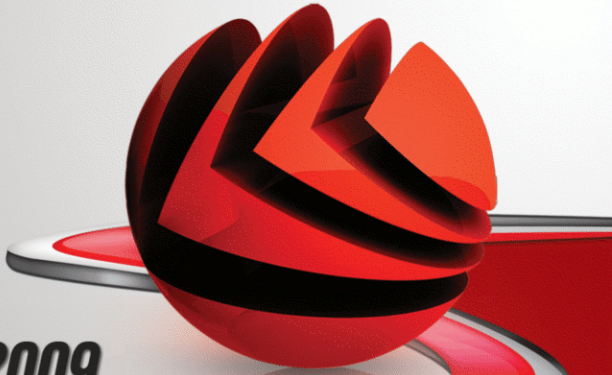
bitdefender



ANTIVIRUS 2009

Manuel d'utilisation

bitdefender

BitDefender Antivirus 2009

Manuel d'utilisation

Publié le 2008.11.05

Notice Légale

bitdefender

Table des matières

Contrat de licence logiciel pour utilisateur final

Si vous n'acceptez pas les termes et conditions de cette licence, 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 de cette licence.

ENREGISTREMENT DU PRODUIT. En acceptant cet accord de licence, vous acceptez d'enregistrer votre logiciel, en utilisant "Mon compte" comme condition pour utiliser le logiciel (et recevoir les mises à jour) et bénéficier du support. Ce contrôle assure que le logiciel s'exécute uniquement sur des ordinateurs avec des clés de licence valides et que les utilisateurs identifiés aient bien accès aux services de support. L'enregistrement nécessite un code d'activation et un e-mail valides pour le renouvellement et autres notifications légales.

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 sur les droits d'auteur et par les traités internationaux concernant le copyright, ainsi que par les autres lois et traités sur la propriété intellectuelle. BitDefender ne vous est pas vendu, la licence vous autorise seulement à l'utiliser. 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 la limite imposée par le nombre d'utilisateurs prévus dans la licence. Vous pouvez faire une seule copie de sauvegarde.

LICENCE POUR ORDINATEUR. Cette licence s'applique au logiciel BitDefender qui peut être installé sur un ordinateur unique et ne fournit pas de services réseau. Chaque utilisateur principal peut installer ce logiciel sur un ordinateur unique et faire une copie de sauvegarde sur un support différent. Le nombre d'utilisateurs principaux correspond au nombre d'utilisateurs prévu dans la licence.

DUREE DE LA LICENCE. La licence accordée ci-dessus entrera en vigueur à la date d'achat et expirera à la fin de la période de validité.

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'une telle tierce partie, quel que soit leur mode d'utilisation.

EXCLUSION DE DOMMAGES. Quiconque utilise, teste ou évalue BitDefender assume tous les risques liés à la qualité et à la performance de BitDefender. En aucun cas BITDEFENDER ne pourra être tenu responsable de tout dommage tel qu'il soit, y compris, mais de manière non-limitative, de dommages directs ou indirects résultant de l'utilisation, de la performance ou de la livraison de BitDefender, et ce même si BITDEFENDER a été informé de la possibilité de tels dommages.

CERTAINS ÉTATS N'AUTORISENT PAS LA LIMITATION OU L'EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES INDIRECTS OU CONSÉCUTIFS, DE SORTE QUE LES LIMITATIONS CI-DESSUS PEUVENT NE PAS S'APPLIQUER À VOUS.

LA RESPONSABILITÉ DE BITDEFENDER NE SAURAIT EN AUCUN CAS DÉPASSER LA SOMME QUI A ÉTÉ DÉPENSÉE POUR L'ACHAT DE BITDEFENDER. Les exclusions et limitations énoncées ci-dessus s'appliquent indépendamment du fait que vous acceptez 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.

ACCORD CONCERNANT LES INFORMATIONS ÉLECTRONIQUES. BitDefender peut avoir à vous envoyer des informations juridiques ou autre, au sujet du logiciel et des services associés à BitDefender ainsi que concernant l'utilisation qui peut être faite des informations que vous nous avez communiquées. BitDefender enverra ces informations sous forme de message via le produit lui même ou par e-mail (en utilisant les coordonnées enregistrés lors de la création de votre compte) ou publiera des informations sur son site Internet. En acceptant cet Accord, vous acceptez de recevoir des informations sous forme électronique et reconnaissez avoir connaissance que ces informations sont disponibles sur les sites Internet de BitDefender.

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 désaccord 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.

Pour contacter BitDefender, rendez-vous sur www.bitdefender.fr, rubrique "Nous contacter" ou "Assistance".

Préface

Ce Manuel d'utilisation est destiné à tous les utilisateurs qui ont choisi **BitDefender Antivirus 2009** 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 2009**, il vous apprendra comment le configurer. Vous y apprendrez les méthodes d'utilisation de **BitDefender Antivirus 2009**, 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. xiv)	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. Instructions pas à pas pour installer BitDefender sur un poste de travail. Il s'agit d'un tutoriel clair sur l'installation de **BitDefender Antivirus 2009**. Commençant par les pré requis pour une installation réussie, vous serez guidé à travers le processus d'installation entier. 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.

Administration avancée. Présentation détaillée des fonctions de sécurité fournies par BitDefender. 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.).

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

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

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. Configuration requise

Vous pouvez installer BitDefender Antivirus 2009 seulement sur les ordinateurs fonctionnant sur les systèmes d'exploitation suivants :

- Windows XP avec le Service Pack 2 (32/64 Bit) ou supérieur
- Windows Vista (32/64 Bit) ou Windows Vista avec le Service Pack 1
- Windows Home Server

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

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

1.1. Matériel

Pour Windows XP

- Processeur 800 MHz ou supérieur
- Mémoire minimum : 256Mo de RAM (1 Go recommandé)
- 170 Mo d'espace disque disponible (200 Mo recommandés)

Pour Windows Vista

- Processeur 800 MHz ou supérieur
- Mémoire minimum : 512Mo de RAM (1 Go recommandé)
- 170 Mo d'espace disque disponible (200 Mo recommandés)

Pour Windows Home Server

- Processeur 800 MHz ou supérieur
- Mémoire minimum : 512Mo de RAM (1 Go recommandé)
- 170 Mo d'espace disque disponible (200 Mo recommandés)

1.2. Logiciels

- Internet Explorer 6.0 (ou version supérieure)
- .NET Framework 1.1 (également disponible dans le kit d'installation)

La protection antiphishing est seulement disponible pour :

- Internet Explorer 6.0 (ou version supérieure)
- Mozilla Firefox 2.0
- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

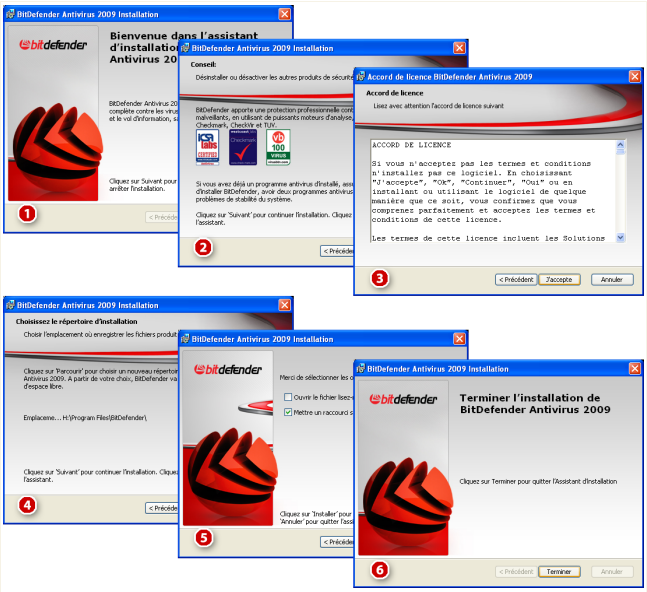
Le cryptage des messageries instantanées est disponible seulement pour :

- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

2. Installation de BitDefender

Localisez le fichier d'installation et double-cliquez dessus. Ceci lancera l'assistant d'installation, qui vous guidera pendant le processus.

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 2009 :

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

   BitDefender Antivirus 2009 vous prévient 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. Veuillez lire les accords de licence et cliquez sur **J'accepte**.

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

4. Par défaut, BitDefender Antivirus 2009 sera installé sur `C:\Programmes Fichiers\BitDefender\BitDefender 2009`. Si vous voulez choisir un autre répertoire, cliquez sur **Parcourir** et 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 BitDefender Antivirus 2009 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** pour commencer l'installation du produit. Si il n'est pas déjà installé, BitDefender commencera par installer .NET Framework 1.1.

   Patientez jusqu'à la fin de l'installation.

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.

Important

Après avoir effectué l'installation et redémarré l'ordinateur, un assistant d'enregistrement et un assistant de configuration apparaîtront. Utilisez ces assistants pour enregistrer et configurer BitDefender Antivirus 2009 ainsi que pour créer un compte BitDefender.

Si vous avez accepté les paramètres par défaut pour le chemin d'installation, vous pouvez constater l'existence d'un nouveau dossier dans `Program Files`, intitulé `BitDefender`, qui contient le sous-dossier `BitDefender 2009`.

2.1. Assistant d'enregistrement

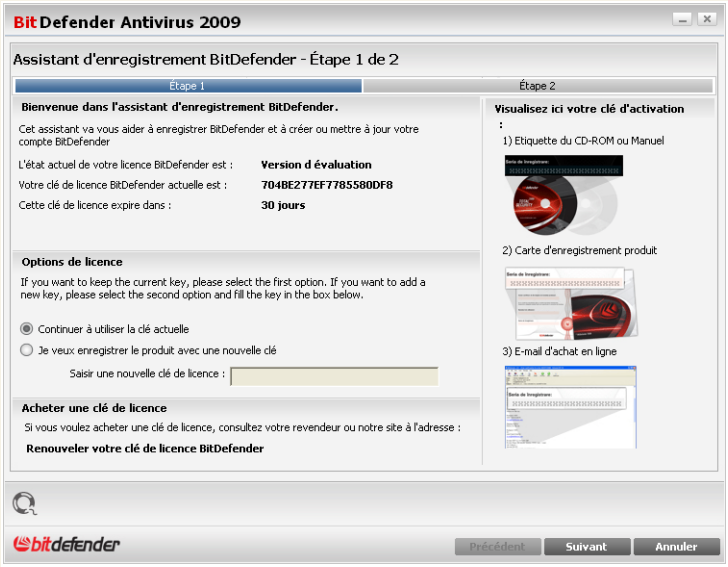
La première fois que vous démarrerez l'ordinateur après l'installation, un assistant d'enregistrement apparaîtra. Cet assistant vous aide à enregistrer votre produit et à configurer un compte BitDefender.

Vous devez créer un compte BitDefender afin de recevoir les mises à jour BitDefender. Le compte BitDefender vous donne accès au support technique gratuit, à des offres spéciales et à des promotions. Si vous perdrez votre clé d'activation BitDefender, vous pouvez la retrouver en vous connectant sur votre compte à l'adresse http://myaccount.bitdefender.com.

Note

Si vous ne voulez pas utiliser cet assistant, cliquez sur **Annuler**. Vous pouvez ouvrir l'assistant d'enregistrement n'importe quand en cliquant sur le lien **Enregistrer**, situé en bas de l'interface du produit.

2.1.1. Étape 1 sur 2 - Enregistrer BitDefender Antivirus 2009



Enregistrement

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

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

Pour enregistrer BitDefender Antivirus 2009 :

1. Sélectionnez **Je veux enregistrer le produit avec une nouvelle clé**.
2. Entrez la clé d'activation dans le champ de saisie.

Note

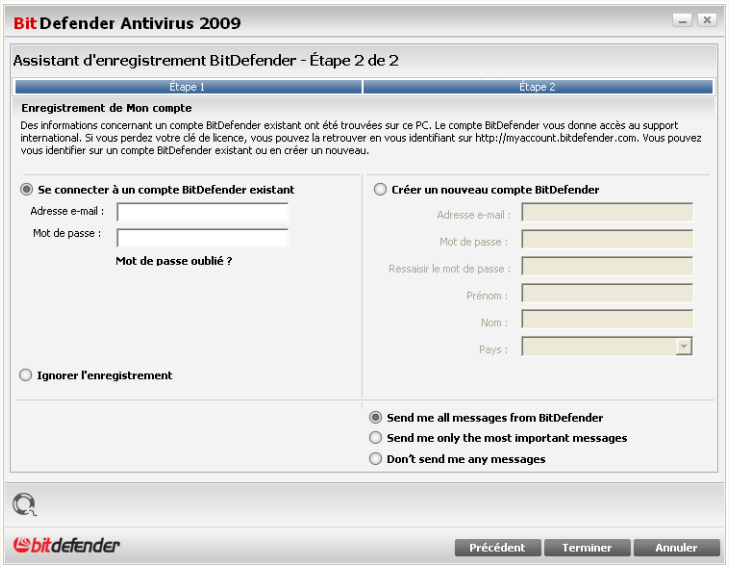
Vous trouverez votre clé d'activation :

- sur l'étiquette du CD.
- sur la carte d'enregistrement du produit.
- sur l'e-mail d'achat en ligne.

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

Cliquez sur **Suivant** pour continuer.

2.1.2. Etape 2 sur 2 - Créer un compte BitDefender



Création de compte

Si vous ne souhaitez pas créer un compte BitDefender, sélectionnez **Passer l'enregistrement** et cliquez sur **Terminer**. Autrement, procédez selon votre situation actuelle :

- « Je n'ai pas de compte BitDefender » (p. 9)
- « J'ai déjà un compte BitDefender » (p. 9)

Important

Vous devez créer un compte dans les 15 jours après l'installation de BitDefender (si vous vous enregistrez, l'expiration est repoussée à 30 jours). Dans le cas contraire, BitDefender ne se mettra plus à jour.

Je n'ai pas de compte BitDefender

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. Le mot de passe doit comporter au moins six 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.

Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte. Sélectionnez l'une des actions disponibles :

- **Envoyez moi tous les messages provenant de BitDefender**
- **Envoyez moi uniquement les messages les plus importants**
- **Je ne veux recevoir aucun message**

Cliquez sur **Terminer**.

J'ai déjà un compte BitDefender

BitDefender détectera automatiquement si vous avez déjà un compte BitDefender actif sur cet ordinateur. Dans ce cas, veuillez fournir le mot de passe de votre compte.

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.

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

Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte. Sélectionnez l'une des actions disponibles :

- **Envoyez moi tous les messages provenant de BitDefender**
- **Envoyez moi uniquement les messages les plus importants**
- **Je ne veux recevoir aucun message**

Cliquez sur **Terminer**.

2.2. Assistant de configuration

Une fois l'enregistrement terminé, un assistant de configuration s'affiche. L'assistant vous aide à configurer les modules spécifiques du produit et à paramétrer BitDefender pour qu'il effectue 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 Antivirus 2009.

