bitdefender

ANTIVIRUS 2008

Manuel d'utilisation

BitDefender Antivirus 2008

Manuel d'utilisation

Publié le 2008.02.08

Notice Légale


bitdefender

Table des matières

Accord de licence

Si vous n'acceptez pas les termes et conditions n'installez pas ce logiciel. En choisissant "J'accepte", "Ok", "Continuer", "Oui" ou en installant ou utilisant le logiciel de quelque manière que ce soit, vous confirmez que vous comprenez parfaitement et acceptez les termes et conditions de cette licence.

Les termes de cette licence incluent les Solutions et Service BitDefender pour votre usage personnel, y compris les documentations relatives aux produits, les mises à jour et mises à niveau des applications ou les services qui vous sont proposés dans le cadre de la licence, ainsi que toute reproduction de ces éléments.

Cet accord de licence est un accord légal entre vous (entité individuelle ou utilisateur final) et BITDEFENDER pour l'usage du produit de BITDEFENDER identifié au-dessus, qui comprend le logiciel et qui peut comprendre les éléments média, les matériels imprimés et la documentation "en ligne" ou électronique (" BitDefender "), le tout étant protégé par la loi française et par les lois et les traités internationaux. En installant, copiant, ou utilisant de toute autre manière le logiciel BitDefender, vous acceptez les termes de cet accord.

Si vous n'acceptez pas les termes de cette licence, n'installez pas ou n'utilisez pas BitDefender.

Accord de licence BitDefender. BitDefender est protégé par les lois du copyright et par les traités internationaux concernant le copyright, ainsi que par les autres lois et traités concernant la propriété intellectuelle. BitDefender est licencié et non pas vendu.

DROITS DE LICENCE. Ce logiciel restant la propriété de BITDEFENDER, vous et vous seul disposez néanmoins de certains droits d'utilisation non exclusifs et non transférables, une fois l'accord de licence accepté. Vos droits et obligations relatifs à l'utilisation de ce logiciel sont les suivants:

LOGICIEL: Vous pouvez installer et utiliser BitDefender, sur autant d'ordinateurs que nécessaire dans le cadre de la limitation imposée par le nombre d'utilisateurs ayant une licence. Vous pouvez réaliser une copie à des fins de sauvegarde.

ACCORD DE LICENCE POUR ORDINATEUR. Cette licence s'applique au logiciel BitDefender qui peut être installé sur un ordinateur unique ne proposant pas de service en réseau. Chaque utilisateur principal peut utiliser ce logiciel sur un ordinateur unique et peut réaliser une copie de sauvegarde sur un support différent. Le nombre d'utilisateurs principal correspond au nombre d'utilisateurs définit dans l'accord de licence.

DUREE DE LA LICENCE. La licence accordée ci-dessus commencera au moment où vous installez, copiez ou utilisez de toute autre manière BitDefender pour la première fois et expirera à la fin de la période pour laquelle la licence a été acquise.

EXPIRATION. Le produit cessera de fonctionner immédiatement à la date d'expiration de la licence.

MISES À JOUR. Si BitDefender constitue une mise à jour, vous devez être correctement licencié pour utiliser le produit identifié par BITDEFENDER comme étant éligible pour la mise à jour, afin d'utiliser BitDefender. Un produit BitDefender qui constitue une mise à jour remplace le produit qui formait la base de votre éligibilité pour la mise à jour. Vous pouvez utiliser le produit résultant seulement en accord avec les termes de cet Accord de licence. Si BitDefender est une mise à jour d'un composant d'un progiciel que vous avez acheté comme un seul produit, BitDefender peut être utilisé et transféré seulement comme une partie de ce progiciel et ne peut pas être séparé pour l'usage sur plus d'un ordinateur.Les termes et conditions de cette licence annule et remplace tout accord préalable ayant pu exister entre vous et BITDEFENDER concernant un produit complet ou un produit mis à jour.

COPYRIGHT. Tous les droits d'auteur de BitDefender (comprenant mais ne se limitant pas à toutes les images, photographies, logos, animations, vidéo, audio, musique, texte et " applets " compris dans BitDefender), les matériels imprimés qui l'accompagnent et les copies de BitDefender sont la propriété de BITDEFENDER. BitDefender est protégé par les lois concernant le copyright et par les traités internationaux. C'est pourquoi vous devez traiter BitDefender comme tout autre matériel protégé par le copyright à l'exception du fait que vous pouvez installer BitDefender sur un seul ordinateur, vu que vous gardez l'original seulement pour archive. Vous ne pouvez pas copier les matériels imprimés qui accompagnent BitDefender. Vous devez produire et inclure toutes les notices de copyright dans leur forme originale pour toutes les copies respectives du média ou de la forme dans laquelle BitDefender existe. Vous ne pouvez pas céder la licence, louer sous quelque forme que ce soit tout ou partie du logiciel BitDefender. Vous ne pouvez pas décompiler, désassembler, modifier, traduire ou tenter de découvrir le code source de ce logiciel ou créer des outils dérivés de BitDefender.

GARANTIE LIMITÉE. BITDEFENDER garantit que le support sur lequel le logiciel est distribué est exempt de vices de matériaux et de fabrication pendant une période de trente (30) jours à compter de la date de livraison du logiciel. Votre seul recours en cas de manquement à cette garantie sera le remplacement par BITDEFENDER du support défaillant durant la période de trente (30) jours à compter de la date de livraison du logiciel. BITDEFENDER ne garantit pas que le logiciel répondra à vos besoins ni qu'il fonctionnera sans interruption ou sans erreur. BITDEFENDER REFUSE TOUTE AUTRE GARANTIE POUR BITDEFENDER, QU'ELLE SOIT EXPRESSE OU

IMPLICITE. LA GARANTIE CI-DESSUS EST EXCLUSIVE ET REMPLACE TOUTES AUTRES GARANTIES, QU'ELLES SOIENT IMPLICITES OU EXPLICITES, Y COMPRIS LES GARANTIES IMPLICITES DE COMMERCIALISATION ET D'APPLICATION PARTICULIÈRE.

A l'exception des termes définis dans cet accord de licence, BITDEFENDER refuse toute autre forme de garantie, explicite ou implicite en rapport avec le produit, ses améliorations, sa maintenance, ou son support ainsi que tout autre matériel relatif (tangible ou intangible) ou service fournit par celui ci. BITDEFENDER refuse explicitement toutes garanties et conditions incluant, sans limitation, les garanties liées à la commercialisation, l'adaptation à un emploi particulier, la non interférence, la précision des données, la précision de contenus d'informations, l'intégration système, et la non violation des droits d'une tierce partie en filtrant, désactivant ou supprimant un logiciel, spyware, adware, des cookies, des emails, des documents, une publicité ou un autre produit du même type, d'un telle tierce partie, quel que soit leur mode d'utilisation.

REFUS DES DOMMAGES. Toute personne qui utilise, teste ou évalue BitDefender accepte les risques qu'il peut encourir concernant la qualité et la performance de BitDefender. En aucun cas BITDEFENDER ne sera tenu responsable à votre égard de tout dommage particulier direct ou indirect, de réclamations liées à une perte quelconque découlant de l'utilisation ou de l'incapacité d'utiliser le logiciel même si BITDEFENDER a été avisé de l'éventualité de tels dommages. CERTAINS ETATS N'AUTORISENT PAS LA LIMITATION OU L'EXCLUSION DE RESPONSABILITE EN CAS DE DOMMAGE. LA REGLE EDICTEE CI-DESSUS CONCERNANT LES LIMITATIONS OU EXCLUSIONS CITEES PEUT NE PAS S'APPLIQUER A VOTRE CAS - QU'ELLES QUE SOIENT LES CONDITIONS LA REPONSABILITE DE BITDEFENDER NE POURRA EXCEDER LE MONTANT QUE VOUS AVEZ PAYE POUR BITDEFENDER. Les limitations édictées ci dessus s'appliqueront que vous acceptiez ou non d'utiliser, d'évaluer ou de tester BitDefender.

INFORMATION IMPORTANTE POUR LES UTILISATEURS. CE LOGICIEL N'EST PAS PREVU POUR DES MILIEUX DANGEREUX, DEMANDANT DES OPÉRATIONS OU UNE PERFORMANCE SANS ERREUR. CE LOGICIEL N'EST PAS RECOMMANDÉ DANS LES OPÉRATIONS DE NAVIGATION AÉRIENNE, INSTALLATIONS NUCLÉAIRES OU DES SYSTÈMES DE COMMUNICATION, SYSTÈMES D'ARMEMENT, SYSTÈMES ASSURANT DIRECTEMENT OU INDIRECTEMENT LE SUPPORT VITAL, CONTROLE DU TRAFFIC AÉRIEN, OU TOUTE AUTRE APPLICATION OU INSTALLATION OU LA DÉFAILLANCE POURRAIT AVOIR COMME EFFET LA MORT DES PERSONNES, DES BLESSURES PHYSIQUES SÉVÈRES OU DES DOMMAGES DE LA PROPRIÉTÉ.

CONDITIONS GÉNÉRALES. Cet accord est régi par les lois de la Roumanie et par les règlements et les traités internationaux concernant le copyright. La seule juridiction compétente en cas de désacord concernant cet accord de licence sera la Cour de justice de Roumanie.

Les prix, les coûts et les frais d'usage de BitDefender peuvent changer sans que vous en soyez prévenu.

Dans l'éventualité d'une invalidité de tout règlement de cet Accord, cette invalidité n'affectera pas la validité du reste de cet Accord.

BitDefender et le logo de BitDefender sont des marques déposées de BITDEFENDER. Toutes les autres marques et produits associés appartiennent à leurs propriétaires respectifs.

La licence prendra fin immédiatement sans qu'il soit besoin de vous avertir si vous ne respectez pas une ou plusieurs des conditions édictées dans cet accord. Il ne vous sera pas possible de demander un remboursement de la part de BITDEFENDER ou d'un de ses représentants en cas de cloture de cette licence. Les termes et conditions de respect de confidentialité et leurs restrictions doivent rester de mise même après la fin du contrat.

BITDEFENDER s'autorise à revoir quand il le souhaite les termes de cette licence, ceux ci s'appliqueront automatiquement aux produits distribués qui incluent les termes modifiés. Dans l'éventualité d'une invalidité d'une partie de cet accord, cette invalidité n'affectera pas la validité du reste de cet Accord.

En cas de controverses ou d'incohérence dans la traduction des termes de cette licence dans une autre langue, seule la version anglaise édité par BITDEFENDER sera déclarée valide. En cas de controverses ou d'incohérence dans la traduction des termes de cette licence dans une autre langue, seule la version anglaise éditée par BITDEFENDER sera déclarée valide.

Contact BITDEFENDER: Rue Fabrica de Glucoza, No. 5, Code postal 020331 - Sector 2, Bucarest, Roumanie, ou au Tel No: +40-21-2330780 ou Fax: +40-21-2330763, adresse e-mail: office@bitdefender.com.

Préface

Ce Manuel d'utilisation est destiné à tous les utilisateurs qui ont choisi **BitDefender Antivirus 2008** comme solution de sécurité pour leur ordinateur personnel. Les informations présentées dans ce livret sont destinées aussi bien aux utilisateurs expérimentés en informatique qu'a n'importe quelle personne sachant utiliser Windows.

Ce Manuel d'utilisation vous guidera pas à pas dans le processus d'installation de **BitDefender Antivirus 2008**, il vous apprendra comment le configurer. Vous y apprendrez les méthodes d'utilisation de **BitDefender Antivirus 2008**, la méthode de mise à jour, de test et de personnalisation. Vous saurez tirer le meilleur de BitDefender.

Nous vous souhaitons un apprentissage agréable et utile.

1. Conventions utilisées dans ce manuel

1.1. Normes Typographiques

Plusieurs styles de texte sont utilisés dans ce livret pour une lisibilité améliorée. Leur aspect et signification sont présentés dans la liste ci dessous.

Apparence	Description
`sample syntax`	Les exemples et quelques données numériques sont imprimés avec des caractères séparés d'un espace.
http://www.bitdefender.com	Les liens URL pointent vers un emplacement externe comme un serveur http ou ftp.
support@bitdefender.com	Les adresses Email sont insérées dans le texte pour plus d'informations sur les contacts.
« Préface » (p. xi)	Ceci représente un lien interne vers un emplacement à l'intérieur de ce document.
`filename`	Les fichiers et répertoires sont imprimés en utilisant des caractères séparés d'un espace.
option	Toutes les informations sur le produit sont imprimées en utilisant des caractères **Gras**.

Apparence	Description
`sample code listing`	Les textes cités sont fournis en guise de référence.

1.2. Avertissements

Les avertissements sont des notes textes graphiquement marquées, offrant à votre attention des informations additionnelles relatives au paragraphe actuel.

Note
La note est une courte observation. Bien que vous puissiez l'omettre, les notes apportent des informations non négligeables, comme des fonctions spécifiques ou un lien à un thème proche.

Important
Cette icône requiert votre attention et il n'est pas recommandé de le passer. Habituellement, il apporte des informations non critiques mais significatives.

Avertissement
Marque une information critique que vous devrez lire attentivement. Rien de négatif ne se passera si vous suivez les indications. A lire très attentivement car décrit une opération potentiellement très risquée.

2. Structure du manuel

Le manuel est composé de plusieurs parties reprenant les thèmes principaux. De plus, un glossaire est fourni pour éclaircir quelques termes techniques.

Installation. Des instructions pas à pas pour installer BitDefender sur un poste. Un tutorial clair sur l'installation et la configuration de **BitDefender Antivirus 2008**. Commencant par les prérequis pour une installation réussie, vous serez guidé à travers le processus d'installation entier et lors de la première session. A la fin, la procédure de désinstallation est décrite au cas où vous auriez besoin de désinstaller BitDefender.

Gestion de base. Description de la gestion et maintenance de base de BitDefender.

Gestion avancée de la sécurité. Présentation détaillée des fonctions de sécurité fournies par BitDefender. Ces pages décrivent en détail l'ensemble des options de la console des paramètres avancés. Vous apprendrez à configurer et à utiliser tous les modules BitDefender afin de protéger efficacement votre ordinateur contre toutes les menaces de codes malveillants (virus, spyware, rootkits, etc.).

CD de secours BitDefender. Description du CD de secours BitDefender. Mode d'emploi pour comprendre l'utilisation du CD bootable de secours.

Demander de l'aide. Où regarder et à qui demander de l'aide si quelque chose d'inattendu apparaît.

Glossaire. Le glossaire tente de vulgariser des termes techniques et peu communs que vous trouverez dans ce document.

3. Commentaires

Nous vous invitons à nous aider à améliorer ce livret. Nous avons testé et vérifié toutes les informations mais vous pouvez trouver que certaines fonctions ont changé. N'hésitez pas à nous écrire pour nous dire si vous avez trouvé des erreurs dans ce livret ou concernant toute amélioration que nous pourrions y apporter pour vous fournir la meilleure documentation possible.

Faîtes-le nous savoir en nous écrivant à cette adresse documentation@bitdefender.com.

Important

Merci d'écrire en anglais vos e-mails concernant le manuel afin que nous puissions les traiter avec la plus grande efficacité.

Installation

1. Installation de BitDefender Antivirus 2008

La section **Installation de BitDefender Antivirus 2008** de ce Manuel d'utilisation concerne les sujets suivants:

- Configuration système
- Etapes d'installation
- Assistant initial de démarrage
- Mise à jour majeure
- Réparer ou supprimer BitDefender

1.1. Configuration requise

Pour assurer un fonctionnement correct du produit, vérifiez avant l'installation que l'un des systèmes d'exploitation suivants fonctionne sur votre ordinateur et que vous disposez de la bonne configuration:

- **Plateforme** - Windows 2000/XP SP2 2b & 64bit/Vista 2b & 64bit; Internet Explorer 6.0 (ou supérieur)

Windows 2000

- Processeur 800 MHz ou supérieur
- Mémoire minimum 256Mo de RAM (512Mo recommandés)
- Au moins 60Mo d'espace disque disponible.

Windows XP

- Processeur 800 MHz ou supérieur
- Mémoire minimum: 512Mo de RAM (1 Go recommandés)
- Au moins 60Mo d'espace disque disponible.

Windows Vista

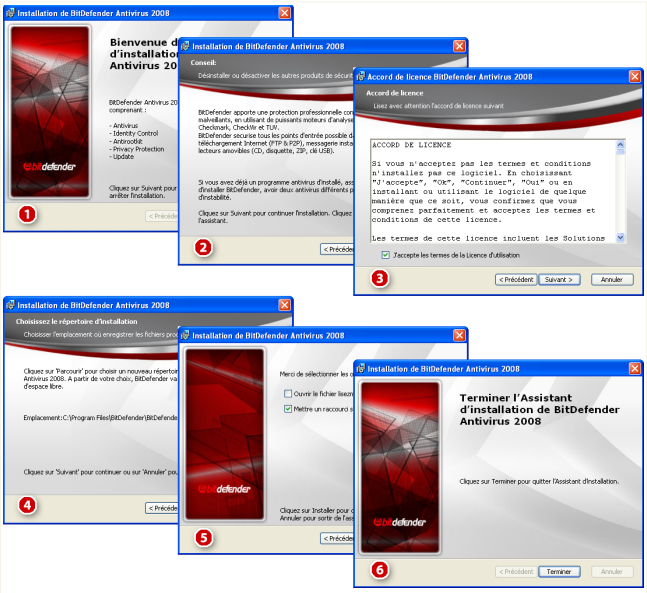
- Processeur 800 MHz ou supérieur
- Mémoire minimum: 512Mo de RAM (1 Go recommandés)
- Au moins 60Mo d'espace disque disponible.

BitDefender Antivirus 2008 peut être téléchargé en version d'évaluation depuis le site http://www.bitdefender.fr.

1.2. Etapes d'installation

Localisez le fichier d'installation et double-cliquez dessus.Cela lancera l'assistant d'installation, qui vous guidera à travers le processus d'installation:

Avant de lancer l'assistant de configuration, BitDefender recherche les nouvelles versions du programme d'installation. Si une nouvelle version est disponible, vous êtes invité à la télécharger. Cliquez sur **Oui** pour télécharger la nouvelle version ou sur **Non** pour continuer à installer la version disponible dans le fichier d'installation.



Etapes d'installation

Voici les étapes à suivre pour installer BitDefender Antivirus 2008:

1. Cliquez sur **Suivant** pour continuer ou sur **Annuler** si vous voulez quitter l'installation.
2. Cliquez sur **Suivant**.

BitDefender Antivirus 2008 vous previent si il y a déjà un autre antivirus installé sur votre ordinateur. Cliquez sur **Supprimer** pour désinstaller le produit correspondant. Si vous souhaitez poursuivre sans supprimer le produit détecté, cliquez sur **Suivant**.

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.

3. Merci de lire l'Accord de Licence, sélectionnez **J'accepte les termes de l'Accord de Licence** et cliquez sur **Suivant**. Si vous n'acceptez pas ces conditions, sélectionnez **Annuler**. Le processus d'installation sera abandonné et vous sortirez de l'installation.
4. Vous pouvez sélectionner le répertoire dans lequel installer le produit. Le répertoire par défaut est `C:\Program Files\BitDefender\BitDefender 2008`. Si vous voulez choisir un autre répertoire, cliquez sur **Parcourir** et, dans la fenêtre qui s'ouvre, choisissez le répertoire d'installation.

   Cliquez sur **Suivant**.
5. Sélectionnez les options du processus d'installation. Certaines sont sélectionnées par défaut.
   - **Ouvrir le fichier lisezmoi** - pour ouvrir le fichier lisez moi à la fin de l'installation.
   - **Créer un raccourci sur le bureau** - pour mettre un raccourci sur le bureau à la fin de l'installation.
   - **Éjecter le CD après l'installation** - pour que le CD soit éjecté à la fin de l'installation, cette option apparaît au moment de l'installation du produit.
   - **Désactiver Windows Defender** - pour désactiver Windows Defender ; cette option n'est disponible que sous Windows Vista.

   Cliquez sur **Installer** afin de commencer l'installation du produit.

Important
Pendant la procédure d'installation un assistant apparaîtra. Il vous aide à enregistrer votre **BitDefender Antivirus 2008**, créer un compte et configurer BitDefender pour exécuter les tâches de sécurité importantes.
Complètez l'assistant d'installation pour passer à l'étape suivante.

6. Cliquez sur **Terminer**. Il vous sera demandé de redémarrer votre système pour terminer le processus d'installation. Nous vous recommandons de le faire dès que possible.

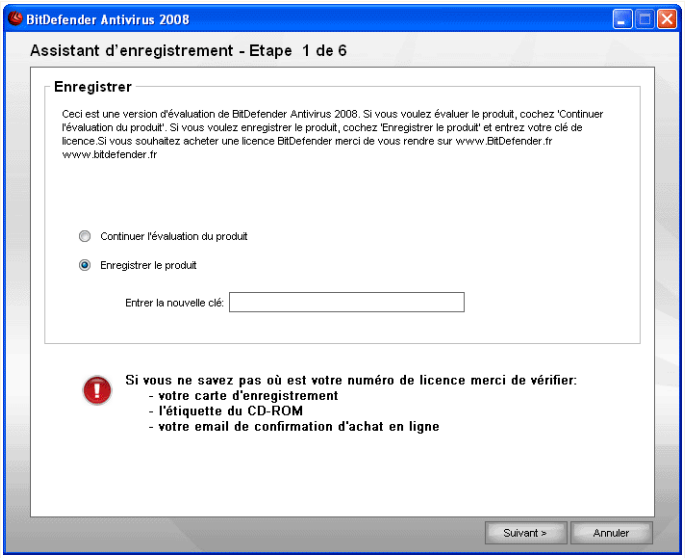
Si vous avez accepté les paramètres par défaut pour le répertoire d'installation, vous pouvez voir dans `Program Files` un nouveau répertoire, nommé `BitDefender`, qui contient le sous répertoire `BitDefender 2008`.

1.3. Assistant de première installation

Pendant la procédure d'installation un assistant apparaîtra. Il vous aide à enregistrer votre **BitDefender Antivirus 2008**, créer un compte et configurer BitDefender pour exécuter les tâches de sécurité importantes.

Compléter cet assistant n'est pas obligatoire. Cependant, nous vous recommandons de le faire pour gagner du temps et vous assurer que votre système est sain même avant l'installation de BitDefender.

1.3.1. Etape 1 sur 6 - Enregistrement de BitDefender Antivirus 2008



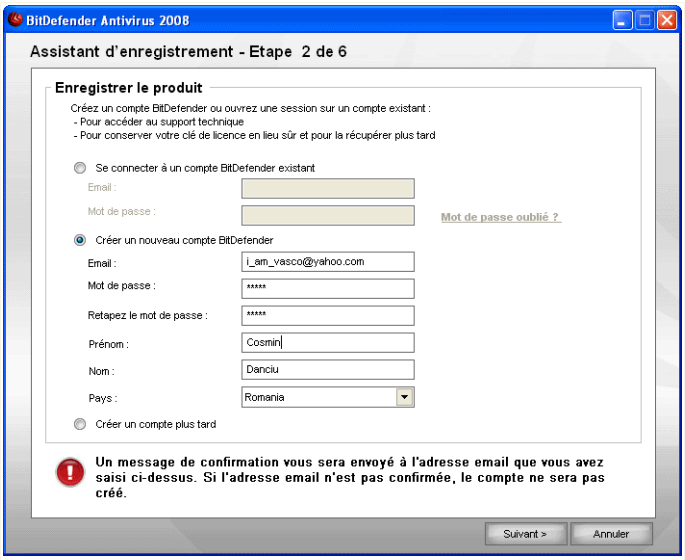
Enregistrement du Produit

Choisissez **Enregistrer le produit** pour enregistrer **BitDefender Antivirus 2008**. Entrer la clé de licence dans le champ **Entrer une nouvelle clé**.

Pour continuer à évaluer le produit, sélectionnez **Continuer l'évaluation du produit**.

Cliquez sur **Suivant**.

1.3.2. Etape 2 sur 6 - Création d'un compte BitDefender



Création de compte

Je n'ai pas de compte BitDefender

Pour bénéficier du support technique gratuit et d'autres services, il faut créer un compte BitDefender.

Note
Si vous voulez créer un compte plus tard, choisissez l'option correspondante.

