planifier pour être exécutées régulièrement ou lorsque votre système est inactif afin de ne pas interférer dans votre travail.Pour des instructions rapides, référez-vous à ces sujets :

- « *Comment analyser des fichiers et des dossiers ?* » (p. 119)
- « *Comment créer une tâche d'analyse personnalisée ?* » (p. 122)
- « *Comment planifier l'analyse de l'ordinateur ?* » (p. 124)

15.2.1. Analyse des fichiers et des dossiers

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

Si vous souhaitez analyser des emplacements spécifiques sur votre ordinateur, vous pouvez configurer et exécuter une tâche d'analyse personnalisée.Pour plus d'informations, reportez-vous à « *Comment créer une tâche d'analyse personnalisée ?* » (p. 122).

Vous pouvez analyser tout ou partie de votre ordinateur en exécutant les tâches d'analyse par défaut ou vos propres tâches d'analyse.Pour exécuter une tâche d'analyse, ouvrez BitDefender et, en fonction du mode d'affichage de l'interface, procédez comme suit :

Mode STANDARD
: Cliquez sur le bouton **Sécurité** et choisissez l'une des tâches d'analyse disponibles.

Mode INTERMÉDIAIRE
: Allez à l'onglet **Sécurité**.Cliquez sur **Analyse Complète** dans la zone Tâches rapides, puis choisissez l'une des tâches d'analyse disponibles.

Mode EXPERT
: Allez à **Antivirus > Analyse**.Pour exécuter une tâche d'analyse système ou définie par un utilisateur, cliquez sur le bouton correspondant **Exécuter Tâche**.

Voici les tâches par défaut que vous pouvez utiliser pour analyser votre ordinateur :

Analyse Complète
Analyse l'ensemble du système, mis à part les archives.Dans la configuration par défaut, l'analyse recherche tous les types de malwares à l'exception des rootkits.

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.

Analyse Approfondie
Analyse l'ensemble du système.La configuration par défaut permet d'analyser tous les types de codes malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.

Avant de lancer un processus d'analyse, vous devez vous assurer que BitDefender est à jour de ses signatures de codes malveillants. 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.

Afin de permettre à BitDefender de réaliser une analyse complète, il est nécessaire de fermer tous les programmes ouverts, tout spécialement les clients de messagerie (ex : Outlook, Outlook Express ou Eudora).

Astuces d'analyse

Voici quelques astuces supplémentaires qui pourraient vous être utiles :

- Selon la taille de votre disque dur, l'analyse complète de votre ordinateur (Analyse approfondie ou Analyse du système) peut prendre un certain temps (jusqu'à une heure ou même plus).Il est donc préférable de lancer ce type d'analyses à un moment où vous cessez d'avoir besoin de votre ordinateur (au cours de la nuit par exemple).

  Vous pouvez planifier l'analyse pour la faire débuter au moment opportun.Pensez à laisser votre ordinateur allumé.Avec Windows Vista, vérifiez que votre ordinateur ne sera pas en mode veille au moment planifié pour l'exécution de la tâche.

- Si vous téléchargez fréquemment des fichiers sur Internet vers un dossier particulier, créez une nouvelle tâche n'analyse et spécifiez que ce dossier est la cible de l'analyse.Planifiez la tâche pour qu'elle s'exécute quotidiennement ou plus souvent.

- Il existe un type de malware paramétré pour s'exécuter au démarrage du système en modifiant les paramètres de Windows.Pour protéger votre ordinateur contre les malwares de ce type, vous pouvez planifier la tâche **Analyse à l'ouverture de session** pour qu'elle s'exécute au démarrage du système.Veuillez noter que

l'analyse à l'ouverture de session peut avoir une influence sur les performances du système pendant un court moment après le démarrage.

15.2.2. Assistant d'analyse antivirus

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

Note

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

Étape 1 sur 3 - Analyse

BitDefender commence à analyser les objets sélectionnés.

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

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

Note

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

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

- **Je souhaite saisir le mot de passe de cet objet.** 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.
- **Je ne souhaite pas saisir le mot de passe de cet objet (ignorer cet objet).** Sélectionnez cette option pour ne pas analyser cette archive.
- **Je ne souhaite saisir le mot de passe d'aucun objet (ignorer tous les objets protégés par un mot de passe).** Sélectionnez cette option si vous ne voulez pas être dérangé au sujet des archives protégées par mot de passe.BitDefender ne pourra pas les analyser, mais un rapport sera conservé dans le journal des analyses.

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

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

Étape 2 sur 3 - Sélectionner des actions

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

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

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

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

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

Désinfecter
Supprime le code malveillant des fichiers infectés.

Supprimer
Supprime du disque les fichiers détectés.

Quarantaine
Déplace les fichiers detectés dans la zone de quarantaine.Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.Pour plus d'informations, reportez-vous à « *Zone de quarantaine* » (p. 82).

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

Veuillez noter que ces fichiers cachés ne sont pas ceux que vous avez choisi de ne pas afficher dans Windows. Ce sont des fichiers qui ont été cachés par des programmes particuliers, connus sous le nom de rootkits.Les rootkits ne

sont pas malveillants en eux-mêmes. Ils sont cependant couramment utilisés pour rendre les virus et les spywares indétectables par les programmes antivirus habituels.

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

Étape 3 sur 3 - Voir les résultats

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

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

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

BitDefender n'a pas pu corriger certains problèmes

Dans la plupart des cas, BitDefender désinfecte ou isole l'infection des fichiers infectés qu'il détecte.Il y a toutefois des problèmes qui ne peuvent pas être résolus automatiquement.Pour plus d'informations et d'instructions sur la méthode permettant de supprimer des malwares manuellement, reportez-vous à « *Suppression de malwares depuis votre système* » (p. 137).

BitDefender a détecté des fichiers suspects

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

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

15.2.3. Afficher les journaux d'analyse

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

1. Lancer BitDefender.

2. Cliquez sur le lien **Journaux**, situé dans le coin inférieur droit de la fenêtre.
3. Cliquez sur **Antivirus** dans le menu de gauche.
4. Dans la section **Tâches à la demande**, vous pouvez consulter les analyses qui ont été réalisées récemment.Double-cliquez sur les événements de la liste pour en consulter le détail.Pour ouvrir le journal d'analyse, cliquez sur **Journal**.Le journal d'analyse s'affichera dans votre navigateur Internet par défaut.

Pour supprimer une entrée de journal, faites un clic droit dessus et sélectionnez **Supprimer**.

15.2.4. Gestion des tâches d'analyse existantes

BitDefender comporte plusieurs tâches créées par défaut qui permettent de traiter les problèmes de sécurité les plus courants. Vous pouvez aussi créer vos propres tâches d'analyse personnalisées.Pour plus d'informations, reportez-vous à « *Comment créer une tâche d'analyse personnalisée ?* » (p. 122).

Pour gérer les tâches d'analyse existantes :

1. Lancer BitDefender.
2. Procédez comme suit, en fonction du mode d'affichage de l'interface utilisateur :

   Mode INTERMÉDIAIRE

   Allez à l'onglet **Sécurité**, puis cliquez sur **Configuration Antivirus** dans la zone Tâches rapides située dans la partie gauche de la fenêtre.

   Allez dans l'onglet **Analyse Antivirus**.

   Mode EXPERT

   Allez à **Antivirus > Analyse**.

Note

En Mode Standard et Intermédiaire, vous pouvez configurer un raccourci afin d'accéder à ces paramètres depuis votre tableau de bord.Pour plus d'informations, reportez-vous à « *Mes Outils* » (p. 32).

Il y a trois catégories de tâches d'analyse:

- **Tâches système** - contiennent une liste des tâches système par défaut. Les tâches suivantes sont disponibles:

  Analyse Complète

  Analyse l'ensemble du système, mis à part les archives.Dans la configuration par défaut, l'analyse recherche tous les types de malwares à l'exception des rootkits.

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.

Analyse automatique à l'ouverture de session

Analyse les éléments qui sont exécutés quand un utilisateur se connecte à Windows.Par défaut, l'analyse à l'ouverture de session est désactivée.

Si vous voulez utiliser cette tâche, faites un clic-droit dessus, sélectionnez **Planifier** et définissez la tâche à exécuter **au démarrage du système**.Spécifiez combien de temps après le démarrage la tâche doit s'exécuter (en minutes).

Analyse Approfondie

Analyse l'ensemble du système.La configuration par défaut permet d'analyser tous les types de codes malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.

Note

Sachant que les tâches d'**Analyse approfondie du système** et d'**Analyse complète du système** analysent l'intégralité du système, l'analyse peut prendre un certain temps. C'est pourquoi nous vous recommandons d'exécuter ces tâches en priorité faible ou, encore mieux, lorsque votre système est inactif.

- **Tâches prédéfinies** - contiennent les tâches prédéfinies par l'utilisateur.

  Une tâche `Mes documents` vous est proposée.Utilisez-la pour analyser les dossiers importants de l'utilisateur actuel: `Mes documents`, `Bureau` et `Démarrage`. Cela vous permet d'assurer la sécurité de vos documents, un espace de travail sécurisé et d'exécuter des applications saines au démarrage.

- **Tâches diverses** - contiennent une liste de tâches diverses. Ces tâches font réference à des modes d'analyse différents qui ne peuvent pas être lancés depuis cette fenêtre. Vous pouvez uniquement modifier leurs paramètres et voir le rapport d'analyse.Les tâches suivantes sont disponibles :

  Analyse des périphériques

  BitDefender peut détecter automatiquement la connexion d'un nouveau périphérique de stockage à l'ordinateur et l'analyser. Utilisez cette tâche pour configurer les options de détection et d'analyse automatiques des dispositifs de stockage (CD/DVD, supports de stockage USB, lecteurs mappés du réseau).

Analyse Contextuelle

Cette tâche est utilisée lors de l'analyse via le menu contextuel Windows ou à l'aide de la barre d'activité d'analyse.Vous pouvez adapter les options d'analyse à vos besoins.

Vous pouvez gérer les tâches d'analyse à l'aide des boutons ou du menu de raccourcis.

Pour exécuter une tâche d'analyse système ou définie par un utilisateur, cliquez sur le bouton correspondant **Exécuter Tâche**.L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse.

Pour définir une tâche d'analyse afin qu'elle s'exécute automatiquement, plus tard ou de façon régulière, cliquez sur le bouton **Planifier**, puis configurez la tâche planifiée en fonction de vos besoins.

Si vous n'avez plus besoin d'une tâche d'analyse que vous avez créée (une tâche définie par l'utilisateur), vous pouvez la supprimer en cliquant sur le bouton **Supprimer**, situé à droite de la tâche.Vous ne pouvez pas supprimer les tâches système ou diverses.

Chaque tâche d'analyse dispose d'une fenêtre Propriétés où vous pouvez configurer ses paramètres et afficher des journaux d'analyse.Pour ouvrir cette fenêtre cliquez sur le bouton **Propriétés** à gauche de la tâche (ou faites un clic droit sur la tâche puis cliquez sur **Propriétés**).

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

- « *Configuration des paramètres d'analyse* » (p. 75)
- « *Définition de la cible à analyser* » (p. 77)
- « *Planification des tâches d'analyse* » (p. 78)

Utilisation du menu de raccourcis

Un menu de raccourcis est également disponible pour chaque tâche. Utilisez le "clic-droit" sur la tâche seléctionnée pour y accéder.

Pour les tâches système et définies par l'utilisateur, les commandes suivantes sont disponibles dans le menu de raccourcis :

- **Analyser** - démarre immédiatement la tâche d'analyse choisie.
- **Chemins** - ouvre la fenêtre **Propriétés** et l'onglet Chemins permettant de modifier la cible à analyser de la tâche sélectionnée.Dans le cas de tâches système, cette option est remplacée par **Montrer les chemins de l'analyse**, car vous ne pouvez voir que leur cible d'analyse.
- **Planifier** - ouvre la fenêtre **Propriétés** et l'onglet Planificateur permettant de planifier la tâche sélectionnée.

- **Afficher les journaux** - ouvre la fenêtre **Propriétés** , et l'onglet Journaux, où vous pouvez voir les rapports générés après l'exécution de la tâche sélectionnée.
- **Cloner la tâche** - reproduit la tâche sélectionnée.Très utile lors de la création de nouvelles tâches car cette fonction vous permet aussi d'en modifier les propriétés si besoin.
- **Effacer** - efface la tâche sélectionnée.

Note

Disponible pour les tâches créées par l'utilisateur uniquement. Vous ne pouvez pas supprimer une tâche par défaut.

- **Propriétés** - ouvre la fenêtre **Propriétés** et l'onglet Résumé permettant de modifier les paramètres de la tâche sélectionnée.

Seules les options des onglets **Propriétés** et **Afficher les journaux** sont disponibles dans la catégorie **Tâches diverses**.

Configuration des paramètres d'analyse

Pour configurer les options d'analyse d'une tâche d'analyse spécifique, faites un clic droit dessus et sélectionnez **Propriétés**.

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

Vous pouvez aussi configurer ces options générales :

- **Exécuter la tâche d'analyse avec une priorité basse.** Décroît la priorité du processus d'analyse. Vous allez permettre aux autres logiciels d'être exécutés à une vitesse supérieure et d'augmenter le temps nécessaire pour le final du processus d'analyse.
- **Réduire l'assistant d'analyse dans la zone de notification.** Réduit la fenêtre d'analyse dans la barre d'état système. Double-cliquez sur l'icône de BitDefender pour l'ouvrir.
- Spécifiez l'action à mener si aucune menace n'a été trouvée.

Les utilisateurs avancés peuvent utiliser les paramètres d'analyse proposés par BitDefender. Le moteur d'analyse peut être configuré pour analyser uniquement des extensions de fichiers spécifiques, pour rechercher des menaces de codes malveillants spécifiques ou pour passer les archives. Cela peut permettre de réduire considérablement la durée d'une analyse et d'améliorer la réactivité de votre ordinateur lors de l'analyse.

Pour configurer les paramètres d'analyse en détail :

1. Cliquez sur **Personnaliser**.
2. Configurez les paramètres d'analyse selon vos besoins. Pour savoir ce qu'une option provoque, placez le curseur dessus et lisez la description affichée au bas de la fenêtre.
3. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Ces informations peuvent vous être utiles :

- Si vous n'êtes pas familiarisé avec certains des termes, consultez le glossaire.Vous pouvez également rechercher des informations sur Internet.
- **Niveau d'analyse .** Indiquez le type de malwares que vous souhaitez que BitDefender analyse en sélectionnant les options correspondantes.
- **Analyser les fichiers.** Vous pouvez paramétrer BitDefender afin qu'il analyse tous types de fichiers, uniquement les applications (fichiers programmes) ou bien des types de fichiers spécifiques que vous estimez dangereux.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 du programme) sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers.Cette catégorie comprend les extensions de fichiers suivantes : `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  Si vous optez pour **Analyser les extensions définies par l'utilisateur**, il est recommandé d'inclure toutes les extensions d'application en plus des extensions de fichier que vous considérez comme dangereuses.
- **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.
- **Analyse dans les archives.** Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système.Les malwares peuvent affecter votre système uniquement si le fichier infecté est extrait de l'archive et exécuté dans que la protection en temps réel ne soit activée. Il est toutefois recommandé d'utiliser cette option afin de détecter et de supprimer toute menace potentielle, même si celle-ci n'est pas imminente.

Note

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

- **Options d'action.** Spécifiez les actions à appliquer pour chaque catégorie de fichiers détectés en utilisant les options de cette catégorie.Il existe trois catégories de fichiers détectés :

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

    Note

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

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

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

  Vous ne devez pas modifier les actions par défaut menées sur les fichiers détectés à moins d'avoir une raison valable.