Note

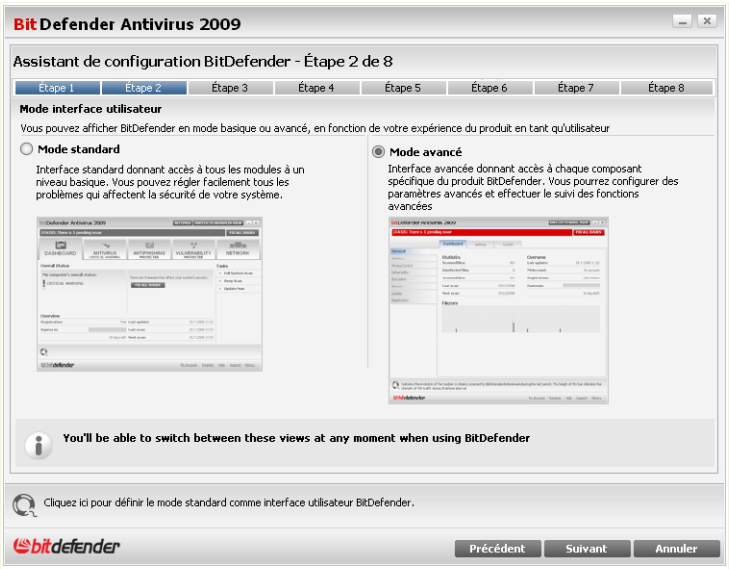
Si vous ne voulez pas utiliser cet assistant, cliquez sur **Annuler**. BitDefender vous avertira des éléments que vous avez besoin de configurer quand vous ouvrirez l'interface utilisateur.

2.2.1. Etape 1/8 - Fenêtre de bienvenue

Fenêtre de bienvenue

Cliquez sur **Suivant** pour continuer.

2.2.2. Étape 2/8 - Sélectionner l'interface



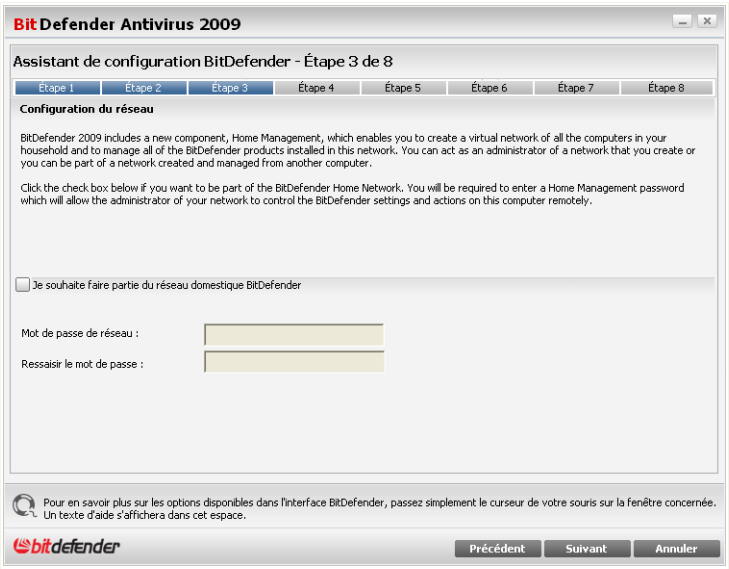
Modes d'affichage

Choisissez l'une ou l'autre des deux interfaces utilisateur, selon l'usage que vous comptez faire de BitDefender :

- **Mode standard.** Interface simplifiée, adaptée aux débutants et aux utilisateurs souhaitant réaliser des tâches basiques et résoudre facilement les problèmes. Il vous suffit de suivre les avertissements et les alertes de BitDefender et de remédier aux problèmes signalés.
- **Mode avancée.** Interface avancée adaptée aux utilisateurs plus techniques, souhaitant entièrement configurer leur produit. Vous pouvez configurer chaque composant du produit et réaliser des tâches avancées.

Cliquez sur **Suivant** pour continuer.

2.2.3. Étape 3/8 - Configurer le réseau BitDefender



Configuration du réseau BitDefender

BitDefender vous permet de créer un réseau virtuel rassemblant tous les ordinateurs de votre foyer, et de gérer ensuite les produits BitDefender installés sur ce réseau.

Si vous voulez que cet ordinateur fasse partie du réseau personnel BitDefender, suivez ces étapes :

1. Sélectionnez l'option **Je veux rejoindre le réseau domestique BitDefender**.
2. Entrez le même mot de passe d'administration dans chacun des champs de saisie.

Important

Ce mot de passe permet à l'administrateur de gérer le produit BitDefender à partir d'un autre ordinateur.

Cliquez sur **Suivant** pour continuer.

2.2.4. Étape 4/8 - Configurer le contrôle d'identité

Configuration du contrôle d'identité

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

Suivez les étapes suivantes pour utiliser le contrôle d'identité :

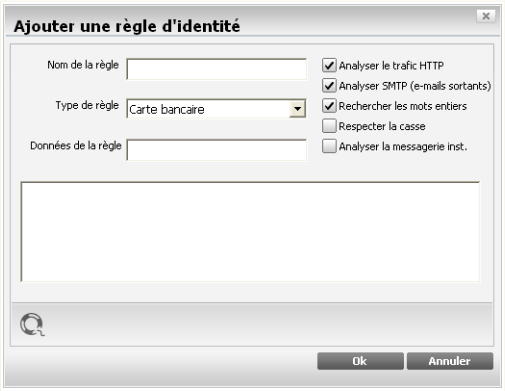
1. Sélectionnez **Je veux le configurer maintenant**.
2. Définissez les règles nécessaires à la protection de vos données sensibles. Pour plus d'informations, reportez-vous à « Création de règles de contrôle d'identité » (p. 15).

3. Définissez si nécessaire des exceptions pour les règles que vous venez de créer. Pour plus d'informations, reportez-vous à « Création d'exceptions au contrôle d'identité » (p. 16).

Cliquez sur **Suivant** pour continuer.

Création de règles de contrôle d'identité

Pour créer une règle de contrôle d'identité, cliquez sur **Ajouter**. La fenêtre de configuration s'affichera.



Règle de contrôle d'identité

Vous devez définir les paramètres suivants:

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

> ***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.

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.

Afin d'identifier aisément les informations bloquées par la règle, vous pouvez spécifier une description détaillée de la règle dans la boîte d'édition.

Pour spécifier le type de trafic à analyser, configurez ces options :

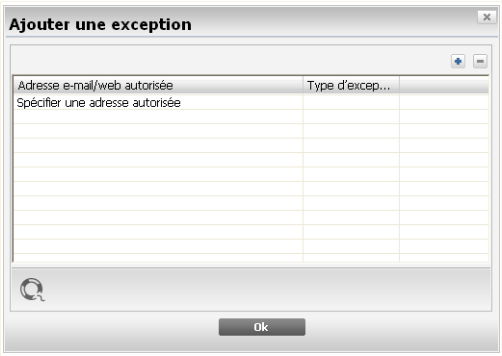
- **Analyse HTTP** - Analyse le flux HTTP (web) et bloque les données qui sont prévues dans la règle de gestion des données.
- **Analyse SMTP** - Analyse le flux SMTP (mail) et bloque les emails sortants qui contiennent les éléments déterminés dans la règle de gestion des données.
- **Analyser la messagerie instantanée** - Analyse le trafic de messagerie instantanée et bloque les échanges sortants qui contiennent les éléments déterminés dans la règle de gestion des données.

Cliquez sur **OK** pour ajouter la règle.

Création d'exceptions au contrôle d'identité

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 au contrôle d'identité

Pour ajouter une exception, procédez comme suit :

1. Cliquez sur le bouton **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 effacer une exception, sélectionnez-la et cliquez sur le bouton **Effacer**.

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

2.2.5. Étape 5/8 - Configurer des rapports d'infection

Options pour les rapports d'infection

BitDefender peut envoyer au laboratoire BitDefender des rapports anonymes listant les virus détectés sur votre ordinateur, afin de garder une trace des alertes virales.

Voici les options d'analyse que vous pouvez configurer :

- **Envoyer des rapports de virus** - envoie aux laboratoires BitDefender des rapports concernant les virus identifiés sur votre ordinateur.
- **Activer l'Outbreak Detection de BitDefender** - envoie des rapports aux laboratoires BitDefender à propos d'apparitions éventuelles de virus.

Note
Ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.

Cliquez sur **Suivant** pour continuer.

2.2.6. Etape 6/8 - Sélectionner les tâches à lancer

Sélection des tâches

Paramétrez BitDefender Antivirus 2009 pour lancer les tâches de sécurité importantes pour la sécurité de votre ordinateur. Les options suivantes sont disponibles:

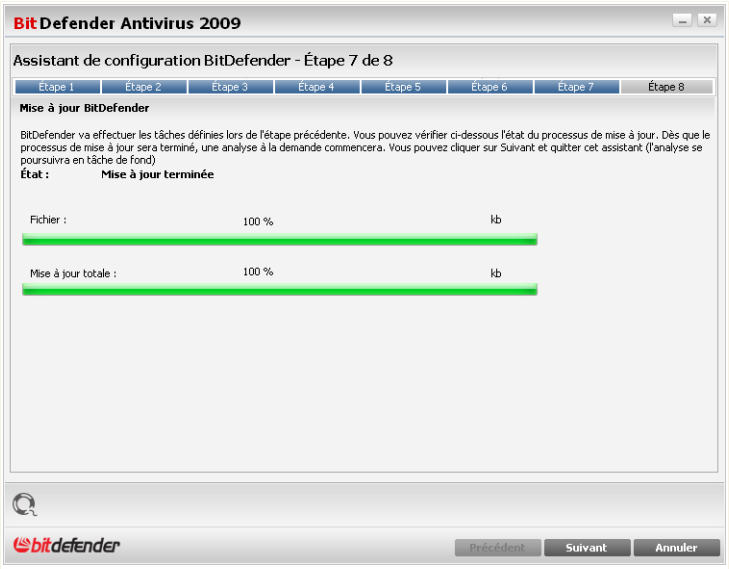
- **Mettre à jour les moteurs BitDefender (peut necéssiter un redémarrage)** - une mise à jour des moteurs de BitDefender aura lieu pendant la prochaine étape pour protéger votre ordinateur contre les dernières menaces.
- **Lancer une analyse rapide (peut necéssiter un redémarrage)** - Une analyse rapide 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.

2.2.7. Etape 7/8 - 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.

2.2.8. Etape 8/8 - Terminer

Terminer

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

Cliquez sur **Terminer**.

3. Mise à jour majeure

Pour mettre à niveau une ancienne version de BitDefender vers BitDefender Antivirus 2009, suivez ces étapes :

1. Supprimer l'ancienne version de BitDefender de votre ordinateur. Pour plus d'informations, veuillez consulter le fichier d'aide ou le manuel du produit.
2. Redémarrer votre système.
3. Installez BitDefender Antivirus 2009 comme décrit dans la « *Installation de BitDefender* » (p. 4) section de ce guide utilisateur.

4. Réparer ou supprimer BitDefender

Si vous souhaitez réparer ou supprimer **BitDefender Antivirus 2009**, suivez le chemin suivant depuis le menu Démarrer de Windows: **Démarrer** → **Programmes** → **BitDefender 2009** → **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.

  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 2009.

  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

  Uniquement Windows Vista ! 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.

  Cliquez sur **Supprimer** pour désinstaller BitDefender Antivirus 2009 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-dossier`BitDefender` du dossier `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

5. Pour commencer

Une fois BitDefender installé, votre ordinateur est protégé.

5.1. Démarrer BitDefender Antivirus 2009

La première étape pour tirer le meilleur de BitDefender est de lancer l'application.

Pour accéder à l'interface principale de BitDefender Antivirus 2009, cliquez dans le menu Démarrer de Windows sur **Démarrer** → **Programmes** → **BitDefender 2009** → **BitDefender Antivirus 2009**. Vous pouvez également aller plus vite en double-cliquant sur **l'icône BitDefender** dans la zone de notification.

5.2. Mode d'affichage de l'interface utilisateur

BitDefender Antivirus 2009 répond aux besoins de tous les utilisateurs, qu'ils soient débutants ou armés de solides connaissances techniques. L'interface utilisateur graphique est donc conçue pour s'adapter à chaque catégorie d'utilisateurs.

Vous pouvez afficher BitDefender en mode standard ou avancé, en fonction de votre expérience du produit en tant qu'utilisateur

Note
Vous pouvez aisément passer d'une fenêtre à l'autre en cliquant respectivement sur le bouton **Passer en Mode standard** ou **Passer en Mode avancée**.

5.2.1. Mode standard

Le mode standard est une interface simple qui vous donne accès à tous les modules à un niveau basique. Vous devrez effectuer le suivi des avertissements et des alertes critiques et corriger les problèmes survenant.

Mode standard

- Comme vous pouvez le constater, la partie supérieure de la fenêtre comporte deux boutons et une barre d'état.

Élément	Description
Paramètres	Ouvre une fenêtre dans laquelle vous pouvez aisément activer ou désactiver des modules de sécurité importants.
Passer en Mode avancé	Ouvre la fenêtre Mode avancé. Celle-ci vous permet d'accéder à la liste complète des modules et de configurer en détail chacun des composants. BitDefender gardera ce paramètre en mémoire pour l'appliquer automatiquement à la prochaine ouverture de l'interface utilisateur.
État	Contient des informations sur les vulnérabilités de sécurité de votre ordinateur et vous aide à y remédier.

- Au milieu de la fenêtre figurent cinq onglets.

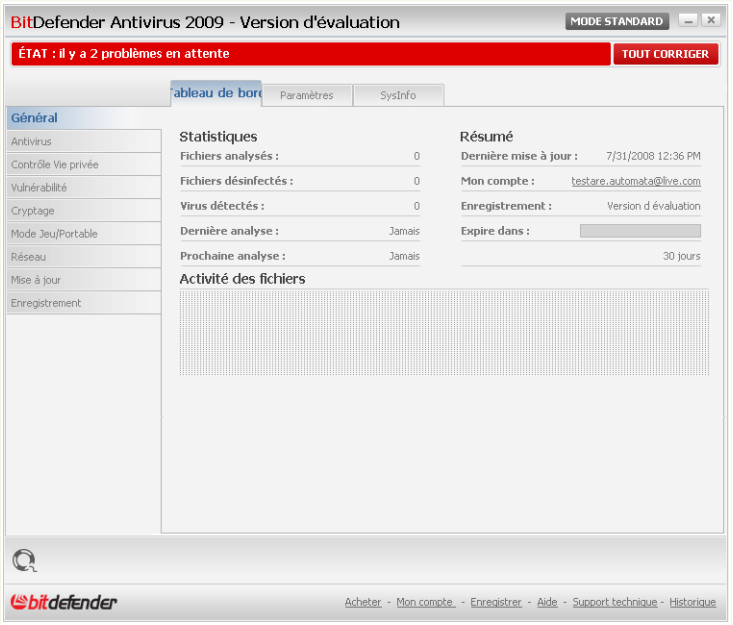
Onglet	Description
Tableau de bord	Affiche des statistiques produit significatives et l'état de votre enregistrement, ainsi que des liens vers les tâches à la demande les plus importantes.
Antivirus	Affiche l'état du module antivirus qui vous aide à maintenir votre antivirus à jour et vous protège des virus.
Antiphishing	Affiche l'état du module antiphishing qui vérifie que toutes les pages Internet auxquelles vous accédez avec Internet Explorer ou Firefox sont sûres.
Vulnerabilité	Affiche l'état du module d'analyse des vulnérabilités qui vous aide à maintenir à jour les logiciels majeurs de votre ordinateur.
Réseau	Affiche la structure du réseau domestique BitDefender.