Pour créer un compte BitDefender, sélectionnez **Créer un nouveau compte BitDefender** et entrez les informations demandées. Les informations communiquées ici resteront confidentielles.

- **E-mail** - Entrez votre adresse e-mail.
- **Mot de passe** - entrez un mot de passe pour votre compte BitDefender.

Note
Le mot de passe doit comporter au moins quatre caractères.

- **Retaper le mot de passe** - re-entrez le mot de passe choisi auparavant.
- **Prénom** - Entrez votre prénom.
- **Nom** - Entrez votre nom.
- **Pays** - sélectionnez le pays dans lequel vous vivez.

Note
Pour accéder à votre compte, connectez-vous sur http://myaccount.bitdefender.com et entrez l'adresse e-mail que vous avez fourni ainsi que votre mot de passe.

Pour créer votre compte vous devez d'abord activer votre adresse e-mail. Vérifiez votre messagerie et suivez les instructions reçues dans l'email qui vous a été envoyé par le service d'enregistrement BitDefender.

Cliquez sur **Suivant**.

J'ai déjà un compte BitDefender

BitDefender détectera automatiquement si vous avez déjà un compte BitDefender actif sur cet ordinateur. Dans ce cas, la seule chose que vous avez à faire est de cliquer sur **Suivant**.

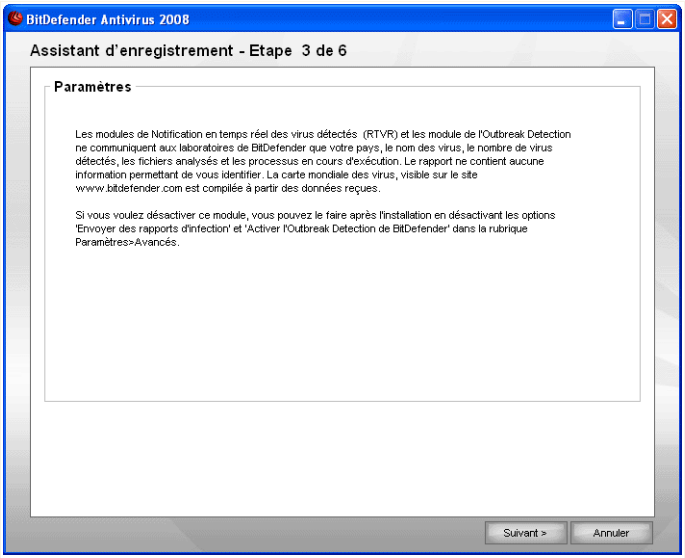
Si vous avez déjà un compte actif, mais que BitDefender ne le détecte pas, sélectionnez **Utiliser un compte BitDefender existant** et indiquez l'adresse e-mail et le mot de passe de votre compte.

Note
Si vous indiquez un mot de passe incorrect, il vous sera demandé de le resaisir lorsque vous cliquerez sur **Suivant**. Cliquez sur **OK** pour entrer de nouveau le mot de passe ou **Annuler** pour quitter l'assistant.

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

Cliquez sur **Suivant**.

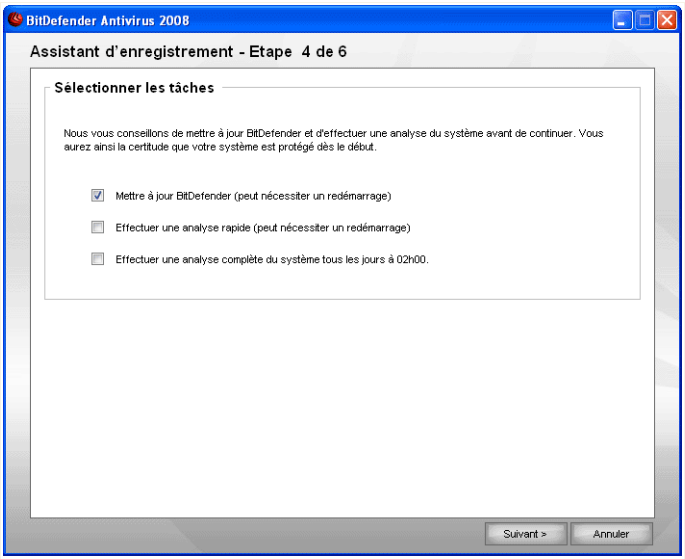
1.3.3. Etape 3 sur 6 - En savoir plus sur le Real Time Virus Reporting (RTVR)



Informations sur le RTVR

Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.

1.3.4. Etape 4 sur 6 - Sélectionner les tâches à lancer



Sélection des tâches

Paramètrez BitDefender Antivirus 2008 pour lancer les tâches de sécurité importantes pour votre ordinateur.

Les options suivantes sont disponibles:

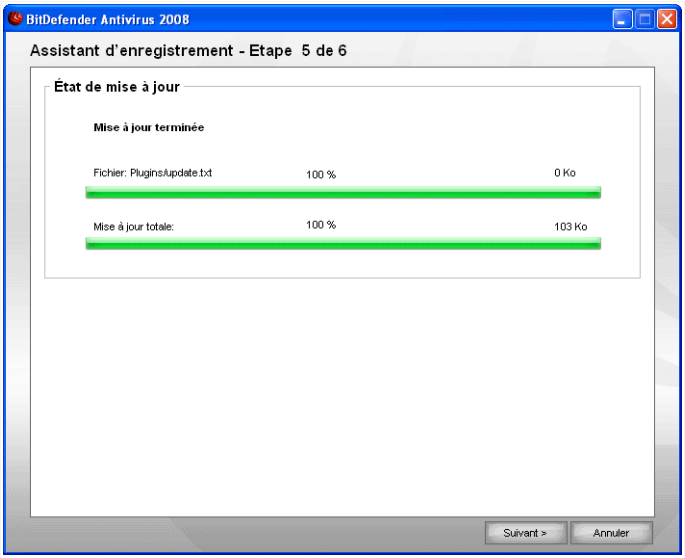
- **Mettre à jour les moteurs BitDefender (peut necéssiter un redémarrage)** - une mise à jour des moteurs de BitDefender aura lieu pendant la prochaine étape pour protéger votre ordinateur contre les dernières menaces.
- **Lancer une analyse rapide (peut necéssiter un redémarrage)** - Une analyse rapide sera lancée pendant la prochaine étape afin que BitDefender s'assure que les fichiers contenus dans le dossier `Windows` and `Program Files` ne sont pas infectés.
- **Lancer une analyse complète de l'ordinateur tous les jours à 02h00 -** Lance une analyse complète du système tous les jours à 02h00.

Important
Il est fortement recommandé d'activer ces options avant de passer à l'étape suivante pour assurer la sécurité de votre système.

Si vous sélectionnez uniquement la dernière option ou aucune option, vous passerez l'étape suivante.

Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.

1.3.5. Etape 5 sur 6 - Merci d'attendre la fin de la tâche

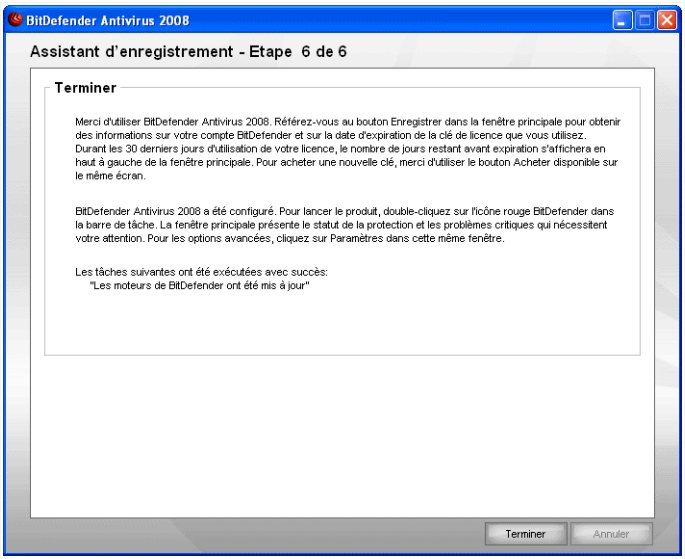


Etat d'avancement de la tâche

Merci d'attendre la fin de la tâche. Vous pouvez vérifier ici l'avancement de la tâche que vous avez sélectionnée lors de l'étape précédente.

Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.

1.3.6. Etape 6 sur 6 - Voir le récapitulatif



Terminer

Il s'agit de l'étape finale de l'assistant de configuration.

Cliquez sur **Terminer** pour terminer l'assistant et continuer avec l'installation du produit.

1.4. Mise à jour majeure

La procédure de mise à jour majeure peut se faire ainsi:

- **Installer sans désinstaller les versions précédentes - pour BitDefender v8 ou plus récent, sauf Internet Security**

  Double-cliquez sur le fichier d'installation et suivez l'assistant décrit dans la section « *Etapes d'installation* » (p. 3).

  Important
  Durant le processus d'installation, un message d'erreur causé par le `Filespy service`, apparaîtra. Cliquez sur **OK** pour continuer l'installation.

- **Désinstallez votre ancienne version et installez la nouvelle - pour toutes les versions BitDefender**

  En premier lieu, vous devez désinstaller la version précédente, redémarrer l'ordinateur et installer la nouvelle comme décrit dans la rubrique « *Etapes d'installation* » (p. 3).

  Important
  En cas de mise à niveau de BitDefender v8 ou supérieur, nous vous recommandons d'enregistrer les paramètres BitDefender, la Liste des amis et la Liste des spammeurs. Une fois le processus de mise à niveau terminé, vous pourrez les charger.

1.5. Réparer ou supprimer BitDefender

Si vous souhaitez réparer ou supprimer **BitDefender Antivirus 2008**, suivez le chemin suivant depuis le menu Démarrer de Windows: **Démarrer** → **Programmes** → **BitDefender 2008** → **Réparer ou supprimer**.

Il vous sera demandé une confirmation de votre choix en cliquant sur **Suivant**. Une nouvelle fenêtre apparaîtra dans laquelle vous pourrez choisir:

- **Réparer** - pour réinstaller tous les composants choisis lors de l'installation précédente.

  Important
  Avant la réparation du produit, nous vous recommandons d'enregistrer la Liste des amis et la Liste des spammeurs. Vous pouvez également enregistrer les paramètres BitDefender et la base de données bayesienne. Une fois le processus de réparation terminé, vous pourrez les télécharger à nouveau.

  Si vous décidez de réparer BitDefender, une nouvelle fenêtre s'affiche. Cliquez sur **Réparer** pour lancer le processus.

  Redémarrez l'ordinateur comme demandé puis cliquez sur **Installer** pour réinstaller BitDefender Antivirus 2008.

  Une fois l'installation achevée, une nouvelle fenêtre s'affiche. Cliquez sur **Terminer**.
- **Supprimer** - pour supprimer tous les composants installés.

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

  Si vous décidez de supprimer BitDefender, une nouvelle fenêtre s'affiche.

Important

Si vous supprimez BitDefender, votre ordinateur ne sera plus protégé contre les menaces de malwares, tels que les virus et les spywares. Si vous souhaitez activer Windows Defender une fois BitDefender désinstallé, cochez la case correspondante. Cette option est disponible uniquement sous Windows Vista.

Cliquez sur **Supprimer** pour désinstaller BitDefender Antivirus 2008 de votre ordinateur.

Pendant ce processus, votre avis vous sera demandé. Veuillez cliquer sur **OK** pour répondre à une enquête en ligne qui comprend seulement cinq petites questions. Si vous ne souhaitez pas répondre à cette enquête, cliquez simplement sur **Annuler**.

Une fois la désinstallation achevée, une nouvelle fenêtre s'affiche. Cliquez sur **Terminer**.

Note

A l'issue de la désinstallation, nous vous recommandons de supprimer le sous-répertoire `BitDefender` du répertoire `Program Files`.

Une erreur est survenue lors de la désinstallation de BitDefender

Si une erreur survient lors de la désinstallation de BitDefender, le processus est abandonné et une nouvelle fenêtre s'affiche. Cliquez sur **Exécuter l'outil de désinstallation** pour vérifier que BitDefender a bien été complètement supprimé. L'outil de désinstallation efface tous les fichiers ainsi que les clés d'enregistrement qui n'ont pas été supprimés lors de la désinstallation automatique.

Gestion de base

2. Pour commencer

Une fois BitDefender installé, votre ordinateur est protégé. Vous pouvez ouvrir le Centre de sécurité BitDefender à tout moment pour vérifier le statut de sécurité de votre système, prendre des mesures préventives ou configurer entièrement le produit.

Pour accéder au Centre de sécurité BitDefender, utilisez le menu Démarrer de Windows en suivant le chemin **Démarrer → Programmes → BitDefender 2008 → BitDefender Antivirus 2008** ou, plus rapide, en double cliquant sur l'**icône BitDefender** dans la barre d'état système.

Centre de sécurité BitDefender

Le Centre de sécurité BitDefender comporte deux zones:

- La zone **Statut**: contient des informations sur les problèmes de vulnérabilité de votre ordinateur en matière de sécurité et vous aide à les résoudre. Vous pouvez facilement voir combien de problèmes affectent votre ordinateur. En cliquant sur le bouton rouge correspondant **Corriger** les problèmes de vulnérabilité de votre ordinateur seront directement résolus ou le système vous guidera pour vous aider

à les résoudre facilement. Par ailleurs, quatre boutons de statut correspondant aux quatre niveaux de sécurité sont disponibles. Les boutons de statut verts indiquent qu'il n'y a pas de risque. Les boutons jaunes ou rouges indiquent des risques moyens ou élevés. Cliquez sur le bouton jaune/rouge, puis sur le bouton **Corriger** pour les supprimer un par un ou sur le bouton **Tout corriger**. Le bouton gris indique un composant non configuré.

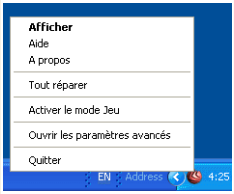
- La zone **Tâches prédéfinies** vous aide à prendre les mesures préventives indispensables à la protection de votre système et de vos données.

Le Centre de sécurité BitDefender comporte en outre de nombreux raccourcis utiles.

Lien	Description
Acheter	Ouvre une page où vous pouvez acheter le produit.
Mon compte	Ouvre la page de votre compte BitDefender.
Enregistrer	Ouvre l'assistant d'enregistrement.
Aide	Ouvre le fichier d'aide.
Support	Ouvre la page Web du support BitDefender.
Paramètres	Ouvre la console des paramètres avancés.
Historique	Ouvre une fenêtre présentant l'historique et les événements BitDefender.

2.1. Icône BitDefender dans la Barre d'Etat Système

Pour gérer l'intégralité du produit plus rapidement, vous pouvez aussi utiliser l'icône BitDefender située dans la barre d'état système.



Icône BitDefender

Double-cliquez sur cette icône pour ouvrir le Centre de sécurité BitDefender. Si vous effectuez un clic droit sur cette icône, le menu contextuel qui apparaît vous permettra de gérer le produit BitDefender plus rapidement.

- **Afficher** - ouvre le Centre de sécurité BitDefender.
- **Aide** - ouvre la documentation d'aide électronique.
- **À propos** - ouvre la page Web BitDefender.
- **Tout corriger** - vous aide à résoudre les problèmes de vulnérabilité de votre ordinateur en matière de sécurité.
- **Activer / désactiver Mode Jeu** - rendre le Mode jeu actif / incatif.
- **Ouvrir les paramètres avancés** - permet d'accéder à la console des paramètres avancés.
- **Mettre à jour** - effectue une mise à jour immédiate. Une nouvelle fenêtre apparaît affichant l'état de la mise à jour.
- **Quitter** - ferme l'application.

A chaque fois que le mode Jeu est activé, vous apercevez la lettre G sur l'icône BitDefender.

Si des problèmes majeurs affectent la sécurité de votre système, un point d'exclamation est affiché sur l'icône BitDefender. Passez votre souris sur l'icône pour voir le nombre de problèmes affectant la sécurité de votre système.

2.2. Barre d'analyse de l'activité

La **Barre d'analyse d'activité** est une visualisation graphique de l'analyse d'activité de votre système.

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

Barre d'activité

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**.

Vous pouvez utiliser la **Barre d'activité d'analyse** pour analyser des objets. Il vous suffit pour cela de faire glisser les objets que vous souhaitez analyser et de les déposer dans cette fenêtre.

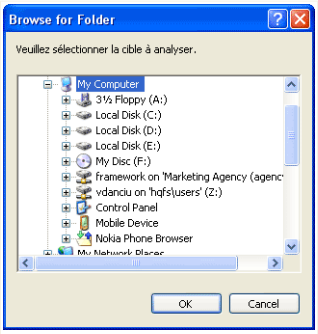
Note
Pour plus d'informations, reportez-vous à « *Analyse par glisser&déposer* » (p. 69).

Si vous ne souhaitez plus voir cette barre, il vous suffit de faire un clic-droit dessus et de choisir **Cacher**. Pour masquer complètement la fenêtre, cliquez sur **Avancé** dans la console des paramètres puis décochez la case **Activer la barre d'activité d'analyse (graphique d'activité du produit)**.

2.3. Analyse Manuelle BitDefender

Si vous souhaitez analyser rapidement un répertoire donné, vous pouvez utiliser l'analyse manuelle BitDefender

Pour accéder à l'Analyse Manuelle Bitdefender,suivez le chemin suivant depuis le menu Démarrer de Windows: **Démarrer** → **Programmes** → **BitDefender 2008** → **Analyse Manuelle BitDefender**. La fenêtre suivante apparaît:



Analyse Manuelle BitDefender

Il vous suffit de parcourir les répertoires, de sélectionner les répertoires souhaités et de cliquer sur **OK**. Le Scanner BitDefender apparaîtra et vous guidera à travers le processus d'analyse.

2.4. Mode Jeu

Le nouveau Mode Jeu modifie temporairement les paramètres de protection afin de minimiser leur impact sur les performances du système. Lorsque vous activez le Mode Jeu, les paramètres suivants sont appliqués :

- Toutes les alertes et pop-ups BitDefender sont désactivées.
- Le niveau de la protection en temps réel de BitDefender est paramétré en **Tolérant**.

A chaque fois que le mode Jeu est activé, vous apercevez la lettre `G` sur l'icône BitDefender.

2.4.1. Utiliser Mode Jeu

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

- Faites un Clic-droit sur l'icône BitDefender dans la barre d''tat et sélectionnez **Activer le Mode Jeu**.
- Pressez `Alt+G` (le raccourci clavier par défaut).

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

2.4.2. Changer le raccoruci clavier du Mode Jeu

Pour changer le raccourci clavier, suivez les étapes suivantes :

1. Cliquez sur **Paramètres** dans le BitDefender Security Center pour ouvrir la console de paramètrage.

   Note
   Vous pouvez également faire un clic-droit sur l'icône BitDefender dans la barre d'état et sélectionner **Ouvrir les paramètres avancés**.

2. Cliquez sur **Avancé**.
3. Sous l'option **Activer le raccourci clavier pour le Mode Jeu**, choisissez le raccourci souhaité :
   - 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
   Supprimer la case à côté de **Activer raccourci clavier pour le Mode Jeu** désactivera le raccourci.

3. Statut de sécurité

Le statut de sécurité affiche une liste organisée de façon systématique et facilement gérable regroupant les problèmes de vulnérabilité de votre ordinateur en matière de sécurité. BitDefender Antivirus 2008 vous avertit de tout problème pouvant affecter la sécurité de votre ordinateur.

Il existe quatre boutons liés au statut de sécurité :

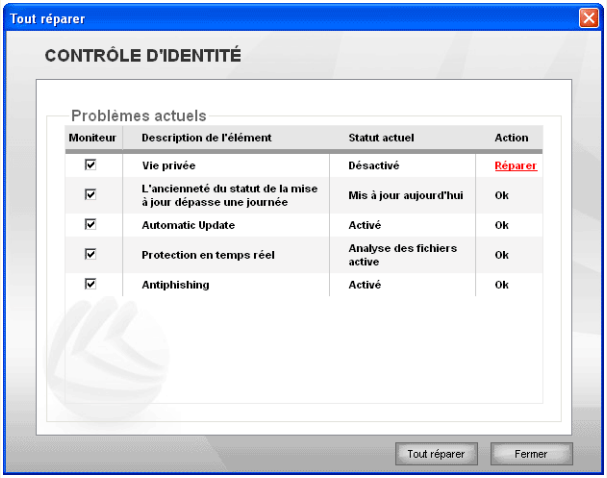
- **ANTIVIRUS**
- **ANTIPHISHING**
- **CONTROLE D'IDENTITE**
- **MISE A JOUR**

Par ailleurs, vous pouvez voir sur la gauche le nombre de problèmes affectant la sécurité de votre système et un bouton rouge **Tout corriger**.

Les quatre boutons de statut peuvent s'afficher en vert, jaune, rouge ou gris en fonction du niveau de protection en cours.

- **Vert** indique un risque faible pour votre ordinateur.
- **Jaune** indique un risque moyen pour votre ordinateur.
- **Rouge** indique un risque élevé pour votre ordinateur.
- **Gris** indique un composant non configuré.

Les problèmes de sécurité peuvent être facilement résolus par un simple clic sur le bouton **Tout corriger**. Une nouvelle fenêtre s'affiche.



Problèmes de sécurité

Vous verrez s'afficher la liste des problèmes de sécurité ainsi qu'une courte description de leur état.

Pour ne résoudre qu'un problème de sécurité spécifique, cliquez sur le bouton **Corriger** correspondant. Le problème sera soit directement résolu, soit résolu après avoir suivi les étapes d'un assistant. Si vous choisissez de résoudre tous les problèmes de sécurité, cliquez sur **Tout corriger** et suivez les étapes de l'assistant correspondant.

Si vous avez besoin d'aide supplémentaire, cliquez sur le bouton **Plus d'aide** qui se situe au bas de la fenêtre. Une page d'aide contextuelle contenant des informations précises sur ces problèmes et la solution pour les résoudre est affichée.

Important
Pour chaque problème, une case est cochée par défaut. Si vous ne souhaitez pas qu'un problème spécifique soit pris en compte lors de l'évaluation du niveau de risque, décochez la case correspondante. Veuillez utiliser cette option avec circonspection, il est très simple d'augmenter le niveau de risque auquel votre ordinateur est exposé.

Pour résoudre ces problèmes de sécurité ultérieurement, cliquez sur **Fermer**.

3.1. Bouton de statut de l'antivirus

Si le bouton du statut est vert, vous n'avez aucune inquiétude à avoir. S'il est jaune, rouge ou gris, cela signifie que votre ordinateur est exposé à un risque moyen ou élevé.

La couleur des boutons de statut peut se modifier non seulement lorsque vous configurez les paramètres pouvant affecter la sécurité de votre ordinateur, mais aussi si vous oubliez d'effectuer des tâches importantes. Si votre système n'a pas été analysé depuis longtemps, par exemple, le bouton du statut de sécurité est affiché en jaune. S'il ne l'a pas été depuis très longtemps, le bouton est affiché en rouge.

Le tableau ci-dessous vous indique quels sont les éléments pris en compte dans l'évaluation des risques de sécurité.

Problème de sécurité	*Couleur*
Votre système n'a pas été analysé depuis longtemps.	Jaune
Votre système n'a pas été analysé depuis très longtemps.	Rouge
La protection en temps réel est désactivée.	Rouge
Le niveau de protection antivirus est réglé sur Tolérant.	Jaune

Pour résoudre les problèmes de sécurité, suivez ces étapes:

1. Cliquez sur le bouton de statut de l'antivirus.
2. Cliquez soit sur les boutons **Corriger** pour les résoudre un à un, soit sur le bouton **Tout corriger** pour toutes les résoudre en un seul clic.
3. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

3.2. Bouton de statut de l'antiphishing

Si le bouton du statut est vert, vous n'avez aucune inquiétude à avoir. Par contre, si le bouton est rouge, votre ordinateur est exposé à un niveau de risque élevé.

Le tableau ci-dessous vous indique quels sont les éléments pris en compte dans l'évaluation des risques de sécurité.