  Pour définir une nouvelle action, cliquez sur **Première action** et sélectionnez l'option souhaitée dans le menu.Indiquez une **Seconde action** qui sera appliquée si la première échoue.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

Définition de la cible à analyser

Vous ne pouvez pas modifier la cible des tâches d'analyse à partir de la catégorie **Tâches Système**.Vous pouvez seulement visualiser leur cible d'analyse.Pour voir la cible d'analyse d'une tâche d'analyse système spécifique, faites un clic-droit sur la tâche et sélectionnez **Montrer les chemins de l'analyse**.

Pour définir la cible d'une tâche d'analyse d'un utilisateur spécifique, faites un clic droit sur la tâche et sélectionnez **Chemins**. Si vous vous trouvez déjà dans la fenêtre Propriétés d'une tâche, vous pouvez aussi sélectionner l'onglet **Chemins**.

Vous pouvez afficher la liste des lecteurs locaux, réseau ou amovibles, ainsi que les fichiers ou dossiers ajoutés précédemment, le cas échéant. Tous les éléments cochés seront analysés lors de l'exécution de la tâche.

Voici les différents boutons proposés:

- **Ajouter** - ouvre une fenêtre de navigation vous permettant de sélectionner le(s) fichier(s)/dossier(s) que vous souhaitez analyser.

Note
Vous pouvez rajouter des fichiers et des dossiers à la liste d'analyse en les glissant-déposant.

- **Supprimer** - supprime les fichiers/dossiers précédemment sélectionnés de la liste des objets à analyser.

En plus de ces boutons, certaines options permettent une sélection rapide des cibles d'analyse.

- **Disques locaux** - pour analyser les disques locaux.
- **Disques réseaux** - pour analyser tous les lecteurs réseaux.
- **Disques amovibles** - pour analyser les disques amovibles (CD-ROM, lecteur de disquettes).
- **Toutes les entrées** - pour analyser l'ensemble des lecteurs, peu importe qu'ils soient locaux, réseaux ou amovibles.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

Planification des tâches d'analyse

Etant donné que l'analyse prendra du temps, et qu'elle fonctionnera mieux si vous avez fermé les autres programmes, il est préférable pour vous de programmer une analyse à une heure où vous n'utilisez pas votre ordinateur. L'utilisateur doit pour cela créer une tâche à l'avance.

Pour voir la planification d'une tâche spécifique ou la modifier, faites un clic droit sur la tâche et sélectionnez **Planifier**. Si vous êtes déjà dans la fenêtre Propriétés d'une tâche, sélectionnez l'onglet **Planificateur**.

La tâche planifiée s'affiche, le cas échéant.

Quand vous programmez une tâche, vous devez choisir une des options suivantes :

- **Non** - lance la tâche uniquement à la demande de l'utilisateur.
- **Une fois** - lance l'analyse une fois seulement, à un certain moment. Spécifiez la date et l'heure de démarrage dans le champ **Démarrer Date/Heure**.

- **Périodiquement** - lance une analyse périodiquement, à des intervalles réguliers (minutes, heures, jours, semaines, mois) à compter d'une date et d'une heure spécifiées.
- **Au démarrage système** - démarre l'analyse au moment défini après que l'utilisateur se soit connecté à Windows.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

15.3. Configuration des exclusions d'analyse

Il peut arriver de devoir exclure certains fichiers de l'analyse. Par exemple, il peut être utile d'exclure un fichier test EICAR d'une analyse à l'accès ou des fichiers `.avi` d'une analyse sur demande.

BitDefender vous permet d'exclure des objets d'une analyse à l'accès ou d'une analyse sur demande ou des deux. Cette fonction permet de réduire la durée d'une analyse et d'éviter d'interférer dans votre travail.

Deux types d'objet peuvent être exclus d'une analyse:

- **Chemins** - un fichier ou un dossier (avec tous les objets qu'il contient) indiqué par un chemin spécifique ;
- **Extensions** - tous les fichiers qui ont cette extension seront exclus de l'analyse, quel que soit leur emplacement sur le disque dur.

Les objets exclus d'une analyse à l'accès ne sont pas analysés, que ce soit vous-même ou une application qui y accédiez.

Note

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

15.3.1. Exclure des Fichiers ou des Dossiers de l'Analyse

Pour exclure des chemins de l'analyse :

1. Lancer BitDefender.
2. Procédez comme suit, en fonction du mode d'affichage de l'interface utilisateur :

   Mode INTERMÉDIAIRE

   Allez à l'onglet **Sécurité**, puis cliquez sur **Configuration Antivirus** dans la zone Tâches rapides située dans la partie gauche de la fenêtre.

   Allez à l'onglet **Exclusions**.

Mode EXPERT

Allez dans **Antivirus > Exclusions**.

Note

En Mode Standard et Intermédiaire, vous pouvez configurer un raccourci afin d'accéder à ces paramètres depuis votre tableau de bord.Pour plus d'informations, reportez-vous à « *Mes Outils* » (p. 32).

3. Cochez la case correspondante pour activer les exclusions d'analyse.
4. Lancez l'assistant de configuration de la manière suivante :
   - Faites un clic droit sur le tableau Fichiers et Dossiers et sélectionnez **Ajouter un nouveau chemin d'accès**.
   - Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
5. Suivez l'assistant de configuration.Vous pouvez naviguer dans l'assistant à l'aide des boutons **Suivant** et **Retour**. Pour quitter l'assistant, cliquez sur **Annuler**.
   a. Sélectionnez l'option d'exclusion d'un chemin de l'analyse.Cette étape apparaît uniquement lorsque vous lancez l'assistant en cliquant sur le bouton **Ajouter**.
   b. Pour spécifier les chemins à exclure de l'analyse, utilisez l'une des méthodes suivantes :
      - Cliquez sur **Parcourir**, sélectionnez le fichier ou le dossier à exclure de l'analyse, puis cliquez sur **Ajouter**.
      - Saisissez le chemin à exclure de l'analyse dans la zone de texte, puis cliquez sur **Ajouter**.

      Les chemins apparaissent dans le tableau au fur et à mesure que vous les ajoutez. Vous pouvez en ajouter autant que vous le souhaitez.
   c. Par défaut, les chemins sélectionnés sont exclus à la fois de l'analyse à l'accès et de l'analyse sur demande. Pour modifier quand appliquer l'exception, cliquez sur la colonne de droite et sélectionnez l'option souhaitée dans la liste.
   d. Il vous est fortement conseillé d'analyser les fichiers dans les chemins spécifiés pour vous assurer qu'ils ne soient pas infectés.Cochez la case pour analyser ces fichiers avant de les exclure de l'analyse.

      Cliquez sur **Terminer** pour ajouter les exceptions d'analyse.
6. N'oubliez pas de cliquer sur **Appliquer** pour enregistrer les modifications.

15.3.2. Exclure des Extensions de Fichiers de l'Analyse

Pour exclure des extensions de fichier de l'analyse :

1. Lancer BitDefender.

2. Procédez comme suit, en fonction du mode d'affichage de l'interface utilisateur :

   Mode INTERMÉDIAIRE

   Allez à l'onglet **Sécurité**, puis cliquez sur **Configuration Antivirus** dans la zone Tâches rapides située dans la partie gauche de la fenêtre.

   Allez à l'onglet **Exclusions**.

   Mode EXPERT

   Allez dans **Antivirus > Exclusions**.

   Note

   En Mode Standard et Intermédiaire, vous pouvez configurer un raccourci afin d'accéder à ces paramètres depuis votre tableau de bord.Pour plus d'informations, reportez-vous à « *Mes Outils* » (p. 32).

3. Cochez la case correspondante pour activer les exclusions d'analyse.
4. Lancez l'assistant de configuration de la manière suivante :
   - Faites un clic droit dans le tableau des extensions, puis sélectionnez **Ajouter de nouvelles extensions**.
   - Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
5. Suivez l'assistant de configuration.Vous pouvez naviguer dans l'assistant à l'aide des boutons **Suivant** et **Retour**. Pour quitter l'assistant, cliquez sur **Annuler**.
   a. Sélectionnez l'option d'exclusion d'extensions de l'analyse.Cette étape apparaît uniquement lorsque vous lancez l'assistant en cliquant sur le bouton **Ajouter**.
   b. Pour spécifier les extensions à exclure de l'analyse, utilisez l'une des méthodes suivantes :
      - Sélectionnez dans le menu l'extension que vous souhaitez exclure de l'analyse, puis cliquez sur **Ajouter**.

        Note

        Le menu contient la liste de toutes les extensions enregistrées dans votre système. Lorsque vous sélectionnez une extension, sa description s'affiche si elle est disponible.

      - Saisissez l'extension à exclure de l'analyse dans la zone de texte, puis cliquez sur **Ajouter**.

      Les extensions apparaissent dans le tableau au fur et à mesure que vous les ajoutez. Vous pouvez en ajouter autant que vous le souhaitez.
   c. Par défaut, les extensions sélectionnées sont exclues à la fois de l'analyse à l'accès et de l'analyse sur demande. Pour modifier quand appliquer l'exception, cliquez sur la colonne de droite et sélectionnez l'option souhaitée dans la liste.

d. Il vous est fortement conseillé d'analyser les fichiers avec les extensions spécifiées pour vous assurer qu'ils ne sont pas infectés.

Cliquez sur **Terminer** pour ajouter les exceptions d'analyse.

6. N'oubliez pas de cliquer sur **Appliquer** pour enregistrer les modifications.

15.3.3. Gestion des Exclusions d'Analyse

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

Pour gérer des exclusions d'analyse :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Antivirus > Exclusions**.

Pour supprimer une entrée du tableau, sélectionnez-la et cliquez sur le bouton **Supprimer**.

Pour modifier une entrée du tableau, 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 **OK**.

Note

Vous pouvez aussi faire un clic droit sur un objet et utiliser les options du menu de raccourcis pour le modifier ou le supprimer.

Pour désactiver des exceptions d'analyse, décochez la case correspondante.

15.4. Zone de quarantaine

BitDefender permet d'isoler les fichiers infectés ou suspects dans une zone sécurisée, nommée quarantaine. En isolant ces fichiers dans la quarantaine, le risque d'être infecté disparaît et, en même temps, vous avez la possibilité d'envoyer ces fichiers pour une analyse par le VirusLab de BitDefender.

Note

Quand un virus est en quarantaine, il ne peut faire aucun dégât car il ne peut ni être exécuté ni lu.

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 afficher et gérer les fichiers en quarantaine et pour configurer les paramètres de la quarantaine :

1. Lancer BitDefender.
2. Procédez comme suit, en fonction du mode d'affichage de l'interface utilisateur :

   Mode INTERMÉDIAIRE

   Allez à l'onglet **Sécurité**, puis cliquez sur **Configuration Antivirus** dans la zone Tâches rapides située dans la partie gauche de la fenêtre.

   Allez dans l'onglet **Quarantaine**.

   Mode EXPERT

   Allez à **Antivirus > Quarantaine**.

Note

En Mode Standard et Intermédiaire, vous pouvez configurer un raccourci afin d'accéder à ces paramètres depuis votre tableau de bord.Pour plus d'informations, reportez-vous à « *Mes Outils* » (p. 32).

Gérer les fichiers en quarantaine

Vous pouvez envoyer un fichier depuis la quarantaine aux BitDefender Labs en cliquant sur **Envoyer**.Par défaut, BitDefender soumettra automatiquement toutes les heures les fichiers mis en quarantaine.

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**.

Configuration des paramètres de la quarantaine

Pour configurer les paramètres de la quarantaine, cliquez sur **Paramètres**.En utilisant les paramètres de la quarantaine, vous pouvez configurer BitDefender pour exécuter automatiquement les actions suivantes :

Supprimer les anciens fichiers. Pour supprimer automatiquement les anciens fichiers en quarantaine, cochez l'option correspondante.Vous devez spécifier après combien de jours les fichiers en quarantaine doivent être supprimés et la fréquence à laquelle BitDefender doit rechercher les anciens fichiers.

Envoyer automatiquement les fichiers. Pour envoyer automatiquement les fichiers en quarantaine, cochez l'option correspondante.Vous devez spécifier la fréquence à laquelle soumettre les fichiers.

Analyser les fichiers en quarantaine après une mise à jour. Pour analyser automatiquement les fichiers en quarantaine après chaque mise à jour effectuée, cochez l'option correspondante.Vous pouvez choisir de remettre automatiquement

vos fichiers sains dans leur emplacement d'origine en sélectionnant **Restaurer les fichiers sains**.

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

16. 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
- Yahoo! Messenger
- Windows Live (MSN) Messenger

16.1. Configuration de la Liste Blanche Antiphishing

Vous pouvez configurer et gérer une liste blanche de sites Web qui ne seront pas analysés par les moteurs antiphishing de BitDefender.La Liste Blanche 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.

Note

Vous pouvez ajouter de nouveaux sites Internet à la liste blanche très simplement à partir de la barre d'outils antiphishing de BitDefender intégrée à votre navigateur Internet.Pour plus d'informations, reportez-vous à « *Gestion de la Protection Antiphishing BitDefender dans Internet Explorer et Firefox* » (p. 86).

Pour configurer et gérer la liste blanche antiphising :

- Si vous utilisez un navigateur web pris en charge, cliquez sur la barre d'outils BitDefender et choisissez **Liste Blanche** dans le menu.
- Vous pouvez également procéder comme suit :
  1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
  2. Allez dans **Antivirus > Résident**.
  3. Cliquez sur **Liste blanche**.

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

Si vous voulez effacer un site Internet de la liste blanche, cliquez sur le bouton **Effacer**.

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

16.2. Gestion de la Protection Antiphishing BitDefender dans Internet Explorer et Firefox

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

- Internet Explorer
- Mozilla Firefox

Vous pouvez gérer facilement et efficacement la protection antiphishing et la liste blanche en utilisant la barre d'outils Antiphishing BitDefender intégrée dans l'un des navigateurs Internet ci-dessus.

La barre d'outils antiphishing, représentée par l'icône BitDefender, est située en haut de la fenêtre du navigateur.Cliquez dessus pour ouvrir le menu de la barre d'outils.

Note

Si vous ne voyez pas la barre d'outils, cliquez sur le menu **Affichage**, sélectionnez **Barres d'outils** et vérifiez **la barre d'outils BitDefender**.

Les commandes suivantes sont disponibles dans le menu de la barre d'outils :

- **Activer / Désactiver** - active / désactive la protection antiphishing BitDefender dans le navigateur Web actuel.
- **Paramètres** - ouvre une fenêtre où vous pouvez définir les paramètres de la barre d'outils antiphishing.Voici les options proposées :
  - **Protection Web Antipishing en Temps Réel** - détecte et vous prévient en temps réel si un site Web est un site de phishing (conçu pour voler des informations personnelles).Cette option contrôle la protection antiphishing BitDefender uniquement dans le navigateur Web actuel.
  - **Demander avant d'ajouter à une liste blanche** - demande votre autorisation avant d'ajouter un site Web à la liste blanche.
- **Ajouter à la liste blanche** - ajoute le site Web actuel à la liste blanche.

Important

Si vous ajoutez un site Web à la liste blanche, BitDefender n'analysera plus le site pour détecter les tentatives de phishing. Nous vous recommandons d'ajouter uniquement à la liste blanche les sites auxquels vous faites pleinement confiance.

- **Liste Blanche** - ouvre la Liste Blanche.Pour plus d'informations, reportez-vous à « *Configuration de la Liste Blanche Antiphishing* » (p. 85).
- **Signaler comme Phishing** - informe les laboratoires BitDefender que vous considérez que le site Web est utilisé pour du phishing.En signalant des sites Web de phishing vous contribuez à protéger d'autres utilisateurs contre le vol d'identité.

- **Aide** - ouvre la documentation électronique.
- **A propos de** - Affichage d'une fenêtre contenant des informations relatives à BitDefender, ainsi que des éléments d'aide si vous rencontrez une situation anormale.

17. Search Advisor

Search Advisor améliore votre protection contre les menaces en ligne en vous signalant le phishing et les pages Web non fiables directement depuis votre page de résultats de recherche.