- De plus, la fenêtre Mode standard de BitDefender contient de nombreux autres raccourcis très utiles.

Lien	Description
Mon compte	Vous permet de créer ou de vous connecter à votre compte BitDefender. Le compte BitDefender vous donne un accès gratuit au Support Technique.
Enregistrer	Vous permet de saisir une nouvelle clé de licence ou de consulter la clé de licence actuelle et l'état de votre enregistrement.
Aide	Vous donne accès à un fichier d'aide qui va vous apprendre à utiliser BitDefender.
Support technique	Vous permet de contacter l'équipe du Support Technique BitDefender.
Historique	Vous permet d'afficher un historique détaillé de toutes les tâches exécutées par BitDefender sur votre système.

5.2.2. Mode avancée

Le Mode avancé vous donne accès à chaque composant spécifique du produit BitDefender. Vous pourrez configurer des paramètres avancés et effectuer le suivi des fonctions avancées.



Mode avancée

- Comme vous pouvez le constater, la partie supérieure de la fenêtre comporte un bouton et une barre d'état.

Élément	Description
Passer en mode standard	Ouvre la fenêtre Mode standard. Celle-ci vous permet de visualiser l'interface de base de BitDefender comprenant les modules principaux (Sécurité, Optimisation, Gestionnaire de fichiers, Réseau) et un tableau de bord. BitDefender gardera

Élément	Description
	ce paramètre en mémoire pour l'appliquer automatiquement à la prochaine ouverture de l'interface utilisateur.
État	Contient des informations sur les vulnérabilités de sécurité de votre ordinateur et vous aide à y remédier.

- À gauche de la fenêtre figure un menu contenant l'intégralité des modules de sécurité.

Module	Description
Général	Vous permet d'accéder aux paramètres généraux ou de consulter le tableau de bord et des informations détaillées sur le système.
Antivirus	Vous permet de configurer en détail votre antivirus et les opérations d'analyse, de définir les exceptions et de configurer le module Quarantaine.
Contrôle Vie privée	Vous permet d'éviter le vol de données sur votre ordinateur et de protéger votre vie privée lorsque vous êtes en ligne.
Cryptage	Vous permet de crypter les communications Yahoo et Windows Live (MSN) Messenger.
Vulnerabilité	Vous permet de maintenir à jour les logiciels majeurs de votre ordinateur.
Mode Jeu/Portable	Vous permet de reporter les tâches programmées BitDefender si votre ordinateur portable fonctionne sur batterie, ainsi que de désactiver toutes les alertes et pop-ups lorsqu'un jeu vidéo est lancé.
Réseau	Vous permet de configurer et de gérer les différents ordinateurs présents dans votre foyer.
Mise à jour	Vous permet d'obtenir des informations sur les dernières mises à jour, de mettre à jour votre produit et de configurer en détail le processus de mise à jour.
Enregistrement	Vous permet d'enregistrer BitDefender Antivirus 2009, de modifier la clé d'activation ou de créer un compte BitDefender.

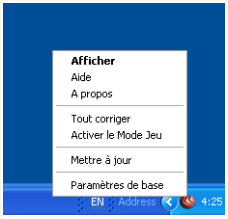
- De plus, la fenêtre Mode avancé de BitDefender contient de nombreux autres raccourcis très utiles.

Lien	Description
Mon compte	Vous permet de créer ou de vous connecter à votre compte BitDefender. Le compte BitDefender vous donne un accès gratuit au Support Technique.
Enregistrer	Vous permet de saisir une nouvelle clé de licence ou de consulter la clé de licence actuelle et l'état de votre enregistrement.
Aide	Vous donne accès à un fichier d'aide qui va vous apprendre à utiliser BitDefender.
Support technique	Vous permet de contacter l'équipe du Support Technique BitDefender.
Historique	Vous permet d'afficher un historique détaillé de toutes les tâches exécutées par BitDefender sur votre système.

5.3. 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.

Un double-clic sur cette icône entraîne l'ouverture de BitDefender. Un clic droit entraîne l'affichage d'un menu contextuel, qui vous permet de gérer rapidement votre produit BitDefender.



Icône BitDefender

- **Afficher** - ouvre BitDefender.
- **Aide** - ouvre le fichier d'aide présentant en détail BitDefender Antivirus 2009.
- **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.
- **Mettre à jour** - effectue une mise à jour immédiate. Une nouvelle fenêtre apparaît affichant l'état de la mise à jour.

- **Paramètres standard** - vous permet d'activer ou de désactiver facilement les modules de sécurité importants. Une nouvelle fenêtre apparaît, vous permettant d'activer/de désactiver un élément d'un simple clic.

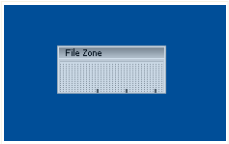
Lorsque vous êtes en Mode Jeu, vous pouvez voir la lettre G incrustée sur l'icône BitDefender.

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.

5.4. 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 grises (la **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. Pour plus d'informations, reportez-vous à « *Analyse par glisser&déposer* » (p. 132).

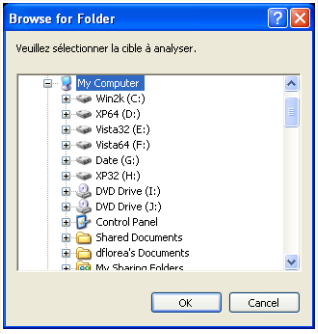
Si vous ne souhaitez plus voir cette barre, il vous suffit de faire un clic-droit dessus et de choisir **Cacher**. Pour masquer cette fenêtre, procédez comme suit:

1. Cliquez sur **Passer en Mode avancé** (si vous êtes en **Mode standard**).
2. Cliquez sur le module **Général** dans le menu situé en partie gauche.
3. Cliquez sur l'onglet **Paramètres**.
4. Décochez la case **Activer la barre d'activité d'analyse (sur le graphique d'activité du produit)**

5.5. 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, cliquez dans le menu Démarrer de Windows sur **Démarrer → Programmes → BitDefender 2009 → 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.

5.6. Mode Jeu

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

- Réduire les sollicitations processeur et la consommation de mémoire
- Reporter les mises à jour automatiques et les analyses
- Éliminer toutes les alertes et pop-ups
- Analyser uniquement les fichiers les plus importants

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

5.6.1. 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**.

- Appuyez sur les touches `Ctrl+Shift+Alt+G` (le raccourci clavier par défaut).

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

5.6.2. Changer le raccoruci clavier du Mode Jeu

Pour changer le raccourci clavier, suivez les étapes suivantes :

1. Cliquez sur **Passer en Mode avancé** (si vous êtes en **Mode standard**).
2. Cliquez sur **Mode Jeu / Portable** dans le menu situé en partie gauche.
3. Cliquez sur l'onglet **Mode Jeu**.
4. Cliquez sur **Paramètres avancés**.
5. Sous l'option **Utiliser le raccourci**, définissez le raccourci clavier désiré :
   - Choisissez la touche que vous souhaitez utiliser en cochant l'une des suivantes : touche Contrôle (`Ctrl`), Touche Shift(`Shift`) ou touche Alt (`Alt`).
   - Dans le champ éditable, entrez la lettre que vous souhaitez utiliser.

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

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

5.7. Intégration dans les navigateurs Internet

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.

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

- Internet Explorer
- Mozilla Firefox

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

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

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

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 définir les paramètres de la barre d'outils antiphishing.

  Les options suivantes sont disponibles:
  - **Activer l'analyse** - active l'analyse antiphishing.

- **Demander avant d'ajouter à une liste blanche** - demande votre autorisation avant d'ajouter un site Web à la liste blanche.

- **Ajouter à la liste blanche** - ajoute le site Web actuel à la liste blanche.

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.

5.8. Intégration dans Messenger

BitDefender dispose d'une fonction de cryptage pour protéger vos documents confidentiels et vos conversations via les messageries instantanées Yahoo Messenger et MSN Messenger.

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

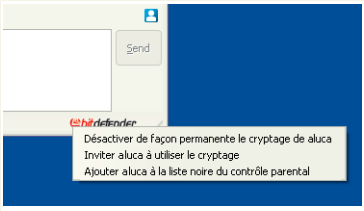
- votre correspondant ait installé sur son ordinateur une version de BitDefender qui prenne en charge le cryptage de messagerie instantanée et que ce dernier soit activé pour l'application de messagerie instantanée utilisée pour converser ;
- vous et votre correspondant utilisiez soit Yahoo Messenger, soit Windows Live (MSN) Messenger.

Important
BitDefender ne cryptera pas la conversation si le correspondant utilise une application à interface Web, telle que Meebo, ou une autre application de chat compatible Yahoo Messenger ou MSN.

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

En faisant un clic-droit sur la barre d'outils BitDefender vous obtiendrez les options suivantes :

- Activer/désactiver de manière permanente le cryptage pour le chat avec un contact en particulier.
- Inviter un contact de chat particulier à utiliser le cryptage
- Supprimer un contact particulier de la Liste noire du contrôle parental



Options de Cryptage des messageries instantanées

Cliquez sur l'option choisie dans la liste ci dessus pour l'utiliser.

6. Tableau de bord

En cliquant sur l'onglet Tableau de bord, vous pourrez accéder à des statistiques produit significatives et à l'état de votre enregistrement, ainsi qu'à des liens vers les tâches à la demande les plus importantes.

Tableau de bord

6.1. Vue d'ensemble

Vous pouvez consulter ici un récapitulatif des statistiques sur l'état de la mise à jour, l'état de votre compte et les informations d'enregistrement et de licence.

Élément	*Description*
Dernière mise à jour	Indique la date à laquelle votre produit BitDefender a été mis à jour pour la dernière fois. Veuillez réaliser des mises à jour régulières afin de bénéficier d'un système parfaitement protégé.
Mon compte	Indique l'adresse e-mail que vous pouvez utiliser pour accéder à votre compte en ligne, afin de récupérer votre clé de licence

Élément	Description
	BitDefender, si vous l'avez perdue, et de bénéficier du Support Technique BitDefender ainsi que d'autres services personnalisés.
Enregistrement	Indique le type et l'état de votre clé de licence. Pour conserver votre système à l'abri des menaces, vous devez renouveler la clé ou mettre à niveau BitDefender si votre clé a expiré.
Expire dans	Indique le nombre de jours avant l'expiration de la clé de licence.

Pour mettre à jour BitDefender, il vous suffit de cliquer sur **Mettre à jour** dans la section Tâches.

Procédez comme suit pour créer votre compte BitDefender ou vous y connecter.

1. Cliquez sur le lien **Mon compte** en bas de la fenêtre. Une page Web s'affiche.
2. Saisissez vos nom d'utilisateur et mot de passe, puis cliquez sur **Connexion**.
3. Pour créer un compte BitDefender, sélectionnez **Vous n'avez pas de compte ?** et spécifiez les informations demandées.

Note
Les informations communiquées ici resteront confidentielles.

Procédez comme suit pour enregistrer BitDefender Antivirus 2009.

1. Cliquez sur le lien **Mon compte** en bas de la fenêtre. Un assistant d'enregistrement en une étape s'affiche.
2. Sélectionnez l'option **Je veux enregistrer le produit avec une nouvelle clé**.
3. Saisissez la nouvelle clé de licence dans la zone de texte correspondante.
4. Cliquez sur **Terminer**.

Procédez comme suit pour acheter une nouvelle clé de licence.

1. Cliquez sur le lien **Mon compte** en bas de la fenêtre. Un assistant d'enregistrement en une étape s'affiche.
2. Cliquez sur le lien **Renouveler votre clé de licence BitDefender**. Une page Web s'affiche.
3. Cliquez sur **Acheter maintenant**.

6.2. Tâches

Vous pouvez trouver ici des liens vers les tâches de sécurité les plus importantes : analyse complète du système, analyse approfondie, mettre à jour.

Voici les différents boutons proposés:

- **Analyse complète du système** -lance une analyse complète de votre ordinateur (hors archives).
- **Analyse approfondie** - lance une analyse complète de votre ordinateur (archives inclues).
- **Mettre à jour** - effectue une mise à jour immédiate.

6.2.1. 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
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 malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse approfondie	Analyse l'ensemble du système. La configuration par défaut permet d'analyser tous les types de codes malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.

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

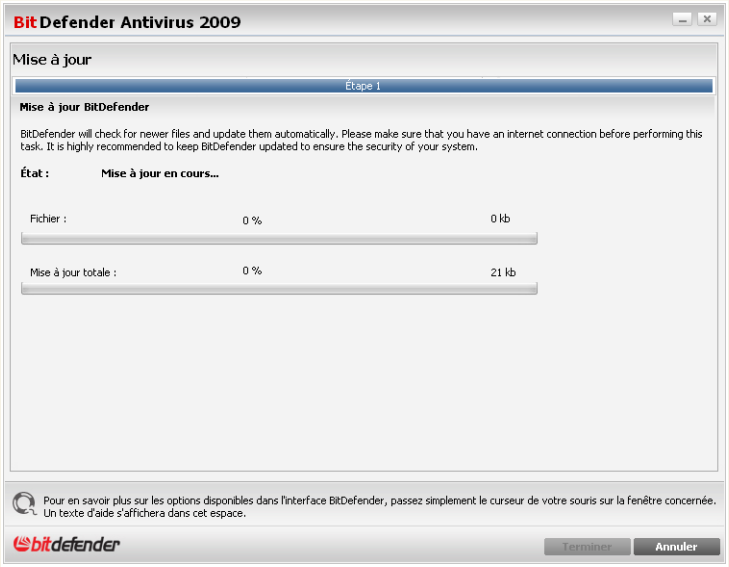
Lorsque vous lancez un processus d'analyse sur demande, que ce soit une analyse rapide ou complète, le moteur d'analyse BitDefender apparaît.

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

6.2.2. 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 voulez fermer cette fenêtre, cliquez simplement sur **Annuler**. 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.

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.

7. Antivirus

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

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

Antivirus

Le module Antivirus se compose de deux sections :

- **Composants contrôlés** - Vous permet de consulter la liste complète des composants contrôlés pour chaque module de sécurité. Vous pouvez définir les modules devant être contrôlés. Nous vous recommandons d'activer le contrôle sur l'intégralité des composants.
- **Tâches** - Vous pouvez trouver ici des liens vers les tâches de sécurité les plus importantes : analyse complète du système, analyse approfondie, mettre à jour.

7.1. Composants contrôlés

Le composant surveillé est le suivant :

Catégorie	Description
Sécurité locale	Vous permet de vérifier l'état des différents modules de sécurité protégeant les objets stockés sur votre ordinateur (fichiers, base de registre, mémoire, etc.).

Cliquez sur une case "+" pour ouvrir une arborescence et sur une case "-" pour la fermer.