Problème de sécurité	*Couleur*
La protection antiphishing est activée.	Vert

Problème de sécurité	Couleur
La protection antiphishing est désactivée.	Rouge

Pour résoudre les problèmes de sécurité, suivez ces étapes:

1. Cliquez sur le bouton de statut de l'antiphishing.
2. Cliquez soit sur les boutons **Corriger** pour les résoudre un à un, soit sur le bouton **Tout corriger** pour toutes les résoudre en un seul clic.
3. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

3.3. Statut du bouton de contrôle d'identité

Si le bouton du statut est vert, vous n'avez aucune inquiétude à avoir. Par contre, si le bouton est rouge ou gris, votre ordinateur est exposé à un niveau de risque élevé.

Le tableau ci-dessous vous indique quels sont les éléments pris en compte dans l'évaluation des risques de sécurité.

Problème de sécurité	Couleur
La protection de la confidentialité est configurée et activée	Vert
La protection de la confidentialité est configurée et désactivée	Rouge
La protection de la confidentialité n'est pas configurée	Gris

Pour résoudre les problèmes de sécurité, suivez ces étapes:

1. Cliquez sur le bouton du Contrôle d'Identité.
2. Cliquez soit sur les boutons **Corriger** pour les résoudre un à un, soit sur le bouton **Tout corriger** pour toutes les résoudre en un seul clic.
3. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

3.4. Bouton de statut des mises à jour

Si le bouton du statut est vert, vous n'avez aucune inquiétude à avoir. Par contre, si le bouton est rouge, votre ordinateur est exposé à un niveau de risque élevé.

Le tableau ci-dessous vous indique quels sont les éléments pris en compte dans l'évaluation des risques de sécurité.

Problème de sécurité	*Couleur*
Mise à jour automatique activée	Vert
La mise à jour automatique est désactivée.	Rouge
La dernière mise à jour remonte à un jour.	Rouge

Pour résoudre les problèmes de sécurité, suivez ces étapes:

1. Cliquez sur le bouton de statut des mises à jour.
2. Cliquez soit sur les boutons **Corriger** pour les résoudre un à un, soit sur le bouton **Tout corriger** pour toutes les résoudre en un seul clic.
3. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

4. Tâches prédéfinies

Sous les quatre boutons de statut se trouve la zone des **tâches prédéfinies**.

4.1. Sécurité

BitDefender comporte un module de Sécurité qui vous permet de maintenir votre système à jour et protégé contre les virus.

Pour accéder au module Sécurité, cliquez sur l'onglet **Sécurité**.

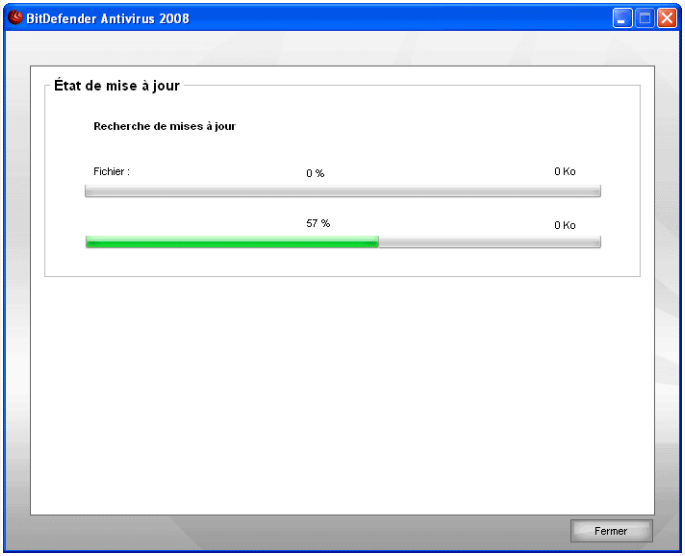
Voici les différents boutons proposés:

- **Mettre à jour** - effectue une mise à jour immédiate.
- **Analyser mes documents** - lance une analyse rapide de vos documents et paramètres.
- **Analyse approfondie du système** -lance une analyse approfondie de votre ordinateur (y compris des archives).
- **Analyse complète du système** -lance une analyse complète de votre ordinateur (hors archives).

4.1.1. Mettre à jour BitDefender

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.

Par défaut, BitDefender recherche des mises à jour au démarrage de votre PC puis **chaque heure** après cela. Cependant, si vous voulez mettre à jour BitDefender, cliquez juste sur **Mettre à jour**. Le processus de mise à jour débutera et la fenêtre suivante apparaîtra immédiatement :



Mettre à jour BitDefender

Dans cette fenêtre, vous pouvez voir le statut du processus de mise à jour.

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.

Si vous souhaitez fermer cette fenêtre, cliquez juste sur **Fermer**. Cependant, cela n'arrêtera pas le processus de mise à jour.

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.

Redémarrez votre ordinateur si nécessaire. En cas de mise à jour majeure, il vous sera demandé de redémarrer votre ordinateur. Si vous ne souhaitez plus être interrogé lorsqu'une mise à jour requiert un redémarrage, cochez **Attendre pour le redémarrage, plutôt que de demander**. Ainsi, la prochaine fois qu'une mise à jour nécessitera un redémarrage, le produit continuera à fonctionner avec les anciens fichiers jusqu'au redémarrage volontaire de votre système.

Cliquez sur **Redémarrer** pour redémarrer immédiatement votre système.

Si vous souhaitez redémarrer votre système plus tard, cliquez juste sur **OK**. Nous vous recommandons de redémarrer votre système dès que possible.

4.1.2. Analyser avec BitDefender

Pour analyser votre ordinateur contre les malwares, lancez une tâche particulière en cliquant sur le bouton correspondant. Le tableau ci-dessous affiche la liste des tâches disponibles, ainsi que leur description :

Tâche	Description
Analyser Mes Documents	Utilisez cette tâche pour analyser les dossiers importants de l'utilisateur actuel: `Mes documents`, `Bureau` et `Démarrage`. Celle assurera la sécurité de vos documents et de votre bureau, ainsi que le contrôle des applications se lançant au démarrage.
Analyse approfondie du système	Analyse l'ensemble du système. La configuration par défaut permet d'analyser tous les types de codes malicieux menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse complète du système	Analyse l'ensemble du système, mis à part les archives. La configuration par défaut permet d'analyser tous les types de codes malicieux menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.

Note

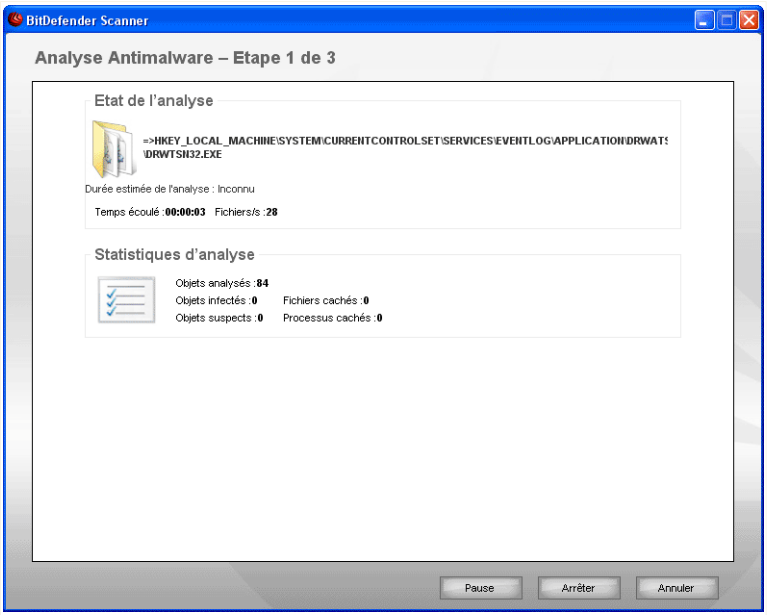
Sachant que les tâches d'**Analyse approfondie du système** et d'**Analyse complète du système** analysent l'intégralité du système, l'analyse peut prendre un certain temps. C'est pourquoi nous vous recommandons d'exécuter ces tâches en priorité faible ou, encore mieux, lorsque votre système est inactif.

Lorsque vous lancez un processus d'analyse sur demande, que ce soit une analyse rapide ou complète, le moteur d'analyse BitDefender apparaît.

Suivez cette procédure en trois étapes pour effectuer le processus d'analyse:

Étape 1 sur 3 - Analyse

BitDefender commence à analyser les objets sélectionnés.



Analyse en cours

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

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

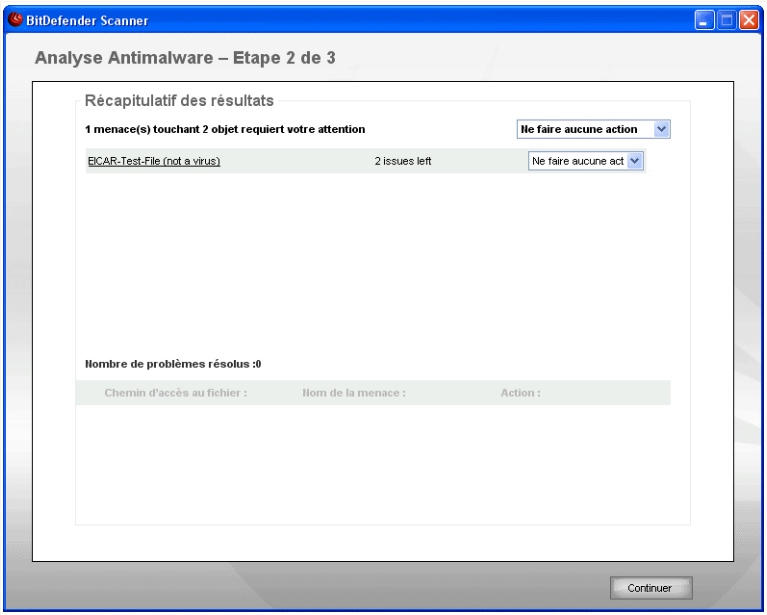
Pour suspendre temporairement le processus d'analyse, cliquez sur **Pause**. Pour reprendre l'analyse, cliquez sur **Reprendre**.

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.

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

Étape 2 sur 3 - Sélectionner des actions

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



Actions

Le nombre de problèmes de sécurité affectant votre système est indiqué.

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 chaque groupe de problèmes de sécurité ou sélectionner des actions spécifiques pour chaque problème.

Les options suivantes peuvent s'afficher dans le menu:

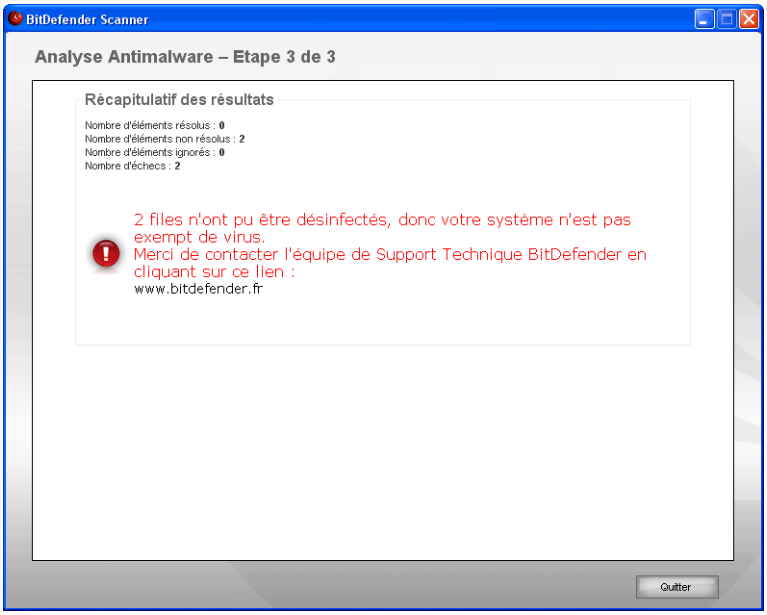
Action	Description
Ne pas mener d'action	Aucune action ne sera menée sur les fichiers détectés.

Action	Description
Désinfecter	Pour désinfecter un fichier infecté.
Supprimer	Supprime les fichiers détectés.
Démasquer	Rend les objets cachés visibles.

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

Étape 3 sur 3 - Voir les résultats

Une fois les problèmes de sécurité résolus par BitDefender, les résultats de l'analyse apparaissent dans une nouvelle fenêtre.



Récapitulatif

Le récapitulatif des résultats s'affiche. Le fichier rapport est sauvegardé automatiquement dans la rubrique Journaux de la fenêtre **Propriétés** de la tâche en question.

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

Cliquez sur **Quitter** pour fermer la fenêtre des résultats.

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. Cependant, il y a des problèmes qui ne peuvent pas être résolus.

Dans ces cas, nous vous recommandons de contacter le support BitDefender sur le site www.bitdefender.fr. Nos équipes du support technique vous aideront à résoudre les problèmes que vous rencontrez.

BitDefender a détecté des objets protégés par mot de passe

Les catégories protégées par mot de passe contiennent deux types d'objets : les archives et les installeurs. Ils ne représentent pas une réelle menace pour la sécurité de votre système à moins qu'ils ne contiennent des fichiers infectés et que ces derniers soient exécutés.

Pour être sur que ces objets ne soient pas infectés :

- Si l'objet protégé par mot de passe est une archive, veuillez extraire les fichiers qu'elle contient et les analyser séparément. La manière la plus simple pour les analyser est de faire un clic-droit sur ces fichiers et de sélectionner **BitDefender Antivirus 2008** à partir du menu.
- Si l'objet protégé par mot de passe est un installeur, vérifiez que la protection en temps réel est activée avant d'éxecuter l'installeur. Si l'installeur est infecté, BitDefender détectera et isolera l'infection.

Si vous ne voulez pas que ces objets soient détectés à nouveau par BitDefender, vous devez les ajouter comme exceptions lors du processus d'analyse. Pour ajouter des exceptions à l'analyse, cliquez sur **Paramètres** pour ouvrir l'interface des paramètres puis allez vers **Antivirus > Exceptions** .

Note
Pour plus d'informations, reportez-vous vers Objets exclus de l'analyse.

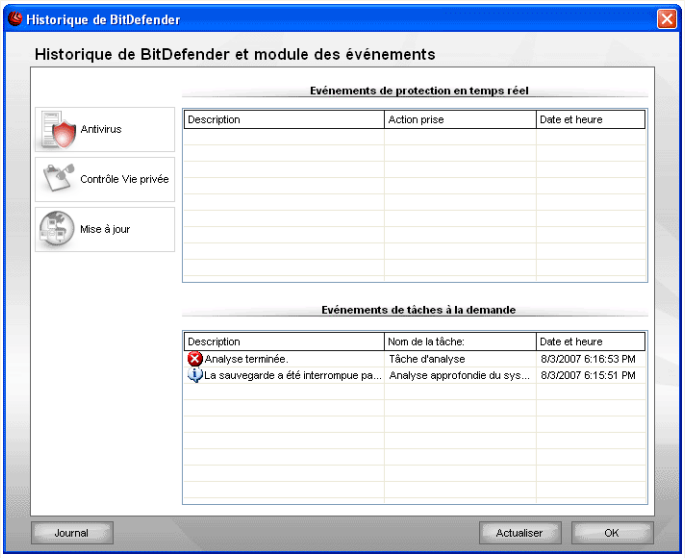
BitDefender a détecté des fichiers suspects

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

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

5. Historique

Le lien **Historique** situé dans la partie inférieure de la fenêtre du Centre de sécurité BitDefender permet d'ouvrir une autre fenêtre comportant l'historique et les événements BitDefender. Cette fenêtre vous offre une vue d'ensemble des événements relatifs à la sécurité. Elle vous permet, par exemple, de vérifier facilement qu'une mise à jour a bien été effectuée, de savoir si des codes malveillants ont été détectés sur votre ordinateur, si vos tâches de sauvegarde sont exécutées sans erreur, etc.



Evénements

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

- **Antivirus**
- **Contrôle Vie privée**
- **Mise à jour**

Une liste d'événements est proposée pour chaque catégorie. Chaque événement comporte les informations suivantes: une courte description de l'événement, l'action

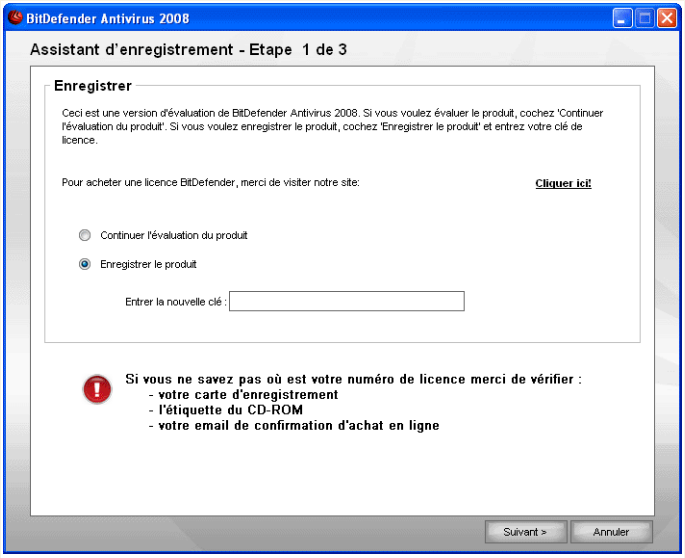
menée par BitDefender, la date et l'heure de l'événement. Pour obtenir plus d'informations sur un événement de la liste en particulier, double-cliquez sur cet événement.

Cliquez sur **Nettoyer le journal** pour supprimer les journaux anciens ou sur **Actualiser** pour vous assurer que les derniers journaux sont bien affichés.

6. Enregistrement du Produit

BitDefender Antivirus 2008 s'accompagne d'une période d'essai de 30 jours. Si vous voulez enregistrer votre produit BitDefender Antivirus 2008, changer la clé d'activation ou créer un compte BitDefender, cliquez sur le lien **Enregistrer** situé en haut de l'interface principale BitDefender. L'assistant d'enregistrement s'affichera.

6.1. Etape 1 sur 3 - Enregistrement de BitDefender Antivirus 2008



Récapitulatif

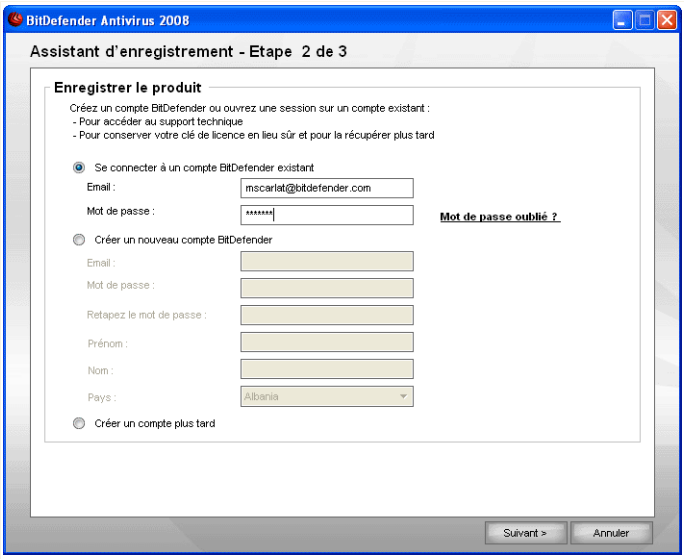
Si vous n'avez pas de licence BitDefender, cliquez sur le lien indiqué pour être redirigé vers la boutique en ligne BitDefender et acquerir une clé d'activation.

Pour enregistrer BitDefender Antivirus 2008, sélectionnez **Enregistrer le produit** et entrez la clé d'activation dans le champ **Entrer une nouvelle clé**.

Si la période d'essai n'est pas terminée et que vous souhaitez continuer à évaluer le produit, sélectionnez **Continuer l'évaluation du produit**.

Cliquez sur **Suivant**.

6.2. Etape 2 sur 3 - Création d'un compte BitDefender



Récapitulatif

Je n'ai pas de compte BitDefender

Pour bénéficier du support technique gratuit et d'autres services, il faut créer un compte BitDefender.

Note
Si vous voulez créer un compte plus tard, choisissez l'option correspondante.

Pour créer un compte BitDefender, sélectionnez **Créer un nouveau compte BitDefender** et entrez les informations demandées. Les informations communiquées ici resteront confidentielles.

- **E-mail** - Entrez votre adresse e-mail.
- **Mot de passe** - entrez un mot de passe pour votre compte BitDefender.

Note
Le mot de passe doit comporter au moins quatre caractères.

- **Retaper le mot de passe** - re-entrez le mot de passe choisi auparavant.
- **Prénom** - Entrez votre prénom.
- **Nom** - Entrez votre nom.
- **Pays** - sélectionnez le pays dans lequel vous vivez.

Note
Pour accéder à votre compte, connectez-vous sur http://myaccount.bitdefender.com et entrez l'adresse e-mail que vous avez fourni ainsi que votre mot de passe.

Pour créer votre compte vous devez d'abord activer votre adresse e-mail. Vérifiez votre messagerie et suivez les instructions reçues dans l'email qui vous a été envoyé par le service d'enregistrement BitDefender.

Cliquez sur **Suivant**.

J'ai déjà un compte BitDefender

BitDefender détectera automatiquement si vous avez déjà un compte BitDefender actif sur cet ordinateur. Dans ce cas, la seule chose que vous avez à faire est de cliquer sur **Suivant**.

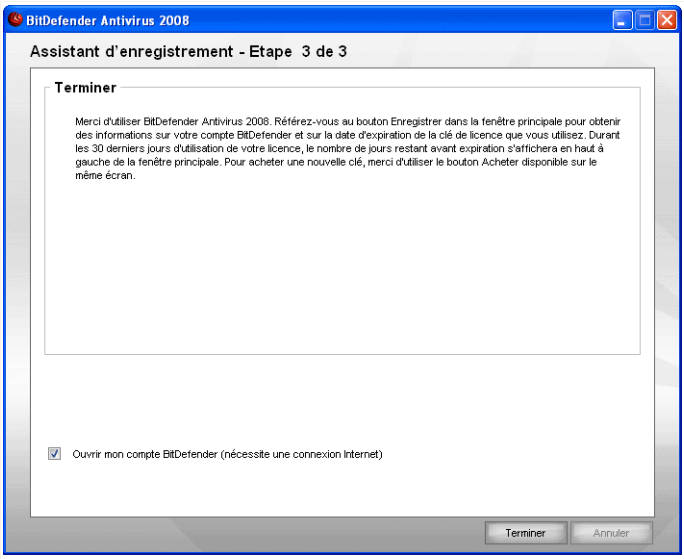
Si vous avez déjà un compte actif, mais que BitDefender ne le détecte pas, sélectionnez **Utiliser un compte BitDefender existant** et indiquez l'adresse e-mail et le mot de passe de votre compte.

Note
Si vous indiquez un mot de passe incorrect, il vous sera demandé de le resaisir lorsque vous cliquerez sur **Suivant**. Cliquez sur **OK** pour entrer de nouveau le mot de passe ou **Annuler** pour quitter l'assistant.

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

Cliquez sur **Suivant**.

6.3. Etape 3 sur 3 - Enregistrement de BitDefender Antivirus 2008



Récapitulatif

Sélectionnez **Ouvrir mon compte BitDefender** pour entrer votre compte BitDefender. Une connexion Internet est nécessaire.

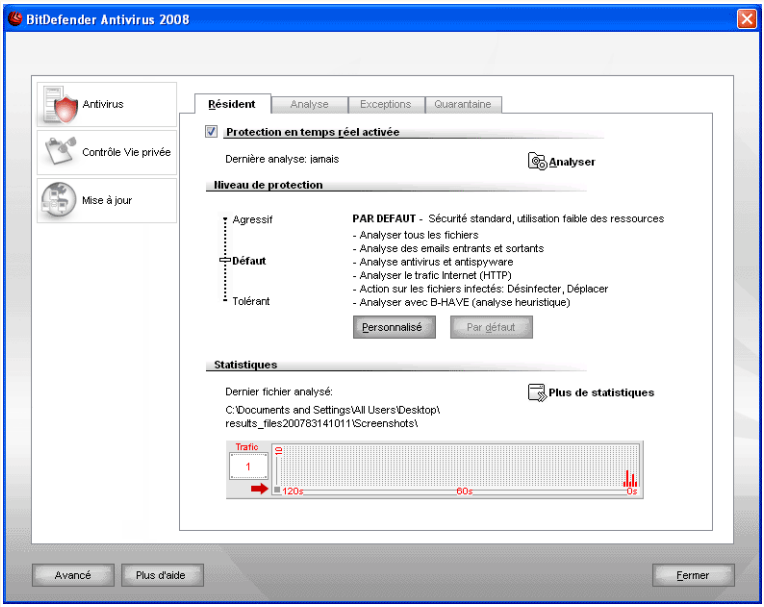
Cliquez sur **Terminer** pour fermer la fenêtre.