Search Advisor fonctionne avec tous les navigateurs web et vérifie les résultats de la recherche affichés par les moteurs de recherche les plus courants :

- Google
- Yahoo!
- Bing

Search Advisor indique si un résultat de recherche est ou non sûr en plaçant une petite icône d'état devant le lien.

Cercle vert coché : Vous pouvez accéder à ce lien en toute sécurité.

Cercle rouge avec un point d'exclamation : Cette page est Non-fiable ou de phishing.Il est recommandé de ne pas ouvrir le lien.Si vous utilisez Internet Explorer ou Firefox et que vous tentez d'ouvrir le lien, BitDefender bloquera automatiquement la page Web et affichera une page d'alerte.Si vous souhaitez ignorer l'alerte et accéder à la page Web, suivez les instructions dans la page d'alerte.

17.1. Désactivation de Search Advisor

Pour désactiver Search Advisor :

1. Ouvrez BitDefender, cliquez sur **Options** dans le coin supérieur droit de la fenêtre, puis choisissez **Préférences**.
2. Allez à **Paramètres de Sécurité**.
3. Utilisez le bouton pour désactiver Search Advisor.

18. Contrôle Vie Privée

BitDefender contrôle des dizaines de “points à risque” dans votre système où les spywares pourraient agir, et analyse également les modifications apportées à votre système et à vos logiciels. C’est efficace contre les chevaux de Troie et autres outils installés par des hackers, qui essaient de compromettre votre vie privée et d’envoyer vos informations personnelles, comme vos numéros de carte bancaire, de votre ordinateur vers le pirate.

Le Contrôle Vie Privée inclut ces composants :

- Le Contrôle d'identité - vous aide à vous assurer que vos informations personnelles ne sont pas envoyées sans votre accord. Il analyse les e-mails et messages instantanés envoyés depuis votre PC et toutes les données envoyées via des pages Web, ainsi que toutes les informations protégées par les règles que vous avez crées dans le Contrôle d'identité.
- Contrôle du Registre - demande votre autorisation dès lors qu'un programme tente de modifier une entrée de registre afin de s'exécuter au démarrage de Windows.
- Contrôle des cookies - demande votre autorisation dès lors qu'un nouveau site Web tente de créer un cookie sur votre ordinateur.
- Contrôle des Scripts - demande votre autorisation dès lors qu'un site Web tente d'exécuter un script ou un autre contenu actif.

Par défaut, seul le Contrôle d'Identité est activé. Vous devez configurer les règles adéquates du Contrôle d'identité pour éviter l'envoi proscrit de données confidentielles.Pour plus d'informations, reportez-vous à « *Configuration du Contrôle d'Identité* » (p. 92).

Les autres composants de Contrôle Vie Privée sont interactifs. Si vous les activez, on vous demandera, via des fenêtres d'alertes, d'autoriser ou de bloquer certaines actions lorsque vous naviguez sur de nouveaux sites Internet ou installez de nouveaux logiciels. C'est pourquoi ils sont généralement utilisés par des utilisateurs avancés.

18.1. Configuration du niveau de protection

Le niveau de protection vous aider à activer ou désactiver facilement les composants du Contrôle Vie Privée.

Pour configurer le niveau de protection :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez à **Contrôle Vie privée > Etat**.

3. Vérifiez que le Contrôle Vie Privée est activé.
4. Il y a deux options :
   - Déplacez le curseur sur l'échelle pour choisir le niveau de protection approprié.Cliquez sur **Niveau par défaut** pour placer le curseur sur le niveau par défaut.

     Reportez-vous à la description à droite de l'échelle pour choisir le niveau de protection le plus adapté à vos besoins de sécurité.
   - Vous pouvez personnaliser le niveau de protection en cliquant sur **Personnaliser**.Dans la fenêtre qui apparaîtra, sélectionnez les contrôles de protection que vous souhaitez activer et cliquez sur **OK**.

18.2. Contrôle d'identité

Le contrôle d'identité vous protège contre le vol de données sensibles lorsque vous êtes connecté à Internet.

Voici un exemple simple : vous avez créé une règle de contrôle d'identité qui protège votre numéro de carte de crédit.Si un logiciel espion parvient d'une manière quelconque à s'installer sur votre ordinateur, il ne peut pas envoyer votre numéro de carte de crédit par e-mail, messages instantanés ou pages Web. En outre, vos enfants ne peuvent pas l'utiliser pour acheter en ligne ou le révéler à des personnes rencontrées sur Internet.

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

- « *À propos du contrôle d'identité* » (p. 90).
- « *Configuration du Contrôle d'Identité* » (p. 92).
- « *Gestion des règles* » (p. 94).

18.2.1. À propos du contrôle d'identité

La protection des données confidentielles est un sujet important qui nous concerne tous. Le vol d'informations a suivi le développement de l'Internet et des communications et utilise de nouvelles méthodes pour pousser les gens à communiquer leurs données privées.

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

Le contrôle d'identité vous protège contre le vol de données sensibles lorsque vous êtes connecté à Internet.En se basant sur les règles définies par vous-même, le contrôle d'identité analyse le trafic Internet, de messagerie et de messagerie instantanée partant de votre ordinateur, pour y rechercher des chaînes de texte spécifiques que vous avez définies (par exemple, votre numéro de carte de crédit).

En cas de correspondance, la page Web, l'e-mail ou l'échange de messagerie instantanée concerné est bloqué.

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

Pourquoi utiliser le Contrôle d'identité?

- Le Contrôle d'identité est très efficace dans le blocage des spywares keylogger.Ce type d'applications malicieuses enregistre vos frappes clavier et les envoie par Internet à des pirates.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.

  Dans l'hypothèse où une application de ce type réussirait à contourner la protection antivirus, elle ne pourra pas envoyer les données subtilisées par email, par le web ou par messagerie instantanée si vous avez créé les règles de protection d'identité adaptées.

- Le Contrôle d'identité peut vous protéger contre les tentatives de phishing (attaques visant à voler les informations personnelles).La technique la plus répandue lors des tentatives de Phishing est l'envoi d'un email trompeur visant à vous amener à communiquer vos informations personnelles sur une fausse page Web.

  Par exemple, vous pouvez recevoir un email prétendument de votre banque vous demandant de mettre à jour rapidement vos informations bancaires.Cet email vous propose de cliquer sur un lien vous redirigeant vers une page Web sur laquelle vous devez communiquer vos informations personnelles.Bien qu'ils aient l'air légitimes, le lien de redirection et la page Web vers laquelle vous êtes redirigé sont faux.Si vous cliquez sur le lien contenu dans l'email et que vous entrez vos informations personnelles sur la fausse page web, vous divulguerez ces informations au pirate qui est l'auteur de cette tentative de phishing.

  Si les règles de protection d'identité sont actives, vous ne pourrez pas soumettre d'information personnelle sur une page Web (comme votre Numéro de carte de crédit par exemple) sauf si vous avez explicitement définit cette page comme étant autorisée à recevoir ce type d'information.

- À l'aide des règles de Contrôle d'Identité, vous pouvez éviter que vos enfants ne transmettent des informations personnelles (comme l'adresse de leur domicile ou leur numéro de téléphone) aux personnes qu'ils rencontrent sur Internet. De

plus, si vous créez des règles pour protéger votre carte bancaire, ils ne pourront pas l'utiliser pour faire des achats en ligne sans votre accord.

18.2.2. Configuration du Contrôle d'Identité

Pour utiliser le contrôle d'identité, suivez les étapes indiquées :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Contrôle Vie Privée > Identité**.
3. Vérifiez que le contrôle d'identité est activé.

Note
Si l'option ne peut être configurée, allez dans l'onglet **État** et activez le Contrôle Vie Privée.

4. Définissez les règles nécessaires à la protection de vos données sensibles.Pour plus d'informations, reportez-vous à « *Création de règles de protection d'identité* » (p. 92).
5. Définissez si nécessaire des exceptions aux règles que vous avez créées.Par exemple, si vous avez créé une règle pour protéger votre numéro de carte bancaire, ajoutez à la liste d'exceptions les sites web sur lesquels vous utilisez généralement votre carte bancaire. Pour plus d'informations, reportez-vous à « *Définition des Exceptions* » (p. 93).

Création de règles de protection d'identité

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

1. **Page d'accueil**
2. **Définition des types de règles et de données**

   Vous devez définir les paramètres suivants:

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

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

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

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

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

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

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

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

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

4. **Décrire la règle**

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

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

Désormais, toute tentative d'envoi des données spécifiées (via e-mail, messagerie instantanée ou sur une page web) échouera. Un message d'alerte s'affichera indiquant que BitDefender a empêché l'envoi de contenu lié à l'identité.

Définition des Exceptions

Il y a certains cas où vous avez besoin de définir des exceptions à des règles d'identité spécifiques.Si vous créez, par exemple, une règle de confidentialité pour

éviter que votre numéro de carte de crédit ne soit envoyé via HTTP (Web), chaque fois que le numéro de votre carte sera soumis sur un site Web depuis votre compte utilisateur, la page correspondante sera bloquée. Si vous voulez, par exemple, acheter des chaussures sur une boutique en ligne (que vous savez fiable), vous devrez spécifier une exception à la règle correspondante.

Pour ouvrir la fenêtre permettant de gérer les exceptions, cliquez sur **Exceptions**.

Pour ajouter une exception, procédez comme suit :

1. Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle entrée au tableau.
2. Double-cliquez sur **Indiquer l'élément à exclure** et précisez le site Web, l'adresse e-mail ou le contact de messagerie instantanée que vous souhaitez ajouter comme exception.
3. Double-cliquez sur **Type de trafic** et sélectionnez dans le menu l'option correspondant au type d'adresse précédemment indiqué.
   - Si vous avez indiqué une adresse Web, sélectionnez **HTTP**.
   - Si vous avez indiqué une adresse e-mail, sélectionnez **E-mail (SMTP)**.
   - Si vous avez indiqué un contact de messagerie instantanée, sélectionnez **Messagerie instantanée**.

Pour supprimer une exception de la liste, sélectionnez-la et cliquez sur le bouton **Supprimer**.

Cliquez **OK** pour sauvegarder les changements.

18.2.3. Gestion des règles

Pour gérer les règles de Contrôle d'Identité :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Contrôle Vie Privée > Identité**.

Vous pouvez voir les règles existantes dans le tableau.

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

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

18.3. Contrôle du Registre

Une partie très importante du système d'exploitation Windows est appelée la **Base de registres**. C'est l'endroit où Windows conserve ses paramétrages, programmes installés, informations sur l'utilisateur et autres.

La **Base de registres** est également utilisée pour définir quels programmes devraient être lancés automatiquement lorsque Windows démarre. Cela est souvent utilisé par les virus afin d'être automatiquement lancé lorsque l'utilisateur redémarre son ordinateur.

Le **Contrôle du Registre** garde un œil sur les registres Windows – ce qui est également utile pour détecter des chevaux de Troie. Il vous alertera dès qu'un programme essaiera de modifier une entrée dans la base de registres afin de s'exécuter au démarrage de Windows.Pour plus d'informations, reportez-vous à « *Alertes registre* » (p. 38).

Pour configurer le Contrôle du Registre :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Contrôle Vie Privée > Registre**.
3. Cochez la case correspondante pour activer le Contrôle du Registre.

Note
Si l'option ne peut être configurée, allez dans l'onglet **État** et activez le Contrôle Vie Privée.

Gestion des règles

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

18.4. Contrôle des cookies

Les Cookies sont très communs sur Internet. Ce sont des petits fichiers stockés sur le PC. Les sites web les créent afin de connaître certaines informations vous concernant.

Les Cookies sont généralement là pour vous rendre la vie plus facile. Par exemple ils peuvent aider un site web se rappeler votre nom et vos préférences, pour ne pas avoir à les introduire chaque fois.

Mais les cookies peuvent aussi être utilisés pour compromettre votre confidentialité, en surveillant vos préférences de navigation.

C'est à ce niveau que le contrôle des cookies peut vous être utile.Lorsqu'il est activé, le contrôle des cookies vous demande votre autorisation lorsqu'un nouveau site essaie de créer ou d'utiliser un cookie.Pour plus d'informations, reportez-vous à « *Alertes de cookies* » (p. 39).

Pour configurer le Contrôle des Cookies :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.

2. Allez à **Contrôle Vie privée > Cookie**.
3. Cochez la case correspondante pour activer le contrôle des cookies.

Note
Si l'option ne peut être configurée, allez dans l'onglet **État** et activez le Contrôle Vie Privée.

4. Vous pouvez configurer des règles pour les sites web que vous consultez régulièrement, mais ce n'est pas réellement nécessaire. Les règles sont créées automatiquement via la fenêtre d'alertes, en fonction de votre réponse.

Note
A cause du grand nombre de cookies utilisés sur Internet, **Cookie Control** peut être gênant au début. Il vous posera beaucoup de questions concernant les sites qui veulent placer des cookies sur votre ordinateur. Au fur et à mesure que vous rajoutez vos sites habituels à la liste des règles, la navigation deviendra aussi simple qu'avant.

Création de Règles Manuellement

Pour créer manuellement une règle, cliquez sur le bouton **Ajouter** et configurer les paramètres de la règle dans la fenêtre de configuration.Vous pouvez définir les paramètres:

- **Adresse domaine** - vous pouvez introduire le domaine sur lequel porte la règle.
- **Action** - sélectionnez l'action de la règle.

Action	Description
Autoriser	Les cookies de ce domaine seront autorisés.
Refuser	Les cookies de ce domaine ne seront pas autorisés.

- **Direction** - sélectionner la direction du trafic.

Type	Description
Sortant	La règle s'applique seulement aux envois d'informations vers les serveurs accédés.
Entrant	La règle s'applique seulement aux envois d'informations en provenance des serveurs accédés.
Tous les deux	La règle s'applique dans les deux directions.

Note
Vous pouvez accepter des cookies et interdire leur envoi en sélectionnant l'action **Interdire** et la direction **Sortant**.

Cliquez sur **Terminer**.

Gestion des règles

Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton **Supprimer**.Pour modifier les paramètres d'une règle, sélectionnez la règle et cliquez sur le bouton **Modifier**, ou double-cliquez dessus. Effectuez les modifications souhaitées dans la fenêtre de configuration.

18.5. Contrôle des Scripts

Les Scripts et d'autres codes comme les contrôles ActiveX et Applets Java, qui sont utilisés pour créer des pages web interactives, peuvent être programmés pour avoir des effets néfastes. Les éléments ActiveX, par exemple, peuvent obtenir un accès total à vos données et peuvent lire des données depuis votre ordinateur, supprimer des informations, capturer des mots de passe et intercepter des messages lorsque vous êtes en ligne. Vous devriez accepter les contenus actifs uniquement sur les sites que vous connaissez et auxquels vous faites parfaitement confiance.

Si vous activez le Contrôle des Scripts, il vous demandera l'autorisation lorsqu'un nouveau site essaiera d'exécuter un script ou un autre contenu actif. Pour plus d'informations, reportez-vous à « *Alertes de scripts* » (p. 39).

Pour configurer le Contrôle des Scripts :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez à **Contrôle Vie privée > Script**.
3. Cochez la case correspondante pour activer le Contrôle des Scripts.

   Note
   Si l'option ne peut être configurée, allez dans l'onglet **État** et activez le Contrôle Vie Privée.

4. Vous pouvez configurer des règles pour les sites web que vous consultez régulièrement, mais ce n'est pas réellement nécessaire. Les règles sont créées automatiquement via la fenêtre d'alertes, en fonction de votre réponse.

Création de Règles Manuellement

Pour créer manuellement une règle, cliquez sur le bouton **Ajouter** et configurer les paramètres de la règle dans la fenêtre de configuration.Vous pouvez définir les paramètres:

- **Adresse domaine** - vous pouvez introduire le domaine sur lequel porte la règle.
- **Action** - sélectionnez l'action de la règle.