7.1.1. Sécurité locale

Nous savons qu'il est important que vous soyez informé dès lors qu'un problème est susceptible d'affecter la sécurité de votre ordinateur. En contrôlant chacun des modules de sécurité, BitDefender Antivirus 2009 vous signalera non seulement les configurations que vous définissez pouvant affecter la sécurité de votre ordinateur, mais vous rappellera aussi à l'ordre lorsque vous oubliez d'exécuter des tâches importantes.

Les problèmes concernant la sécurité locale sont décrits à l'aide de messages très explicites. Si un élément est susceptible de compromettre la sécurité de votre ordinateur, vous verrez apparaître en regard de chacun de ces messages un bouton d'état rouge intitulé **Corriger**. Dans le cas contraire, un bouton d'état vert **OK** est affiché.

Problème de sécurité	Description
Protection des fichiers en temps réel activée	Garantit que tous les fichiers sont analysés dès qu'un accès se produit (par vous ou par une application s'exécutant sur ce système).
Vous avez analysé votre ordinateur pour rechercher des malwares aujourd'hui	Il est fortement recommandé d'exécuter une analyse à la demande dès que possible pour contrôler que les fichiers présents sur votre ordinateur ne contiennent pas de malwares.
Mise à jour automatique activée	Laissez la mise à jour automatique activée pour vous assurer que les signatures de malwares de votre programme BitDefender sont mises à jour de manière régulière.
Mise à jour en cours	La mise à jour du programme et des signatures de malwares est en cours.

Lorsque les boutons d'état sont verts, le risque de sécurité pour votre système est au niveau minimum. Procédez comme suit pour obtenir des boutons d'état verts :

1. Cliquez sur les boutons **Corriger** pour corriger une à une les vulnérabilités de sécurité.
2. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

Si vous souhaitez exclure un problème du contrôle, il vous suffit de décocher la case correspondante **Oui, contrôler ce composant**.

7.2. Tâches

Vous pouvez trouver ici des liens vers les tâches de sécurité les plus importantes : analyse complète du système, analyse approfondie, mettre à jour.

Voici les différents boutons proposés:

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

7.2.1. 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
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 malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse approfondie	Analyse l'ensemble du système. La configuration par défaut permet d'analyser tous les types de codes

Tâche	Description
	malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
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 personnalisée	Utilisez cette tâche pour définir des fichiers et dossiers spécifiques à analyser.

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:

Analyse personnalisée

En cliquant sur le bouton **Analyse personnalisée** et en suivant les instructions de l'assistant, vous pouvez créer des tâches d'analyse personnalisées et les définir comme tâches rapides.

Etape 1/4- Fenêtre d'accueil

Page d'accueil.

Fenêtre de bienvenue

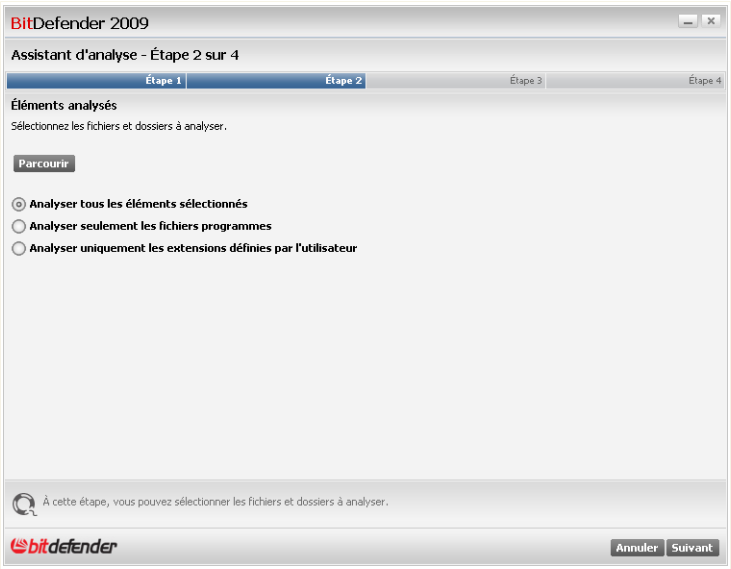
Cet assistant va vous aider à analyser votre ordinateur pour rechercher d'éventuelles menaces pouvant l'affecter. Vous pourrez sélectionner des fichiers et/ou dossiers à être analysés et définir des actions à entreprendre sur les fichiers infectés. Vous recevrez également un rapport d'analyse qui vous aidera à évaluer le niveau de sécurité de votre système. Parcourez chaque étape et configurer les processus d'analyse selon vos besoins.

Note
Pour passer cette étape dans les analyses futures, cochez simplement la case correspondante.

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

Étape 2/4 - Définir les éléments à analyser

Durant cette étape, vous pouvez choisir les fichiers et dossier à analyser.



Définir les éléments à analyser

Cliquez sur Parcourir pour sélectionner les dossiers et/ou fichiers spécifiques sur votre ordinateur.

Les options suivantes sont disponibles:

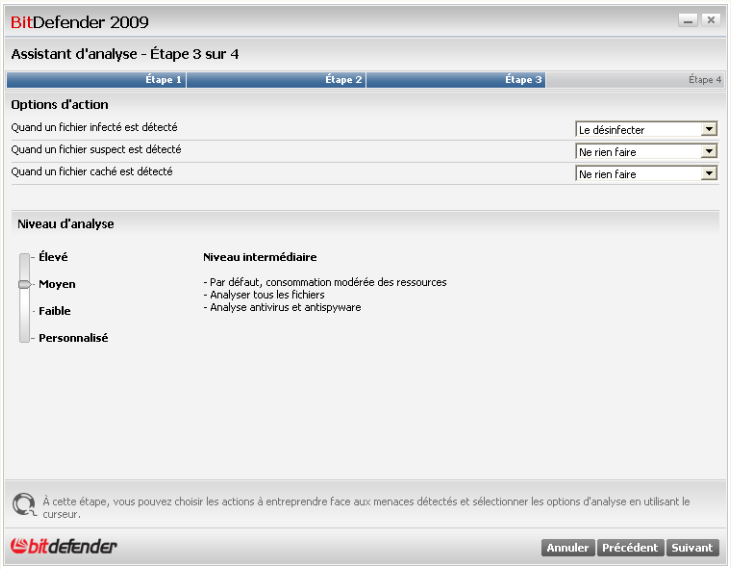
Option	*Description*
Analyser tous les éléments sélectionnés	Sélectionnez cette option pour analyser uniquement les éléments sélectionnés précédemment.
Analyse des extensions à risques seulement	Sélectionnez cette option pour n'analyser que les programmes et les applications.
Analyser uniquement les extensions définies par l'utilisateur	Sélectionnez cette option pour analyser uniquement les extensions spécifiques que vous voulez analyser. Une boîte de dialogue s'affichera dans laquelle vous pourrez entrer ces extensions.

Option	Description
	Note Les extensions doivent être séparées par un point-virgule “;”.

Cliquez sur **Suivant** pour continuer ou sur **Annuler** si vous voulez quitter l’assistant.

Étape 3/4 - Sélectionner les actions à entreprendre

Durant cette étape, vous pouvez choisir quelles actions entreprendre lorsque des menaces sont détectées et sélectionner des options d'analyse en utilisant le curseur.



Sélectionner les actions à entreprendre

Vous pouvez sélectionner les actions à entreprendre à partir du menu correspondant :

- **Lorsqu'un fichier infecté est détecté**
- **Lorsqu'un fichier suspect est détecté**

■ **Lorsqu'un fichier camouflé est détecté**

Au même moment, vous avez la possibilité de configurer le niveau de protection de l'analyse. 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 4 niveaux de protection :

Niveau de protection	*Description*
Agressif	Offre un niveau de sécurité élevé. La consommation de ressources système est importante. ■ Analyser tous les fichiers et archives ■ Analyser pour rechercher les virus et spyware ■ Analyser pour rechercher les processus et fichiers camouflés
Moyen	Offre un niveau de sécurité moyen. La consommation de ressources système est modérée. ■ Analyser tous les fichiers ■ Analyser pour rechercher les virus et spyware
Basse	Couvre les besoins de sécurité de base. La consommation de ressources système est très faible. ■ Analyser les programmes uniquement ■ Analyser pour rechercher les virus
Personnalisé	C'est ici que vous pouvez sélectionner vos propres options d'analyse. Cliquez sur Personnalisé et définissez votre niveau d'analyse. Cochez les cases pour indiquer les types de malware que vous voulez rechercher sur votre ordinateur au cours de l'analyse.

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

Etape 4/4 - Définir des options supplémentaires

Durant cette étape, vous pouvez définir des options supplémentaires avant le démarrage d'une analyse.

Paramétrer des options supplémentaires

Afin de sauvegarder la tâche d'analyse pour l'utiliser tel quel, cochez les cases correspondantes et entrez un nom dans la zone de texte prévue à cet effet.

Note
Un nouveau bouton avec le nom mentionné ci-dessus apparaîtra sous le menu des tâches.

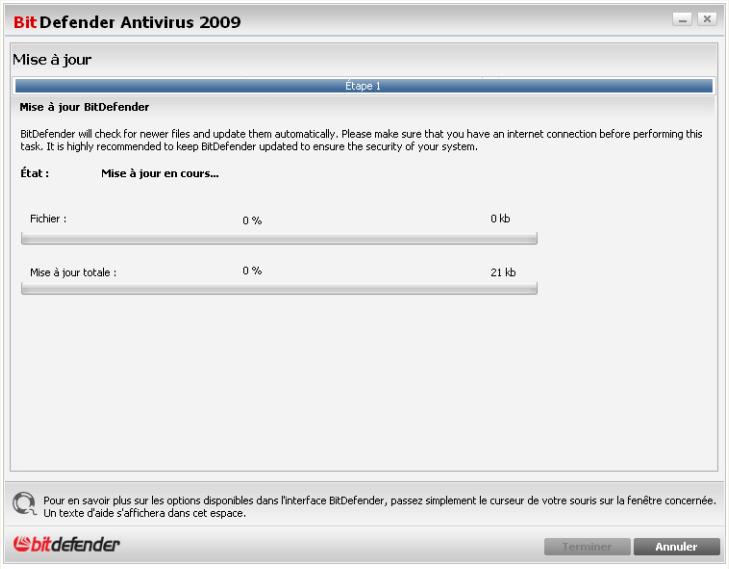
Si vous voulez éteindre l'ordinateur après l'analyse, cochez la case correspondante.

Cliquez sur **Démarrer l'analyse** et suivez la procédure en 3 étapes pour effectuer l'analyse.

7.2.2. 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 voulez fermer cette fenêtre, cliquez simplement sur **Annuler**. 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.

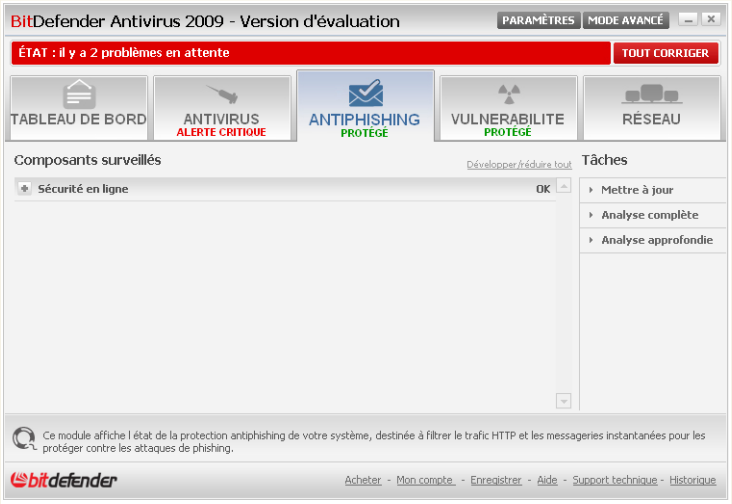
Cliquez sur **Redémarrer** pour redémarrer immédiatement votre système.

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

8. Antiphishing

BitDefender comporte un module Antiphishing qui s'assure que toutes le pages auxquelles vous accédez avec Internet Explorer ou Firefox sont sûres.

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



Antiphishing

Le module Antiphishing se compose de deux sections :

- **Composants contrôlés** - Vous permet de consulter la liste complète des composants contrôlés pour chaque module de sécurité. Vous pouvez définir les modules devant être contrôlés. Nous vous recommandons d'activer le contrôle sur l'intégralité des composants.
- **Tâches** - Vous pouvez trouver ici des liens vers les tâches de sécurité les plus importantes : analyse complète du système, analyse approfondie, mettre à jour.

8.1. Composants contrôlés

Le composant surveillé est le suivant :

Catégorie	Description
Sécurité en ligne	Vous permet de vérifier l'état des différents modules de sécurité protégeant vos transactions en ligne et votre ordinateur, lorsque vous êtes connecté à Internet.

Cliquez sur une case "+" pour ouvrir une arborescence et sur une case "-" pour la fermer.

8.1.1. Sécurité en ligne

Les problèmes concernant la sécurité en ligne sont décrits à l'aide de messages très explicites. Si un élément est susceptible de compromettre la sécurité de votre ordinateur, vous verrez apparaître en regard de chacun de ces messages un bouton d'état rouge intitulé **Corriger**. Dans le cas contraire, un bouton d'état vert **OK** est affiché.

Problème de sécurité	Description
Cryptage des conversations pour la messagerie instantanée activé	Si vos contacts de messagerie instantanée ont installé BitDefender 2009, toutes les conversations via Yahoo! Messenger et Windows Live Messenger seront cryptées. Nous vous recommandons d'activer le cryptage des conversations pour la messagerie instantanée afin de vous assurer que vos conversations restent privées.
Protection antiphishing Firefox activée	BitDefender protège votre ordinateur contre les tentatives de phishing lorsque vous naviguez sur Internet.
Protection antiphishing Internet Explorer activée	BitDefender protège votre ordinateur contre les tentatives de phishing lorsque vous naviguez sur Internet.

Lorsque les boutons d'état sont verts, le risque de sécurité pour votre système est au niveau minimum. Procédez comme suit pour obtenir des boutons d'état verts :

1. Cliquez sur les boutons **Corriger** pour corriger une à une les vulnérabilités de sécurité.
2. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

Si vous souhaitez exclure un problème du contrôle, il vous suffit de décocher la case correspondante **Oui, contrôler ce composant**.

8.2. Tâches

Vous pouvez trouver ici des liens vers les tâches de sécurité les plus importantes : analyse complète du système, analyse approfondie, mettre à jour.

Voici les différents boutons proposés:

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

8.2.1. 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
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 malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse approfondie	Analyse l'ensemble du système. La configuration par défaut permet d'analyser tous les types de codes malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
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

Tâche	Description
	documents et de votre bureau, ainsi que le contrôle des applications se lançant au démarrage.
Analyse personnalisée	Utilisez cette tâche pour définir des fichiers et dossiers spécifiques à analyser.

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:

Analyse personnalisée

En cliquant sur le bouton **Analyse personnalisée** et en suivant les instructions de l'assistant, vous pouvez créer des tâches d'analyse personnalisées et les définir comme tâches rapides.