Gestion avancée de la sécurité

7. Pour commencer

BitDefender Antivirus 2008 comporte une console de paramètres centralisée qui permet la configuration et la gestion avancée de BitDefender.

Pour accéder à la console des paramètres, cliquez sur le lien **Paramètres** situé dans la partie inférieure du Centre de sécurité.



Console des paramètres

La console des paramètres est organisée par modules: **Antivirus**, **Contrôle Vie privée** et **Mise à jour**. Cela permet de gérer facilement BitDefender selon le type de problème de sécurité à traiter.

Sur la partie gauche de la console, vous pouvez sélectionner les modules suivants:

- Antivirus - pour accéder à la fenêtre de configuration de l'**Antivirus**.
- Contrôle Vie privée - dans cette section, vous pouvez configurer le module **Contrôle Vie privée**.

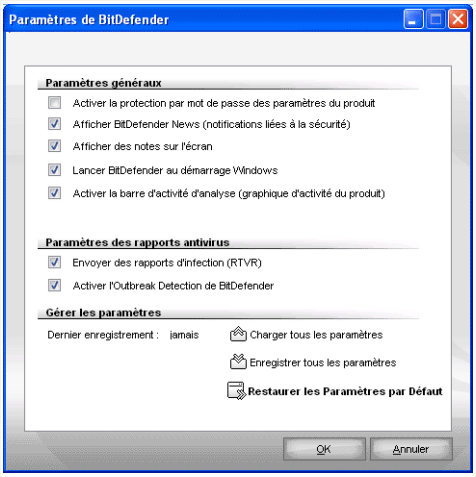
■ Mise à jour - pour accéder à la fenêtre de configuration des **Mises à jour**.

En bas de l'interface des paramètres se trouve un bouton **Plus d'aide** qui ouvre une page d'aide contextuelle. Cliquez sur ce bouton pour avoir plus d'informations sur la section dans laquelle vous vous trouvez, à chaque fois que vous avez besoin d'aide .

Si vous avez besoin d'aide supplémentaire, cliquez sur le bouton **Plus d'aide** qui se situe au bas de la fenêtre. Une page d'aide contextuelle s'affiche et vous apporte des informations précises sur la section dans laquelle vous vous trouvez.

7.1. Configuration des paramètres généraux

Pour configurer les paramètres généraux de BitDefender Antivirus 2008 et pour les gérer, cliquez sur **Avancé**. Une nouvelle fenêtre s'affiche.



Paramètres Généraux

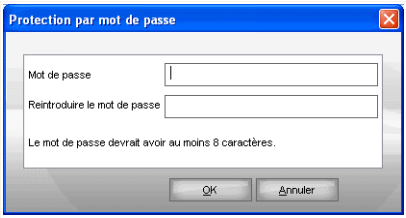
Vous pouvez dans cette rubrique paramétrer le fonctionnement de BitDefender. Par défaut, BitDefender est chargé au démarrage de Windows et se minimise automatiquement.

7.1.1. Paramètres Généraux

- **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.

  Si vous sélectionnez cette option, la fenêtre suivante apparaîtra :



Entrer le mot de passe

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

  Une fois le mot de passe paramétré, il vous sera demandé dès que vous voudrez changer 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.

- **Recevoir alertes de sécurité** - affiche régulièrement des informations de sécurité sur des risques de virus et/ou de failles, envoyées par les serveurs de BitDefender.
- **Afficher des notes sur l'écran** - affiche des fenêtres de notifications sur l'état de votre produit.
- **Lancer BitDefender au démarrage Windows** - lance automatiquement BitDefender au démarrage du système. Nous vous recommandons de garder cette option activée.
- **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.

- **Activer raccourci clavier pour le Mode Jeu** - permet d'utiliser une combinaison de touches clavier (raccourci) pour activer / désactiver le Mode Jeu. Le raccourci par défaut est `Alt+G`.

  Pour modifier le raccourci, suivez ces instructions :

  1. Cochez la combinaison que vous souhaitez utiliser : touche Contrôle (`Ctrl`), touche Shift (`Shift`) ou Alt (`Alt`).
  2. Dans le champ éditable, entrez la lettre que vous souhaitez utiliser.

7.1.2. Paramètres du rapport des virus

- **Envoyer des rapports de virus** - envoie aux BitDefender Labs des rapports concernant les virus identifiés sur vote ordinateur. Les informations envoyées nous servent à garder une trace des apparitions 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 le nom des virus et seront utilisées dans le seul but de 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.

7.1.3. Gérrer les paramètres

Utilisez les boutons **Enregistrer tous les paramètres** / **Charger tous les paramètres** pour sauvegarder / charger les paramètres établis pour BitDefender dans un endroit spécifié. Ainsi, vous pouvez utiliser les mêmes paramètres après la réinstallation ou la réparation de votre BitDefender.

Important
Seuls les utilisateurs ayant des droits administrateurs peuvent sauvegarder et charger les paramètres.

Pour charger les paramètres par défaut, cliquez sur **Restaurer les paramètres par défaut**.

8. Antivirus

BitDefender protège votre ordinateur contre tous les types de malware (virus, chevaux de Troie, spywares, rootkits, etc.).

Au-delà de l'analyse classique basée sur les signatures de codes malveillants, BitDefender effectue aussi une analyse heuristique des fichiers analysés. L'analyse heuristique a pour objectif d'identifier de nouveaux virus sur la base de certains modèles et algorithmes, avant qu'une définition de virus ne soit détectée. De faux messages d'alerte peuvent s'afficher. Lorsqu'un fichier de ce type est détecté, il est considéré comme étant suspect. Dans ce cas, nous vous recommandons de l'envoyer au laboratoire BitDefender pour analyse.

La protection offerte par BitDefender est divisée en deux catégories:

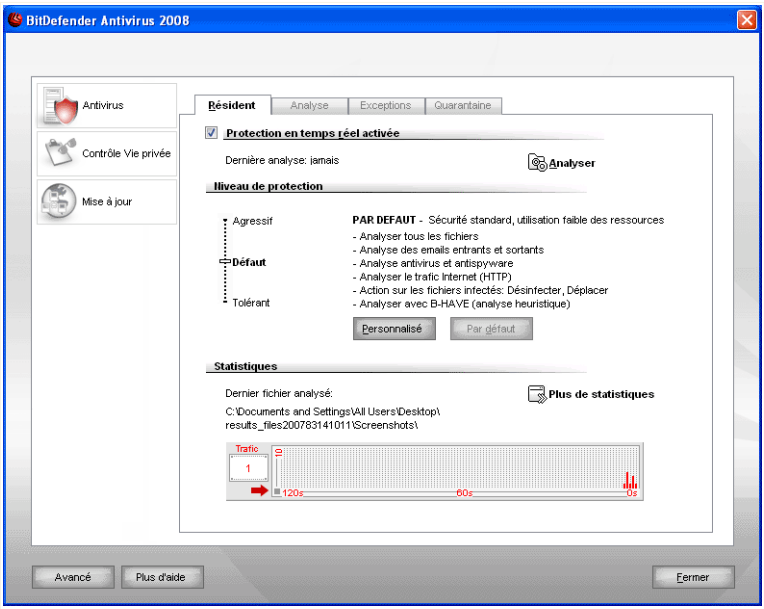
- **Analyse à l'accès** - empêche les nouveaux virus d'infecter votre ordinateur. Il s'agit d'un bouclier antivirus – les fichiers sont analysés au moment où l'utilisateur y accède. BitDefender analyse chaque fichier auquel un utilisateur accède ou copie sur le disque dur. BitDefender analysera par exemple un document Word quand vous l'ouvrez, et les e-mails lors de leur réception.
- **Analyse à la demande** - permet de détecter et de supprimer les malwares déjà présents dans votre 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.

La rubrique **Antivirus** de ce manuel d'utilisation contient les thèmes suivants:

8.1. Analyse à l'accès

L'analyse à l'accès, également appelée protection en temps réel, protège votre ordinateur 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).

Pour configurer et contrôler la protection en temps réel, cliquez sur **Antivirus > Résident** dans la console des paramètres. La fenêtre suivante apparaît:



Protection en temps réel.

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

Dans la partie inférieure de cette rubrique, vous pouvez voir les statistiques de **protection en temps réel** sur les fichiers et emails analysés. Cliquez sur **Plus de statistiques** si vous voulez ouvrir une fenêtre plus détaillée.

Pour lancer une analyse rapide du système, cliquez sur **Analyser**.

8.1.1. Configuration du niveau de protection

Vous pouvez choisir le niveau de protection qui répond le mieux à vos besoins de sécurité. Déplacez le curseur sur l'échelle pour choisir le niveau approprié.

Il existe trois niveaux de protection:

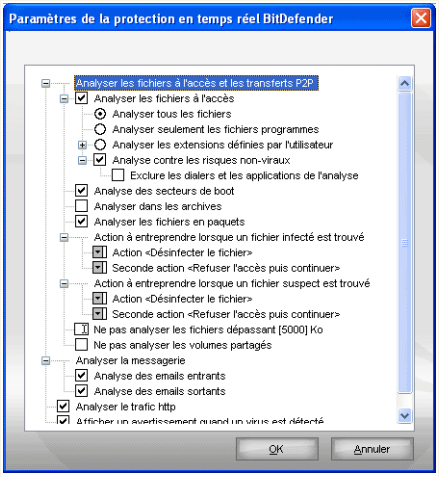
Niveau de protection	*Description*
Tolérant	Couvre les besoins de sécurité de base. La consommation de ressources système est très faible. Les programmes et emails entrants ne sont analysés que pour rechercher les virus. En plus de la recherche classique par signature, BitDefender utilise aussi un moteur d'analyse heuristique. Les actions prises contre les fichiers infectés sont les suivantes: nettoyer le fichier / refuser l'accès.
Défaut	Offre un niveau de sécurité standard. La consommation de ressources système est faible. Tous les fichiers et les emails entrants ou sortants sont analysés pour rechercher les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise aussi un moteur d'analyse heuristique. Les actions prises contre les fichiers infectés sont les suivantes: nettoyer le fichier / refuser l'accès.
Agressif	Offre un niveau de sécurité élevé. La consommation de ressources système est modérée. Tous les fichiers, les emails entrants ou sortants et le trafic Web, sont analysés pour rechercher les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise aussi un moteur d'analyse heuristique. Les actions prises envers les fichiers infectés sont les suivantes: nettoyer le fichier / refuser l'accès.

Pour appliquer les paramètres de protection en temps réel, cliquez sur **Par Défaut**.

8.1.2. Personnaliser le niveau de protection

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 personnaliser la **protection en temps réel** en cliquant sur **Niveau personnalisé**. La fenêtre suivante apparaîtra:



Configuration du résident

Les options d'analyse sont organisées en menus extensibles similaires à ceux utilisés dans l'explorateur Windows. Cliquez sur la case avec "+" pour ouvrir une option ou la case avec "-" pour fermer une option.

Note
Vous pourrez observer que certaines options d'analyse ne peuvent pas s'ouvrir, même si un signe "+" apparaît à leur côté. La raison est que ces options n'ont pas encore été sélectionnées. Si vous les cochez, elles pourront être ouvertes.

- Sélectionnez **Analyser à l'accès les fichiers et les transferts P2P** pour analyser les fichiers à l'accès ainsi que les communications et échanges Peer To Peer (messageries instantanées comme ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger – logiciels de téléchargement comme Kazaa, Emule, Shareaza). Après cela, sélectionnez le type de fichiers que vous voulez analyser.

Option		Description
Analyser les fichiers accédés	**Analyse de tous les fichiers**	Tous les fichiers à l'accès seront analysés, quel que soit leur type.
	Analyse des extensions à risques seulement	Seuls les fichiers avec les extensions suivantes seront analysés: `.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` et `.nws`.
	Analyse des extensions définies par l'utilisateur	Seuls les fichiers avec les extensions définies par l'utilisateur seront analysés. Ces extensions doivent être séparées par ";".
	Rechercher des riskware	Analyses contre les risques non-viraux Les fichiers détectés sont traités en tant que fichiers infectés. Un logiciel incluant des composants de type adware peut ne plus fonctionner si cette option est activée. Sélectionnez **Exclure les dialers et les applications de l'analyse** si vous souhaitez exclure ce genre de fichiers de l'analyse.
Analyse des secteurs de boot		Analyser les secteurs de boot du système.
Analyser dans les archives		Les archives seront également analysées. Avec cette option activée, l'ordinateur sera ralentit.
Analyser dans les fichiers compressés		Tous les fichiers compressés seront analysés.
Première action		Sélectionnez à partir du menu déroulant la première action à entreprendre sur les fichiers suspicieux et infectés.
	Interdire l'accès et continuer	Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.

Option		Description
	Désinfecter le fichier	Pour désinfecter un fichier infecté.
	Effacer le fichier	Supprime immédiatement les fichiers infectés, sans avertissement.
	Déplacer en quarantaine	Déplace les fichiers infectés dans la zone de quarantaine.
Deuxième action		Sélectionnez à partir du menu déroulant la deuxième action à entreprendre sur les fichiers infectés, au cas où la première action échoue.
	Interdire l'accès et continuer	Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.
	Effacer le fichier	Supprime immédiatement les fichiers infectés, sans avertissement.
	Déplacer en quarantaine	Déplace les fichiers infectés dans la zone de quarantaine.
Ne pas analyser les fichiers d'une taille supérieure à [x] Ko		Tapez la taille maximum des fichiers à analyser. Si vous mettez la taille à 0, tous les fichiers seront analysés.
Ne pas analyser les volumes partagés		Si cette option est activée, BitDefender n'analysera pas les volumes partagés, permettant un accès plus rapide au réseau. Nous vous recommandons d'activer cette option uniquement si le réseau dont fait partie votre ordinateur est protégé par un antivirus.

- **Analyser le trafic de messagerie** - analyse le trafic de la messagerie.

  Les options suivantes sont disponibles:

Option	Description
Analyser les emails entrants	Analyser tous les emails entrants.
Analyser les emails sortants	Analyser tous les emails sortants.

- **Analyser le trafic http** - analyse le trafic http.

- **Afficher une alerte si un virus est trouvé** - une fenêtre d'alerte sera affichée lorsqu'un virus sera détecté dans un fichier ou message e-mail.

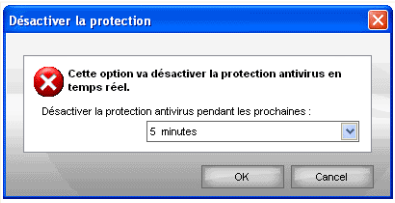
  Pour un fichier infecté, la fenêtre d'alerte contiendra le nom du virus, le chemin, l'action effectuée par BitDefender et un lien vers le site BitDefender où l'on peut trouver plus d'informations sur ce virus. Pour un message e-mail infecté, la fenêtre d'alerte contiendra également des informations sur l'expéditeur et le destinataire.

  Au cas où un fichier suspect est détecté vous pouvez lancer un assistant à partir de la fenêtre d'alerte qui vous aidera à envoyer ce fichier aux BitDefender Labs pour une analyse ultérieure. Vous pouvez saisir votre adresse email pour recevoir des informations sur ce rapport.

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

8.1.3. Désactivation de la protection en temps réel

Si vous tentez de désactiver la protection en temps réel, une fenêtre d'avertissement apparaît.



Désactiver la protection en temps réel

Vous devez confirmer votre choix en sélectionnant dans le menu la durée pendant laquelle vous souhaitez désactiver la protection en temps réel. Vous pouvez désactiver la protection en temps réel pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.

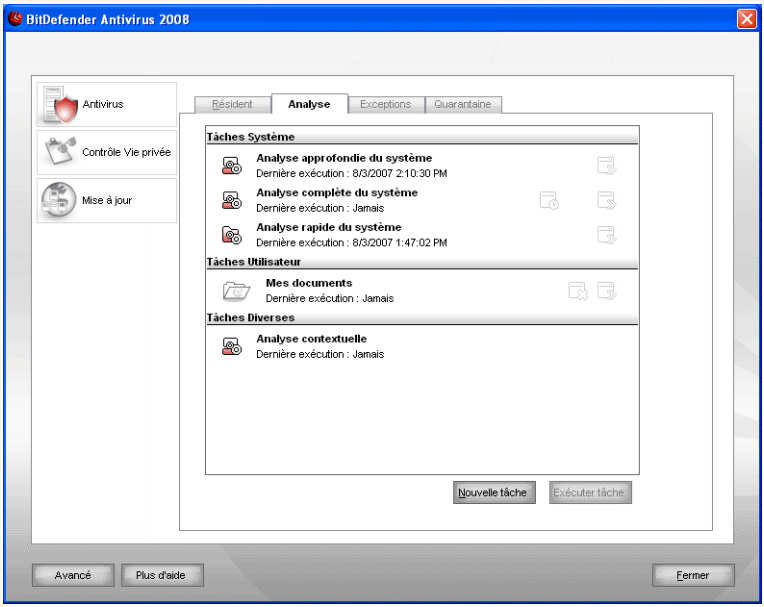
Avertissement
Cela peut poser un problème de sécurité important. Nous vous recommandons de désactiver la protection en temps réel pendant le moins de temps possible. Si la protection en temps réel est désactivée, vous ne serez pas protégé contre les menaces de codes malveillants.

8.2. Analyse à la demande

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

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

Pour configurer et lancer une analyse sur demande, cliquez sur **Antivirus > Analyse** dans la console des paramètres. La fenêtre suivante apparaît:



Tâches d'analyse

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.

8.2.1. Tâches d'analyse

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.

Chaque tâche comporte une fenêtre **Propriétés** vous permettant de configurer la tâche et d'afficher les résultats de l'analyse. Pour plus d'informations, reportez-vous à « *Configuration des tâches d'analyse* » (p. 57).

Il y a trois catégories de tâches d'analyse:

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

Tâche d'analyse par défaut	*Description*
Analyse approfondie du système	Analyse l'ensemble du système. La configuration par défaut permet d'analyser tous les types de codes malicieux menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse complète du système	Analyse l'ensemble du système, mis à part les archives. La configuration par défaut permet d'analyser tous les types de codes malicieux menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse rapide du système	Analyse les répertoires `Windows`,`Program Files` et `All Users`). La configuration par défaut permet d'analyser tous les types de codes malicieux, à l'exception des rootkits, mais ne permet pas d'analyser la mémoire, les registres et les cookies.

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.

Trois boutons sont disponibles à la droite de chaque tâche:

- **Planifier** - indique que la tâche sélectionnée est planifiée pour être exécutée ultérieurement. Cliquez sur ce bouton pour ouvrir la fenêtre **Propriétés** et l'onglet Planificateur permettant d'afficher la tâche planifiée et de la modifier.
- **Supprimer** - supprime la tâche selectionnée.

  Note
  Option non disponible pour les tâches d'analyse du système. Vous ne pouvez pas supprimer une tâche d'analyse du système.

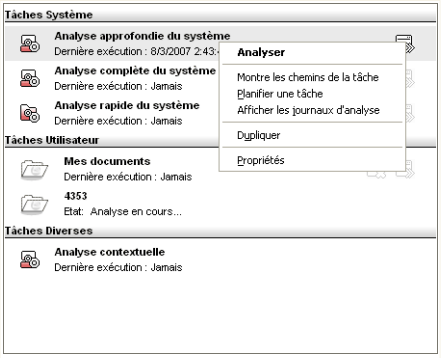
- **Analyser** - lance la tâche selectionnée, démarrant ainsi une analyse immédiate.

A la gauche de chaque tâche vous pouvez voir le bouton **Propriétés**, dans lesquelles vous pouvez configurer une tâche ou voir le rapport d'analyse.

8.2.2. Utilisation du menu de raccourcis

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

Les commandes suivantes sont disponibles dans le menu de raccourcis:



Menu de raccourci

- **Lancer l'analyse** - démarre immédiatement la tâche d'analyse choisie.
- **Changer le chemin d'analyse** - ouvre la fenêtre **Propriétés** et l'onglet Cible permettant de modifier la cible à analyser de la tâche sélectionnée.

Note
Dans le cas d'une tâche système, cette option est remplacée par **Montrer le chemin de la tâche**, car vous ne pouvez voir que la cible d'analyse.

- **Planifier la tâche** - ouvre la fenêtre **Propriétés** et l'onglet Planificateur permettant de planifier la tâche sélectionnée.
- **Afficher les journaux d'analyse** - ouvre la fenêtre **Propriétés**, l'onglet Journaux, où vous pouvez consulter les rapports générés après l'éxécution des tâches sélectionnées.
- **Dupliquer** - duplique une tâche sélectionnée.

Note
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
Option non disponible pour les tâches d'analyse du système. Vous ne pouvez pas supprimer une tâche d'analyse du système.

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

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

8.2.3. Création de tâches d'analyse

Pour créer une tâche d'analyse, utilisez l'une des méthodes suivantes:

- Dupliquez une tâche existante, renommez-la et effectuez les modifications nécessaires dans la fenêtre Propriétés.
- **Nouvelle tâche**: permet de créer une nouvelle tâche et de la configurer.

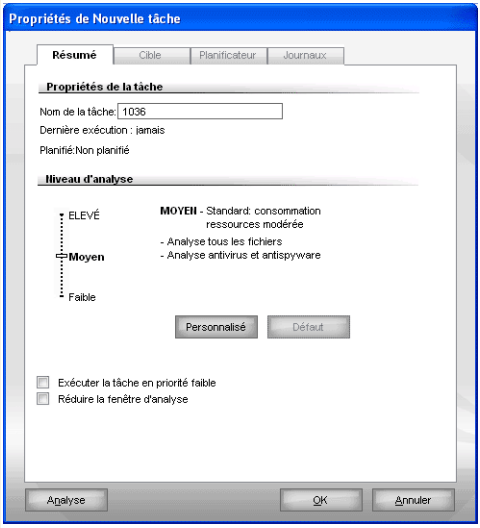
8.2.4. Configuration des tâches d'analyse

Chaque tâche d'analyse dispose de sa propre fenêtre de **Propriétés**, dans laquelle vous pouvez configurer les options d'analyse, définir les éléments à analyser, programmer une tâche ou voir le rapport. Pour ouvrir cette fenêtre, cliquez sur le bouton **Ouvrir** , situé à droite de la tâche (ou cliquez sur la tâche avec le bouton droit de la souris puis sélectionnez **Ouvrir**.

Note
Pour plus d'informations sur l'affichage des journaux et sur l'onglet **Journaux**, reportez-vous à « *Afficher les journaux d'analyse* » (p. 75).

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**. La fenêtre suivante apparaît:



Vue d'ensemble

Vous trouverez dans cette rubrique les informations concernant les tâches (nom, dernière analyse, planification) et aurez la possibilité de définir les paramètres d'analyse.

Sélection du niveau d'analyse

Vous pouvez facilement configurer les paramètres d'analyse en sélectionnant le niveau d'analyse. Déplacez le curseur sur l'échelle pour définir le niveau d'analyse approprié.

Il y a 3 niveaux d'analyse:

Niveau de protection	*Description*
Basse	Offre un niveau de détection correct. La consommation de ressources est faible. Seuls les programmes sont scannés pour détecter les virus. En plus de la recherche classique par signature, BitDefender utilise un moteur d'analyse heuristique.

Niveau de protection	Description
Moyenne	Offre un niveau de détection efficace. La consommation de ressources système est modérée. Tous les fichiers sont scannés pour détecter les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise un moteur d'analyse heuristique.
Agressif	Offre un niveau de détection élevé. La consommation de ressources système est élevée. Tous les fichiers et les fichiers archives sont scannés pour détecter les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise un moteur d'analyse heuristique.