Action	Description
Autoriser	Les scripts de ce domaine seront exécutés.
Refuser	Les scripts de ce domaine ne seront pas exécutés.

Cliquez sur **Terminer**.

Gestion des règles

Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton **Supprimer**.Pour modifier les paramètres d'une règle, sélectionnez la règle et cliquez sur le bouton **Modifier**, ou double-cliquez dessus. Effectuez les modifications souhaitées dans la fenêtre de configuration.

19. Vulnérabilité

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.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 vérifie à intervalle régulier les vulnérabilités de votre système et vous informe des problèmes rencontrés.

19.1. Rechercher des vulnérabilités

Vous pouvez rechercher des vulnérabilités et les corriger pas à pas à l'aide de l'assistant de l'**Analyse de Vulnérabilité**.Pour lancer l'assistant, ouvrez BitDefender et, en fonction du mode d'affichage de l'interface, procédez comme suit :

Mode INTERMÉDIAIRE
: Allez dans l'onglet **Sécurité** et cliquez sur **Analyse de Vulnérabilité** dans la zone Tâches Rapides de la partie gauche de la fenêtre.

Mode EXPERT
: Allez dans **Vulnérabilité > Etat** et cliquez sur **Vérifier**.

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**.

1. **Protection de votre PC**

   Sélectionnez les vulnérabilités à rechercher.

2. **Analyser les problèmes sélectionnés...**

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

3. **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.

4. **Mises à jour d'applications**

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

5. **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.

6. **Récapitulatif**

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

19.2. État

Pour voir l'état des vulnérabilités et activer/désactiver l'analyse automatique des vulnérabilités, suivez les étapes suivantes :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Vulnérabilité > État**.

Le tableau affiche les problèmes traités lors du dernier contrôle de vulnérabilité ainsi que leur état.Vous pouvez consulter l'action à entreprendre pour réparer chaque vulnérabilité, s'il y en a.Si l'action est **Aucune**, alors le problème en question ne représente pas une vulnérabilité.

Important

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

En fonction du problème, procédez comme suit pour corriger une vulnérabilité spécifique :

- Si les mises à jour Windows sont disponibles, cliquez sur **Installer** dans la colonne **Action** pour les installer.
- Si une application n'est pas à jour, cliquez sur **Plus d'informations** pour afficher des informations sur la version et 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 **Afficher &Corriger** 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 Fort, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).
- Si la fonction Exécution automatique des médias est activée sous Windows, cliquez sur **Corriger** pour la désactiver.

19.3. Configuration

Pour configurer les paramètres de la vérification automatique des vulnérabilités, suivez ces étapes :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Vulnérabilité > Paramètres**.
3. Cochez les cases correspondantes aux vulnérabilités système que vous voulez analyser régulièrement :
   - **Mises à jour critiques Windows**
   - **Mises à jour Windows régulières**
   - **Mises à jour d'applications**
   - **Mots de passe vulnérables**
   - **Exécution automatique des médias (clés ou disques USB, CD/DVD...)**

Note

Si vous décochez la case correspondant à une certaine vulnérabilité, BitDefender ne vous informera plus des problèmes la concernant.

20. Messagerie Inst.

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

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

- votre correspondant 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 correspondant utilisiez soit Yahoo Messenger, soit Windows Live (MSN) Messenger.

Important

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

Pour configurer le cryptage de messagerie instantanée :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez à **Cryptage > Cryptage de Messagerie Instantanée**.

Note

Vous pouvez aisément configurer le cryptage de messagerie instantanée pour chaque correspondant en utilisant la barre d'outils BitDefender dans la fenêtre de chat.

Par défaut, le cryptage de messagerie instantanée est activé pour Yahoo Messenger et Windows Live (MSN) Messenger.Vous pouvez désactiver ce cryptage de messagerie instantanée soit entièrement, soit uniquement pour une application de chat spécifique.

Deux tableaux sont affichés :

- **Exclusions de Cryptage** - Liste les contacts de messagerie et les messageries correspondantes pour lesquels le cryptage est désactivé.Pour effacer un contact de la liste, sélectionnez-le et cliquez sur le bouton **Effacer**.
- **Connexions actuelles** - Liste les connexions de messageries instantanées qui sont cryptées ou non. (Contacts et messageries associées)Une connexion peut ne pas être cryptée pour les raisons suivantes :

- Vous avez volontairement désactivé le cryptage pour un contact particulier.
- Votre contact n'a pas de version BitDefender installée supportant le cryptage des messageries instantanées.

20.1. Désactiver le cryptage pour des utilisateurs spécifiques

Pour désactiver le cryptage pour un utilisateur spécifique, suivez ces étapes :

1. Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre de configuration.
2. Tapez dans le champ de saisie l'identifiant utilisateur de votre contact.
3. Sélectionnez l'application de messagerie instantanée associée au contact.
4. Cliquez sur **OK**.

20.2. Barre d'outils BitDefender dans la Fenêtre de Chat

Vous pouvez configurer facilement le cryptage de messagerie instantanée en utilisant la barre d'outils BitDefender dans la fenêtre de chat.

La barre d'outils devrait être située à l'angle inférieur droit de la fenêtre de la conversation. Cherchez le logo BitDefender pour la trouver.

Note

La barre d'outils indique qu'une conversation est cryptée en affichant une petite clé à côté du logo BitDefender.

En cliquant sur la barre d'outils BitDefender vous obtiendrez les options suivantes :

- **Désactiver en permanence le cryptage pour le contact.**
- **Inviter le contact à utiliser le cryptage.** Pour crypter vos conversations, votre contact doit installer BitDefender et utiliser un programme de Messagerie Instantanée compatible.

21. Mode Jeu / Portable

Le module Réglages du produit vous permet de configurer les modes de fonctionnement spéciaux de BitDefender :

- Mode Jeu - modifie temporairement les paramètres du produit, de façon à minimiser la consommation de ressources lorsque vous jouez à un jeu vidéo.
- Mode Portable - évite l'exécution de tâches planifiées lorsque l'ordinateur portable est alimenté par sa batterie, afin de préserver l'autonomie de celle-ci.
- Le Mode Silencieux modifie temporairement les paramètres du produit afin de minimiser les interruptions lorsque vous regardez des films ou des présentations.

21.1. Mode Jeu

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

- Toutes les alertes et fenêtres pop-up BitDefender sont désactivées.
- Le niveau de la protection en temps réel de BitDefender est paramétré sur **Tolérant**.
- Les mises à jour sont désactivées par défaut.

Note

Pour modifier ce paramètre, rendez-vous dans Mise à jour>Paramètres et décochez la case **Ne pas mettre à jour si le Mode Jeu est actif**.

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.Vous pouvez passer manuellement en Mode Jeu en utilisant le raccourci clavier par défaut `Ctrl+Alt+Shift+G`.Nous vous recommandons vivement de quitter le Mode Jeu lorsque vous avez fini de jouer (vous pouvez pour ce faire utiliser le même raccourci clavier par défaut `Ctrl+Alt+Shift+G`).

Note

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

Pour configurer le Mode Jeu :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez à **Mode Portable/Jeu > Mode Jeu**.

Vous pouvez vérifier l'état du Mode Jeu dans la partie supérieure de la section.Vous pouvez cliquer sur **Mode Jeu activé** ou **Mode Jeu désactivé** pour modifier l'état actuel.

21.1.1. Configuration du Mode Jeu automatique

Le Mode Jeu automatique permet à BitDefender de passer automatiquement en Mode Jeu lorsque l'exécution d'un jeu est détectée.Voici les options d'analyse que vous pouvez configurer :

- **Utiliser la liste de jeux par défaut fournie par BitDefender** - permet de passer automatiquement en Mode Jeu lorsque vous lancez un jeu figurant dans la liste de jeux connus de BitDefender.Pour afficher cette liste, cliquez sur **Gérer les Jeux** puis sur **Liste des Jeux**.
- **Action plein écran** - vous pouvez choisir de passer automatiquement en Mode Jeu ou en Mode Silencieux lorsqu'une application s'exécute en mode plein écran.
- **Demander si l'application en plein écran doit être ajoutée à la liste de jeux** - pour que l'on vous propose d'ajouter une nouvelle application à la liste de jeux lorsque vous quittez le plein écran.Si vous ajoutez une nouvelle application à la liste de jeux, la prochaine fois que vous lancerez celle-ci, BitDefender passera automatiquement en Mode Jeu.

Note

Si vous ne souhaitez pas que BitDefender passe automatiquement en Mode Jeu, décochez la case **Mode Jeu automatique activé**.

21.1.2. Gestion de la liste de jeux

BitDefender passe automatiquement en Mode Jeu lorsque vous lancez une application figurant dans la liste de jeux.Pour consulter et gérer la liste de jeux, cliquez sur **Gérer les jeux**.Une nouvelle fenêtre s'affiche.

De nouvelles applications sont automatiquement ajoutées à la liste dans les situations suivantes :

- Vous lancez un jeu figurant dans la liste de jeux connus de BitDefender.Pour afficher cette liste, cliquez sur **Liste des Jeux**.
- Lors de la fermeture du mode plein écran, vous ajoutez l'application à la liste de jeux à partir de la fenêtre d'invite.

Si vous voulez désactiver le Mode Jeu automatique pour une application spécifique de la liste, décochez la case correspondante.Vous avez tout intérêt à désactiver le Mode Jeu automatique pour les applications standard qui utilisent le mode plein écran, telles que les navigateurs Web et les lecteurs vidéo.

Pour gérer la liste de jeux, vous pouvez utiliser les boutons disposés en haut du tableau :

- **Ajouter** - ajoute une nouvelle application à la liste de jeux.
- **Supprimer** - supprime une application de la liste des jeux.
- **Éditer** - permet de modifier une entrée existante dans la liste de jeux.

21.1.3. Ajout ou édition de jeux

Lorsque vous ajoutez ou modifiez une entrée de la liste de jeux, une nouvelle fenêtre apparaît.

Cliquez sur **Parcourir** pour sélectionner l'application, ou tapez le chemin d'accès complet à l'application dans le champ de saisie.

Si vous ne voulez pas passer automatiquement en Mode Jeu lorsque l'application sélectionnée s'exécute, sélectionnez **Désactiver**.

Cliquez sur **OK** pour ajouter l'entrée à la liste de jeux.

21.1.4. Configuration des paramètres du Mode Jeu

Utilisez ces options pour configurer le comportement avec des tâches planifiées :

- **Activer ce module pour modifier les planifications d'analyses antivirus** - permet d'éviter l'exécution d'analyses antivirus planifiées lorsque le Mode Jeu est activé.Vous pouvez choisir une des options suivantes :

Option	Description
Ignorer la tâche	Annule complètement l'exécution de la tâche planifiée.
Reporter la tâche	Exécute la tâche planifiée juste après la désactivation du Mode Jeu.

21.1.5. Changer le raccoruci clavier du Mode Jeu

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

1. Cliquez sur **Paramètres Avancés**.Une nouvelle fenêtre s'affiche.
2. Sous l'option **Utiliser le raccourci**, définissez le raccourci clavier désiré :
   - Choisissez la touche que vous souhaitez utiliser en cochant l'une des suivantes : touche Contrôle (`Ctrl`), Touche Shift(`Shift`) ou touche Alt (`Alt`).
   - Dans le champ éditable, entrez la lettre que vous souhaitez utiliser.

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

Note
En décochant la case **Utiliser le raccourci**, vous désactivez le raccourci clavier.

3. Cliquez **OK** pour sauvegarder les changements.

21.2. 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.

En Mode Portable, les tâches planifiées sont désactivées par défaut.

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 configurer le Mode Portable :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez à **Mode Portable/Jeu > Mode Portable**.

Vous pouvez vérifier si le Mode Portable est activé ou désactivé.Si le Mode Portable est activé, BitDefender applique les paramètres configurés lorsque l'ordinateur portable fonctionne sur batterie.

21.2.1. Configuration des paramètres du Mode Portable

Utilisez ces options pour configurer le comportement avec des tâches planifiées :

- **Activer ce module pour modifier les planifications d'analyses antivirus** - permet d'éviter l'exécution d'analyses planifiées lorsque le Mode Portable est activé.Vous pouvez choisir une des options suivantes :

Option	Description
Ignorer la tâche	Annule complètement l'exécution de la tâche planifiée.
Reporter la tâche	Exécuter la tâche planifiée lorsque vous quitterez le Mode Portable.

21.3. Mode Silencieux

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

- Toutes les alertes et fenêtres pop-up BitDefender sont désactivées.
- Les tâches d'analyse planifiées sont désactivées par défaut.

Par défaut, BitDefender passe automatiquement en Mode Silencieux lorsque vous regardez un film ou une présentation ou lorsque l'application est en mode plein écran.Nous vous recommandons vivement de quitter le Mode Silencieux lorsque vous avez fini de regarder le film ou la présentation.

Note
Lorsque vous êtes en Mode Silencieux, vous pouvez constater de légères modifications de la petite icône de BitDefender, située à côté de l'horloge de votre ordinateur.

Pour configurer le Mode Silencieux :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Mode Jeu/Portable> Mode Silencieux**.

Vous pouvez vérifier l'état du Mode Silencieux dans la partie supérieure de la section.Vous pouvez cliquer sur le **Le Mode Silencieux est activé** ou le **Le Mode Silencieux est désactivé** pour modifier l'état actuel.

21.3.1. Configuration d'Action Plein Écran

Voici les options d'analyse que vous pouvez configurer :

- **Action plein écran** - vous pouvez choisir de passer automatiquement en Mode Jeu ou en Mode Silencieux lorsqu'une application s'exécute en mode plein écran.

Note
Si vous ne voulez pas que BitDefender passe automatiquement en Mode Silencieux, décochez la case **Action Plein Écran**.

21.3.2. Configuration des paramètres du Mode Silencieux

Utilisez ces options pour configurer le comportement avec des tâches planifiées :

- **Activer ce module pour modifier les planifications d'analyses antivirus** - permet d'éviter l'exécution d'analyses planifiées lorsque le Mode Silencieux est activé.Vous pouvez choisir une des options suivantes :

Option	Description
Ignorer la tâche	Annule complètement l'exécution de la tâche planifiée.
Reporter la tâche	Exécutez la tâche planifiée dès que vous quittez le Mode Silencieux.

22. Réseau Domestique

Le module Réseau vous permet de gérer les produits BitDefender installés sur tous les ordinateurs de votre foyer à partir d'un seul et même ordinateur.Pour accéder au module Réseau Domestique, ouvrez BitDefender et, en fonction du mode d'affichage de l'interface, procédez comme suit :

Mode INTERMÉDIAIRE
Allez dans l'onglet **Réseau**.

Mode EXPERT
Allez dans **Réseau Domestique**.

Note
Vous pouvez également ajouter un raccourci à Mes Outils.

Vous devez suivre ces étapes pour pouvoir gérer les produits BitDefender installés sur tous les ordinateurs de votre foyer :

1. Activez le réseau domestique de BitDefender sur votre ordinateur.Définissez votre ordinateur comme un serveur.
2. Allumez chaque ordinateur que vous voulez gérer et rejoignez le réseau à partir de ceux-ci (en saisissant le mot de passe).Configurez chaque ordinateur sur Standard.
3. Revenez sur votre ordinateur et ajoutez les ordinateurs que vous voulez gérer.

22.1. Activation du Réseau BitDefender

Pour activer le réseau domestique de BitDefender, suivez ces étapes :

1. Cliquez sur **Activer le Réseau**.Vous serez invité à définir le mot de passe de gestion de réseau domestique.
2. Entrez le même mot de passe dans chacun des champs de saisie.
3. Définissez le rôle de l'ordinateur dans le réseau domestique de BitDefender :
   - **Ordinateur serveur** - sélectionnez cette option sur l'ordinateur qui sera utilisé pour administrer tous les autres.
   - **Ordinateur standard** - sélectionnez cette option sur les ordinateurs qui seront gérés par l'ordinateur serveur.
4. Cliquez sur **OK**.