Etape 1/4- Fenêtre d'accueil

Page d'accueil.

Fenêtre de bienvenue

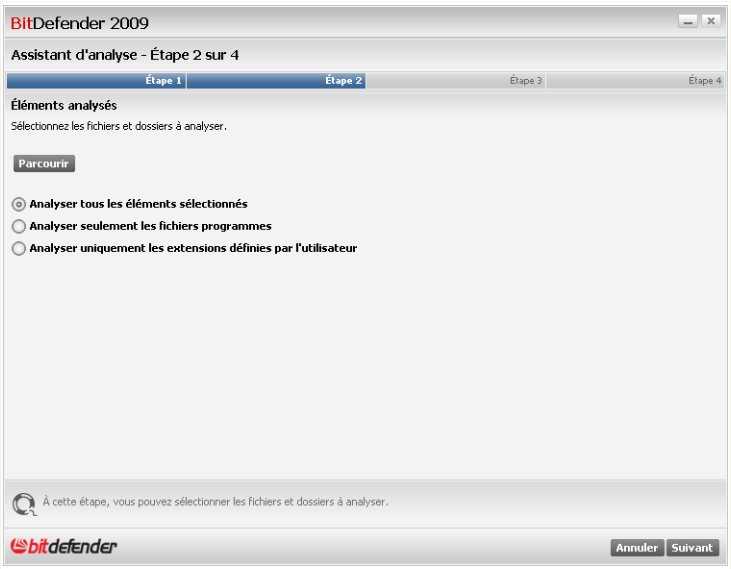
Cet assistant va vous aider à analyser votre ordinateur pour rechercher d'éventuelles menaces pouvant l'affecter. Vous pourrez sélectionner des fichiers et/ou dossiers à être analysés et définir des actions à entreprendre sur les fichiers infectés. Vous recevrez également un rapport d'analyse qui vous aidera à évaluer le niveau de sécurité de votre système. Parcourez chaque étape et configurer les processus d'analyse selon vos besoins.

Note
Pour passer cette étape dans les analyses futures, cochez simplement la case correspondante.

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

Étape 2/4 - Définir les éléments à analyser

Durant cette étape, vous pouvez choisir les fichiers et dossier à analyser.



Définir les éléments à analyser

Cliquez sur Parcourir pour sélectionner les dossiers et/ou fichiers spécifiques sur votre ordinateur.

Les options suivantes sont disponibles:

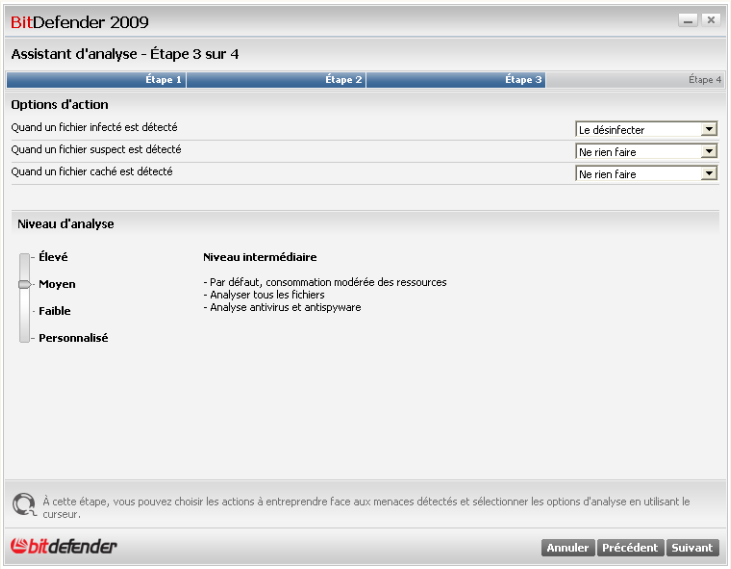
Option	*Description*
Analyser tous les éléments sélectionnés	Sélectionnez cette option pour analyser uniquement les éléments sélectionnés précédemment.
Analyse des extensions à risques seulement	Sélectionnez cette option pour n'analyser que les programmes et les applications.
Analyser uniquement les extensions définies par l'utilisateur	Sélectionnez cette option pour analyser uniquement les extensions spécifiques que vous voulez analyser. Une boîte de dialogue s'affichera dans laquelle vous pourrez entrer ces extensions.

Option	Description
	Note Les extensions doivent être séparées par un point-virgule “;”.

Cliquez sur **Suivant** pour continuer ou sur **Annuler** si vous voulez quitter l’assistant.

Étape 3/4 - Sélectionner les actions à entreprendre

Durant cette étape, vous pouvez choisir quelles actions entreprendre lorsque des menaces sont détectées et sélectionner des options d'analyse en utilisant le curseur.



Sélectionner les actions à entreprendre

Vous pouvez sélectionner les actions à entreprendre à partir du menu correspondant :

- **Lorsqu'un fichier infecté est détecté**
- **Lorsqu'un fichier suspect est détecté**

■ **Lorsqu'un fichier camouflé est détecté**

Au même moment, vous avez la possibilité de configurer le niveau de protection de l'analyse. 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 4 niveaux de protection :

Niveau de protection	*Description*
Agressif	Offre un niveau de sécurité élevé. La consommation de ressources système est importante. ■ Analyser tous les fichiers et archives ■ Analyser pour rechercher les virus et spyware ■ Analyser pour rechercher les processus et fichiers camouflés
Moyen	Offre un niveau de sécurité moyen. La consommation de ressources système est modérée. ■ Analyser tous les fichiers ■ Analyser pour rechercher les virus et spyware
Basse	Couvre les besoins de sécurité de base. La consommation de ressources système est très faible. ■ Analyser les programmes uniquement ■ Analyser pour rechercher les virus
Personnalisé	C'est ici que vous pouvez sélectionner vos propres options d'analyse. Cliquez sur Personnalisé et définissez votre niveau d'analyse. Cochez les cases pour indiquer les types de malware que vous voulez rechercher sur votre ordinateur au cours de l'analyse.

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

Etape 4/4 - Définir des options supplémentaires

Durant cette étape, vous pouvez définir des options supplémentaires avant le démarrage d'une analyse.

Paramétrer des options supplémentaires

Afin de sauvegarder la tâche d'analyse pour l'utiliser tel quel, cochez les cases correspondantes et entrez un nom dans la zone de texte prévue à cet effet.

Note
Un nouveau bouton avec le nom mentionné ci-dessus apparaîtra sous le menu des tâches.

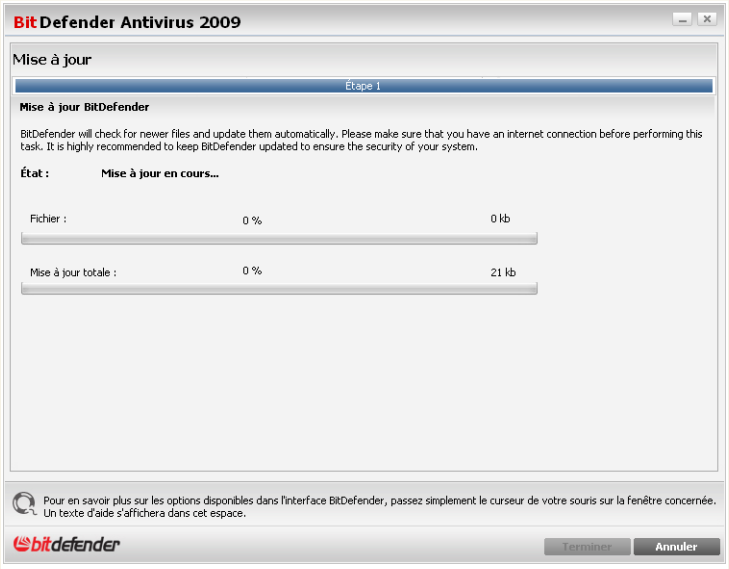
Si vous voulez éteindre l'ordinateur après l'analyse, cochez la case correspondante.

Cliquez sur **Démarrer l'analyse** et suivez la procédure en 3 étapes pour effectuer l'analyse.

8.2.2. 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 voulez fermer cette fenêtre, cliquez simplement sur **Annuler**. 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.

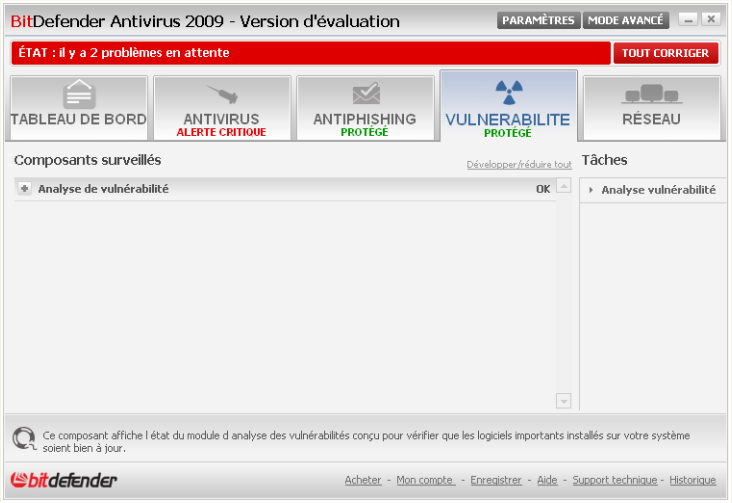
Cliquez sur **Redémarrer** pour redémarrer immédiatement votre système.

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

9. Vulnérabilité

BitDefender comporte un module Vulnérabilité qui vous permet de maintenir les logiciels essentiels pour votre PC constamment à jour.

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



Vulnérabilité

Le module Vulnérabilité comporte deux sections :

- **Composants contrôlés** - Vous permet de consulter la liste complète des composants contrôlés pour chaque module de sécurité. Vous pouvez définir les modules devant être contrôlés. Nous vous recommandons d'activer le contrôle sur l'intégralité des composants.
- **Tâches** - C'est ici que vous pouvez trouver des liens vers les plus importantes tâches de sécurité.

9.1. Composants contrôlés

Le composant surveillé est le suivant :

Catégorie	Description
Analyse de vulnérabilité	Vous permet de vérifier si les logiciels essentiels de votre PC sont bien à jour. Les mots de passe des comptes Windows sont également testés selon les règles de sécurité.

Cliquez sur une case "+" pour ouvrir une arborescence et sur une case "-" pour la fermer.

9.1.1. Analyse de vulnérabilité

Les problèmes concernant les vulnérabilités sont décrits à l'aide de messages très explicites. Si un élément est susceptible de compromettre la sécurité de votre ordinateur, vous verrez apparaître en regard de chacun de ces messages un bouton d'état rouge intitulé **Corriger**. Dans le cas contraire, un bouton d'état vert **OK** est affiché.

Problème de sécurité	Description
Contrôle de vulnérabilité activé	Surveille les mises à jour de Microsoft Windows et de Microsoft Office, ainsi que les mots de passe des comptes d'accès à Microsoft Windows pour garantir que votre système d'exploitation est à jour et n'est pas vulnérable au contournement de mot de passe.
Mises à jour critiques de Microsoft	Installe les mises à jour critiques disponibles de Microsoft.
Autres mises à jour de Microsoft	Installe les mises à jour non critiques disponibles de Microsoft.
Mises à jour automatiques de Windows activées	Installe les nouvelles mises à jour de sécurité de Windows dès lors qu'elles sont disponibles.
Admin (mot de passe fort)	Indique la force du mot de passe d'utilisateurs spécifiques.

Lorsque les boutons d'état sont verts, le risque de sécurité pour votre système est au niveau minimum. Procédez comme suit pour obtenir des boutons d'état verts :

1. Cliquez sur les boutons **Corriger** pour corriger une à une les vulnérabilités de sécurité.
2. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

Si vous souhaitez exclure un problème du contrôle, il vous suffit de décocher la case correspondante **Oui, contrôler ce composant**.

9.2. Tâches

C'est ici que vous pouvez trouver des liens vers les tâches de sécurité les plus importantes.

Voici les différents boutons proposés:

- **Analyse des vulnérabilités**

9.2.1. Rechercher des vulnérabilités

L'analyse des vulnérabilités surveille les mises à jour de Microsoft Windows et de Microsoft Office, ainsi que les mots de passe des comptes d'accès à Microsoft Windows pour garantir que votre système d'exploitation est à jour et n'est pas vulnérable au contournement de mot de passe.

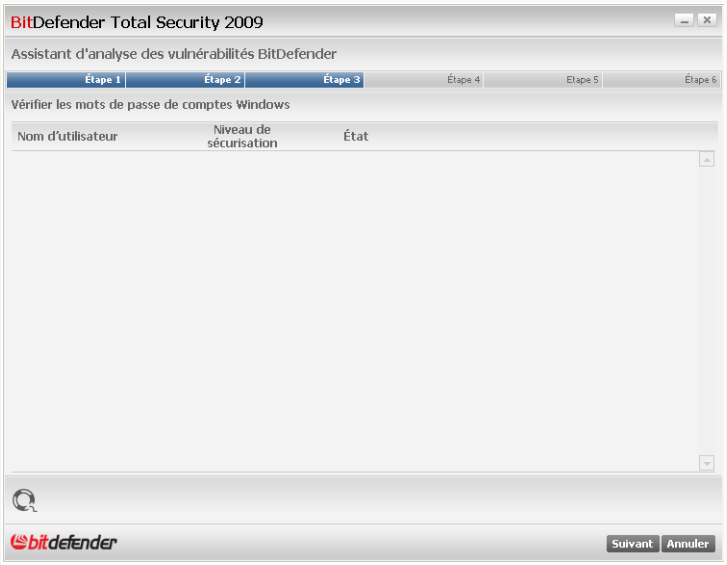
Pour rechercher des vulnérabilités sur votre ordinateur, cliquez sur **Analyse des vulnérabilités** et suivez les instructions de l'assistant.

Etape 1/6 - Sélectionnez les vulnérabilités à vérifier

Vulnérabilités

Cliquez sur **Suivant** pour lancer l'analyse des vulnérabilités sélectionnées.

Etape 2/6 - Vérifier les vulnérabilités



Analyse de vulnérabilité

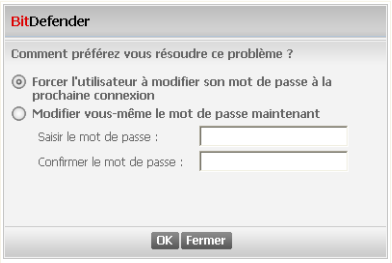
Patientez jusqu'à ce que BitDefender ait terminé l'analyse des vulnérabilités.

Étape 3/6 - Modifier les mots de passe vulnérables

Mots de passe utilisateur

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

Cliquez sur **Réparer** pour modifier les mots de passe vulnérables. Une nouvelle fenêtre s'affiche.



Changer le mot de passe

Choisir la méthode à utiliser pour régler ce problème :

- **Obliger l'utilisateur à changer son mot de passe à la prochaine connexion.** BitDefender demandera à l'utilisateur de modifier son mot de passe lors de sa prochaine connexion à Windows
- **Changer le mot de passe utilisateur.** Vous devez saisir le nouveau mot de passe dans les champs de modification.