Une série d'options générales de paramétrage de l'analyse sont également disponibles:

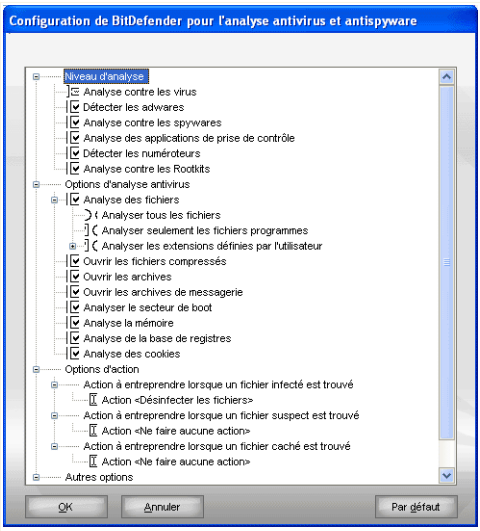
Option	Description
Exécuter la tâche d'analyse avec une priorité basse	Diminue la priorité du processus d'analyse. Vous allez permettre aux autres logiciels de s'exécuter à une vitesse supérieure en augmentant le temps nécessaire pour que l'analyse soit finie.
Réduire la fenêtre d'analyse au démarrage dans la barre d'état système	Réduit la fenêtre d'analyse dans la barre d'état système. Double-cliquez sur l'icône de BitDefender pour l'ouvrir.

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

Personnalisation du niveau d'analyse

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.

Cliquez sur **Personnalisé** pour définir vos propres options d'analyse. Une nouvelle fenêtre est alors affichée.



Options d'analyse

Les options d'analyse sont organisées en menus extensibles similaires à ceux utilisés dans l'explorateur Windows. Cliquez sur la case avec "+" pour ouvrir une option ou la case avec "-" pour fermer une option.

Les options d'analyse sont groupées en quatre catégories:

- **Niveau d'analyse**
- **Options d'analyse des virus**
- **Options d'action**
- **Autres options**

- Spécifiez le type de codes malicieux que vous souhaitez que BitDefender analyse en sélectionnant les options correspondantes dans la catégorie **Niveau d'analyse**.

  Les options suivantes sont disponibles:

Option	Description
Analyse antivirus	Analyse les virus connus. BitDefender détecte également les corps de virus incomplets, permettant ainsi d'écarter toute menace potentielle pouvant affecter la sécurité de votre système.
Détecter les adwares	Analyse les menaces d'adwares. Les fichiers détectés sont traités en tant que fichiers infectés. Un logiciel incluant des composants de type adware peut ne plus fonctionner si cette option est activée.
Rechercher les spywares	Analyse les menaces de spywares connus. Les fichiers détectés sont traités en tant que fichiers infectés.
Analyse des applications	Analyse les applications (fichiers `.exe` et `.dll`).
Détecter les numéroteurs	Analyse les applications qui appellent des numéros surtaxés. Les fichiers détectés sont traités en tant que fichiers infectés. Un logiciel incluant des composants de type numéroteur peut ne plus fonctionner si cette option est activée.
Analyse des rootkits	Analyse les objets cachés (fichiers et processus), plus connus sous le nom de rootkits.

- Spécifiez le type d'objets à analyser (archives, emails et autres) ainsi que d'autres options. Cela se fait par la sélection de certaines options dans la catégorie **Options d'analyse des virus**.

  Les options suivantes sont disponibles:

Option		Description
Analyser les fichiers	**Analyse de tous les fichiers**	Tous les fichiers seront analysés à l'accès, quel que soit leur type.
	Analyse des extensions à risques seulement	Seuls les fichiers avec les extensions suivantes seront analysés: `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`;

Option		Description
		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 et nws.
	Analyse des extensions définies par l'utilisateur	Seuls les fichiers avec les extensions définies par l'utilisateur seront analysés. Ces extensions doivent être séparées par ";".
Ouvrir les fichiers compressés		Analyser les fichiers compressés.
Ouvrir les fichiers archives		Analyser l'intérieur des fichiers archives.
Ouvrir les archives de messagerie		Analyser dans les archives de messagerie.
Analyser les secteurs de boot		Analyser les secteurs de boot du système.
Analyse de la mémoire		Analyser la mémoire pour détecter les virus et les autres malwares.
Analyse de la base de registre		Analyse les entrées du Régistre.
Analyse des cookies		Analyse les cookies.

- Spécifiez les actions à mener sur les fichiers infectés, suspects ou cachés détectés dans la catégorie **Options d'action**. Vous pouvez spécifier une action différente pour chaque catégorie.
  - Sélectionnez l'action à mener sur les fichiers infectés détectés. Les options suivantes sont disponibles:

Action	Description
Aucune	Aucune action ne sera prise sur les fichiers infectés. Ceux-ci vont apparaître dans le fichier des rapports.
Désinfecter	Pour désinfecter un fichier infecté.
Effacer	Supprime immédiatement les fichiers infectés, sans avertissement.
Déplacer en quarantaine	Déplace les fichiers infectés dans la zone de quarantaine.

- Sélectionnez l'action à mener sur les fichiers suspects détectés. Les options suivantes sont disponibles:

Action	Description
Aucune	Aucune action ne sera menée sur les fichiers suspects. Ces fichiers apparaîtront dans le fichier d'état.
Effacer	Supprime immédiatement les fichiers suspects, sans avertissement.
Déplacer en quarantaine	Déplace les fichiers suspects dans la zone de quarantaine.

Note
Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique. Nous vous recommandons de les envoyer au laboratoire BitDefender.

- Sélectionnez l'action à mener sur les objets cachés (rootkits) détectés. Les options suivantes sont disponibles:

Action	Description
Aucune	Aucune action ne sera menée sur les fichiers cachés. Ces fichiers apparaîtront dans le fichier d'état.
Déplacer en quarantaine	Déplace les fichiers cachés dans la zone de quarantaine.
Rendre visible	Affiche les fichiers cachés pour vous permettre de les visualiser.

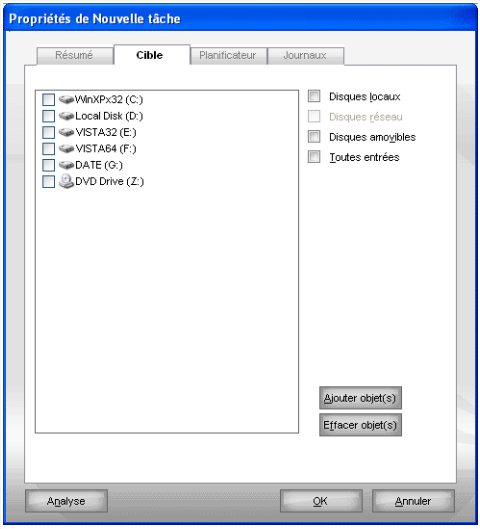
Note
Si vous choisissez d'ignorer les fichiers détectés ou si l'action sélectionnée échoue, vous devrez sélectionner une action dans l'assistant d'analyse.

- Pour être invité à envoyer tous les fichier suspects au laboratoire BitDefender une fois le processus d'analyse terminé, cliquez sur **Soumettre les fichiers suspects au laboratoire BitDefender** dans la catégorie **Autres options**.

Si vous cliquez sur **Défaut** vous chargerez les paramètres par défaut. Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

Définition de la cible à analyser

Pour définir la cible à analyser d'une tâche d'analyse spécifique, faites un clic droit sur la tâche et sélectionnez **Cible**. La fenêtre suivante apparaît:



Analyser la cible

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.

Cette partie contient les boutons suivants:

- **Ajouter éléments** - ouvre une fenêtre permettant de sélectionner les fichiers/dossiers que vous souhaitez analyser.

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

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

Note
Seuls les fichiers/dossiers rajoutés après peuvent être effacés, pas ceux automatiquement "proposés" par BitDefender.

Ces options permettent une sélection rapide des cibles d'analyses.

- **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.

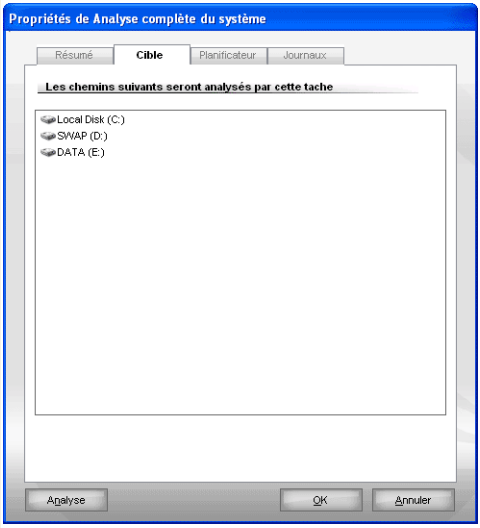
Note
Si vous voulez analyser l'ensemble de votre ordinateur, cochez la case **Toutes les entrées**.

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

Voir les cibles d'analyse des tâches systèmes.

Vous ne pouvez pas modifier la cible à analyser des tâches d'analyse depuis 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, faîtes un clic-droit sur la tâche et sélectionnez **Voir les chemins de la tâche**. Pour **Analyse complète du système**, par exemple, la fenêtre suivante apparaîtra :



Analyser la cible de l'analyse complète du système

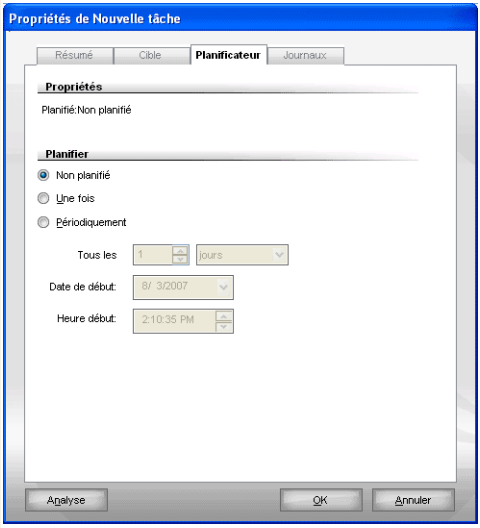
Analyse complète du système et **Analyse approfondie du système** analysera tous les disques locaux, alors que **Analyse rapide du système** analysera uniquement le répertoire `Windows` et `Program Files`.

Cliquez sur **OK** pour fermer la fenêtre. Pour exécuter la tâche, cliquez juste 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 afficher la planification d'une tâche spécifique ou la modifier, faites un clic droit sur la tâche et sélectionnez **Planifier**. La fenêtre suivante apparaît:



Planificateur

La tâche planifiée s'affiche, le cas échéant.

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

- **Non planifiée** - 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**.
- Si vous souhaitez que l'analyse soit répétée à intervalle régulier, cochez la case **Périodiquement**.

  Si vous voulez que l'analyse se répète à intervalle régulier, cochez la case **Périodiquement** et précisez dans les champs prévus minutes/heures/jours/semaines/mois/années. Vous devez également déterminer la date de début et de fin dans le champ **Date de début/Heure**.

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

8.2.5. Analyse des objets

Avant de lancer un processus d'analyse, assurez-vous que BitDefender est à jour dans les signatures de codes malveillants. L'analyse de votre ordinateur au moyen d'une base de données de signatures obsolète pourrait empêcher BitDefender de détecter les nouveaux codes malveillants à rechercher depuis la dernière mise à jour. Pour vérifier la date de la dernière mise à jour, cliquez sur **Mise à jour > Mise à jour** dans la console des paramètres.

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

Méthodes d'analyse

BitDefender permet quatre types d'analyse à la demande:

- Analyse immediate - lance une tâche d'analyse depuis les tâches disponibles.
- Analyse contextuelle - faîtes un clic-droit sur un fichier ou répertoire et sélectionnez BitDefender Antivirus 2008;
- Analyse par glisser-déposer - glissez & déposez un fichier ou un répertoire sur la barre d'analyse d'activité.
- Analyse manuelle - utilisez l'analyse manuelle BitDefender pour sélectionner directement les fichiers ou répertoires que vous souhaitez analyser.

Analyse immédiate

Vous pouvez analyser tout ou partie de votre ordinateur en exécutant les tâches d'analyse par défaut ou vos propres tâches d'analyse. Cela s'appelle l'analyse immédiate.

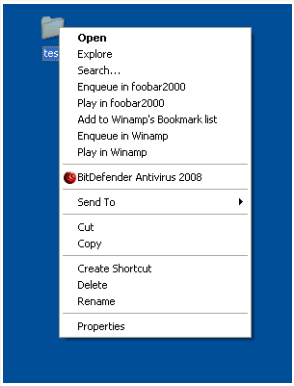
Pour exécuter une tâche d'analyse, utilisez l'une des méthodes suivantes:

- Double-cliquez sur la tâche d'analyse souhaitée dans la liste.
- Cliquez sur le bouton **Analyser** correspondant à la tâche.
- Sélectionnez la tâche, puis cliquez sur **Exécuter la tâche**.

Lorsque le moteur d'analyse BitDefender apparaît, l'analyse est lancée. Pour plus d'informations, reportez-vous à « *Moteur d'analyse BitDefender* » (p. 70).

Analyse contextuelle

Pour analyser un fichier ou un dossier sans configurer de nouvelle tâche d'analyse, vous pouvez utiliser le menu contextuel. Cela s'appelle l'analyse contextuelle.



Analyse contextuelle

Faîtes un clic-droit sur le fichier ou répertoire que vous souhaitez analyser et sélectionnez l'option **BitDefender Antivirus 2008**.

Lorsque le moteur d'analyse BitDefender apparaît, l'analyse est lancée. Pour plus d'informations, reportez-vous à « *Moteur d'analyse BitDefender* » (p. 70).

Vous pouvez modifier les options d'analyse et voir les fichiers de rapport à partir de la fenêtre **Propriétés** de la tâche **Analyse via le menu contextuel**.

Analyse par glisser&déposer

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

Lorsque le moteur d'analyse BitDefender apparaît, l'analyse est lancée. Pour plus d'informations, reportez-vous à « *Moteur d'analyse BitDefender* » (p. 70).

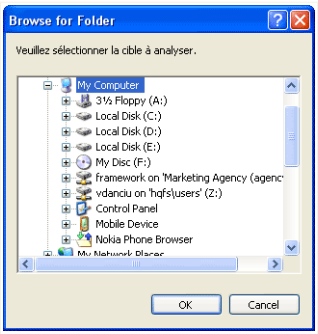
Analyse manuelle

L'analyse manuelle consiste à sélectionner directement les fichiers ou répertoires que vous souhaitez analyser avec l'option d'analyse manuelle Bitdefender disponible depuis le menu Démarrer de Windows dans le groupe de programme BitDefender.

> ***Note***
> L'analyse manuelle est très pratique car elle peut également être effectuée lorsque Windows est en mode sans échec.

Pour sélectionner les fichiers ou répertoires que BitDefender doit analyser, suivez le chemin suivant depuis le menu Démarrer de Windows: **Démarrer → Programmes → BitDefender 2008 → Analyse manuelle BitDefender**.

La fenêtre suivante apparaît:



Analyse manuelle

Choisissez les fichiers ou répertoires que vous souhaitez analyser et cliquez sur **OK**.

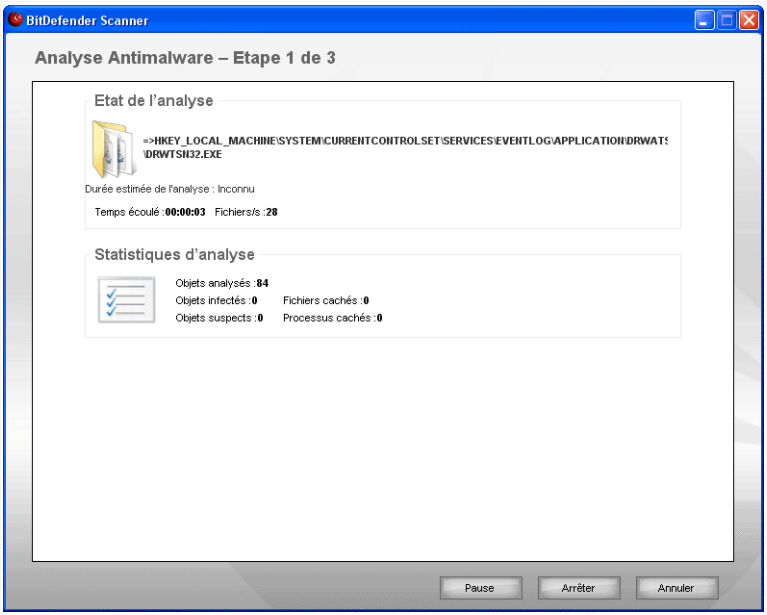
Lorsque le moteur d'analyse BitDefender apparaît, l'analyse est lancée. Pour plus d'informations, reportez-vous à « *Moteur d'analyse BitDefender* » (p. 70).

Moteur d'analyse BitDefender

Lorsque vous lancez un processus d'analyse sur demande, le moteur d'analyse BitDefender apparaît. Suivez cette procédure en trois étapes pour effectuer le processus d'analyse:

Étape 1 sur 3 - Analyse

BitDefender commence à analyser les objets sélectionnés.



Analyse en cours

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

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

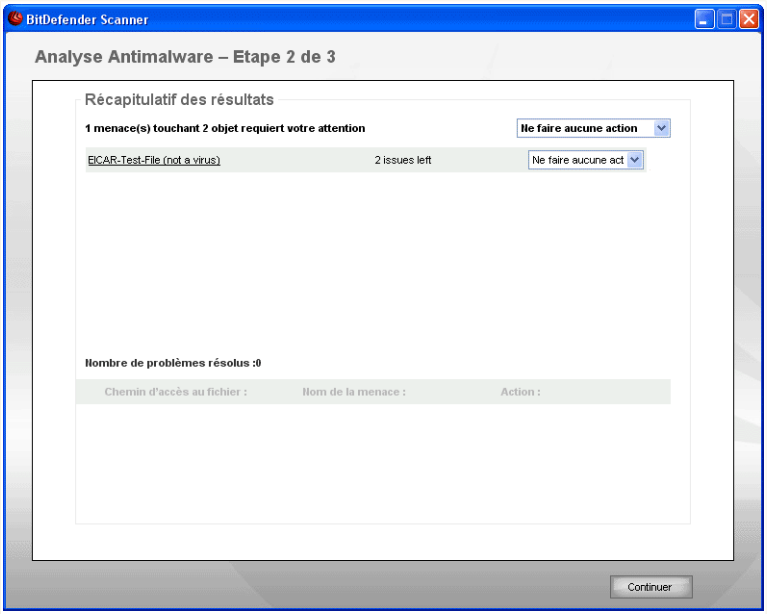
Pour suspendre temporairement le processus d'analyse, cliquez sur **Pause**. Pour reprendre l'analyse, cliquez sur **Reprendre**.

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.

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

Étape 2 sur 3 - Sélectionner des actions

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



Actions

Le nombre de problèmes de sécurité affectant votre système est indiqué.

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 chaque groupe de problèmes de sécurité ou sélectionner des actions spécifiques pour chaque problème.

Les options suivantes peuvent s'afficher dans le menu:

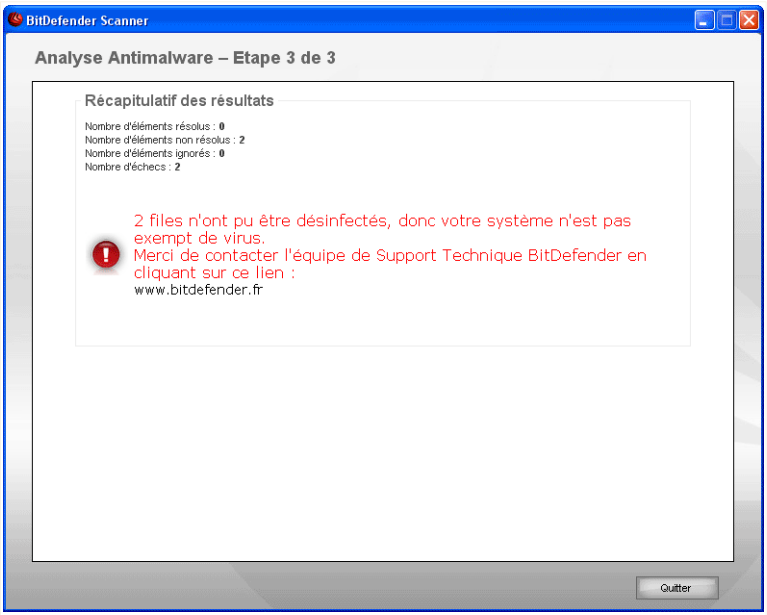
Action	*Description*
Ne pas mener d'action	Aucune action ne sera menée sur les fichiers détectés.

Action	Description
Désinfecter	Pour désinfecter un fichier infecté.
Supprimer	Supprime les fichiers détectés.
Démasquer	Rend les objets cachés visibles.

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

Étape 3 sur 3 - Voir les résultats

Une fois les problèmes de sécurité résolus par BitDefender, les résultats de l'analyse apparaissent dans une nouvelle fenêtre.



Récapitulatif

Le récapitulatif des résultats s'affiche. Le fichier rapport est sauvegardé automatiquement dans la rubrique Journaux de la fenêtre **Propriétés** de la tâche en question.

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

Cliquez sur **Quitter** pour fermer la fenêtre des résultats.

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. Cependant, il y a des problèmes qui ne peuvent pas être résolus.

Dans ces cas, nous vous recommandons de contacter le support BitDefender sur le site www.bitdefender.fr. Nos équipes du support technique vous aideront à résoudre les problèmes que vous rencontrez.

BitDefender a détecté des objets protégés par mot de passe

Les catégories protégées par mot de passe contiennent deux types d'objets : les archives et les installeurs. Ils ne représentent pas une réelle menace pour la sécurité de votre système à moins qu'ils ne contiennent des fichiers infectés et que ces derniers soient exécutés.

Pour être sur que ces objets ne soient pas infectés :

- Si l'objet protégé par mot de passe est une archive, veuillez extraire les fichiers qu'elle contient et les analyser séparément. La manière la plus simple pour les analyser est de faire un clic-droit sur ces fichiers et de sélectionner **BitDefender Antivirus 2008** à partir du menu.
- Si l'objet protégé par mot de passe est un installeur, vérifiez que la protection en temps réel est activée avant d'exécuter l'installeur. Si l'installeur est infecté, BitDefender détectera et isolera l'infection.

Si vous ne voulez pas que ces objets soient détectés à nouveau par BitDefender, vous devez les ajouter comme exceptions lors du processus d'analyse. Pour ajouter des exceptions à l'analyse, cliquez sur **Paramètres** pour ouvrir l'interface des paramètres puis allez vers **Antivirus > Exceptions** .

Note
Pour plus d'informations, reportez-vous vers Objets exclus de l'analyse.

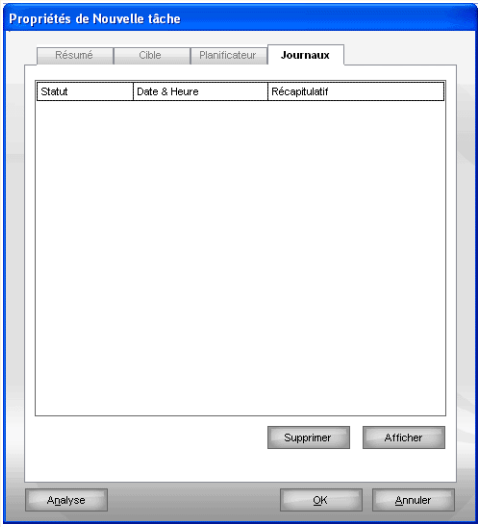
BitDefender a détecté des fichiers suspects

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.

8.2.6. Afficher les journaux d'analyse

Pour afficher les résultats de l'analyse une fois la tâche exécutée, faites un clic droit sur la tâche et sélectionnez **Journaux**. La fenêtre suivante apparaît:



Journaux d'analyse

Vous pouvez consulter ici les fichiers de rapport générés à chaque fois que la tâche était exécutée.

Pour chaque fichier, vous obtenez des informations sur l'état du processus d'analyse, la date et l'heure de l'analyse et un résumé des résultats de l'analyse.