Vous pouvez voir apparaître le nom de l'ordinateur sur la carte réseau.

Le bouton **Désactiver le réseau** apparaît.

22.2. Ajout d'ordinateurs au réseau BitDefender

Tout ordinateur sera ajouté automatiquement au réseau s'il répond aux critères suivants :

- le réseau domestique de BitDefender a été activé sur celui-ci.
- le rôle a été défini sur Ordinateur Standard.
- le mot de passe défini lors de l'activation du réseau est le même que celui de l'Ordinateur Serveur.

Note

En Mode Expert, vous pouvez analyser le réseau domestique à la recherche d'ordinateurs correspondant aux critères à tout moment en cliquant sur le bouton **Auto discover**.

Pour ajouter manuellement un ordinateur au réseau domestique de BitDefender, à partir de l'ordinateur serveur, suivez ces étapes :

1. Cliquez sur **Ajouter un PC**.
2. Tapez le mot de passe de gestion de réseau domestique et cliquez sur **OK**.Une nouvelle fenêtre s'affiche.

   Vous pouvez voir à l'écran la liste des ordinateurs rattachés au réseau.La signification des icônes est la suivante :

    Indique un ordinateur en ligne sans aucun produit BitDefender installé.

    Indique un ordinateur en ligne avec BitDefender installé.

    Indique un ordinateur hors connexion avec BitDefender installé.
3. Choisissez l'une des possibilités suivantes :
   - Sélectionnez dans la liste le nom de l'ordinateur à ajouter.
   - Tapez l'adresse IP ou le nom de l'ordinateur à ajouter dans le champ correspondant.
4. Cliquez sur **Ajouter**.Vous serez invité à saisir le mot de passe de gestion de réseau domestique de l'ordinateur concerné.
5. Tapez le mot de passe de gestion de réseau domestique défini sur l'ordinateur concerné.
6. Cliquez sur **OK**.Si vous avez spécifié le bon mot de passe, le nom de l'ordinateur sélectionné apparaît sur la carte réseau.

22.3. Gestion du réseau BitDefender

Une fois votre réseau domestique BitDefender créé, vous pouvez gérer l'ensemble des produits BitDefender à partir d'un seul et même ordinateur.

Si vous déplacez le curseur sur un ordinateur de la carte réseau, vous pouvez consulter quelques informations le concernant (nom, adresse IP, nombre de problèmes affectant la sécurité du système, état d'enregistrement de BitDefender).

En cliquant sur le nom d'un ordinateur sur la carte du réseau, vous pouvez voir toutes les tâches administratives que vous pouvez lancer sur cet ordinateur distant.

- **Enregistrer BitDefender sur cet ordinateur**

  Vous permet d'enregistrer BitDefender sur cet ordinateur en entrant une clé de licence.

- **Définir un mot de passe des paramètres sur un PC distant**

  Vous permet de créer un mot de passe pour limiter l'accès aux paramètres de BitDefender sur ce PC.

- **Exécuter une tâche d'analyse à la demande**

  Vous permet de lancer une analyse à la demande sur un ordinateur distant. Vous pouvez réaliser l'une des tâches d'analyse suivantes : Analyse de Mes Documents, Analyse du Système ou Analyse Approfondie du Système.

- **Tout corriger sur ce PC**

  Vous permet de corriger les problèmes qui affectent la sécurité de cet ordinateur à l'aide de l'assistant Tout corriger.

- **Afficher Historique/Événements**

  Vous permet d'accéder au module **Historique&Événements** du produit BitDefender installé sur cet ordinateur.

- **Mettre à jour**

  Lance le processus de Mise à jour du produit BitDefender installé sur cet ordinateur.

- **Définir comme serveur de mise à jour pour ce réseau**

  Vous permet de définir cet ordinateur comme serveur de mise à jour pour tous les produits BitDefender installés sur les ordinateurs de ce réseau.Utiliser cette option réduira le trafic Internet car seul un ordinateur du réseau se connectera à Internet pour télécharger des mises à jour.

- **Retirer le PC du réseau domestique**

  Vous permet de retirer un PC du réseau.

Lorsque l'interface BitDefender est en Mode Intermédiaire, vous pouvez exécuter plusieurs tâches sur tous les ordinateurs administrés simultanément en cliquant sur les boutons correspondants.

- **Analyser tout** - vous permet d'analyser en une seule opération l'ensemble des ordinateurs gérés.

- **Tout mettre à jour** vous permet de mettre à jour en une seule opération l'ensemble des ordinateurs gérés.
- **Enregistrer tout** vous permet d'enregistrer en une seule opération l'ensemble des ordinateurs gérés.

Avant de lancer une tâche sur un ordinateur spécifique, vous serez invité à saisir le mot de passe local de gestion de réseau domestique.Tapez le mot de passe de gestion de réseau domestique et cliquez sur **OK**.

Note

Si vous prévoyez de lancer plusieurs tâches, il peut s'avérer utile de sélectionner l'option **Ne plus afficher ce message durant cette session**.En sélectionnant cette option, vous n'aurez plus à saisir le mot de passe pour la session en cours.

23. Mise à jour

Chaque jour, de nouveaux codes malveillants sont détectés et identifiés. C'est pourquoi il est très important que BitDefender soit à jour dans les signatures de codes malveillants.

Si vous êtes connecté à Internet par câble ou DSL, BitDefender s'en occupera automatiquement. Il lance la procédure de mise à jour de la base virale à chaque fois que vous démarrez votre ordinateur puis toutes les **heures**.

Si une mise à jour a été trouvée, elle sera installée automatiquement ou il vous sera demandé de confirmer son installation, selon les paramètres de mise à jour automatique.

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, il est impératif de laisser la **mise à jour automatique** active.

La section Mise à jour de ce Manuel d'utilisation contient les thèmes suivants:

- **Mise à jour des moteurs antivirus** - comme de nouvelles menaces apparaissent, les fichiers contenant les signatures de virus doivent être mis à jour en permanence contre elles. Elles s'affichent sous le nom de **Virus Definitions Update**.
- **Mise à jour des moteurs antispyware** - de nouvelles signatures seront ajoutées à la base de données. Elles s'affichent sous le nom de **Spyware Definitions Update**.
- **Mise à jour produit** - lorsqu'une nouvelle version du produit est prête, de nouvelles fonctions et techniques d'analyse sont introduites afin d'augmenter les performances du produit. Ces mises à jour sont affichées sous le nom de **Product Update**.

23.1. Mise à jour en cours

La mise à jour automatique peut aussi etre effectuée n'importe quand en cliquant sur **Mettre à jour**. Cette mise à jour est connue aussi sous l'appellation **Mettre à jour a la demande de l'utilisateur**.

Pour mettre à jour BitDefender, en fonction du mode d'affichage de l'interface utilisateur, procédez comme suit :

Mode STANDARD
Cliquez sur l'icône **Mettre à jour** dans la zone Protection de votre PC.

Mode INTERMÉDIAIRE
Allez dans l'onglet **Sécurité**, puis cliquez sur **Mettre à jour** dans la zone Tâches rapides situées dans la partie gauche de la fenêtre.

Mode EXPERT
Allez à **Mise à jour > Mise à jour**.

Le module **Mise à jour**se connecte au serveur de mise à jour BitDefender et recherche les mises à jour disponibles. Si une mise à jour est détectée, vous serez invité à la confirmer ou elle sera effectuée automatiquement en fonction des options que vous aurez définies dans la section Paramètres de la mise à jour manuelle.

Important
Il peut être nécessaire de redémarrer votre PC lorsque vous avez terminé une mise à jour. Nous vous recommandons de le faire dès que possible.

Note
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 « *Comment mettre à jour BitDefender avec une connexion Internet lente* » (p. 134).

23.2. Configuration 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.

Pour configurer les paramètres de mise à jour :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Mise à jour > Configuration**.
3. Configurez les paramètres selon vos besoins.Pour savoir ce qu'une option provoque, placez le curseur dessus et lisez la description affichée au bas de la fenêtre.
4. N'oubliez pas de cliquer sur **Appliquer** pour enregistrer les modifications.

Pour appliquer les paramètres par défaut, cliquez sur **Défaut**.

Les paramètres de mise à jour sont regroupés en quatre catégories (**Paramètres d'emplacement de mise à jour**, **Paramètres de mise à jour automatique**, **Paramètres de mise à jour manuelle** et **Paramètres avancés**). Chaque catégorie est décrite séparément.

23.2.1. Paramétrage des emplacements de mise à jour

Pour configurer les emplacements de mise à jour, utilisez les options de la catégorie **Paramètres d'emplacement de mise à jour**.

Note

Ne configurez ces paramètres que si vous êtes connecté à un réseau local qui stocke les signatures de codes malveillants BitDefender localement ou si vous êtes connecté à Internet via un serveur proxy.

Pour effectuer des mises à jour plus fiables et plus rapides, vous pouvez configurer deux emplacements de mise à jour: un **premier emplacement de mise à jour** et un **emplacement alternatif de mise à jour** . Par défaut, ces emplacements sont identiques: `http://upgrade.bitdefender.com`.

Pour modifier l'un des emplacements de mise à jour, indiquez l'URL du site miroir local dans le champ **URL** correspondant à l'emplacement que vous souhaitez modifier.

Note

Nous vous recommandons de configurer le miroir local en tant qu'emplacement primaire, et de conserver l'emplacement secondaire inchangé, par mesure de sécurité, au cas où le miroir local deviendrait indisponible.

Si votre entreprise utilise un serveur proxy pour se connecter à Internet, cochez la case **Utiliser un proxy**, puis cliquez sur **Paramètres Proxy** pour configurer les paramètres du proxy.Pour plus d'informations, reportez-vous à« Paramètres de connexion » (p. 55)

23.2.2. Configuration de la mise à jour automatique

Pour configurer le processus de mise à jour exécuté automatiquement par BitDefender, utilisez les options de la catégorie **Paramètres de mise à jour automatique**.

Vous pouvez spécifier le nombre d'heures entre deux recherches consécutives de mises à jour dans le champ **Mettre à jour tous/toutes les**. Par défaut, l'intervalle est d'une heure.

Pour déterminer comment le processus de mise à jour automatique doit être exécuté, sélectionnez l'une des options suivantes :

- **Mise à jour silencieuse** - BitDefender télécharge et implémente automatiquement la mise à jour.
- **Demander avant de télécharger les mises à jour** - chaque fois qu'une mise à jour est disponible, le système demande votre autorisation avant de la télécharger.

- **Demander avant d'installer les mises à jour** - chaque fois qu'une mise à jour est téléchargée, le système demande votre autorisation avant de l'installer.

23.2.3. Configuration de la mise à jour manuelle

Pour déterminer comment la mise à jour manuelle (mise à jour à la demande de l'utilisateur) doit être exécutée, sélectionnez l'une des options suivantes dans la catégorie **Paramètres de la mise à jour manuelle**:

- **Mise à jour silencieuse** - la mise à jour manuelle est exécutée automatiquement en tâche de fond, sans l'intervention de l'utilisateur.
- **Demander avant de télécharger les mises à jour** - chaque fois qu'une mise à jour est disponible, le système demande votre autorisation avant de la télécharger.

23.2.4. Configuration des paramètres avancés

Pour éviter que les mises à jour de BitDefender n'interfèrent avec votre travail, configurez les options au niveau des **Paramètres avancés**:

- **Attendre le redémarrage, au lieu de le demander à l'utilisateur** - Si une mise à jour nécessite un redémarrage, le produit continuera à utiliser les anciens fichiers jusqu'à la réinitialisation du système. L'utilisateur ne sera pas averti qu'il doit redémarrer et ne sera donc pas perturbé dans son travail par la mise à jour de BitDefender.
- **Ne pas faire la mise à jour si une analyse est en cours** - BitDefender ne se mettra pas à jour si une analyse est en cours. Ainsi, le processus de mise à jour de BitDefender n'interférera pas avec les tâches d'analyse.

Note
Si une mise à jour de BitDefender a lieu pendant l'analyse, celle-ci sera interrompue.

- **Ne pas mettre à jour si le Mode Jeu est activé** - BitDefender n'effectuera pas de mise à jour si le Mode Jeu est activé.Ainsi, vous limitez l'influence du produit sur les performances du système lorsque vous jouez.
- **Activer le partage des mises à jour** - Si vous souhaitez minimiser l'influence du trafic réseau sur les performances du système pendant les mises à jour, utilisez l'option de partage des mises à jour.
- **Téléchargement des fichiers BitDefender depuis ce PC** - BitDefender vous permet de partager les dernières signatures de virus disponibles sur votre PC avec d'autres utilisateurs de BitDefender.

Comment faire pour

24. Comment analyser des fichiers et des dossiers ?

Avec BitDefender, l'analyse est facile et souple.Il existe plusieurs façons de paramétrer BitDefender pour qu'il analyse les fichiers et les dossiers à la recherche de virus et autres malwares :

- Utilisation du menu contextuel de Windows
- Utilisation des tâches d'analyse
- Utilisation de la barre d'activité d'analyse

Quand vous lancez une analyse, l'assistant d'analyse antivirus s'affiche et vous guide pendant tout le processus.For detailed information about this wizard, please refer to « *Assistant d'analyse antivirus* » (p. 69).

Note

Pour savoir comment effectuer une analyse lorsque BitDefender est en Mode sans échec Windows, référez-vous à « *Comment analyser mon ordinateur en mode sans échec ?* » (p. 141).

24.1. Utilisation du menu contextuel de Windows

C'est le moyen le plus simple conseillé pour analyser un fichier ou un dossier sur votre ordinateur.Faites un clic droit sur l'objet que vous souhaitez analyser et sélectionnez **Analyser avec BitDefender** dans le menu.Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse.

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.

24.2. Utilisation des tâches d'analyse

Si vous souhaitez analyser régulièrement votre ordinateur ou des dossiers particuliers, il est préférable d'utiliser les tâches d'analyse.Les tâches d'analyse indique à BitDefender les emplacements à analyser, les options d'analyse à utiliser et les mesures à prendre. En outre, vous pouvez les planifier pour qu'elles s'exécutent à un rythme régulier ou à un moment donné.

Pour analyser votre ordinateur en utilisant les tâches d'analyse, vous devez ouvrir l'interface BitDefender et lancer la tâche d'analyse voulue.En fonction du mode

d'affichage de l'interface utilisateur, différentes étapes doivent être suivies pour lancer la tâche d'analyse.

Lancement des tâches d'analyse en Mode standard

En Mode standard, vous pouvez lancer un nombre de tâches d'analyse pré-configurées.Cliquez sur le bouton **Sécurité**, puis choisissez la tâche d'analyse souhaitée.Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse.

Exécution des tâches d'analyse en Mode Intermédiaire

En Mode Intermédiaire, vous pouvez exécuter de nombreuses tâches d'analyse préconfigurées. Vous pouvez également configurer et exécuter des tâches d'analyse personnalisées pour analyser des emplacements spécifiques sur votre ordinateur à l'aide d'options d'analyse personnalisées.Suivez ces étapes pour exécuter une tâche d'analyse en Mode Intermédiaire :

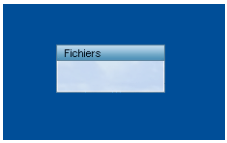
1. Cliquez sur l'onglet **Sécurité**.
2. Dans la partie gauche de la zone Tâches Rapides, cliquez sur **Analyse Complète** et choisissez la tâche d'analyse souhaitée. Pour configurer et lancer une analyse personnalisée, cliquez sur **Analyse Personnalisée**.
3. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse.Si vous avez choisi de lancer une analyse personnalisée, vous devez utiliser l'assistant d'Analyse Personnalisée.