Note
Pour avoir un mot de passe Fort, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

Cliquez sur **OK** pour changer le mot de passe.

Cliquez sur **Suivant**.

Étape 4/6 - Mettre à jour les applications

Applications

Vous pouvez voir la liste des applications vérifiées par BitDefender et savoir si ces dernières sont à jour. Si une application n'est pas à jour, cliquez sur le lien fourni pour télécharger la dernière version.

Cliquez sur **Suivant**.

Étape 6/6 - Mettre à jour Windows

Mises à jours Windows

Vous pouvez voir la liste des mises à jour Windows (critiques et non-critiques) qui ne sont pas installées actuellement sur votre ordinateur. Cliquez sur **Installer toutes les mises à jour système** pour installer toutes les mises à jour disponibles.

Cliquez sur **Suivant**.

Étape 6/6 - Voir les résultats

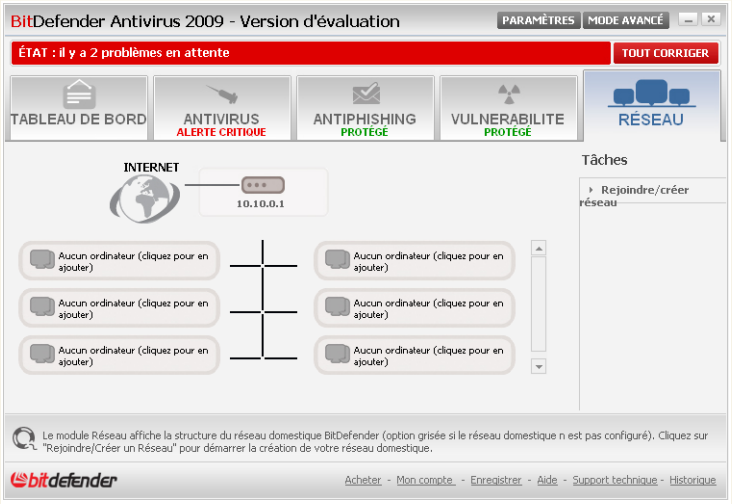
Résultats

Cliquez sur **Fermer**.

10. Réseau

Le module Réseau vous permet de gérer les produits BitDefender installés sur tous les ordinateurs de votre foyer à partir d'un seul et même ordinateur.

Pour accéder au module Réseau, cliquez sur l'onglet **Gestionnaire de fichiers**.



Réseau

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

1. Rejoindre le réseau domestique BitDefender via votre ordinateur. Rejoindre le réseau consiste à configurer un mot de passe d'administration pour la gestion de réseau domestique.
2. Allumez chaque ordinateur que vous voulez gérer et rejoignez le réseau à partir de ceux-ci (en saisissant le mot de passe).
3. Revenez sur votre ordinateur et ajoutez les ordinateurs que vous voulez gérer.

10.1. Tâches

Au début, seul un bouton est disponible.

- **Rejoindre/créer un réseau** - vous permet de définir le mot de passe réseau et donc d'entrer sur le réseau.

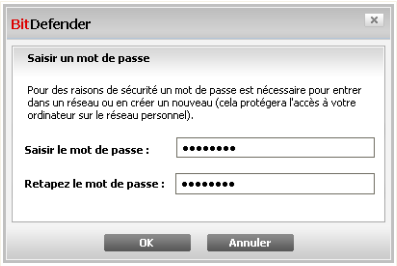
Après avoir rejoint le réseau, plusieurs autres boutons sont accessibles.

- **Quitter le réseau** - vous permet de quitter le réseau.
- **Gérer le réseau** - vous permet d'ajouter des ordinateurs à votre réseau.
- **Analyser tout** - vous permet d'analyser en une seule opération l'ensemble des ordinateurs gérés.
- **Tout mettre à jour** vous permet de mettre à jour en une seule opération l'ensemble des ordinateurs gérés.
- **Enregistrer tout** vous permet d'enregistrer en une seule opération l'ensemble des ordinateurs gérés.

10.1.1. Rejoindre le réseau BitDefender

Procédez comme suit pour rejoindre le réseau domestique BitDefender :

1. Cliquez sur **Rejoindre/créer un réseau**. Vous serez invité à définir le mot de passe de gestion de réseau domestique.



Définir le mot de passe

2. Entrez le même mot de passe dans chacun des champs de saisie.
3. Cliquez sur **OK**.

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

10.1.2. Ajout d'ordinateurs au réseau BitDefender

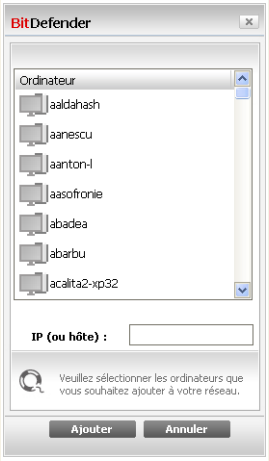
Avant de pouvoir ajouter un ordinateur au réseau domestique BitDefender, vous devez définir le mot de passe de gestion de réseau domestique BitDefender sur l'ordinateur à ajouter.

Procédez comme suit pour ajouter un ordinateur au réseau domestique BitDefender :

1. Cliquez sur **Gérer le réseau**. Vous serez invité à saisir le mot de passe local de gestion de réseau domestique.

Saisir le mot de passe

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

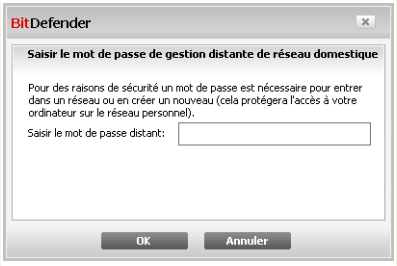


Ajouter un ordinateur

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

- Indique un ordinateur en ligne sans aucun produit BitDefender installé.
- Indique un ordinateur en ligne avec BitDefender installé.
- Indique un ordinateur hors connexion avec BitDefender installé.

3. Choisissez une des possibilités suivantes :
   - Sélectionnez dans la liste le nom de l'ordinateur à ajouter.
   - Tapez l'adresse IP ou le nom de l'ordinateur à ajouter dans le champ correspondant.
4. Cliquez sur **Ajouter**. Vous serez invité à saisir le mot de passe de gestion de réseau domestique de l'ordinateur concerné.



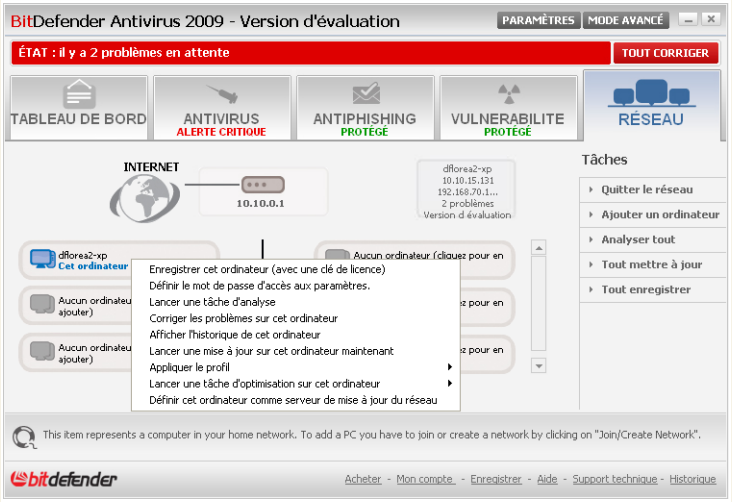
Authentification

5. Tapez le mot de passe de gestion de réseau domestique défini sur l'ordinateur concerné.
6. Cliquez sur **OK**. Si vous avez spécifié le bon mot de passe, le nom de l'ordinateur sélectionné apparaît sur la carte réseau.

Note
Vous pouvez ajouter jusqu'à cinq ordinateurs sur la carte réseau.

10.1.3. Gestion du réseau BitDefender

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



Carte réseau

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

Si vous faites un clic-droit sur un ordinateur présent sur la carte du réseau, vous pourrez voir les tâches administratives que vous pouvez lancer sur cet ordinateur distant.

- **Enregistrer cet ordinateur**
- **Définir le mot de passe des paramètres**
- **Lancer une tâche d'analyse**
- **Réparer les problèmes sur cet ordinateur**
- **Afficher l'historique de cet ordinateur**
- **Lancer une mise à jour sur cet ordinateur**
- **Appliquer le profil**
- **Lancer une tâche d'optimisation sur cet ordinateur**
- **Définir cet ordinateur comme serveur de mise à jour sur ce réseau**

Avant de lancer une tâche sur un ordinateur spécifique, vous serez invité à saisir le mot de passe local de gestion de réseau domestique.

Saisir le mot de passe

Tapez le mot de passe de gestion de réseau domestique et cliquez sur **OK**.

Note

Si vous prévoyez de lancer plusieurs tâches, il peut s'avérer utile de sélectionner l'option **Ne plus afficher ce message durant cette session**. En sélectionnant cette option, vous n'aurez plus à saisir le mot de passe pour la session en cours.

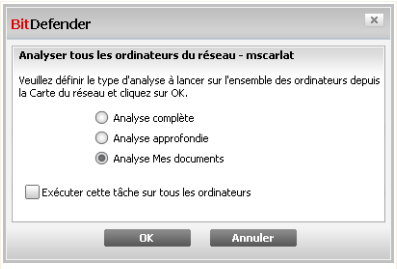
10.1.4. Analyse de tous les ordinateurs

Procédez comme suit pour analyser tous les ordinateurs gérés :

1. Cliquez sur **Analyser tout**. Vous serez invité à saisir le mot de passe local de gestion de réseau domestique.

Saisir le mot de passe

2. Sélectionnez un type d'analyse.
   - **Analyse complète du système** -lance une analyse complète de votre ordinateur (hors archives).
   - **Analyse approfondie** - lance une analyse complète de votre ordinateur (archives inclues).
   - **Analyser mes documents** - lance une analyse rapide de vos documents et paramètres.



Sélectionner le type d'analyse

3. Cliquez sur **OK**.

10.1.5. Mise à jour de tous les ordinateurs

Procédez comme suit pour mettre à jour tous les ordinateurs gérés :

1. Cliquez sur **Tout mettre à jour**. Vous serez invité à saisir le mot de passe local de gestion de réseau domestique.

Saisir le mot de passe

2. Cliquez sur **OK**.

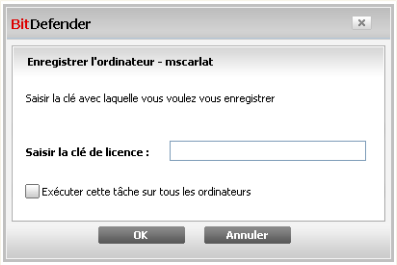
10.1.6. Enregistrement de tous les ordinateurs

Procédez comme suit pour enregistrer tous les ordinateurs gérés :

1. Cliquez sur **Enregistrer tout**. Vous serez invité à saisir le mot de passe local de gestion de réseau domestique.

Saisir le mot de passe

2. Saisissez la clé avec laquelle vous voulez vous enregistrer.



Enregistrer tout

3. Cliquez sur **OK**.

11. Paramètres de base

Le module Paramètres de base vous permet d'activer ou de désactiver aisément des modules de sécurité importants.

Pour entrer dans le module Paramètres de base, cliquez sur **Paramètres**, dans la partie supérieure de la Mode standard.

Paramètres de base

Les modules de sécurité disponibles ont été regroupés en plusieurs catégories.

Catégorie	Description
Sécurité locale	Vous pouvez ici activer/désactiver la protection en temps réel des fichiers ou la mise à jour automatique.
Sécurité en ligne	C'est ici que vous pouvez activer/désactiver la protection en temps réel e-mail et Internet.
Paramètres généraux	Vous pouvez ici activer/désactiver le Mode Jeu, le mode Portable, les mots de passe, la barre d'activité d'analyse et d'autres options.

Cliquez sur une case "+" pour ouvrir une arborescence et sur une case "-" pour la fermer.

11.1. Sécurité locale

Vous pouvez activer/désactiver les modules de sécurité d'un simple clic.

Module de sécurité	Description
Protection en temps réel antivirus et antispyware des fichiers	La protection de fichiers en temps réel garantit que tous les fichiers sont analysés dès qu'un accès se produit (par vous ou par une application s'exécutant sur ce système).
Mise à jour automatique	La mise à jour automatique permet de télécharger et d'installer automatiquement et régulièrement les dernières versions du produit BitDefender et des fichiers de signature
Analyse des vulnérabilités automatique	La vérification automatique des vulnérabilités s'assure que les logiciels majeurs de votre ordinateur sont à jour.

11.2. Sécurité en ligne

Vous pouvez activer/désactiver les modules de sécurité d'un simple clic.

Module de sécurité	Description
Protection antiphishing en temps réel du trafic Web	La protection antiphishing en temps réel du trafic Web garantit que tous les téléchargements de fichiers via le protocole HTTP sont analysés contre les tentatives de phishing.
Contrôle d'identité	Le contrôle d'identité contribue à protéger les données confidentielles en analysant l'ensemble du trafic Web et mail pour rechercher des chaînes de caractères spécifiques.
Cryptage de messagerie instantanée	Si vos contacts de messagerie instantanée ont installé BitDefender 2009, toutes les conversations via Yahoo! Messenger et Windows Live Messenger seront cryptées.

11.3. Configuration générale

Vous pouvez activer/désactiver les éléments associés à la sécurité d'un simple clic.

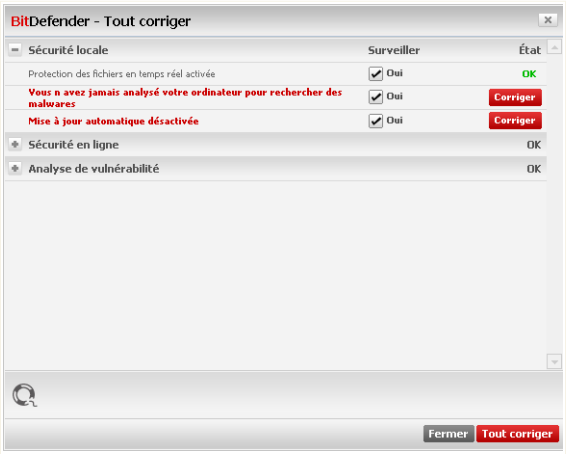
Élément	Description
Mode jeu	Le Mode Jeu modifie de manière temporaire les paramètres de protection afin de préserver les ressources de votre système lorsque vous jouez à un jeu vidéo.
Mode Portable	Le Mode Portable modifie de manière temporaire les paramètres de protection afin de préserver l'autonomie de la batterie de votre ordinateur portable.
Mot de passe pour les paramètres	Cette option garantit que les paramètres BitDefender ne puissent être modifiés que par une personne connaissant ce mot de passe.
BitDefender News	En activant cette option, vous serez informé par BitDefender de l'actualité de la société, des mises à jour de produits ou des nouvelles menaces de sécurité.
Alertes de notification produit	En activant cette option, vous recevrez des alertes d'information.
Barre d'activité d'analyse	La barre d'activité d'analyse est une petite barre transparente qui indique la progression de l'activité d'analyse de BitDefender. La ligne verte correspond à l'activité d'analyse relative à votre système local, tandis que la ligne rouge indique l'activité d'analyse relative à votre connexion Internet.
Lancer BitDefender au démarrage	En activant cette option, l'interface utilisateur de BitDefender est chargée automatiquement au démarrage de l'ordinateur. Cette option n'affecte pas le niveau de protection.
Envoyer rapports d'infection	En activant cette option, les rapports d'analyse virale sont envoyés aux laboratoires BitDefender pour être examinés. Notez que ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et qu'ils ne seront pas utilisés à des fins commerciales.
Détection des alertes	En activant cette option, les rapports concernant les potentielles alertes virales sont envoyés aux laboratoires BitDefender pour être examinés. Notez que ces rapports ne comprendront aucune

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

12. Barre d'état

Comme vous pouvez le constater, la partie supérieure de la fenêtre BitDefender Antivirus 2009 comporte une barre d'état qui affiche le nombre de problèmes restant à résoudre. Cliquez sur **Tout corriger** pour supprimer en une seule opération toutes les menaces sur la sécurité de votre ordinateur. Une fenêtre d'état de sécurité apparaît.