Deux boutons sont disponibles:

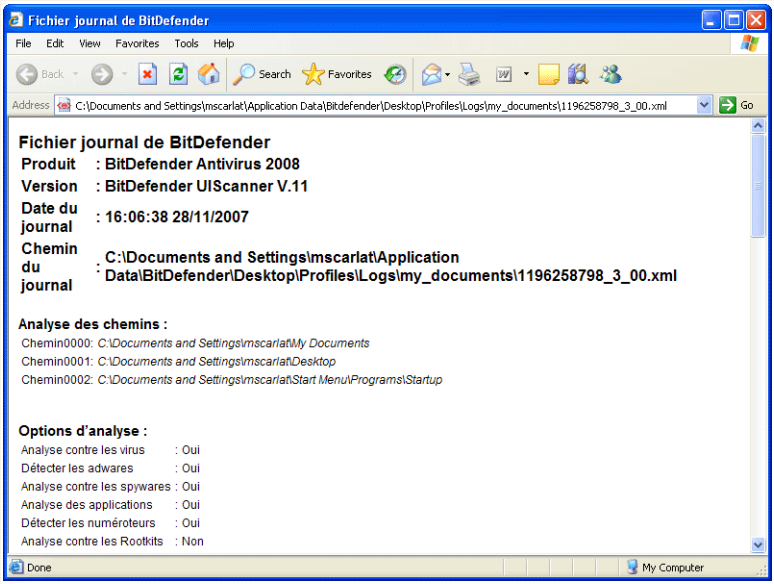
- **Supprimer** - supprime le fichier rapport sélectionné.
- **Afficher** - ouvre le fichier rapport sélectionné. Le rapport d'analyse sera ouvert dans votre navigateur web par défaut.

Note
Pour effacer ou visualiser un fichier, vous pouvez également faire un "clic-droit" sur le fichier et choisir l'option correspondante.

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

Exemple de rapport d'analyse

La capture suivante représente un exemple d'un rapport d'analyse :



Exemple de rapport d'analyse

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.

8.3. Objets exclus de l'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.

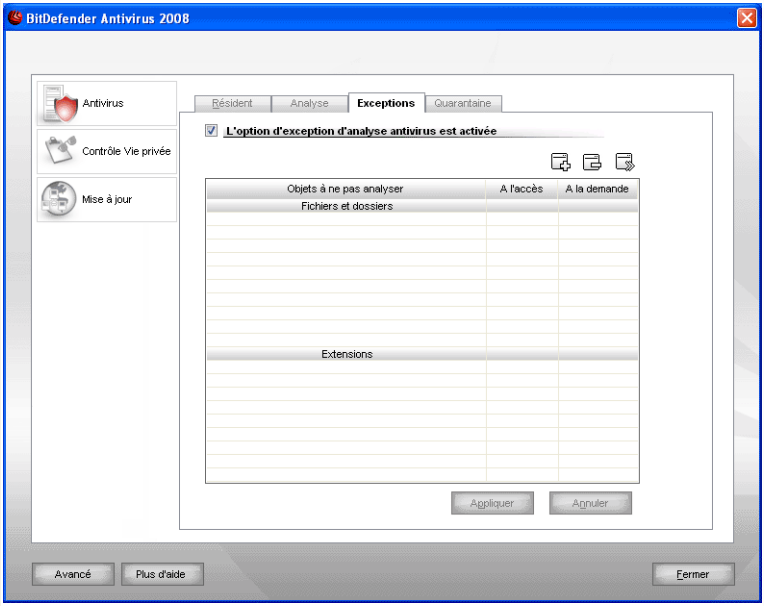
BitDefender vous permet d'exclure des objets d'une analyse à l'accès ou d'une analyse sur demande ou des deux. Cette fonction permet de réduire la durée d'une analyse et d'éviter d'interférer dans votre travail.

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 ayant une extension spécifique.

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

Pour afficher et gérer les objets exclus de l'analyse, cliquez sur **Antivirus > Exceptions** dans la console des paramètres. La fenêtre suivante apparaît:



Exceptions

Les objets (fichiers, dossiers, extensions) exclus de l'analyse s'affichent. Il est indiqué pour chaque objet si celui-ci est exclus d'une analyse à l'accès, d'une analyse sur demande ou des deux.

Note
Les exceptions spécifiées ici ne s'appliquent PAS à l'analyse contextuelle.

Pour effacer un objet de la liste, sélectionnez le et cliquez sur le bouton **Effacer**.

Pour editer un objet de la liste, sélectionnez le et cliquez sur le bouton **Editer**. 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**.

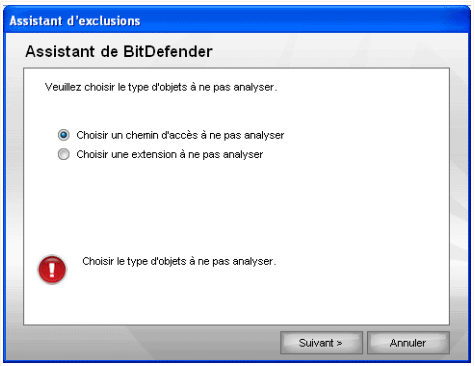
Note
Vous pouvez aussi faire un clic droit sur un objet et utiliser les options du menu de raccourcis pour le modifier ou le supprimer.

Vous pouvez cliquer sur **Annuler** pour revenir aux modifications effectuées dans le tableau des règles, à condition que vous ne les ayez pas enregistrées en cliquant sur **Appliquer**.

8.3.1. Exclusion des chemins de l'analyse

Pour exclure des chemins de l'analyse, cliquez sur le bouton **Ajouter**. Vous serez guidé tout au long du processus d'exclusion par l'assistant de configuration qui apparaîtra.

Étape 1 sur 3 - Sélectionner le type d'objet

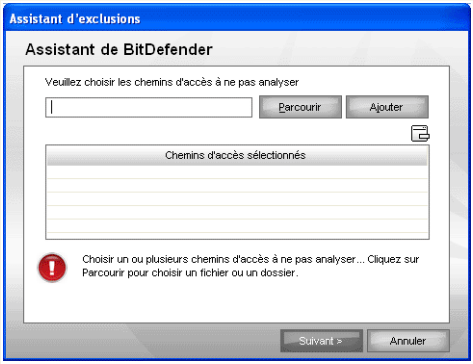


Type d'objet

Sélectionnez l'option d'exclusion d'un chemin de l'analyse.

Cliquez sur **Suivant**.

Étape 2 sur 3 - Spécifier les chemins à exclure



Chemins à exclure

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**.

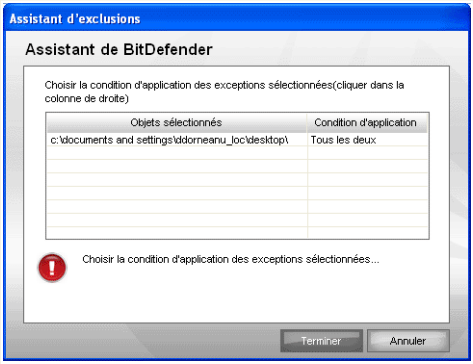
> ***Note***
> Si le chemin indiqué n'existe pas, un message d'erreur apparaît. Cliquez sur **OK** et vérifiez la validité du chemin.

Les chemins apparaissent dans le tableau au fur et à mesure que vous les ajoutez. Vous pouvez en ajouter autant que vous le souhaitez.

Pour effacer un objet de la liste, sélectionnez le et cliquez sur le bouton **Effacer**.

Cliquez sur **Suivant**.

Étape 3 sur 3 - Sélectionner le type d'analyse



Type d'analyse

Un tableau contenant les chemins à exclure de l'analyse et le type d'analyse dont ils sont exclus est affiché.

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.

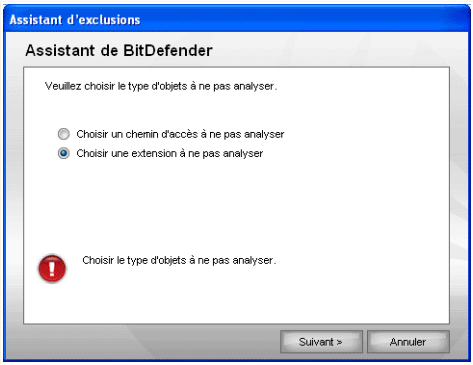
Cliquez sur **Terminer**.

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

8.3.2. Exclusion des extensions de l'analyse

Pour exclure des extensions de l'analyse, cliquez sur le bouton **Ajouter**. Vous serez guidé tout au long du processus d'exclusion par l'assistant de configuration qui apparaîtra.

Étape 1 sur 3 - Sélectionner le type d'objet

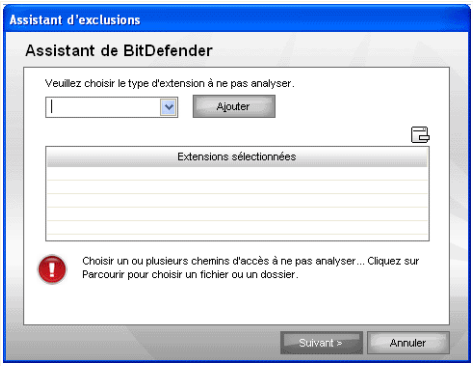


Type d'objet

Sélectionnez l'option d'exclusion d'une extension de l'analyse.

Cliquez sur **Suivant**.

Étape 2 sur 3 - Spécifier les extensions à exclure



Extensions à exclure

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.

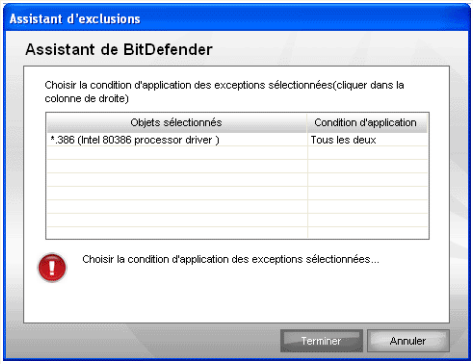
- Saisissez l'extension à exclure de l'analyse dans la zone de texte, puis cliquez sur **Ajouter**.

Les extensions apparaissent dans le tableau au fur et à mesure que vous les ajoutez. Vous pouvez en ajouter autant que vous le souhaitez.

Pour effacer un objet de la liste, sélectionnez le et cliquez sur le bouton **Effacer**.

Cliquez sur **Suivant**.

Étape 3 sur 3 - Sélectionner le type d'analyse



Type d'analyse

Un tableau s'affiche contenant les extensions devant être exclues de l'analyse et le type d'analyse dont elles sont exclues.

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.

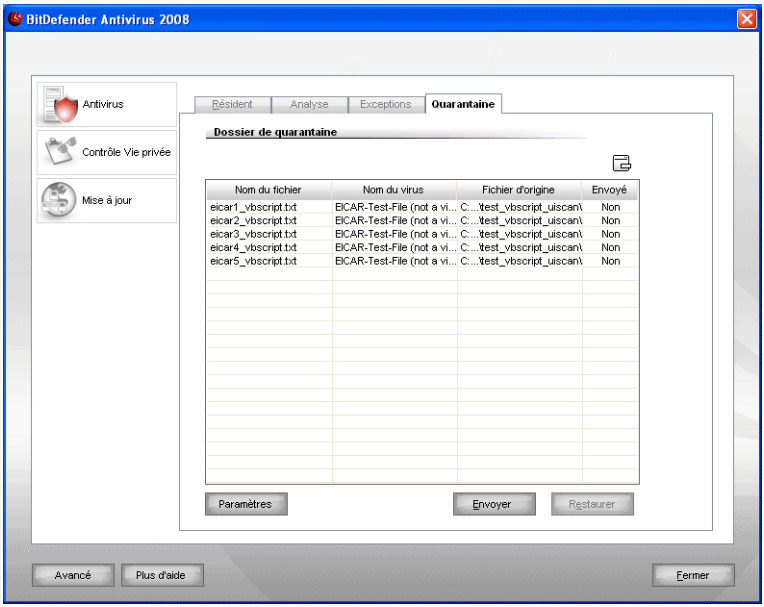
Cliquez sur **Terminer**.

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

8.4. 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.

Pour afficher et gérer les fichiers en quarantaine et pour configurer les paramètres de la quarantaine, cliquez sur **Antivirus > Quarantaine** dans la console des paramètres.



Quarantaine

8.4.1. Gérer les fichiers en quarantaine

Comme vous le constaterez, la rubrique **Quarantaine** contient une liste de tous les fichiers qui ont été isolés jusque là. Chaque fichier intègre son nom, sa taille, sa date d'isolation et sa date de soumission.

Note
Lorsque le virus est en quarantaine, il ne peut faire aucun dégât puisqu'il ne peut être exécuté ou lu.

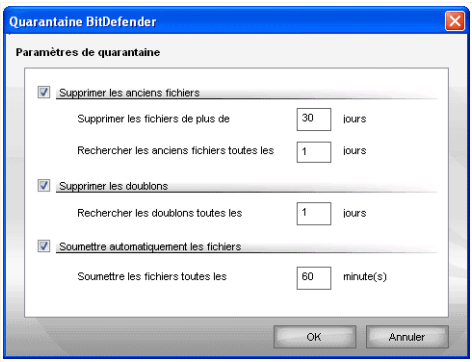
Pour effacer un fichier sélectionné dans la zone de quarantaine, cliquez sur le bouton **Déplacer**. Si vous voulez restaurez un fichier sélectionné dans son emplacement d'origine, cliquez sur **Restaurer**.

Vous pouvez envoyer un fichier depuis la quarantaine aux BitDefender Labs en cliquant sur **Envoyer**.

Menu contextuel. Le menu contextuel qui vous est proposé vous permet de gérer facilement les fichiers en quarantaine. Les options disponibles sont les mêmes que celles mentionnées précédemment. Vous pouvez aussi sélectionner **Actualiser** pour rafraîchir la zone de quarantaine.

8.4.2. Configuration des paramètres de la quarantaine

Pour configurer les paramètres de la quarantaine, cliquez sur **Paramètres**. Une nouvelle fenêtre s'affiche.



Configuration de la zone de quarantaine

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.

Note
Par défaut, BitDefender recherche les anciens fichiers chaque jour et supprime les fichiers de plus de 10 jours.

Supprimer les doublons. Pour supprimer automatiquement les doublons de fichiers en quarantaine, cochez l'option correspondante. Vous devez spécifier le nombre de jours entre deux recherches consécutives de doublons.

Note
Par défaut, BitDefender recherche les doublons de fichiers en quarantaine chaque jour.

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

Note
Par défaut, BitDefender soumettra automatiquement toutes les heures les fichiers mis en quarantaine.

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

9. 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.

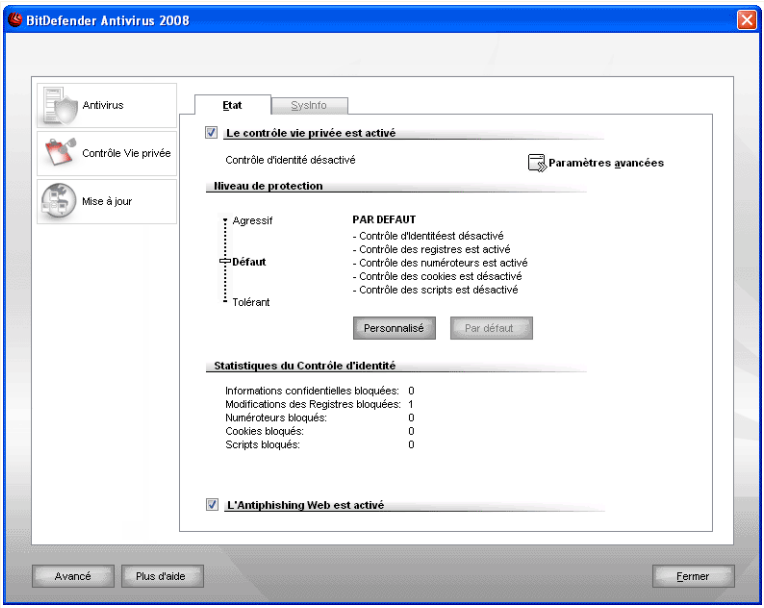
BitDefender peut également analyser les sites Internet que vous visitez et vous alerter si une menace de phishing est détectée.

Le chapitre **Contrôle Vie privée** de ce guide utilisateur contient les rubriques suivantes:

- Statut du contrôle vie privée
- Paramètres avancés - Contrôle d'identité
- Paramètres avancés - Contrôle de la base de registres
- Paramètres avancés - Contrôle des cookies
- Paramètres avancés - Contrôle des scripts
- Information Système
- Barre d'outils Antiphishing

9.1. Statut du Contrôle Vie privée

Pour configurer le Contrôle Vie privée et consulter les informations concernant son activité, cliquez sur **Contrôle Vie privée>Statut** dans les paramètres de la console. La fenêtre suivante apparaît:



Statut du Contrôle Vie privée

9.1.1. Contrôle Vie privée

Important
Pour prévenir le vol d'informations et protéger votre vie privée, laissez le module **Contrôle Vie Privée** activé.

Le Contrôle Vie privée protège votre ordinateur en effectuant les 5 contrôles majeurs de sécurité:

- Contrôle d'identité - protège vos informations confidentielles en filtrant tout le trafic HTTP sortant (pages Web) et SMTP (emails) selon les règles crées dans la rubrique Identité

Note
En bas de la section, vous pouvez consulter les **statistiques concernant le contrôle d'identité**.

- Contrôle de la base de registres - demande votre autorisation quand un programme tente de modifier la base de registres pour être éxécuté au démarrage de Windows.
- Contrôle des cookies - demande votre autorisation quand un nouveau site Internet tente de déposer un cookie sur votre ordinateur.
- Contrôle des scripts - demande votre autorisation quand un site Internet tente d'activer un script ou tout autre contenu actif.

Pour configurer les paramètres de ces contrôles, cliquez sur Paramètres avancés.

Configuration du niveau de protection

Vous pouvez choisir le niveau de protection qui répond le mieux à vos besoins de sécurité. Déplacez le curseur sur l'échelle pour choisir le niveau approprié.

Il existe trois niveaux de protection:

Niveau de protection	*Description*
Tolérant	Seul le **Contrôle de la base de registre** est activé.
Défaut	Le **Contrôle de la base de registre** et le **Contrôle d'Identité** sont activés.
Agressif	Le **Contrôle de la base de regsitre**, le **Contrôle d'identité** et le **Contrôle des scripts** sont activés.

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**.

Cliquez sur **Niveau par défaut** pour placer le curseur sur le niveau par défaut.

9.1.2. Protection antiphishing

Le phishing est une activité criminelle pratiquée sur Internet qui repose sur les techniques d'ingénierie sociale ; son but est de piéger des personnes afin de leur soutirer des renseignements d'ordre personnel.

La plupart du temps, les tentatives de phishing se traduisent par l'envoi massif d'emails qui prétendent émaner d'une société digne de confiance. Ces faux messages sont envoyés dans l'espoir que quelques-uns des destinataires qui correspondent au profil de la cible du phishing divulgueront alors des renseignements d'ordre personnel.

En règle générale, un message de phishing signale un problème avec votre compte en ligne. Il vous invite à cliquer sur un lien fourni dans le message pour accéder à un site Web supposé authentique (en fait un site frauduleux) où des renseignements d'ordre privé vous sont ensuite demandés. On peut par exemple vous demander de confirmer vos identifiants de connexion à votre compte, c'est-à-dire votre nom d'utilisateur et votre mot de passe, et de fournir vos coordonnées bancaires ou votre numéro de sécurité sociale. Une approche encore plus convaincante consiste à vous faire croire que votre compte a déjà été ou risque d'être suspendu si vous ne cliquez pas sur le lien fourni.

Le phishing utilise également les spywares, tels que des keyloggers introduits par un cheval de Troie, pour dérober des informations concernant votre compte directement au sein de votre ordinateur.

Les principales cibles du phishing sont les clients de services de paiement en ligne, comme eBay et PayPal, ainsi que les banques qui proposent des prestations en ligne. Récemment, les utilisateurs de sites de réseau social ont également fait l'objet de tentatives de phishing pour obtenir des renseignements d'ordre privé et usurper ensuite leur identité.

Pour vous prémunir contre les tentatives de phishing lors de votre navigation sur Internet, **l'antiphishing** doit être activé. Ainsi, BitDefender analysera chaque site Internet avant que vous y accédiez et il vous alertera en cas de menaces de phishing. Il est possible de configurer une liste blanche de sites Internet qui ne seront pas analysés par BitDefender.

Afin de gérer facilement la protection antiphishing et la liste blanche, utilisez la barre d'outils antiphishing BitDefender intégrée à Internet Explorer. Pour plus d'informations, reportez-vous à « *Barre d'outils antiphishing* » (p. 106).

9.2. Contrôle d'identité - Paramètres avancés

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.

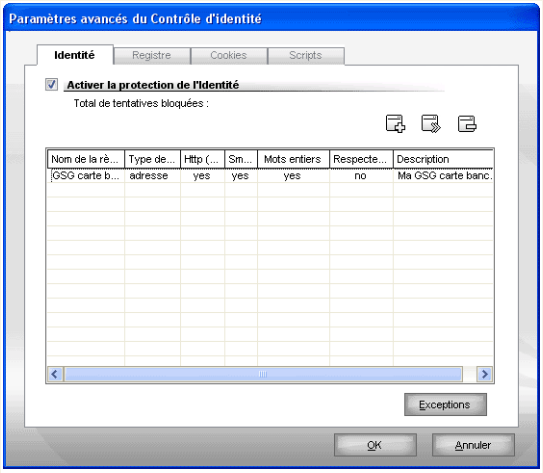
Le module **Contrôle d'Identité** vous aide à garder vos informations confidentielles en sécurité. Il analyse le trafic HTTP et SMTP à la recherche des séquences de

caractères que vous avez définies et bloque les emails ou les pages Web si il les trouve.

Le support multi-utilisateurs fourni empêche les autres utilisateurs du système d'accéder aux règles que vous avez configurées.

Les règles de confidentialité peuvent être configurées dans la section **Identité**. Pour accéder à cette section, ouvrez la fenêtre des **Paramètres avancés de Contrôle Vie privée** et cliquez sur l'onglet **Identité**.

Note
Pour ouvrir la fenêtre des **Paramètres avancés de Contrôle Vie privée**, cliquez sur **Contrôle Vie privée>Statut** dans la console des paramètres et cliquez sur **Paramètres avancés**.



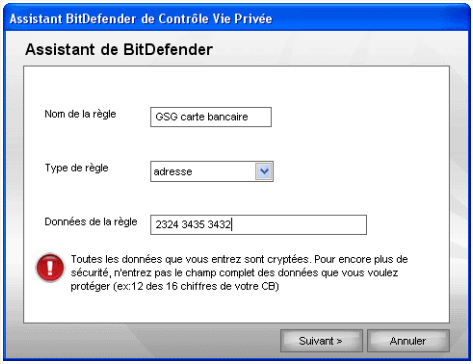
Contrôle d'identité

9.2.1. Création de règles d'Identité

Les règles doivent être entrées manuellement (cliquez sur le bouton **Ajouter** et choisissez les paramètres de la règle). L'assistant de configuration apparaîtra.

L'assistant de configuration contient 3 étapes.

Etape 1 sur 3 - Définition des types de règles et de données



Définition des types de règles et de données

Entrez le nom de la règle dans le champ correspondant.

Vous devez définir les paramètres suivants:

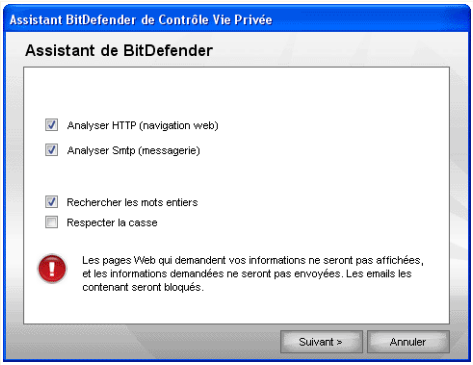
- **Type de règle** - détermine le type de règle (addresse, nom, carte de crédit, code PIN, etc.)
- **Données de la règle** - Renseigner les données de la règle.

> ***Note***
> 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.

Cliquez sur **Suivant**.