Lancement des tâches d'analyse en Mode Expert

En Mode Expert, vous pouvez lancer toutes les tâches d'analyse pré-configurées et modifier leurs options d'analyse. Vous pouvez également créer des tâches personnalisées si vous souhaitez analyser des emplacements particuliers de votre ordinateur.Suivez ces étapes pour exécuter une tâche d'analyse en Mode Expert :

1. Cliquez sur **Antivirus** dans le menu de gauche.
2. Cliquez sur l'onglet **Analyse antivirus**.Vous pouvez trouver ici les tâches d'analyse par défaut et créer vos propres tâches d'analyse.
3. Double-cliquez sur la tâche d'analyse que vous souhaitez exécuter.
4. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse.

24.3. Utilisation de la barre d'activité d'analyse



Barre de l'activité d'analyse

La **Barre d'analyse d'activité** est une visualisation graphique de l'analyse d'activité de votre système.Cette petite fenêtre est disponible par défaut uniquement en Mode Expert.

Vous pouvez utiliser la barre d'activité d'analyse pour analyser rapidement des fichiers et des dossiers. Faites glisser-déposer le fichier ou le dossier que vous souhaitez analyser dans la barre d'activité d'analyse. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse.

Note
Pour plus d'informations, reportez-vous à « *Barre de l'activité d'analyse* » (p. 20).

25. Comment créer une tâche d’analyse personnalisée ?

Pour créer une tâche d’analyse, ouvrez BitDefender puis, en fonction du mode d’affichage de l’interface utilisateur, procédez comme suit :

Mode INTERMÉDIAIRE

Allez à l’onglet **Sécurité**, puis cliquez sur **Analyse personnalisée** dans la zone Tâches rapides située dans la partie gauche de la fenêtre.

Un assistant apparaîtra pour vous aider à créer une tâche d'analyse.Vous pouvez naviguer dans l'assistant à l'aide des boutons **Suivant** et **Retour**. Pour quitter l'assistant, cliquez sur **Annuler**.

1. **Bienvenue**
2. **Choisir la Cible**

   Cliquez sur **Ajouter cible** pour sélectionner les fichiers ou les dossiers à analyser.

   Cliquez sur **Paramètres Avancés**.Dans l'onglet **Présentation**, réglez les options d'analyse en déplaçant le curseur le long de l'échelle. Si vous souhaitez configurer les options d’analyse en détail, cliquez sur **Personnalisé**.Allez dans l'onglet **Planificateur** et sélectionnez le moment de l'exécution de la tâche.
3. **Terminer**

   Vous pouvez indiquer ici le nom de la tâche et éventuellement, ajouter l'analyse à la zone Tâches Rapides.

   Cliquez sur **Démarrer l’analyse** pour créer la tâche et lancer l’assistant d’analyse.

Mode EXPERT

1. Allez à **Antivirus > Analyse**.
2. Cliquez sur **Nouvelle tâche**. Une nouvelle fenêtre s’affiche.

   Note

   Vous pouvez aussi faire un clic-droit sur une tâche d'analyse prédéfinie, telle qu'une **Analyse approfondie** et choisir **Cloner la tâche**.Très utile lors de la création de nouvelles tâches, car vous pouvez modifier les paramètres de la tâche que vous avez reproduite.
3. Dans l'onglet **Présentation**, saisissez le nom de la tâche et réglez les options d'analyse en déplaçant le curseur le long de l'échelle.

Si vous souhaitez configurer les options d'analyse en détail, cliquez sur **Personnalisé**.

4. Allez dans l'onglet **Chemins** pour sélectionner la cible à analyser. Cliquez sur **Ajouter** pour sélectionner les fichiers ou les dossiers à analyser.
5. Allez dans l'onglet **Planificateur** et sélectionnez le moment de l'exécution de la tâche.
6. Cliquez sur **Ok** pour enregistrer la tâche.La nouvelle tâche apparaît sous les tâches définies par l'utilisateur et peut être modifiée, supprimée ou exécutée à tout moment depuis cette fenêtre.

26. Comment planifier l'analyse de l'ordinateur ?

Analyser régulièrement votre ordinateur est le meilleur moyen de le conserver à l'abri du malware.BitDefender vous permet de planifier des tâches d'analyse qui font que votre ordinateur est analysé automatiquement.

Pour planifier l'analyse de votre ordinateur avec BitDefender, les étapes sont les suivantes :

1. Lancer BitDefender.
2. Procédez comme suit, en fonction du mode d'affichage de l'interface utilisateur :

   Mode INTERMÉDIAIRE
   Allez à l'onglet **Sécurité**, puis cliquez sur **Configuration Antivirus** dans la zone Tâches rapides située dans la partie gauche de la fenêtre.

   Mode EXPERT
   Cliquez sur **Antivirus** dans le menu de gauche.
3. Cliquez sur l'onglet **Analyse antivirus**.Vous pouvez trouver ici les tâches d'analyse par défaut et créer vos propres tâches d'analyse.

   - Des tâches système sont disponibles et peuvent s'exécuter sur n'importe quel compte utilisateur Windows.
   - Seul le créateur des tâches utilisateur peut avoir accès à elles et les lancer.

   Voici les tâches d'analyse par défaut que vous pouvez planifier :

   Analyse Complète
   Analyse l'ensemble du système, mis à part les archives.Dans la configuration par défaut, l'analyse recherche tous les types de malwares à l'exception des rootkits.

   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.

   Analyse automatique à l'ouverture de session
   Analyse les éléments qui sont exécutés quand un utilisateur se connecte à Windows.Pour utiliser cette tâche vous devez la planifier pour qu'elle s'exécute au démarrage du système.Par défaut, l'analyse à l'ouverture de session est désactivée.

Analyse Approfondie
Analyse l'ensemble du système.La configuration par défaut permet d'analyser tous les types de codes malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.

Mes documents
Utilisez-la pour analyser les dossiers importants de l'utilisateur actuel: `Mes documents`, `Bureau` et `Démarrage`. Cela vous permet d'assurer la sécurité de vos documents, un espace de travail sécurisé et d'exécuter des applications saines au démarrage.

Si aucune de ces tâches d'analyse ne correspond à vos besoins, vous pouvez en créer une nouvelle, que vous pourrez alors programmer pour qu'elle s'exécute selon vos souhaits.

4. Faites un clic droit sur la tâche désirée et sélectionnez **Planifier**.Une nouvelle fenêtre s'affiche.
5. Planifier la tâche pour qu'elle s'exécute comme souhaité :
   - Pour ne lancer la tâche d'analyse qu'une fois, sélectionnez **Une fois** et indiquer la date et l'heure du démarrage.
   - Pour lancer la tâche d'analyse au démarrage du système, sélectionnez **Au démarrage du système**.Spécifiez combien de temps après le démarrage la tâche doit s'exécuter (en minutes).
   - Pour lancer la tâche d'analyse à un rythme régulier, sélectionnez **Périodiquement** et indiquez la fréquence et la date et l'heure du démarrage.

   
   Note
   Par exemple, pour analyser votre ordinateur tous les samedis à 2 heures du matin, vous devez procéder comme suit :
   a. Sélectionnez **Périodiquement**.
   b. Dans le champ **Tous/Toutes les**, tapez 1, puis sélectionnez **semaines** dans le menu.La tâche s'exécute ainsi une fois par semaine.
   c. Indiquez que la tâche doit débuter samedi prochain.
   d. Indiquez l'heure de début `02.00.00`.
6. Cliquez sur **OK** pour enregistrer la planification.La tâche d'analyse s'exécutera automatiquement au moment que vous aurez planifié.Si l'ordinateur est éteint au moment prévu, la tâche s'exécutera la prochaine fois que vous le rallumerez.

27. Comment mettre à jour BitDefender à l'aide d'un serveur proxy ?

Normalement, BitDefender détecte et importe automatiquement les paramètres proxy de votre système. Si vous vous connectez à Internet via un serveur proxy, il peut s'avérer nécessaire de trouver les paramètres du proxy, puis de configurer BitDefender en conséquence.Pour savoir comment faire cela, reportez-vous à « *Comment connaître mes paramètres de proxy ?* » (p. 157).

Après avoir trouvé les paramètres du proxy, procédez comme suit :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Général > Configuration**.
3. Cliquez sur **Paramètres proxy** dans les **Paramètres de connexion**.
4. Saisissez les paramètres du proxy dans les champs correspondants.
5. Cliquez sur **OK**.

Note

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support BitDefender comme indiqué dans la section « *Support* » (p. 149).

28. Comment mettre à niveau vers un autre produit BitDefender 2011 ?

Avec BitDefender 2011 vous pouvez facilement effectuer une mise à niveau d'un produit BitDefender 2011 à un autre.

Prenons l'exemple suivant : vous utilisez BitDefender Antivirus Pro 2011 2011 depuis un certain temps et avez récemment décidé d'adopter BitDefender Total Security 2011 et les fonctionnalités supplémentaires qu'il propose.

Il vous suffit d'acheter une clé de licence pour le produit BitDefender 2011 que vous souhaitez mettre à niveau et de la saisir dans la fenêtre d'enregistrement du produit BitDefender 2011 que vous utilisez actuellement.

Suivez ces étapes :

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

   a. **Confirmer l'Action**

   b. **Mise à niveau en cours**

      Patientez jusqu'à la fin du processus de mise à niveau de BitDefender.Cela prendra quelques minutes.

   c. **Mise à niveau terminée**

      Le processus est terminé. Un redémarrage du système sera peut-être nécessaire.

Aide et résolution des problèmes

29. Résolution des problèmes

Ce chapitre présente certains problèmes que vous pouvez rencontrer lorsque vous utilisez BitDefender et vous fournit des solutions possibles à ces problèmes.La plupart de ces problèmes peuvent être résolus via la configuration appropriée des paramètres du produit.

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du support technique BitDefender comme indiqué dans le chapitre « *Support* » (p. 149).

29.1. Problèmes d'installation

Cet article vous aide à résoudre les problèmes d'installation les plus fréquents avec BitDefender.Ces problèmes peuvent être regroupés dans les catégories suivantes :

- Erreurs de validation de l'installation : l'assistant de configuration ne peut pas être exécuté en raison de conditions spécifiques sur votre système.
- Échec des installations : vous avez lancé une installation à partir de l'assistant de configuration, mais elle n'a pas abouti.

29.1.1. Erreurs de Validation de l'Installation

Lorsque vous lancez l'assistant de configuration, certaines conditions sont vérifiées afin de s'assurer que l'installation peut démarrer. Le tableau suivant présente les erreurs de validation de l'installation les plus fréquentes et les solutions pour les corriger.

Erreur	Description et Solution
Vous n'avez pas suffisamment de privilèges pour installer le programme.	Pour lancer l'assistant de configuration et installer BitDefender, vous avez besoin des privilèges administrateur.Choisissez une des possibilités suivantes : ● Connectez-vous à un compte Windows administrateur et relancez l'assistant de configuration. ● Faites un clic droit sur le fichier d'installation et sélectionnez **Exécuter en tant que**.Tapez le nom d'utilisateur et le mot de passe du compte Windows administrateur de ce système.

Erreur	Description et Solution
Le programme d'installation a détecté une version précédente de BitDefender qui n'a pas été désinstallée correctement.	BitDefender a déjà été installé sur votre système, et n'a pas été complètement désinstallé. Cela empêche une nouvelle installation de BitDefender. Pour corriger cette erreur et installer BitDefender, suivez ces étapes : 1. Sur 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. 4. Relancez l'assistant de configuration pour installer BitDefender.
Ce programme BitDefender n'est pas compatible avec votre système d'exploitation.	Vous essayez d'installer BitDefender sur un système d'exploitation non pris en charge.Veuillez consulter « *Configuration requise* » (p. 2) pour savoir sur quels systèmes d'exploitation vous pouvez installer BitDefender. Si votre système d'exploitation est Windows XP avec Service Pack 1 ou sans Service Pack, vous pouvez installer le Service Pack 2 ou supérieur et relancer ensuite l'assistant de configuration.
Le fichier d'installation est conçu pour un autre type de processeur.	Si vous obtenez cette erreur, c'est parce que vous essayez d'exécuter une mauvaise version du fichier d'installation. Il existe deux versions du fichier d'installation BitDefender : l'une pour les processeurs 32 bits et l'autre pour les processeurs 64 bits. Pour être sûr(e) d'avoir la version adaptée à votre système, téléchargez le fichier d'installation directement à partir de www.bitdefender.com.

29.1.2. L'installation a échoué

Plusieurs raisons peuvent expliquer l'échec de l'installation :

- Pendant l'installation, un écran d'erreur s'affiche. Il se peut qu'on vous demande d'annuler l'installation ou un bouton peut vous proposer un outil de désinstallation pour nettoyer le système.

Note

Juste après avoir lancé l'installation, on peut vous signaler qu'il n'y a pas assez d'espace disque libre pour installer BitDefender. Dans ce cas, libérez l'espace disque demandé sur la partition où vous souhaitez installer BitDefender puis reprenez ou relancez l'installation.

- L'installation s'interrompt et, éventuellement, votre système se bloque. Seul un redémarrage rétablit la réactivité du système.
- L'installation est terminée, mais vous ne pouvez pas utiliser certaines ou toutes les fonctions de BitDefender.

Pour corriger une installation ayant échoué et installer BitDefender, suivez ces étapes :

1. **Nettoyez le système après l'échec de l'installation. .** Si l'installation échoue, certaines clés de registre et fichiers BitDefender peuvent demeurer sur votre système. De tels restes peuvent empêcher une nouvelle installation de BitDefender. Ils peuvent aussi affecter la performance du système et sa stabilité. C'est pourquoi vous devez les supprimer avant d'essayer de réinstaller le programme.

   Si c'est le cas, la solution la plus simple consiste à désinstaller complètement BitDefender de votre système et à le réinstaller ensuite.Pour plus d'informations, reportez-vous à « *Comment désinstaller complètement BitDefender ?* » (p. 157).
2. **Vérifiez les causes pouvant expliquer l'échec de l'installation. .** Avant de réinstaller le programme, vérifiez que l'échec de l'installation n'est pas dû aux conditions suivantes :

   a. 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.

   b. Vous devriez également vérifier que votre système n'est pas infecté. Choisissez une des possibilités suivantes :

      - Utilisez le CD de Secours BitDefender pour analyser votre ordinateur et supprimer toutes les menaces présentes.Pour plus d'informations, reportez-vous à « *CD de Secours BitDefender* » (p. 137).
      - Ouvrez une fenêtre Internet Explorer, allez sur www.bitdefender.com et lancez une analyse en ligne (cliquez sur **Analyse en ligne**).
3. Réessayez d'installer BitDefender.Nous vous recommandons de télécharger et d'exécuter la dernière version du fichier d'installation à partir de www.bitdefender.com.
4. Si l'installation échoue de nouveau, contactez le support BitDefender comme indiqué dans « *Support* » (p. 149).

29.2. 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. 155).

- **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. 2).

- **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**.

29.3. 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**.

  Si c'est le cas, la solution la plus simple consiste à désinstaller complètement BitDefender de votre système et à le réinstaller ensuite.Pour plus d'informations, reportez-vous à « *Comment désinstaller complètement BitDefender ?* » (p. 157).

- **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. 155).
  2. Désinstaller complètement BitDefender du système.

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 « *Support* » (p. 149).

29.4. 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 BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Antivirus > Résident**.
3. Cliquez sur **Paramètres Avancés**.
4. Dans la nouvelle fenêtre, allez dans l'onglet **Exceptions**, cliquez sur le bouton **Ajouter** et rendez-vous à l'endroit où se trouve le fichier .exe du programme (il se trouve généralement dans `C:\Program Files`).
5. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.
6. Fermez la fenêtre de BitDefender et vérifiez que le problème a toujours lieu.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support BitDefender comme indiqué dans la section « *Support* » (p. 149).