Le statut de sécurité affiche une liste organisée de façon systématique regroupant les problèmes de vulnérabilité de votre ordinateur en matière de sécurité. BitDefender Antivirus 2009 vous avertit de tout problème pouvant affecter la sécurité de votre ordinateur.



Barre d'état

12.1. Sécurité locale

Nous savons qu'il est important que vous soyez informé dès lors qu'un problème est susceptible d'affecter la sécurité de votre ordinateur. En contrôlant chacun des modules de sécurité, BitDefender Antivirus 2009 vous signalera non seulement les configurations que vous définissez pouvant affecter la sécurité de votre ordinateur, mais vous rappellera aussi à l'ordre lorsque vous oubliez d'exécuter des tâches importantes.

Les problèmes concernant la sécurité locale sont décrits à l'aide de messages très explicites. Si un élément est susceptible de compromettre la sécurité de votre ordinateur, vous verrez apparaître en regard de chacun de ces messages un bouton d'état rouge intitulé **Corriger**. Dans le cas contraire, un bouton d'état vert **OK** est affiché.

Problème de sécurité	*Description*
Protection des fichiers en temps réel activée	Garantit que tous les fichiers sont analysés dès qu'un accès se produit (par vous ou par une application s'exécutant sur ce système).
Vous avez analysé votre ordinateur pour rechercher des malwares aujourd'hui	Il est fortement recommandé d'exécuter une analyse à la demande dès que possible pour contrôler que les fichiers présents sur votre ordinateur ne contiennent pas de malwares.
Mise à jour automatique activée	Laissez la mise à jour automatique activée pour vous assurer que les signatures de malwares de votre programme BitDefender sont mises à jour de manière régulière.
Mise à jour en cours	La mise à jour du programme et des signatures de malwares est en cours.

Lorsque les boutons d'état sont verts, le risque de sécurité pour votre système est au niveau minimum. Procédez comme suit pour obtenir des boutons d'état verts :

1. Cliquez sur les boutons **Corriger** pour corriger une à une les vulnérabilités de sécurité.
2. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

Si vous souhaitez exclure un problème du contrôle, il vous suffit de décocher la case correspondante **Oui, contrôler ce composant**.

12.2. Sécurité en ligne

Les problèmes concernant la sécurité en ligne sont décrits à l'aide de messages très explicites. Si un élément est susceptible de compromettre la sécurité de votre ordinateur, vous verrez apparaître en regard de chacun de ces messages un bouton

d'état rouge intitulé **Corriger**. Dans le cas contraire, un bouton d'état vert **OK** est affiché.

Problème de sécurité	*Description*
Cryptage des conversations pour la messagerie instantanée activé	Si vos contacts de messagerie instantanée ont installé BitDefender 2009, toutes les conversations via Yahoo! Messenger et Windows Live Messenger seront cryptées. Nous vous recommandons d'activer le cryptage des conversations pour la messagerie instantanée afin de vous assurer que vos conversations restent privées.
Protection antiphishing Firefox activée	BitDefender protège votre ordinateur contre les tentatives de phishing lorsque vous naviguez sur Internet.
Protection antiphishing Internet Explorer activée	BitDefender protège votre ordinateur contre les tentatives de phishing lorsque vous naviguez sur Internet.

Lorsque les boutons d'état sont verts, le risque de sécurité pour votre système est au niveau minimum. Procédez comme suit pour obtenir des boutons d'état verts :

1. Cliquez sur les boutons **Corriger** pour corriger une à une les vulnérabilités de sécurité.
2. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

Si vous souhaitez exclure un problème du contrôle, il vous suffit de décocher la case correspondante **Oui, contrôler ce composant**.

12.3. Analyse de vulnérabilité

Les problèmes concernant les vulnérabilités sont décrits à l'aide de messages très explicites. Si un élément est susceptible de compromettre la sécurité de votre ordinateur, vous verrez apparaître en regard de chacun de ces messages un bouton d'état rouge intitulé **Corriger**. Dans le cas contraire, un bouton d'état vert **OK** est affiché.

Problème de sécurité	*Description*
Contrôle de vulnérabilité activé	Surveille les mises à jour de Microsoft Windows et de Microsoft Office, ainsi que les mots de passe des comptes d'accès à Microsoft Windows pour garantir que votre système d'exploitation est à jour et n'est pas vulnérable au contournement de mot de passe.
Mises à jour critiques de Microsoft	Installe les mises à jour critiques disponibles de Microsoft.
Autres mises à jour de Microsoft	Installe les mises à jour non critiques disponibles de Microsoft.
Mises à jour automatiques de Windows activées	Installe les nouvelles mises à jour de sécurité de Windows dès lors qu'elles sont disponibles.
Admin (mot de passe fort)	Indique la force du mot de passe d'utilisateurs spécifiques.

Lorsque les boutons d'état sont verts, le risque de sécurité pour votre système est au niveau minimum. Procédez comme suit pour obtenir des boutons d'état verts :

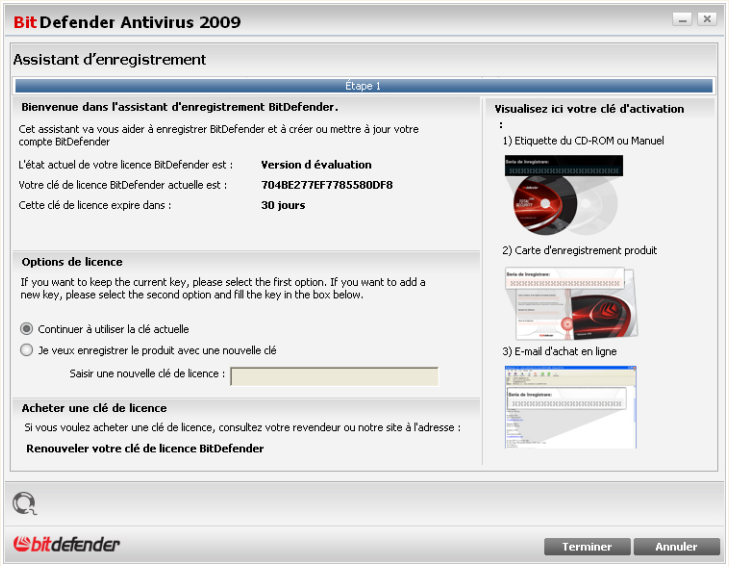
1. Cliquez sur les boutons **Corriger** pour corriger une à une les vulnérabilités de sécurité.
2. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

Si vous souhaitez exclure un problème du contrôle, il vous suffit de décocher la case correspondante **Oui, contrôler ce composant**.

13. Enregistrement

BitDefender Antivirus 2009 s'accompagne d'une période d'essai de 30 jours. Si vous voulez enregistrer BitDefender Antivirus 2009, modifier la clé d'activation ou créer un compte BitDefender, cliquez sur le lien **Enregistrer**, situé dans la partie inférieure de la fenêtre BitDefender. L'assistant d'enregistrement s'affichera.

13.1. Etape 1/1 - Enregistrer BitDefender Antivirus 2009



Enregistrement

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

Pour enregistrer BitDefender Antivirus 2009 :

1. Sélectionnez **Je veux enregistrer le produit avec une nouvelle clé**.

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

Note

Vous trouverez votre clé d'activation :

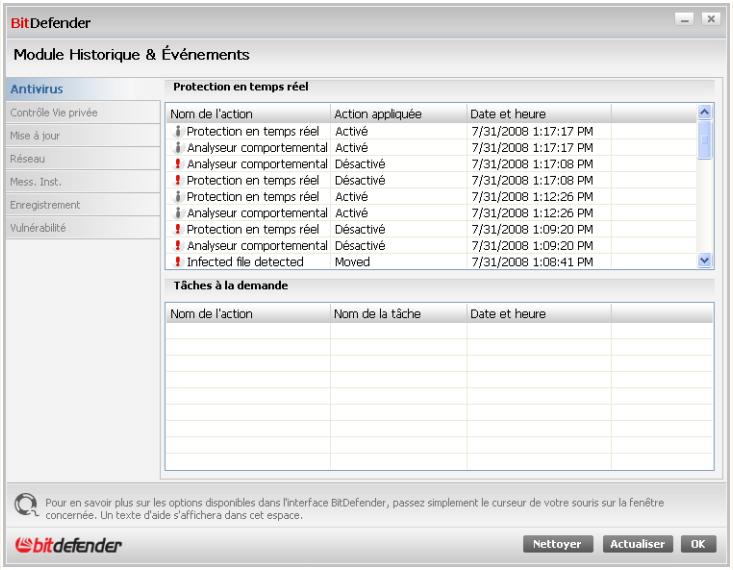
- sur l'étiquette du CD.
- sur la carte d'enregistrement du produit.
- sur l'e-mail d'achat en ligne.

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

Cliquez sur **Terminer**.

14. Historique

Le lien **Historique** situé en bas de la fenêtre du Centre de sécurité BitDefender permet d'ouvrir une nouvelle fenêtre comprenant l'historique etamp; les événements BitDefender. Cette fenêtre vous offre une vue d'ensemble des événements relatifs à la sécurité. Par exemple, vous pouvez facilement vérifier qu'une mise à jour s'est effectuée correctement, s'il y a eu des malwares détectés sur votre ordinateur, etc.



Evénements

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

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

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.

Administration avancée

15. Général

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

15.1. Tableau de bord

Pour consulter les statistiques d'activité du produit et l'état de votre enregistrement, rendez-vous dans **Général>Tableau de bord** dans le Mode avancé.

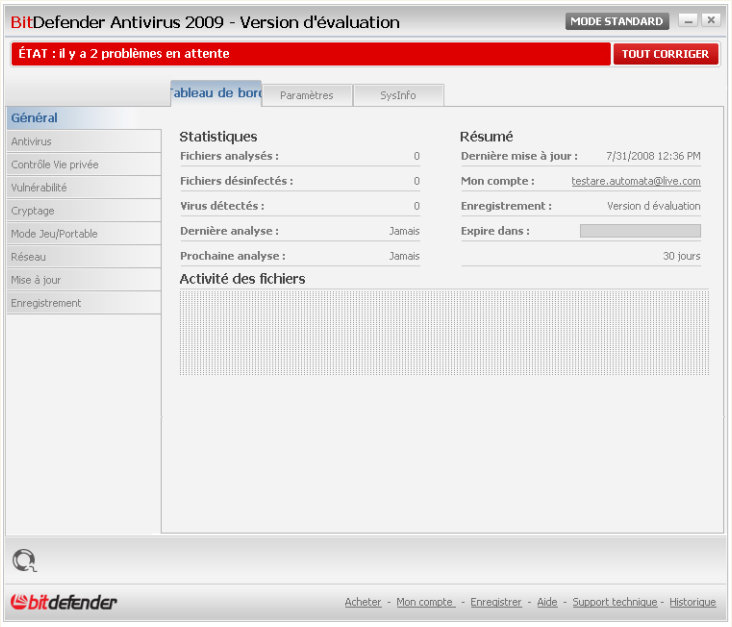


Tableau de bord

Le tableau de bord se compose de plusieurs sections :

- **Statistiques** - Affiche des informations importantes sur l'activité de BitDefender.
- **Vue d'ensemble** - Affiche l'état des mises à jour et de votre compte ainsi que les informations sur votre enregistrement et votre licence BitDefender.

- **Fichiers** - Indique l'évolution du nombre d'objets analysés par l'Antimalware BitDefender. La hauteur de la barre indique l'intensité du trafic lors de l'intervalle de temps correspondant.

15.1.1. Statistiques

Si vous voulez garder un œil sur l'activité de BitDefender, vous pouvez commencer par consulter la section Statistiques. Vous pouvez consulter les éléments suivants :

Élément	Description
Fichiers analysés	Indique le nombre de fichiers ayant fait l'objet d'une analyse antimalware lors de votre dernière analyse.
Fichiers désinfectés	Indique le nombre de fichiers désinfectés lors de votre dernière analyse.
Virus détectés	Indique le nombre de virus détectés sur votre système lors de votre dernière analyse.

15.1.2. Vue d'ensemble

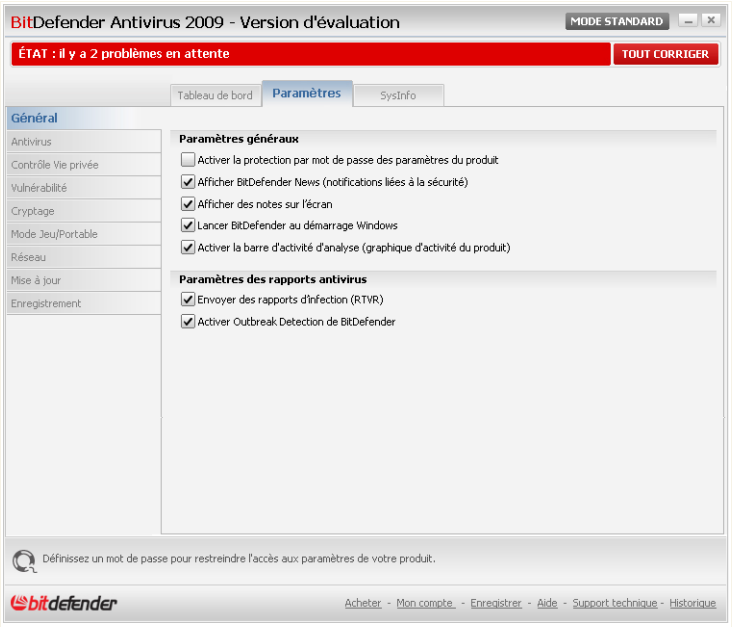
Vous pouvez consulter ici un récapitulatif des statistiques sur l'état de la mise à jour, l'état de votre compte et les informations d'enregistrement et de licence.