Etape 2 sur 3 - Sélection du trafic



Sélection du trafic

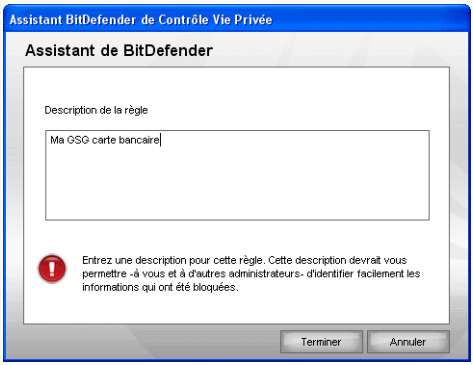
Sélectionnez le type de trafic que BitDefender doit analyser. Les options suivantes sont disponibles:

- **Analyse HTTP** - Analyse le flux HTTP (web) et bloque les données qui sont prévues dans la règle de gestion des données.
- **Analyse SMTP** - Analyse le flux SMTP (mail) et bloque les emails 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.

Cliquez sur **Suivant**.

Etape 3 sur 3 – Description de la règle



Description de la règle

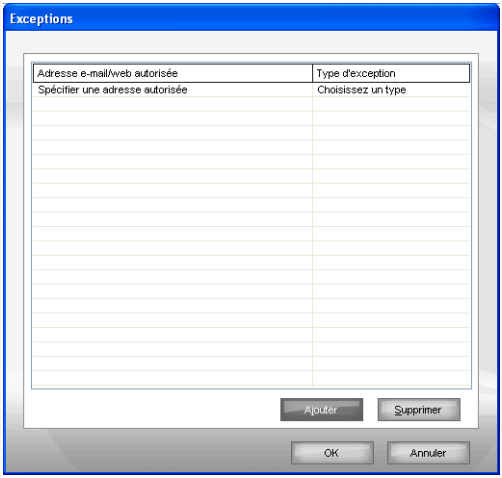
Entrez une description courte de la règle dans le champ correspondant.

Cliquez sur **Terminer**.

9.2.2. 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**.



Exceptions

Pour ajouter une exception, procédez comme suit :

1. Cliquez sur **Ajouter** pour ajouter une nouvelle entrée dans le tableau.
2. Double-cliquez sur **Spécifier adresse autorisée** et indiquez l'adresse Web ou l'adresse e-mail que vous souhaitez ajouter en tant qu'exception.
3. Double-cliquez sur **Choisissez un type** et sélectionnez dans le menu l'option correspondant au type d'adresse précédemment indiquée.
   - Si vous avez indiqué une adresse Web, sélectionnez **HTTP**.
   - Si vous avez indiqué une adresse e-mail, sélectionnez **SMTP**.

Pour supprimer une exception de la liste, sélectionnez-la, puis cliquez sur **Supprimer**.

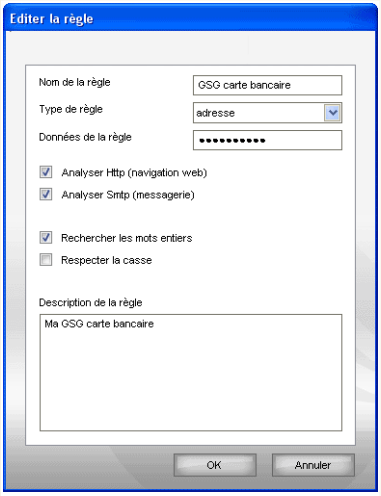
Cliquez**OK** pour sauvegarder les changements.

9.2.3. Gestion des règles

Vous pouvez voir les règles existantes dans le tableau correspondant.

Pour supprimer un règle, sélectionnez-la et cliquez sur le bouton **Effacer**. Pour désactiver temporairement une règle sans pour autant la supprimer, décochez la case correspondante.

Pour modifier une règle, sélectionnez-la, puis cliquez sur le bouton **Éditer** ou double-cliquez dessus. Une nouvelle fenêtre est alors affichée.



Editer une règle

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.

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

9.3. Contrôle de la base de registre -Paramètres avancés

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. Cette fonction est souvent détournée par les virus afin d'être automatiquement lancé lorsque l'utilisateur redémarre son ordinateur.

Le **Contrôle des registres** surveille les registres Windows – cette fonction 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.

Alerte registres

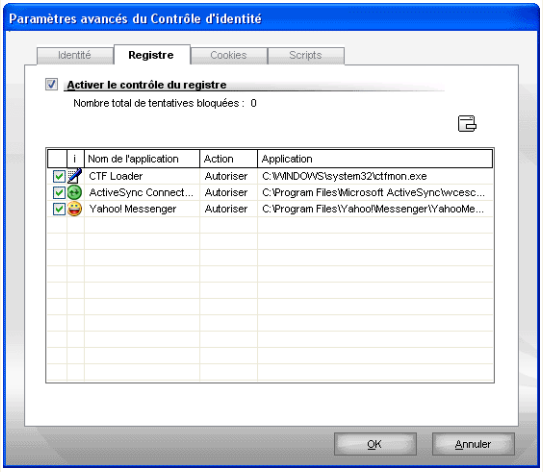
Vous pouvez refuser cette modification en cliquant sur **Non** ou l'autoriser en cliquant sur **Oui**.

Si vous souhaitez que BitDefender se souvienne de votre réponse, cochez la case **Toujours appliquer cette action pour ce programme**. Une règle est alors générée et la même action sera appliquée à chaque fois que ce programme tentera de modifier une entrée du registre à exécuter au démarrage de Windows.

Note
BitDefender vous alertera lors de l'installation de nouveaux logiciels nécessitant d'être lancés après le prochain démarrage de votre ordinateur. Dans la plupart des cas, ces programmes sont légitimes et peuvent être autorisés.

Il est possible d'accéder à chaque règle qui a été traitée dans la section **Registre** pour peaufiner les réglages. Pour accéder à cette section, ouvrez la fenêtre des **Paramètres avancés de Contrôle Vie privée** et cliquez sur l'onglet **Registre**.

Note
Pour ouvrir la fenêtre des **Paramètres avancés de Contrôle Vie privée**, cliquez sur **Contrôle Vie privée>Statut** dans la console des paramètres et cliquez sur **Paramètres avancés**.



Contrôle de la base de registre

Vous pouvez voir les règles existantes dans le tableau correspondant.

Pour supprimer une règle, il suffit de la sélectionner et de cliquer sur le bouton **Effacer la règle**. Pour désactiver temporairement une option sans l'effacer, décochez la case correspondante.

Pour modifier l'action d'une règle, double-cliquez sur le champ de l'action et sélectionnez l'option correspondante dans le menu.

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

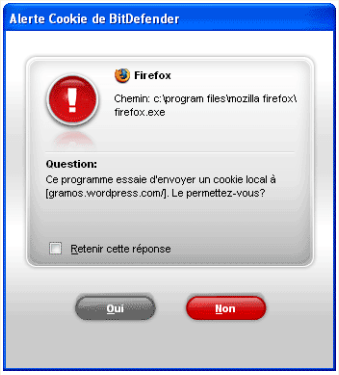
9.4. Contrôle des cookies - Paramètres avancés

Les Cookies sont très communs sur Internet. Ce sont des petits fichiers stockés sur l'ordinateur. Les sites web les créent afin de connaître certaines informations concernant vos habitudes de surf.

Les Cookies sont généralement là pour vous faciliter la navigation. Par exemple, ils peuvent permettre à un site web de mémoriser votre nom et vos préférences, pour que vous n'ayez pas à les renseigner à nouveau.

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

C'est là que la fonction **Contrôle des cookies** est très utile. Si elle est activée, la fonction **Contrôle des cookies** vous demandera une validation à chaque fois qu'un nouveau site Web tentera de déposer un cookie.



Alerte de cookies

Vous pouvez voir le nom de l'application qui tente d'envoyer un fichier de type cookie.

Sélectionnez **Retenir cette réponse** et cliquez sur **Oui** ou **Non** et une règle sera créée, appliquée et listée dans le tableau des règles.

Cette fonction vous aide à choisir à quels sites faire confiance et quels sites vous préférez éviter.

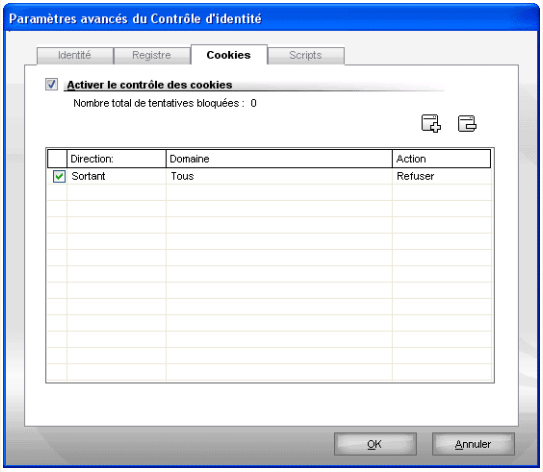
Note

A cause du grand nombre de cookies utilisés sur Internet, le module **Contrôle des Cookies** peut être légèrement gênant au départ. Il vous posera beaucoup de questions concernant l'acceptation de nouveaux cookies sur votre ordinateur. Au fur et à mesure que vous ajouterez vos sites Web favoris à la liste des règles, votre navigation redeviendra aussi simple qu'auparavant.

Vous pouvez éditer chaque règle mémorisée dans la section **Cookie** pour y apporter des modifications. Pour accéder à cette section, ouvrez la fenêtre des **Paramètres avancés de Contrôle Vie privée** et cliquez sur l'onglet **Cookie**.

Note

Pour ouvrir la fenêtre des **Paramètres avancés de Contrôle Vie privée**, cliquez sur **Contrôle Vie privée>Statut** dans la console des paramètres et cliquez sur **Paramètres avancés**.



Contrôle des cookies

Vous pouvez voir les règles existantes dans le tableau correspondant.

Important
Les règles sont listées dans l'ordre de priorité en commençant par le haut de la liste, la première règle a la priorité la plus élevée. Glisser & déposer les règles afin de changer leur priorité.

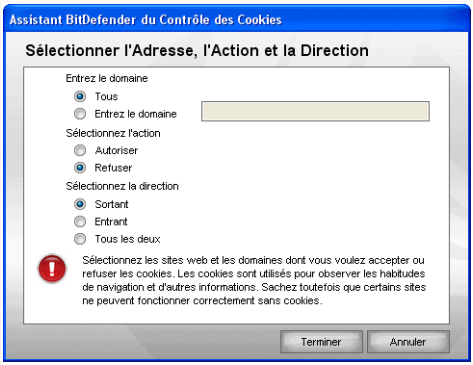
Pour supprimer une règle, selectionnez la et cliquez sur le bouton **Effacer**. Pour modifier les paramètres d'une règle, double-cliquez sur son champ et faîtes la modification souhaitée. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante.

Les règles peuvent être entrées automatiquement (via la fenêtre d'alerte) ou manuellement (cliquez sur le bouton **Ajouter** et choisissez les paramètres de la règle). L'assistant de configuration apparaîtra.

9.4.1. Assistant de configuration

L'assistant de configuration ne comporte qu'une seule étape.

Etape 1 sur 1 - Selection de l'Adresse, de l'Action et de la Direction



Selection de l'Adresse, de l'Action et de la Direction

Vous pouvez définir les paramètres:

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

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

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

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

Cliquez sur **Terminer**.

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

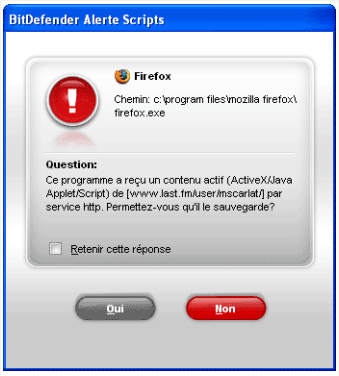
Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

9.5. Contrôle des scripts - Paramètres avancés

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. Il est recommandé de n'accepter les contenus actifs que sur les sites que vous connaissez et auxquels vous faites parfaitement confiance.

BitDefender vous laisse le choix d'exécuter ou de bloquer ces éléments.

Avec le **Contrôle de scripts** vous pourrez définir les sites web auxquels vous faites confiance ou non. BitDefender vous demandera une validation dès qu'un site Web essaiera d'activer un script ou tout type de contenu actif:



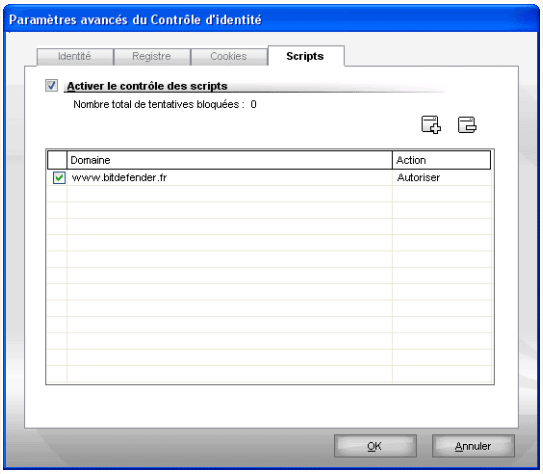
Alerte de scripts

Vous pouvez voir le nom de la ressource.

Sélectionnez **Retenir cette réponse** et cliquez sur **Oui** ou **Non** et une règle sera créée, appliquée et listée dans le tableau des règles. Vous ne serez dès lors plus interrogé lorsque ce même site essaiera de vous envoyer un contenu actif.

Chaque règle mémorisée peut être éditée dans la partie **Scripts** pour y apporter des modification. Pour accéder à cette section, ouvrez la fenêtre des **Paramètres avancés de Contrôle Vie privée** et cliquez sur l'onglet **Script**.

Note
Pour ouvrir la fenêtre des **Paramètres avancés de Contrôle Vie privée**, cliquez sur **Contrôle Vie privée>Statut** dans la console des paramètres et cliquez sur **Paramètres avancés**.



Contrôle des scripts

Vous pouvez voir les règles existantes dans le tableau correspondant.

Important
Les règles sont listées dans l'ordre de priorité en commençant par le haut de la liste, la première règle a la priorité la plus élevée. Glisser & déposer les règles afin de changer leur priorité.

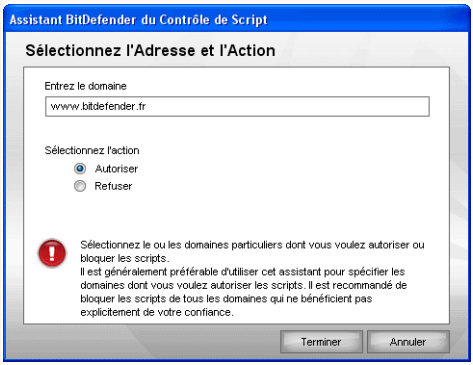
Pour supprimer une règle, selectionnez la et cliquez sur le bouton **Effacer**. Pour modifier les paramètres d'une règle, double-cliquez sur son champ et faîtes la modification souhaitée. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante.

Les règles peuvent être entrées automatiquement (via la fenêtre d'alerte) ou manuellement (cliquez sur le bouton **Ajouter** et choisissez les paramètres de la règle). L'assistant de configuration apparaîtra.

9.5.1. Assistant de configuration

L'assistant de configuration ne comporte qu'une seule étape.

Etape 1 sur 1 - Sélection des adresses de nom de domaine et Action



Sélection des adresses de domaine et Action

Vous pouvez définir les paramètres:

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

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

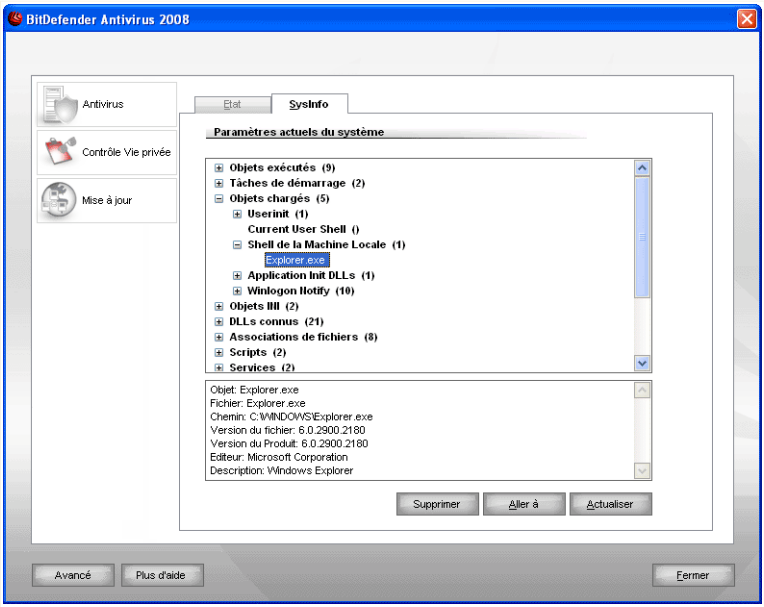
Cliquez sur **Terminer**.

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

9.6. 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, cliquez sur **Contrôle Vie privée>Informations système** dans les paramètres de la console. La fenêtre suivante apparaît:



Informations Système

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

Trois boutons sont disponibles:

- **Retirer** - supprime les objets sélectionnés. Vous devez cliquer sur **Oui** pour confirmer votre choix.

Note
Si vous ne souhaitez plus être invité à confirmer votre choix lors de la session en cours, cochez la case **Ne plus me poser la question pendant cette session**.

- **Aller à** - ouvre une fenêtre dans laquelle l'objet a été placé (la **Base de Registres** par exemple).
- **Actualiser** - re-ouvre la rubrique **Informations système**.

Note
Suivant l'objet sélectionné, un ou deux de ces boutons peut ne pas apparaître **Supprimer** ou **Aller à**.

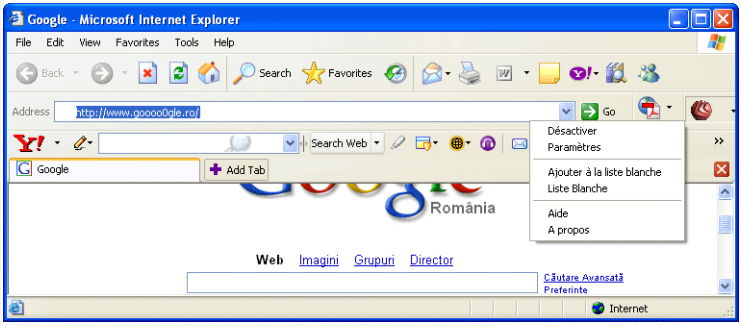
9.7. Barre d'outils antiphishing

BitDefender protège votre ordinateur contre les tentatives de phishing lorsque vous naviguez sur Internet. Il analyse les sites Web auxquels vous accédez et vous prévient en cas de menaces de phishing. Il est possible de configurer une liste blanche de sites Internet qui ne seront pas analysés par BitDefender.

La barre d'outils antiphishing BitDefender intégrée à Internet Explorer vous permet de gérer facilement et efficacement la protection antiphishing et la liste blanche.

La barre d'outils antiphishing, représentée par **l'icône BitDefender** , est située en haut de la fenêtre d'Internet Explorer. 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 que **la barre d'outils BitDefender** y figure bien.



Barre d'outils antiphishing

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

- **Activer / Désactiver** - active / désactive la barre d'outils antiphishing BitDefender.

> ***Note***
> Si vous choisissez de désactiver la barre d'outils antiphishing, votre ordinateur ne sera plus protégé contre les tentatives de phishing.

- **Paramètres** - ouvre une fenêtre où vous pouvez préciser les paramètres de la barre d'outils antiphishing.

  Les options suivantes sont disponibles:
  - **Activation de l'analyse**- Activation de l'analyse antiphishing.
  - **Demander avant d'ajouter à une liste blanche** - Demande d'autorisation pour ajouter un site Web à la liste blanche.
- **Ajouter à la liste blanche** - Ajout du site Web actuel à la liste blanche.

> ***Note***
> 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.

- **Afficher la liste blanche** - Ouverture de la liste blanche.

  Vous pouvez consulter la liste de tous les sites Web qui ne seront pas analysés par les moteurs BitDefender d'antiphishing.

Si vous souhaitez supprimer un site de la liste blanche – pour pouvoir être prévenu de tout risque de phishing sur la page correspondante, cliquez sur le bouton **Supprimer** en regard du nom du site.

Vous pouvez ajouter à la liste blanche les sites auxquels vous faites pleinement confiance, pour qu'ils ne soient plus analysés par les moteurs d'antiphishing. Pour ajouter un site à la liste blanche, entrez son adresse dans le champ correspond et cliquez sur le bouton **Ajouter**.

- **Aide** - ouvre la documentation d'aide 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.

10. 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 xDSL, BitDefender s'en occupera automatiquement. Il lance la procédure de mise à jour de la base virale à chaque fois que vous démarrez votre ordinateur puis toutes les heures.

Si une mise à jour est détectée, vous serez invité à la confirmer ou elle sera effectuée automatiquement en fonction des options que vous aurez définies dans la section 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.

La rubrique Mise à jour de ce manuel d'utilisation contient les thèmes suivants:

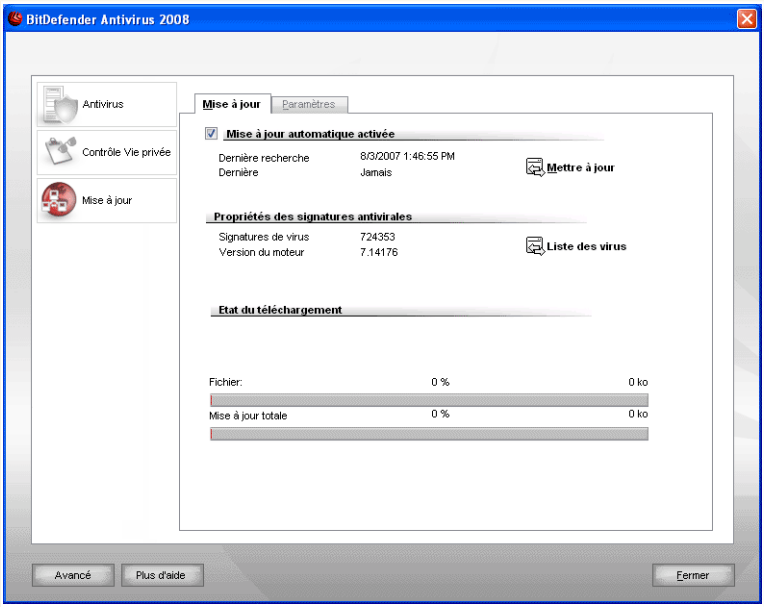
- **Mise à jour des moteurs antivirus** - comme de nouvelles menaces apparaissent, les fichiers contenant les signatures de virus doivent être mis à jour en permanence contre elles. Elles s'affichent sous le nom de **Virus Definitions Update**.
- **Mise à jour pour le moteur antispam** - de nouvelles règles seront ajoutées aux filtres heuristique et URL et de nouvelles images seront ajoutées au filtre d'images. Cela augmentera l'efficacité de votre moteur Antispam. Elles s'affichent sous le nom de **Antispam 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**.

Le chapitre **Mise à jour** de ce manuel d'utilisation contient les thèmes suivants:

- Mise à jour automatique
- Paramètres de mise à jour

10.1. Mise à jour automatique

Pour afficher des informations sur les mises à jour et exécuter des mises à jour automatiques, cliquez sur **Mise à jour > Mise à jour** dans la console des paramètres. La fenêtre suivante apparaît:



Mise à jour automatique

C'est ici que vous pouvez consulter la date de la dernière recherche de mises à jour et celle de la dernière mise à jour, ainsi que des informations sur la dernière mise à jour effectuée (ou les erreurs rencontrées). Sont également affichées des informations sur la version actuelle du moteur de recherche et le nombre de signatures.

Vous pouvez accéder aux signatures de codes malveillants de votre application BitDefender en cliquant sur **Liste des virus**. Un fichier HTML contenant toutes les signatures disponibles est créé et s'ouvre dans un navigateur Web. Vous pouvez rechercher dans la base de données une signature de code malveillant spécifique ou cliquez sur **Liste des virus BitDefender** pour accéder à la base de données en ligne des signatures BitDefender.

Si vous ouvrez cette section pendant une mise à jour, vous pourrez accéder à l'état du téléchargement.

Important
Pour être protégé contre les dernières menaces, il est impératif de laisser la **mise à jour automatique** active.

10.1.1. Demandes de mise à jour

La mise à jour automatique peut être faite quand vous le souhaitez en cliquant sur **Mise à jour**. Cette mise à jour correspond à une **Mise à jour a la demande**.