29.5. 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 BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez dans **Mise à jour > Configuration**.
3. Sous **Paramètres de la mise à jour manuelle**, sélectionnez **Demander avant de télécharger les mises à jour**.
4. Dans l'onglet **Appliquer**, allez à l'onglet **Mise à jour**.
5. Cliquez sur **Mettre à jour** et une nouvelle fenêtre s'affiche.
6. Sélectionnez uniquement **Mises à jour de signatures**, puis cliquez sur **OK**.
7. BitDefender ne téléchargera et n'installera que les mises à jour des signatures de malwares.

29.6. Mon ordinateur n'est pas connecté à Internet. Comment mettre à jour BitDefender ?

Si votre ordinateur n'est pas connecté à Internet, vous devez télécharger manuellement les mises à jour sur un ordinateur avec accès Internet, puis les transférer sur votre ordinateur à l'aide d'un dispositif amovible comme une clé USB.

Suivez ces étapes :

1. Sur un ordinateur connecté à Internet, ouvrez le navigateur Web et allez sur :

   http://www.bitdefender.fr/site/Main/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 ne savez pas 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. 156).
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 l'assistant.

29.7. 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 une fenêtre pop-up 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.
- des virus sur votre système affectent le fonctionnement de 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.
4. Si l'erreur persiste, il se peut qu'il y ait un problème plus sérieux (il se peut par exemple que vous soyez infecté par un virus qui interfère avec BitDefender).Veuillez contacter le support BitDefender comme indiqué dans la section « *Support* » (p. 149).

29.8. La désinstallation de BitDefender a échoué

Cet article vous aide à régler les erreurs pouvant se produire lors de la désinstallation de BitDefender.Deux situations sont possibles :

- Pendant la désinstallation, un écran d'erreur s'affiche. L'écran comporte un bouton permettant de lancer un outil de désinstallation pour nettoyer le système.
- La désinstallation s'interrompt et, éventuellement, votre système se bloque. Cliquez sur **Annuler** pour abandonner la désinstallation. Si cela ne fonctionne pas, redémarrez le système.

Si la désinstallation échoue, certaines clés de registre et fichiers BitDefender peuvent demeurer sur votre système. De tels restes peuvent empêcher une nouvelle installation de BitDefender. Ils peuvent aussi affecter la performance du système et sa stabilité.Pour désinstaller complètement BitDefender de votre système, vous devez lancer l'outil de désinstallation.

Pour plus d'informations, reportez-vous à « *Comment désinstaller complètement BitDefender ?* » (p. 157).

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support BitDefender comme indiqué dans la section « *Support* » (p. 149).

30. Suppression de malwares depuis 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.

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du support technique BitDefender comme indiqué dans le chapitre « *Support* » (p. 149).

30.1. CD de Secours BitDefender

Le CD de secours BitDefender est une fonction incluse dans la plupart des CD d'installation BitDefender. Elle vous permet d'analyser et de désinfecter tous les disques durs existants avant de démarrer votre système d'exploitation.Il peu également vous aider à enregistrer des données de votre PC Windows menacé sur un support amovible.

Si vous ne possédez pas de CD de secours BitDefender, vous pouvez le télécharger sous forme d'image ISO depuis cet emplacement :

http://download.bitdefender.com/rescue_cd/

Téléchargez le fichier .iso et gravez le sur un CD ou un DVD à l'aide de l'outil de votre choix.

Analyse du système avec le CD de secours BitDefender

Pour analyser votre système avec le CD de secours BitDefender, procédez comme suit :

1. Configurez le BIOS de votre ordinateur pour démarrer à partir du CD.
2. Placez le CD dans le lecteur et redémarrez l'ordinateur.
3. Patientez jusqu'à ce que l'écran BitDefender apparaisse et sélectionnez **Lancer le CD de Secours BitDefender** dans la langue de votre choix.
4. Patientez jusqu'à la fin du processus de démarrage. Cela peut prendre un certain temps.
5. Dès que le processus d'initialisation est terminé, les signatures de BitDefender sont mises à jour automatiquement et une analyse de toutes les partitions détectées sur le disque dur est lancée.

Enregistrement de données avec le CD de secours BitDefender

Imaginons que vous ne puissiez pas démarrer votre session Windows en raison d'un problème inexpliqué et que vous deviez à tout prix accéder à des données importantes se trouvant dans votre ordinateur. c'est ici que le CD de secours BitDefender vous sera utile.

Pour enregistrer vos données sur un support amovible, comme une clé USB, procédez comme suit :

1. Configurez le BIOS de votre ordinateur pour démarrer à partir du CD.
2. Placez le CD dans le lecteur et redémarrez l'ordinateur.
3. Patientez jusqu'à ce que l'écran BitDefender apparaisse et sélectionnez **Lancer le CD de Secours BitDefender** dans la langue de votre choix.
4. Patientez jusqu'à la fin du processus de démarrage. Cela peut prendre un certain temps.
5. Dès que le processus d'initialisation est terminé, les signatures de BitDefender sont mises à jour automatiquement et une analyse de toutes les partitions détectées sur le disque dur est lancée.

   Vous partitions de disque dur apparaîtront sur le bureau. Pour afficher le contenu d'un disque dans une fenêtre similaire à Windows Explorer, double-cliquez dessus.

   Note

   Lorsque vous utilisez le CD de Secours BitDefender, vous verrez des noms de partitions de type Linux. Les disques qui n'ont pas été indexés sous Windows apparaîtront sous la forme `[LocalDisk-0]`, correspondant probablement à la partition de type Windows `(C:)`, `[LocalDisk-1]` correspondant à `(D:)` etc.

6. Connectez le périphérique amovible à un port USB de votre ordinateur. Dans quelques instants, une fenêtre va apparaître et afficher le contenu de l'appareil.
7. Vous pouvez copier des fichiers et des dossiers comme vous le feriez sous Windows.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support BitDefender comme indiqué dans la section « *Support* » (p. 149).

30.2. 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 malware, puis exécutez une analyse approfondie du système.

Dès que l'analyse approfondie est terminée, sélectionnez l'action souhaitée à mener sur les 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.Pour savoir comment faire cela, reportez-vous à « *Comment activer/désactiver la protection en temps réel ?* » (p. 158).
2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, reportez-vous à « *Comment afficher des objets cachés dans Windows ?* » (p. 158).
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. 156).
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 « *Support* » (p. 149).

30.3. Comment nettoyer un virus dans un fichier compressé?

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 approfondie du système.
2. Désactivez la protection antivirus en temps réel de BitDefender.
3. Rendez-vous à l'emplacement de l'archive et décompressez-la à l'aide d'une application d'archivage, comme WinZip.
4. Identifier le fichier infecté et le supprimer.
5. Supprimez l'archive d'origine afin de vous assurer que l'infection est totalement supprimée.
6. Recompressez les fichiers dans une nouvelle archive à l'aide d'une application d'archivage, comme WinZip.
7. Activez la protection antivirus en temps réel de BitDefender et exécutez une analyse approfondie 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 « *Support* » (p. 149).

30.4. Comment nettoyer un virus dans une archive de messagerie électronique ?

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.
3. Ouvrez le rapport d'analyse et utilisez les informations d'identification (Sujet, Expéditeur, Destinataire) des messages infectés pour les localiser dans le client de messagerie.
4. Supprimez les messages infectés.La plupart des clients de messagerie placent les messages supprimés dans un dossier de récupération permettant de les restaurer.Il est recommandé de vous assurer que le message a été supprimé également dans ce dossier de récupération.
5. Compactez le dossier contenant le message infecté.
   - Dans Outlook Express :Dans le menu Fichier, cliquez sur Dossier, puis sur Compacter tous les dossiers.
   - Dans Microsoft Outlook :Dans le menu Fichier, cliquez sur Gestion des fichiers de données.Sélectionnez les dossiers de fichiers personnels (.pst) que vous souhaitez compresser, puis cliquez sur Configuration.Cliquez sur Compacter.
6. Activez la protection antivirus en temps réel de BitDefender.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support BitDefender comme indiqué dans la section « *Support* » (p. 149).

30.5. Comment analyser mon ordinateur en mode sans échec ?

L'Analyse Manuelle BitDefender vous permet d'analyser un dossier particulier ou une partition d'un disque dur sans avoir à créer une tâche d'analyse.

Cette fonctionnalité est conçue pour être utilisée lorsque Windows a été démarré en Mode sans échec

Si votre système est infecté par un virus qui ne peut pas être supprimé en mode normal, vous pouvez essayer de le supprimer en démarrant Windows en Mode sans échec, puis en analysant chaque partition du disque dur à l'aide de BitDefender Manual Scan.

Pour savoir comment accéder au Mode sans échec, reportez-vous à « *Comment redémarrer en mode sans échec ?* » (p. 156).

1. Pour analyser votre ordinateur à l'aide de l'Analyse Manuelle BitDefender, suivez ce chemin à partir du menu démarrage de Windows : **Démarrer → Tous les programmes → BitDefender 2011 → Analyse Manuelle BitDefender**.
2. Cliquez sur **Ajouter un Dossier** pour sélectionner la cible à analyser. Une nouvelle fenêtre apparaîtra.
3. Sélectionnez la cible à analyser :
   - pour analyser le bureau, sélectionnez **Bureau**.
   - pour analyser la totalité d'une partition du disque dur, sélectionnez-la dans **Poste de travail**.
   - pour analyser un dossier particulier, recherchez-le et sélectionnez-le.
4. Cliquez sur **OK**, puis sur **Continuer** pour démarrer l'analyse.
5. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse.

30.6. Que faire lorsque BitDefender détecte 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.Pour savoir comment faire cela, reportez-vous à « *Comment activer/désactiver la protection en temps réel ?* » (p. 158).
2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, reportez-vous à « *Comment afficher des objets cachés dans Windows ?* » (p. 158).
3. Restaurer le fichier à partir de la zone de Quarantaine.
4. Insérez le fichier dans la Zone des exceptions.
5. 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 « *Support* » (p. 149).

30.7. 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 « *Support* » (p. 149).

30.8. 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.

30.9. 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.

30.10. Que Sont les Fichiers Sur-Compressés du Journal d'Analyse ?

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

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

30.11. Pourquoi BitDefender a t'il effacé 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.

31. Support

BitDefender fait le maximum pour apporter à ses clients une aide hors pair, rapide et efficace.Si vous rencontrez le moindre problème ou si vous avez des questions sur le produit BitDefender, vous pouvez utiliser plusieurs ressources en ligne pour trouver rapidement une solution ou une réponse.Si vous le préférez, vous pouvez également contacter l'équipe du Service Client de BitDefender. Nos membres du support technique répondront à vos questions aussi rapidement que possible et vous fourniront l'assistance dont vous avez besoin.

31.1. Ressources En Ligne

De nombreuses ressources en ligne sont disponibles pour vous aider à résoudre vos questions et problèmes liés à BitDefender.

- Base de connaissances BitDefender :http://www.bitdefender.fr/site/KnowledgeBase
- Forum du Support BitDefender :http://forum.bitdefender.com
- le portail de sécurité informatique Malware City :http://www.malwarecity.fr
- les tutoriels vidéo

Vous pouvez également utiliser votre moteur de recherche favori pour obtenir plus d'informations sur la sécurité informatique, les produits et l'entreprise BitDefender.

31.1.1. Base de connaissances BitDefender

La base de connaissances de BitDefender est une base en ligne d'information concernant les logiciels BitDefender. Elle 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.

La base de connaissances de BitDefender est accessible au public et consultable gratuitement. Cet ensemble d'informations est une autre manière de fournir aux clients 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 la base de données BitDefender, comme les rapports de corrections de bugs, solutions de rechange, ou articles d'informations venant compléter les fichiers d'aide des produits.

La base de connaissances BitDefender est disponible en permanence sur http://www.bitdefender.fr/site/KnowledgeBase.

31.1.2. 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 nouveaux messages afin de vous aider. Vous pouvez aussi obtenir une réponse ou une solution grâce à un utilisateur de BitDefender plus expérimenté.

Avant de publier un problème ou une question, recherchez s'il existe une rubrique similaire ou connexe dans le forum.

Le forum de support de BitDefender est disponible à http://forum.bitdefender.com, dans 5 langues différentes : français, anglais, allemand, espagnol et roumain.Cliquez sur le lien **Protection des indépendants & des petites entreprises** pour accéder à la section dédiée aux produits de consommation.

31.1.3. Portail Malware City

Le portail Malware City est une riche source d'informations sur la sécurité informatique. Vous y trouverez des articles sur les différentes menaces auxquelles votre ordinateur est exposé lorsqu'il est connecté à Internet (malwares, phishing, spam, cybercriminels).Un dictionnaire vous aide à comprendre les termes de sécurité informatique que vous ne connaissez pas.

De nouveaux articles sont régulièrement publiés pour vous tenir au courant des dernières menaces découvertes, des tendances actuelles en matière de sécurité et vous fournir encore d'autres informations sur le secteur de la sécurité informatique.

La page Web de Malware City est http://www.malwarecity.fr.

31.1.4. Tutoriels vidéo

Les tutoriels vidéos vous guideront pas à pas dans la configuration du produit. Elles sont créées de manière directe et simple, permettant de faire passer le message.

Le principal objectif est d'assurer une expérience agréable en fournissant des informations de base et intermédiaires sur les principes de sécurité, et sur comment configurer et comment utiliser BitDefender.

L'objectif principal est de remplacer le recours à une aide spécialisée en utilisant des tutoriels vidéo qui procurent des informations spécifiquement liées à l'utilisation et à la configuration de BitDefender.

Par exemple, au lieu d'appeler le support BitDefender pour obtenir de l'aide ou essayer de suivre des procédures compliquées, vous pouvez regarder et suivre les étapes présentées par les tutoriels vidéos.

31.2. Demander de l'aide

La section **Aide et résolution des problèmes** vous fournit les informations nécessaires concernant les problèmes les plus fréquents que vous pouvez rencontrer lors de l'utilisation de ce produit.

Si vous ne trouvez pas de solution à votre problème dans les ressources fournies, vous pouvez nous contacter directement :

- « Contactez-Nous Directement à partir de Votre Produit BitDefender » (p. 148)
- « Contactez-Nous via Notre Base de Connaissances en Ligne » (p. 149)

Important

Pour contacter le Service Client de BitDefender, il faut que votre produit BitDefender soit activé. Pour plus d'informations, reportez-vous à « *Enregistrement et Mon compte* » (p. 49).

Contactez-Nous Directement à partir de Votre Produit BitDefender

Si vous disposez d'une connexion Internet (accès à Internet), vous pouvez contacter l'assistance de BitDefender directement à partir de l'interface du produit (fenêtre du programme).

Pour demander de l'aide, vous pouvez utiliser le Support Intégré disponible dans ce produit.

Pour utiliser le Support Intégré, procédez comme suit :

1. Lancer BitDefender.
2. Cliquez sur le lien **Aide et Support**, situé dans le coin inférieur droit de la fenêtre.
3. Vous avez deux options maintenant :
   - Lancez une recherche dans notre base de données pour trouver les informations qui vous intéressent.
   - Sélectionnez le service en fonction du problème rencontré.

     Le **Service Clients** gère l'achat, les licences, les remboursements ou les renouvellements.

     Le **Support Technique** gère tous les problèmes relatifs au produit et à ses fonctionnalités.

     Combattre les malwares s'attaque aux problèmes liés aux virus.

4. Consultez les articles et les documents pertinents et essayez les solutions proposées.
5. Si cette solution ne règle pas votre problème, utilisez le lien indiqué dans l'article pour lancer l'Outil Support.
6. Indiquez votre adresse e-mail, sélectionnez le département et décrivez brièvement le problème.

   Cliquez sur **Suivant**.
7. 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.

   Cliquez sur **Suivant**.
8. Cliquez sur **Terminer** pour envoyer les informations au Service Client de BitDefender. Nous vous contacterons dès que possible.

Contactez-Nous via Notre Base de Connaissances en Ligne

Si vous ne parvenez pas à accéder aux informations nécessaires à l'aide du produit BitDefender, consultez notre base de connaissances en ligne :

1. Allez à http://www.bitdefender.com/help.La base de connaissances de BitDefender contient de nombreux articles apportant des solutions aux problèmes liés à BitDefender.
2. Cherchez dans la base de connaissances de BitDefender les articles susceptibles de fournir des solutions au problème que vous rencontrez.
3. Consultez les articles et les documents pertinents et essayez les solutions proposées.
4. Si la solution ne permet pas de corriger le problème, utilisez le lien dans l'article pour contacter le Service Client BitDefender.
5. Contactez le support technique de BitDefender par e-mail, par chat ou par téléphone.

31.3. Support Technique Editions Profil / BitDefender

Centre d'Assistance des Laboratoires Technologiques et Scientifiques

Les Laboratoires d'Editions Profil et de BitDefender assurent un niveau d'assistance sur tous les produits maintenus par l'équipe de développement. La résolution d'un problème peut nous amener à vous proposer de mettre gratuitement à niveau la version de votre produit.

Ce service offre une assistance pour les questions ou problèmes liés à des applications courantes pour l'utilisateur final ou les entreprises, telles que :

- Des configurations personnalisées des produits BitDefender.
- Des conseils de prise en main en monoposte ou en relation avec des réseaux simples.
- Des problèmes techniques après l'installation des produits BitDefender.
- Des aides afin de contrer les activités de codes malicieux présents sur un système.
- L'accès à notre site internet de maintenance personnalisée et de FAQ en ligne 24h/24 et 7j/7 : http://supportbd.fr.
- 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/liveAssistance. 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**
- **Pour la Belgique**
- **Pour la Suisse**

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://supportbd.fr.

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.

32. Contacts

Une communication efficace est la clé d'une relation réussie. Au cours des dix dernières années, BITDEFENDER s'est bâti une réputation incontestable dans sa recherche constante d'amélioration de la communication pour dépasser les attentes de ses clients et de ses partenaires. N'hésitez pas à nous contacter pour toute question que vous pourriez avoir.

32.1. Adresses Web et e-mails

Ventes : bitdefender@editions-profil.eu
Support technique : http://supportbd.fr
Media Relations: communication@editions-profil.eu
Site Web du produit :http://www.bitdefender.fr
Distributeurs locaux : http://www.bitdefender.fr/site/Partnership/list/
Base de connaissances BitDefender :http://www.bitdefender.fr/site/KnowledgeBase/

32.2. 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/site/Partnership/list/.
2. Les informations de contact des distributeurs locaux de BitDefender devraient s'afficher automatiquement. Si ce n'est pas le cas, utilisez l'outil Localisateur de partenaires à gauche dans le menu pour sélectionner la zone et le pays où vous résidez.
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.

32.3. 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.supportbd.fr
Site Web : http://www.bitdefender.fr

Spain

BitDefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Fax : +34 93 217 91 28
Téléphone : +34 902 19 07 65
Ventes : comercial@bitdefender.es
Support technique : www.bitdefender.es/ayuda
Site Internet : http://www.bitdefender.es

Allemagne

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Service administratif : +49 2301 91 84 222
Ventes : vertrieb@bitdefender.de
Support technique : http://kb.bitdefender.de
Site Web : http://www.bitdefender.de

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

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
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

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
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

33. Informations Utiles

Ce chapitre présente certaines des procédures les plus importantes à connaître avant de commencer à résoudre un problème technique.

Le dépannage d'un problème technique dans BitDefender nécessite quelques notions de Windows, c'est pourquoi les prochaines étapes concernent principalement le système d'exploitation Windows.

33.1. Comment supprimer les autres solutions de sécurité ?

La principale raison à l'utilisation d'une solution de sécurité est d'assurer la protection et la sécurité de vos données. Mais qu'arrive-t-il quand vous avez plus d'un produit de sécurité sur le même système ?

Lorsque vous utilisez plusieurs solutions de sécurité sur le même ordinateur, le système devient instable. Le programme de désinstallation de BitDefender Antivirus Pro 2011 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.

33.2. Comment redémarrer en mode sans échec ?

Le mode sans échec est un mode de fonctionnement de diagnostic, utilisé principalement pour résoudre des problèmes affectant le fonctionnement normal de Windows. Ce type de problèmes peut intervenir lors de conflits de drivers et de virus empêchant Windows de démarrer normalement.En Mode sans échec, seules quelques applications fonctionnent et Windows ne charge que les pilotes de base et un minimum de composants du système d'exploitation.C'est pourquoi la plupart des virus sont inactifs lorsque Windows est en Mode sans échec et qu'ils peuvent être supprimés facilement.

Pour démarrer Windows en Mode sans échec :

1. Redémarrer votre système.
2. Appuyez plusieurs fois sur la touche **F8** avant que Windows ne démarre afin d'accéder au menu de démarrage.
3. Sélectionnez le **Mode sans échec** dans le menu de démarrage, puis appuyez sur **Entrée**.
4. 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.

33.3. 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.

33.4. Comment connaître mes paramètres de proxy ?

Pour trouver ces paramètres, procédez comme suit :

- Pour Internet Explorer 8 :
  1. Ouvrez Internet Explorer.
  2. Sélectionnez **Outils** > **Options Internet**.
  3. Dans l'onglet **Connexions**, cliquez sur **Paramètres LAN**.
  4. Regardez sous **Utiliser un serveur proxy pour votre réseau local**, vous devriez y voir l'**Adresse** et le **Port** du proxy.
- Pour Mozilla Firefox 3.6 :
  1. Ouvrez Firefox.
  2. Sélectionnez **Outils** > **Options**.
  3. Dans l'onglet **Avancé**, allez à l'onglet **Réseau**.
  4. Cliquez sur **Paramètres**.
- Pour Opera 10.51 :
  1. Ouvrez Opera.
  2. Sélectionnez **Outils** > **Préférences**.
  3. Dans l'onglet **Avancé**, allez à l'onglet **Réseau**.
  4. Cliquez sur le bouton **Serveurs proxy** pour ouvrir la boîte de dialogue des paramètres proxy.

33.5. Comment désinstaller complètement BitDefender ?

Suivez ces étapes afin de supprimer BitDefender correctement :

1. Sur 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.

33.6. Comment activer/désactiver la 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).

En mode de fonctionnement normal, la protection en temps réel de BitDefender est activée et il est recommandé de ne pas la désactiver.

Il peut s'avérer nécessaire de désactiver la protection en temps réel lorsque vous tentez de résoudre un problème ou de supprimer un virus. Ils s'appliquent à l'une de ces situations :

- Un problème de ralentissement avec le système après l'installation de BitDefender
- Un problème avec l'un des programmes ou applications après l'installation de BitDefender
- Messages d'erreurs pouvant apparaître peu après l'installation de BitDefender

Suivez ces étapes afin de pouvoir activer ou désactiver temporairement la protection en temps réel :

1. Ouvrez BitDefender, cliquez sur **Options** dans l'angle supérieur droit de la fenêtre et choisissez **Mode Expert**.
2. Allez à **Antivirus** > **Résident**.
3. Décochez la case **Protection en temps réel activée** pour désactiver temporairement la protection antivirus (ou cochez-la si vous souhaitez activer la protection).
4. Vous devez confirmer votre choix en sélectionnant dans le menu pour combien de temps vous souhaitez désactivez la protection en temps- réel.

Note

Les étapes pour désactiver la protection en temps réel dans BitDefender devraient être utilisées comme solution temporaire et uniquement pendant une courte période.

33.7. Comment afficher des objets cachés dans Windows ?

Ces étapes sont utiles en cas de malwares, si vous avez besoin de détecter et de supprimer les fichiers infectés, qui peuvent être cachés.

Suivez ces étapes pour afficher les objets cachés dans Windows :

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et sélectionnez **Options des dossiers**.
2. Allez dans l'onglet **Afficher**.

3. Sélectionnez **Afficher le contenu des dossiers système** (pour Windows XP uniquement).
4. Sélectionnez **Afficher les fichiers et les dossiers cachés**.
5. Effacez **Masquer les extensions de fichier pour les types de fichier connus**.
6. Décochez **Masquer les fichiers protégés du système d'exploitation**.
7. Cliquez sur **Appliquer** puis sur **Ok**.

Glossaire

ActiveX

ActiveX est un modèle pour écrire des programmes tels que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour faire des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent demander ou répondre à des questions, utiliser des boutons et interagir d'autres façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic.

Active X est connu pour son manque total de commandes de sécurité ; les experts en sécurité informatique déconseillent son utilisation sur Internet.

Adware

Les adwares sont souvent associés à des applications gratuites ce qui implique leur acceptation par l'utilisateur. Ces adwares étant généralement installés après que l'utilisateur en a accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant les « pop up » publicitaires peuvent devenir contrariant et dans certains cas dégrader les performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui ne s'étaient pas complètement rendu compte des termes de l'accord de licence.

Archive

Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés.

Un fichier qui contient un ou plusieurs fichiers dans un format compressé.

Backdoor

Il s'agit d'une faille dans la sécurité d'un système délibérément laissé en place par des développeurs ou mainteneurs. La motivation n'est pas toujours négative ; quelques logiciels permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Secteur de boot

Un secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge la plate-forme.

Virus de boot

Un virus qui infecte le secteur de boot d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus de boot rendra le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.

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.

Ligne de commande

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

Cookies

Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une épée à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent (vous voyez seulement des annonces vous intéressant) mais d'autre part, cela implique en réalité "le pistage" et "le suivi" d'où vous allez et de ce sur quoi vous cliquez sur Internet. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple " numéro SKU " (vous savez, le code barres à l'arrière des produits). Bien que ce point de vue puisse paraître extrême, dans certains cas cette perception est justifiée.

Disk drive

C'est une appareil qui lit et écrit des données sur un disque.

Une unité de disque dur lit et écrit sur un disque dur.

Un lecteur de disquette accède à des disquettes.

Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).

Télécharger

Copier des données (généralement un fichier entier) d'une source principale à un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.

Messagerie électronique

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

Événements
Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme l'analyse de la mémoire.

Fausse alerte
Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.

Extension de fichier
La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier.

De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS Dos. Elles comportent communément une à trois lettres (certains vieux OS ne supportent pas plus de trois). Exemples : "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

Heuristique
Méthode permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique est de pouvoir détecter des variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

IP
Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP chargé de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Applette Java
Il s'agit d'un programme Java conçu pour s'exécuter seulement dans une page Web. Pour utiliser un applet dans une page Web, vous devez spécifier le nom de l'applet et la taille (la longueur et la largeur - en pixels) qu'il peut utiliser. Lors d'un accès à la page Web, le navigateur télécharge l'applet depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applets diffèrent des applications par le fait qu'ils sont régis par un protocole de sécurité strict.

Par exemple, bien que les applets s'exécutent sur le client, ils ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les applets sont également limités pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.

Virus Macro
Un type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent des langages macro.

Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.

Client de messagerie
Un client de messagerie est un logiciel qui vous permet d'envoyer et recevoir des messages (e-mails).

Mémoire
Zone de stockage interne dans votre ordinateur. Le terme mémoire regarde le stockage des données dans les "chips" (composants), et le terme stockage regarde les disques. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

Non-heuristique
Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut paraître un virus et ne génère donc pas de fausses alertes.

Programmes empaquetés
Un fichier comprimé. Beaucoup de plates-formes et applications contiennent des commandes vous permettant de comprimer un fichier pour qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide". Normalement, cela nécessite 10 octets.

Pourtant, un logiciel qui comprime les fichiers remplace la série d'espaces par un caractère spécial série d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. C'est juste une technique de compression, il y en a une multitude.

Chemin
Les directions exactes vers un fichier. Ces directions sont décrites d'habitude par arborescence, de haut en bas.

La connexion entre deux points, telle le canal de communication entre deux ordinateurs.

Phishing
Action d'envoyer un e-mail à un utilisateur en prétendant être une entreprise connue dans le but d'obtenir frauduleusement des informations privées qui permettront d'utiliser l'identité du destinataire du mail. Cet e-mail dirige l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

Virus polymorphique
Un virus qui change de forme avec chaque fichier qu'il infecte. Comme ils n'ont pas une forme unique bien définie, ces virus sont plus difficiles à identifier.

Port

Une interface de l'ordinateur à laquelle vous pouvez connecter un périphérique. Les PCs comportent plusieurs sortes de ports. A l'intérieur, il y a quelques ports pour la connexion des disques, cartes vidéo. A l'extérieur, les PCs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Fichier journal (Log)

Un fichier qui enregistre les actions qui surviennent. BitDefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.

Rootkit

Un rootkit est un ensemble d'outils logiciels permettant aux administrateurs d'accéder à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs systèmes.

Le principale rôle des rootkits est de cacher des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseaux, s'ils incluent les logiciels appropriés.

Les Rootkits ne sont pas malveillants par nature. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler des codes malveillants ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des codes malveillants, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, corrompre des fichiers et des logs et éviter leur détection.

Scripts

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

Spam

Message électronique ou envoi de messages souvent répertoriés comme des emails « non sollicités ».

Spyware

Tout type de logiciel qui récupère secrètement les informations des utilisateurs au travers de leur connexion Internet sans les avertir, généralement à des fins publicitaires. Les spywares sont généralement cachés dans des logiciels shareware ou freeware qui peuvent être téléchargés sur Internet. Cependant, la majorité des applications shareware ou freeware ne comportent pas de

spyware. Après son installation, le spyware surveille l'activité de l'utilisateur sur Internet et transmet discrètement des informations à une tierce personne. Les spywares peuvent également récupérer des informations sur les adresses mail, les mots de passe ou même les numéros de cartes de crédit.

Leur point commun avec les Chevaux de Troie est que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une de manière les plus classique pour être victime de spywares est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d'éthique et de respect de la vie privée, les spywares volent aussi les ressources de l'ordinateur de l'utilisateur en utilisant de la bande passante lors de l'envoi d'information au travers de sa connexion Internet. A cause de cette utilisation de la mémoire et des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu'à entraîner des plantages ou provoquer une instabilité globale du système.

Objets menu démarrage

Tous les fichiers placés dans ce dossier s'ouvrent au démarrage. Par exemple, un écran de démarrage, un fichier son pour quand l'ordinateur démarre, un calendrier, des programmes, peuvent être placées dans ce dossier. D'habitude c'est un raccourci vers le fichier qui est mis dans le dossier, et pas le fichier.

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.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés avec divers architectures hardware et diverses plates-formes. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Trojan (Cheval de Troie)

Un programme destructif qui prétend être une application normale. Les Trojans ne sont pas des virus et ne se repliquent pas, mais peuvent être tout aussi destructifs. Un des types les plus répandu de Trojans est un logiciel prétendant désinfecter votre PC (mais au lieu de faire cela il l'infecte).

Le terme provient de la fameuse histoire de l'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Trojans, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur

ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Mise à jour

Une nouvelle version du logiciel ou d'un produit hardware, destinée à remplacer une ancienne version du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, sinon la mise à jour ne se fait pas.

BitDefender a son propre module de mise à jour permettant à l'utilisateur de vérifier manuellement les mises à jour ou de les programmer automatiquement.

Virus

Programme ou morceau de code qui est chargé dans votre ordinateur sans que vous le sachiez et fonctionne contre votre gré. La plupart des virus peuvent se répliquer. Tous les virus sont créés par des personnes. Un virus simple capable de se copier continuellement est relativement facile à créer. Même un virus simple de ce type est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est capable de se transmettre via un réseau et d'échapper aux systèmes de sécurité.

Définition virus

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

Ver

Un programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure qu'il se propage. Il ne peut pas s'attacher aux autres programmes.