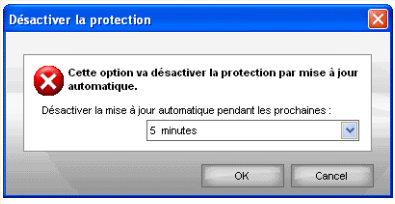
Le module **Mise à jour**se connecte au serveur de mise à jour BitDefender et recherche les mises à jour disponibles. Si une mise à jour est détectée, vous serez invité à la confirmer ou elle sera effectuée automatiquement en fonction des options que vous aurez définies dans la section Paramètres de 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 pour bénéficier de la meilleure protection disponible.

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.

10.1.2. Désactiver la mise à jour automatique

Si vous tentez de désactiver la mise à jour automatique, une fenêtre d'avertissement apparaît.



Désactiver la mise à jour automatique

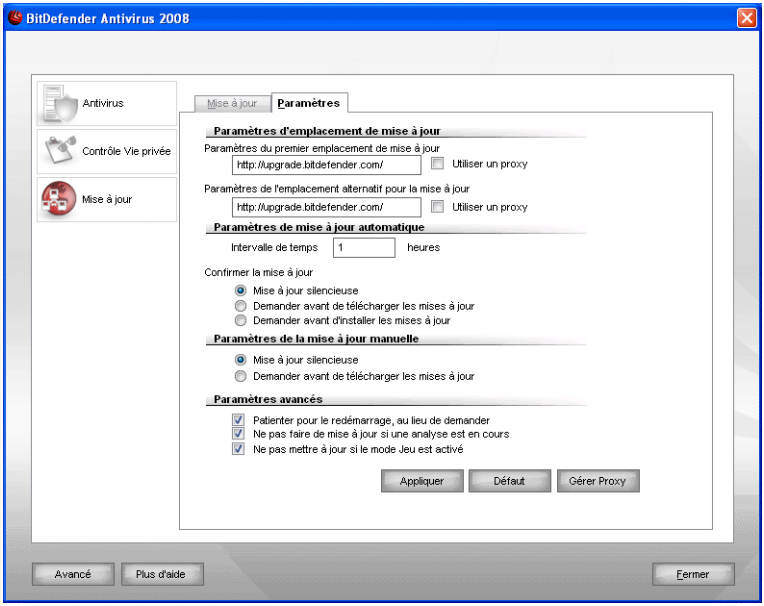
Vous devez confirmer votre choix en sélectionnant dans le menu la durée pendant laquelle vous souhaitez désactiver la mise à jour automatique. Vous pouvez désactiver la mise à jour automatique pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.

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

10.2. Configuration des Mises à jour

Les mises à jour peuvent être réalisées depuis un réseau local, directement depuis Internet, ou au travers d'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 et gérer les serveurs proxy, cliquez sur **Mise à jour > Paramètres** dans la console des paramètres. La fenêtre suivante apparaît:



Configuration des Mises à jour

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.

10.2.1. Configuration 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 malicieux 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 que premier emplacement de mise à jour et de conserver l'emplacement alternatif de mise à jour inchangé par 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 **Gérer les serveurs proxy** pour configurer les paramètres du proxy.

Note
Pour plus d'informations, reportez-vous à « *Gestion des serveurs proxy* » (p. 116)

10.2.2. 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 **Intervalle de temps**. 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 installe automatiquement la mise à jour de manière transparente pour 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.

Note
L'autorisation vous est demandée avant que la mise à jour ne soit téléchargée, même si vous quittez le Centre de sécurité.

- **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.

Note
L'autorisation vous est demandée avant que la mise à jour ne soit installée, même si vous quittez le Centre de sécurité.

10.2.3. 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.

Note
L'autorisation vous est demandée avant que la mise à jour ne soit téléchargée, même si vous quittez le Centre de sécurité.

10.2.4. 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**:

- **Patientez pour redémarrer, 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 l'analyse est en cours** - BitDefender ne se mettra pas à jour si une analyse est en cours afin de ne pas la perturber.

Note
Si une mise à jour de BitDefender a lieu pendant l'analyse, celle-ci sera interrompue.

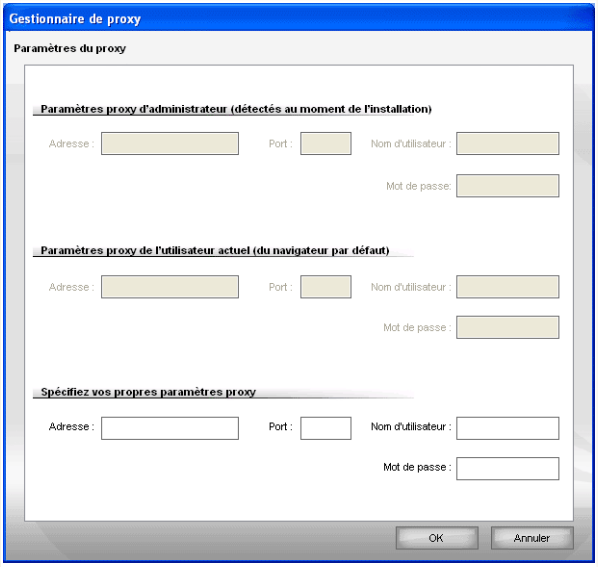
- **Ne pas mettre à jour si le mode jeu est actif** - BitDefender n'effectuera pas de mise à jour si le mode jeu est activé. Ainsi, vous limitez l'influence du produit sur les performances du système lorsque vous jouez.

10.2.5. Gestion des serveurs proxy

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.

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

Pour gérer les paramètres du proxy, cliquez sur **Gérer les serveurs proxy**. La fenêtre **Gestionnaire de proxy** s'affiche.



Gestionnaire de proxy

Il existe trois catégories de paramètres de proxy:

- **Paramètres de configuration du proxy (détectés à l'installation)** - Paramètres de configuration du proxy détectés pendant l'installation avec le compte

Administrateur ; ces paramètres peuvent être modifiés uniquement si vous êtes connecté avec ce compte. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, vous devez les indiquer dans les champs correspondants.

- **Paramètres du proxy de l'utilisateur actuel (du navigateur par défaut)** - paramètres du proxy de l'utilisateur actuel provenant du navigateur par défaut. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, vous devez les indiquer dans les champs correspondants.

  Note
  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.

- **Votre propre catégorie de paramètres de proxy** - paramètres de proxy que vous pouvez configurer si vous êtes connecté 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.

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 fermer la fenêtre.

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

CD de secours BitDefender

11. Vue d'ensemble

BitDefender Antivirus 2008 est fourni sur un CD bootable (CD de secours BitDefender), capable d'analyser et désinfecter tous les disques durs existants avant que votre système d'exploitation ne démarre.

Il est recommandé d'utiliser le CD de secours BitDefender à chaque fois que votre système d'exploitation ne fonctionne pas correctement à cause d'une infection virale. Ceci se produit généralement quand vous n'utilisez pas un produit antivirus.

La mise à jour de la base de signatures de virus se fait automatiquement, sans intervention de l'utilisateur, à chaque fois que vous lancez le CD de secours BitDefender.

Le CD de secours BitDefender est une distribution Knoppix remasterisée de BitDefender qui intègre les dernières solutions de sécurité BitDefender pour Linux dans le Live CD de GNU/Linux Knoppix, offrant un antivirus pour poste de travail capable d'analyser et de désinfecter les disques durs (y compris les partitions Windows NTFS). Le CD de secours BitDefender peut aussi être utilisée pour restaurer toutes vos données importantes lorsque Windows ne démarre pas.

Note
Le CD de secours BitDefender peut être téléchargé à partir de cette adresse: http://download.bitdefender.com/rescue_cd/

11.1. Configuration requise

Avant de booter sur le CD de secours BitDefender, vous devez d'abord vérifier que votre système remplit les conditions suivantes :

Type de processeur
x86 compatible, minimum 166 MHz pour des performances minimales, un processur de la génération i686 à 800MHz au moins sera un meilleur choix.

Mémoire
Mémoire minimum: 512Mo de RAM (1 Go recommandés)

CD-ROM
Le CD de secours BitDefender démarre à partir d'un CD-ROM, vous devez donc en posséder un et avoir un BIOS capable de booter depuis ce CD.

Connexion directe à Internet
Bien que le CD de secours BitDefender puisse être exécuté sans connexion Internet, le processus de mise à jour nécéssite un lien HTTP actif pour se télécharger et assurer la meilleure protection possible, même à travers un serveur proxy. La connexion Internet est donc indispensable.

Résolution graphique
Carte graphique standard compatible SVGA.

11.2. Logiciels inclus

Le CD de secours BitDefender inclut le package de logiciels suivant:

Xedit
Il s'agit d'un éditeur de fichier texte.

Vim
C'est un éditeur puissant comportant la mise en évidence de la syntaxe, une IUG et plus encore. Pour plus d'informations, veuillez consulter la page d'accueil de Vim.

Xcalc
Il s'agit d'un calculateur.

RoxFiler
RoxFiler est un gestionnaire de fichiers graphiques rapide et puissant.

Pour plus d'informations, veuillez consulter la page d'accueil de RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) est un gestionnaire de fichiers en mode texte.

Pour plus d'informations, veuillez consulter la page d'accueil de MC.

Pstree
Pstree affiche les processus en cours d'exécution.

Top
Top affiche les tâches Linux.

Xkill
Xkill supprime un client par ses ressources X.

Partition Image

Partition Image vous aide à sauvegarder les partitions aux formats de système de fichiers EXT2, Reiserfs, NTFS, HPFS, FAT16 et FAT32 dans un fichier image. Ce programme peut être utilisé à des fins de sauvegarde.

Pour plus d'informations, veuillez consulter la page d'accueil de Partimage.

GtkRecover

GtkRecover est une version GTK du programme recover. Il permet de restaurer des fichiers.

Pour plus d'informations, veuillez consulter la page d'accueil de GtkRecover.

ChkRootKit

ChkRootKit est un outil qui permet de rechercher les rootkits de votre ordinateur.

Pour plus d'informations, veuillez consulter la page d'accueil de ChkRootKit.

Nessus Network Scanner

Nessus est un moteur d'analyse de sécurité à distance pour Linux, Solaris, FreeBSD et Mac OS X.

Pour plus d'informations, veuillez consulter la page d'accueil de Nessus.

Iptraf

Iptraf est un logiciel de contrôle des réseaux IP.

Pour plus d'informations, veuillez consulter la page d'accueil d'Iptraf.

Iftop

Iftop affiche la bande passante sur une interface.

Pour plus d'informations, veuillez consulter la page d'accueil d'Iftop.

MTR

MTR est un outil de diagnostic réseau.

Pour plus d'informations, veuillez consulter la page d'accueil de MTR.

PPPStatus

PPPStatus affiche des statistiques sur le trafic TCP/IP entrant et sortant.

Pour plus d'informations, veuillez consulter la page d'accueil de PPPStatus.

Wavemon

Wavemon est une application de contrôle des périphériques réseau sans fil.

Pour plus d'informations, veuillez consulter la page d'accueil de Wavemon.

USBView

USBView affiche des informations sur les appareils connectés au bus USB.

Pour plus d'informations, veuillez consulter la page d'accueil USBView.

Pppconfig

Pppconfig permet de configurer automatiquement une connexion ppp commutée.

DSL/PPPoe

DSL/PPPoe configure une connexion PPPoE (ADSL).

I810rotate

I810rotate active et désactive la sortie vidéo du matériel i810 à l'aide de l'outil i810switch(1).

Pour plus d'informations, veuillez consulter la page d'accueil de I810rotate.

Mutt

Mutt est un client de messagerie texte MIME puissant.

Pour plus d'informations, veuillez consulter la page d'accueil de Mutt.

Mozilla Firefox

Mozilla Firefox est un navigateur Web bien connu.

Pour plus d'informations, veuillez consulter la page d'accueil de Mozilla Firefox.

Elinks

Elinks est un navigateur Web en mode texte.

Pour plus d'informations, veuillez consulter la page d'accueil d'Elinks.

12. Comment utiliser le CD de secours BitDefender

Ce chapitre vous explique comment démarrer et arrêter le CD de secours BitDefender, analyser votre ordinateur contre les codes malveillants et enregistrer les données de votre PC sur un support amovible si cela s'avère nécessaire. Les applications logicielles qui accompagnent le CD vous offriront la possibilité d'effectuer de nombreuses tâches, mais leur description dépasse toutefois largement le cadre de ce guide d'utilisation.

12.1. Démarrer le CD de secours BitDefender

Pour lancer le CD, configurez les options de votre BIOS pour autoriser le boot sur le CD au démarrage de l'ordinateur, mettez le CD dans le lecteur et redémarrez. Vérifiez bien que votre ordinateur puisse booter sur un CD.

Patientez jusqu'à l'apparition du prochain message et suivez les instructions pour démarrer le CD de secours BitDefender.

Page d'accueil au démarrage

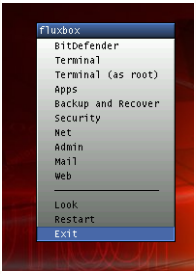
Au démarrage, la mise à jour des signatures de virus est effectuée automatiquement. Cela peut prendre un certain temps.

Quand le processus de démarrage sera terminé, vous pourrez utiliser l'interface du CD de secours BitDefender.

L'interface

12.2. Arrêter le CD de secours BitDefender

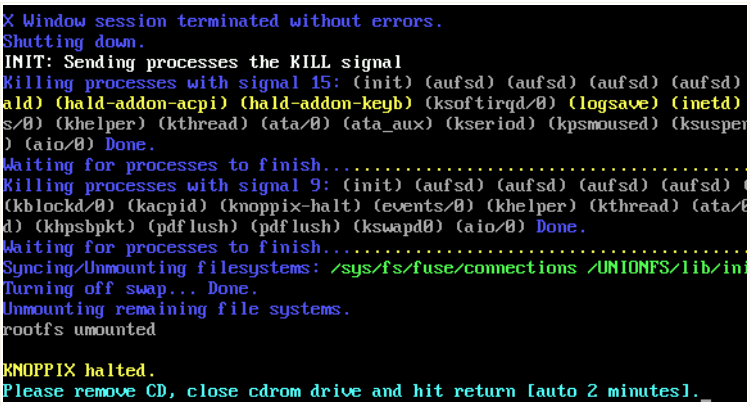
Vous pouvez éteindre votre ordinateur en toute sécurité en sélectionnant **Quitter** dans le menu contextuel du CD de secours BitDefender (double-cliquez pour l'ouvrir) ou en lançant la commande **Arrêt** depuis un terminal.



Choisissez "Sortir"

Lorsque le CD de secours BitDefender a terminé de fermer tous les programmes, il affiche un écran similaire à l'illustration suivante. Vous pourrez retirer le CD pour

démarrer depuis votre disque dur. Vous pouvez maintenant éteindre votre ordinateur ou le redémarrer.



Patientez jusqu'à l'apparition de ce message quand vous fermez le programme.

12.3. Comment lancer une analyse antivirus ?

Un assistant apparaitra lorsque le processu sde démarrage sera terminé et vous permettra de lancer une analyse complète de votre ordinateur. Tout ce que vous avez à faire est de cliquer sur le bouton **Start**.

Note
Si la résolution de votre écran n'est pas suffisante, il vous sera demander de commencer l'analyse en mode texte.

Suivez cette procédure en trois étapes pour effectuer le processus d'analyse:

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

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

2. Le nombre de problèmes de sécurité affectant votre système est indiqué.

Les problèmes de sécurité sont affichés en groupes. Cliquez sur "+" pour ouvrir un groupe ou sur "-" pour fermer un groupe.

Vous pouvez sélectionner une action globale à mener pour chaque groupe de problèmes de sécurité ou sélectionner des actions spécifiques pour chaque problème.

3. Le récapitulatif des résultats s'affiche.

Si vous souhaitez analyser seulement certains répertoires, procédez ainsi :

Parcourez vos dossiers, faites un clic-droit sur un fichier ou un dossier et choisissez **Send to**.Puis lancez l'analyse en cliquant sur **BitDefender Scanner**.

Vous pouvez également lancer les commandes suivantes depuis un terminal. Le moteur d'analyse **BitDefender Antivirus Scanner** considérera le fichier ou dossier sélectionné comme étant l'endroit à analyser par défaut.

```
# bdscan /path/to/scan/
```

12.4. Comment actualiser BitDefender via un proxy ?

S'il y a un serveur proxy entre votre ordinateur et Internet, certaines configurations devront être modifiées pour actualiser les signatures de virus.

Pour mettre à jour BitDefender à travers un proxy, suivez juste ces différentes étpaes :

1. Faîtes un clic-droit sur le bureau. Le menu contextuel du CD de Secours BitDefender apparaîtra.
2. Sélectionnez **Terminal (as root)**.
3. Tapez la commande : **cd /ramdisk/BitDefender-scanner/etc**.
4. Tapez la commande : **mcedit bdscan.conf** pour éditer ce fichier en utilisant GNU Midnight Commander (mc).
5. Pour la ligne suivante : `#HttpProxy =` (just delete the `#` sign) spécifiez le domaine, le nom d'utilisateur, le mot de passe et le port du serveur proxy. Par exemple, la ligne en question doit ressembler à cela :

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Tapez sur **F2** pour enregistrer le fichier en cours, confirmer la sauvegarde, et tapez sur **F10** pour le fermer.

7. Tapez la commande : **bdscan update**.

12.5. Comment enregistrer mes données ?

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 carte mémoire flash USB, procédez comme suit:

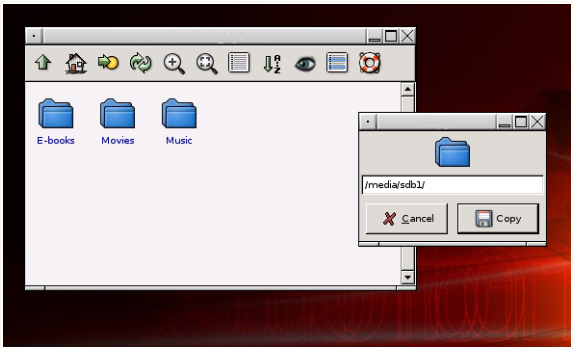
1. Insérez le CD de secours BitDefender dans le lecteur CD, la carte mémoire flash dans le lecteur USB, puis redémarrez l'ordinateur.
2. Patientez jusqu'à ce que le CD de secours BitDefender finisse de démarrer. La fenêtre suivante apparaît:

Écran du bureau

3. Double-cliquez sur la partition où se trouvent les données que vous souhaitez enregistrer (par ex., `[sda3]`).

Note
En utilisant le CD de secours BitDefender, vous rencontrerez des noms de partition de type Linux. Ainsi, `[sda1]` correspondra probablement à la partition `(C:)` de type Windows, `[sda3]` à `(F:)` et `[sdb1]` à la carte mémoire flash.

4. Parcourez vos dossiers et ouvrez le répertoire souhaité. Par exemple, `MesDonnées`, qui contient les sous répertoires `Vidéos`, `Musique` et `Livres électroniques`.
5. Faites un clic droit sur le répertoire souhaité, puis sélectionnez **Copier**. La fenêtre suivante apparaît:



Enregistrement des données

6. Saisissez `/media/sdb1/` dans la zone texte correspondante, puis cliquez sur **Copier**.

Demander de l'aide

13. Support Technique Editions Profil / BitDefender

Editions Profil et BitDefender s'efforcent de toujours vous fournir des réponses rapides et précises à vos questions. Le centre de support en ligne, dont vous trouverez les coordonnées ci-dessous, est actualisé en continu et vous donne accès aux réponses aux questions les plus fréquemment posées.

Vous disposez de plusieurs moyens pour obtenir de l'aide concernant votre produit :

1. **Mise à disposition d'une foire aux questions sur le site BitDefender :**

   http://www.bitdefender.fr/site/KnowledgeBase/faq/.

2. **Support technique par email :**

   Si votre problème n'est toujours pas résolu après avoir utilisé l'aide en ligne, vous pouvez alors nous envoyer une demande personnalisée. Merci d'utiliser pour cela le formulaire présent sur notre site dans le volet "Assistance Technique" à droite de la page de "foire aux questions" de votre produit.

3. **Par téléphone, du lundi au vendredi :**

   Pour la France : 08.92.950.950 (0,34 TTC / min)

   Pour la Belgique : 02 290.83.04

   Pour la Suisse : 0900 000 118

4. **Par prise de contrôle à distance**

   Cette possibilité requiert de contacter le support téléphonique. Suivant le problème, nos techniciens vous proposeront de prendre à distance le contrôle de votre ordinateur afin de solutionner votre problème et vous éviter ainsi de devoir réaliser vous-même les manipulations.

5. **Par chat online – Accessible 7j/7 – 365j/an**

   Ce service permet de vous mettre en relation direct avec un technicien y compris durant les jours fériés ou la nuit. Pour y accéder, veuillez saisir l'adresse ci-dessous dans votre navigateur :

   http://www.bitdefender.com/site/KnowledgeBase/liveAssistance.

   Attention, ce service est un service international, assuré majoritairement en anglais.

Glossaire

ActiveX

ActiveX est un modèle pour écrire des programmes afin que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour faire des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent demander ou répondre à des questions, utiliser des boutons et interagir de multiples façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic.

Active X est reconnu pour un 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 ait accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant les « pop up » publicitaires peuvent devenir contrariants et dans certains cas dégrader les performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui ne s'étaient pas complètement rendu compte des termes de l'accord de licence.

Archive

Disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés.

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

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

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 Internet

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.

Cookie

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.

Lecteur de disque

C'est un 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).

Téléchargement

Copie 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.

Email

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

Evénements

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.

Faux positif

Se produit lorsqu'une analyse détecte un fichier comme étant infecté alors qu'il ne l'est pas.

Extension de fichier

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 qui se charge de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Applet Java

Il s'agit d'un programme Java conçu pour s'exécuter seulement dans une page Web. Pour utiliser une applet dans une page Web, vous devez spécifier le nom

de l'applet et la taille (la longueur et la largeur - en pixels) qu'elle 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 dans le fait qu'elles sont dirigées selon un protocole de sécurité strict.

Par exemple, bien que les applets s'exécutent sur le client, elles ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les applets sont également limitées pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.

Virus de Macro

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

Logiciel qui vous permet d'envoyer et recevoir des messages (e-mails).

Mémoire

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

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 compressés

Fichier dans un format compressé. Beaucoup de plates-formes et applications contiennent des commandes vous permettant de compresser 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 compresse les fichiers remplace la série d'espaces par un caractère spécial pour les séries d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. C'est juste une technique de compression, il y en a une multitude.

Chemin

Directions exactes vers un fichier. Ces directions sont décrites d'habitude par arborescence, de haut en bas.

Connexion entre deux points, tel le canal de communication entre deux ordinateurs.

Phishing

Action d'envoyer un email à un utilisateur en feignant d'être une entreprise connue dans le but d'obtenir frauduleusement des informations privées et qui permettront d'utiliser l'identité du destinataire du mail. Cet email oriente l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

Virus polymorphique

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

Connectique de l'ordinateur pour périphérique. Les ordinateurs comportent plusieurs sortes de ports. A l'intérieur, il y a quelques ports pour la connexion des disques, cartes vidéo. A l'extérieur, les ordinateurs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Fichier journal (Log)

Fichier qui enregistre les actions entreprises. BitDefender établit 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 malicieux 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.

Script

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention de la part de l'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 des manières 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.

Barre d'état système

Introduit avec Windows 95, la barre d'état système se situe dans la barre de tâches Windows (à côté de l'horloge) et contient des icônes miniatures pour des accès faciles aux fonctions système: fax, imprimante, modem, volume etc. Double-cliquez ou clic-droit sur une icône pour voir 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.

Troyen - Trojan (Cheval de Troie)

Programme destructeur qui prétend être une application normale. Les Trojans ne sont pas des virus et ne se repliquent pas, mais peuvent être tout aussi destructeurs. 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 Troyens, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Mise à jour

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 comporte un module spécial pour la mise à jour. Ce module vous permet de chercher manuellement les mises à jour ou de faire la mise à jour 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 crées par des personnes. Un virus simple peut faire

une copie de lui-même très vite et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est capable de se transmettre via un réseau par exemple.

Définition virus

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

Ver Internet

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.