Élément	Description
Dernière mise à jour	Indique la date à laquelle votre produit BitDefender a été mis à jour pour la dernière fois. Veuillez réaliser des mises à jour régulières afin de bénéficier d'un système parfaitement protégé.
Mon compte	Indique l'adresse e-mail que vous pouvez utiliser pour accéder à votre compte en ligne, afin de récupérer votre clé de licence BitDefender, si vous l'avez perdue, et de bénéficier du Support Technique BitDefender ainsi que d'autres services personnalisés.
Enregistrement	Indique le type et l'état de votre clé de licence. Pour conserver votre système à l'abri des menaces, vous devez renouveler la clé ou mettre à niveau BitDefender si votre clé a expiré.

Élément	Description
Expire dans	Indique le nombre de jours avant l'expiration de la clé de licence.

15.2. Paramètres

Pour configurer les paramètres généraux de BitDefender et gérer sa configuration, rendez-vous dans **Général>Paramètres** dans le Mode avancé.



Paramètres Généraux

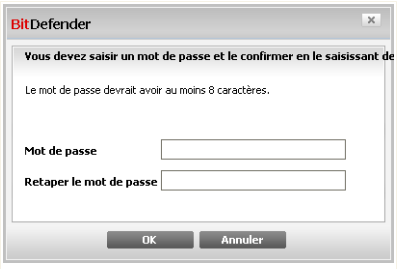
Vous pouvez dans cette rubrique paramétrer le fonctionnement de BitDefender. Par défaut, BitDefender est chargé au démarrage de Windows et se minimise automatiquement.

15.2.1. 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 **Resaisir 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. Vous pouvez configurer BitDefender pour qu'il affiche des notifications seulement lors de l'utilisation du mode Standard ou du mode Avancé.
- **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.

15.2.2. 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.

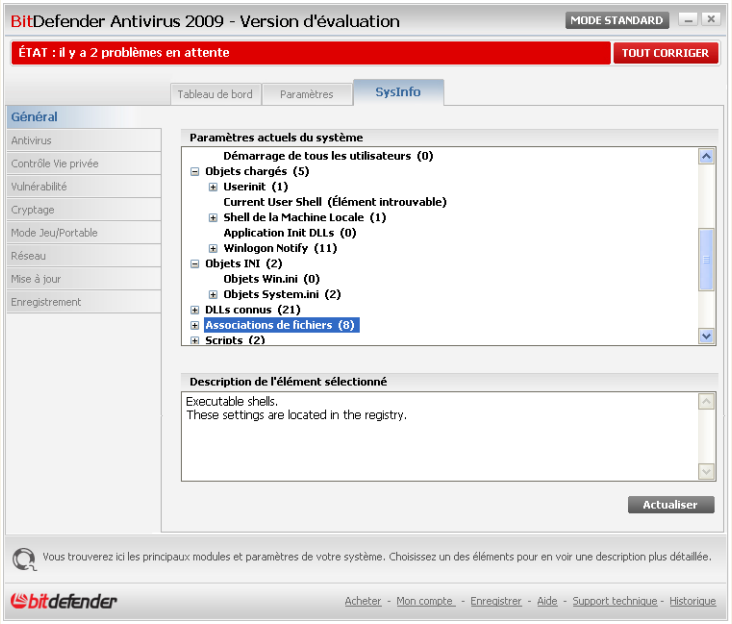
- **Activer l'Outbreak Detection de BitDefender** - envoie des rapports aux BitDefender Labs à propos d'apparitions éventuelles de virus.

  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.

15.3. 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, rendez-vous dans **Général>Infos système** dans le Mode avancé.



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:

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

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

- **Actualiser** - re-ouvre la rubrique **Informations système**.

16. Antivirus

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

- Protection en temps réel - empêche les nouvelles menaces d'infecter votre système. BitDefender analysera par exemple un document Word quand vous l'ouvrez, et les e-mails lors de leur réception.

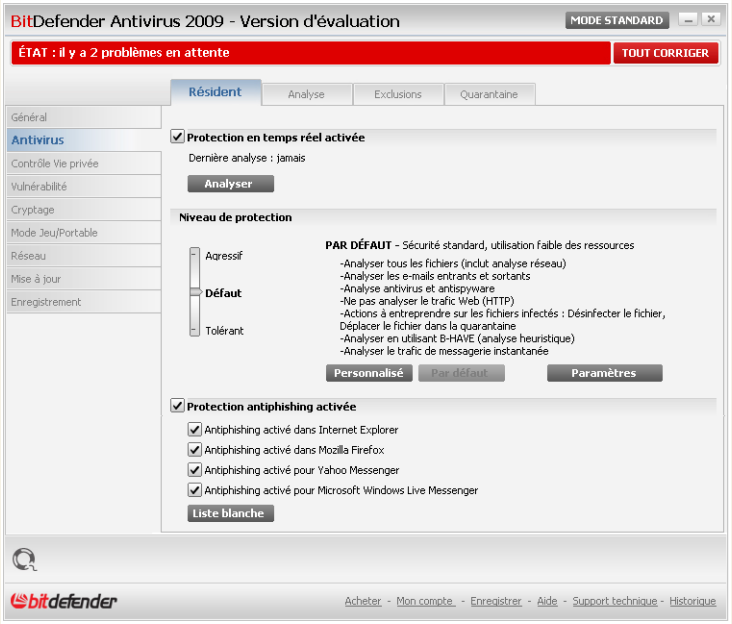
  Note
  A propos de la protection en temps réel, on parle aussi d'analyse à l'accès – les fichiers sont analysés quand l'utilisateur veut les ouvrir.

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

16.1. Protection en temps réel.

BitDefender protège votre ordinateur de manière continue et en temps réel contre toutes les menaces de codes malveillants en analysant tous les fichiers à l'accès, les e-mails et les communications via les applications de messagerie instantanée (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). L'antiphishing BitDefender empêche la divulgation de vos informations personnelles sur Internet en vous alertant sur les pages Internet potentiellement de type phishing.

Pour configurer la protection en temps réel et l'antiphishing BitDefender, dirigez vous vers **Antivirus>Shield** dans le Mode avancé.



Protection en temps réel.

Vous pouvez vérifier si la protection en temps réel est activée ou désactivée. Si vous voulez modifier l'état de la protection en temps réel, cochez ou décochez la case correspondante.

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

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

16.1.1. 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:

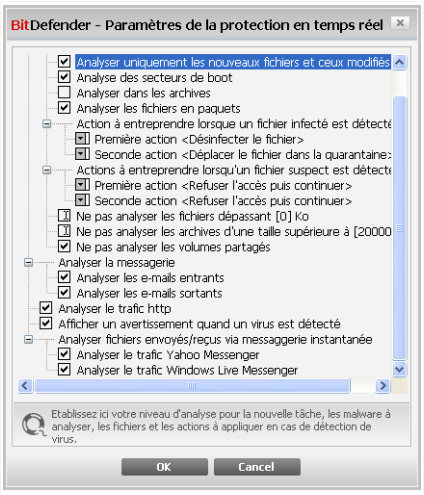
Niveau de protection	Description
Tolérant	Couvre les besoins de sécurité de base. La consommation de ressources système est très faible. Les programmes et emails entrants ne sont analysés que pour rechercher les virus. En plus de la recherche classique par signature, BitDefender utilise aussi un moteur 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**.

16.1.2. 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.

Option		Description
	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.
Analyser les secteurs 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 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.
	Désinfecter le fichier	Pour désinfecter un fichier infecté.

Option		Description
	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 archives d'une taille supérieure à [20000] Ko		Entrez la taille maximum des fichiers archives qui doivent être analysées (En Ko) Pour analyser toutes les archives, quelle que soit leur taille, leur type.
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.

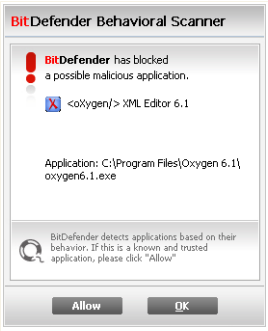
  Au cas où un fichier suspect est détecté vous pouvez lancer un assistant à partir de la fenêtre d'alerte qui vous aidera à envoyer ce fichier aux BitDefender Labs pour une analyse ultérieure. Vous pouvez saisir votre adresse email pour recevoir des informations sur ce rapport.
- **Analyser les fichiers reçus/envoyés par la messagerie instantanée.** Pour analyser les fichiers que vous recevez ou envoyez via Yahoo ou Windows Live Messenger, cochez la case correspondante.

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

16.1.3. Configurer l'analyse comportementale

L'analyse comportementale est un niveau de protection supplémentaire contre les menaces pour lesquelles aucune signature n'est encore disponible. Elle surveille et analyse en permanence le comportement des applications qui s'exécutent sur votre ordinateur et vous prévient en cas de comportement suspicieux.

L'Analyse comportementale vous alerte quand une application tente d'effectuer une action potentiellement malicieuse et vous demande quelle action entreprendre.

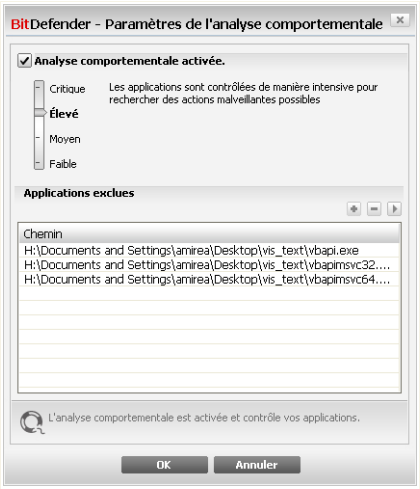


Alerte d'Analyse Comportementale

Si vous connaissez l'application et la savez de confiance, cliquez sur **Autoriser**. L'analyse comportementale n'analysera plus les applications contre de potentiels comportements malicieux.

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

Pour configurer l'analyse comportementale, cliquez sur **Paramètres d'analyse**.



Paramètres d'analyse comportementale

Si vous souhaitez désactiver l'analyse comportementale, décochez la case **Analyse comportementale activée**.

Important
Conservez l'analyse comportementale activée pour être protégé contre les virus inconnus.

Configurer le niveau de protection

Le niveau de protection de l'analyse comportementale change automatiquement quand vous modifiez le niveau de protection en temps réel. Si vous n'êtes pas satisfait des paramètres par défaut, vous pouvez configurer manuellement le niveau de protection.

Note
Gardez à l'esprit que si vous modifiez le niveau de protection en temps réel, l'analyse comportementale sera également modifiée de manière équivalente.

Déplacez le curseur vers le niveau qui correspond le mieux à vos besoins en termes de niveau de protection.

Niveau de protection	Description
Critique	Les applications sont surveillées étroitement contre toute action potentiellement malicieuse.
Agressif	Les applications sont surveillées contre les actions potentiellement malicieuses.
Moyen	Les applications sont surveillées modérément contre les actions potentiellement malicieuses.
Basse	Les applications sont surveillées contre les possibles actions malicieuses.

Gestion des Applications Exclues.

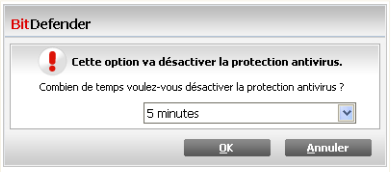
Vous pouvez paramétrer l'analyse comportementale afin qu'elle n'analyse pas certaines applications. Les applications qui ne sont pas actuellement vérifiées par l'analyse comportementale sont énumérées dans le tableau **Applications exclues**.

Pour gérer les applications exclues, vous pouvez utiliser les boutons disposés en haut du tableau :

- **Add** - exclude a new application from scanning.
- **Remove** - remove an application from the list.
- **Edit** - edit an application path.

16.1.4. 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.

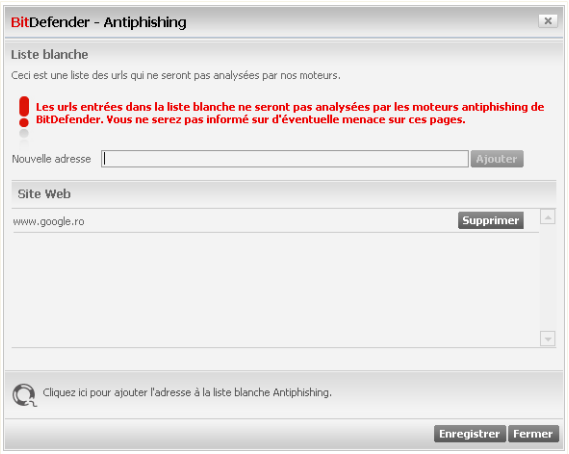
16.1.5. Configurer la protection antiphishing

BitDefender fournit une protection antiphishing en temps réel pour :

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Vous pouvez désactiver la protection antiphishing entièrement ou pour des applications spécifiques uniquement.

Cliquez sur **Liste blanche** pour configurer et gérer une liste de sites Internet à ne pas être analysée par les moteurs antiphishing BitDefender.



Liste blanche antiphishing

Vous pouvez visualiser la liste de tous les sites Internet qui ne seront pas analysés par les moteurs antiphishing BitDefender.

Pour ajouter un site Internet à la liste blanche, entrez son adresse url dans le champ **Nouvelle adresse** et cliquez sur **Ajouter**. La Liste Blanche ne doit contenir que des sites web de confiance. Par exemple, ajoutez les sites Web sur lesquels vous avez l'habitude de faire vos achats en ligne.

Note

Vous pouvez ajouter de nouveaux sites Internet à la liste blanche très simplement à partir de la barre d'outils antiphishing de BitDefender intégrée à votre navigateur Internet.

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

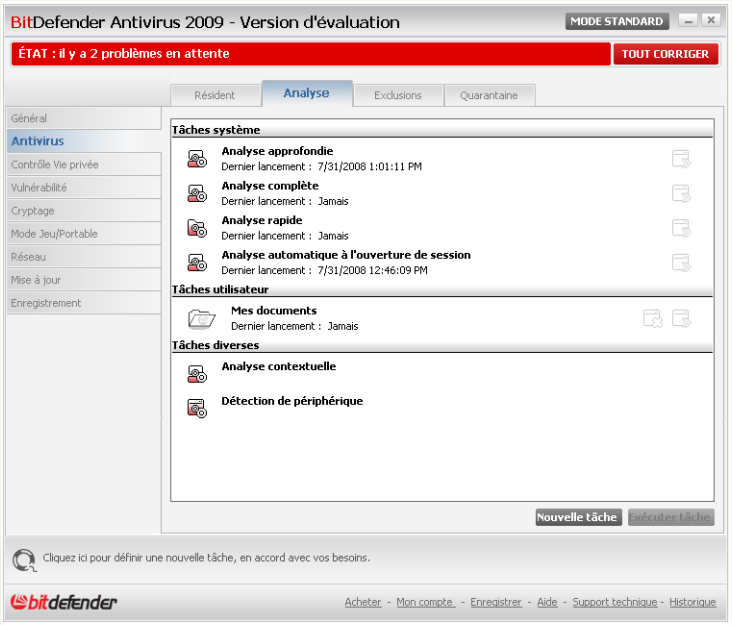
Cliquez sur **Fermer** pour sauvegarder les modifications et fermer la fenêtre.

16.2. 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 l'interface avancée.



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.

16.2.1. 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. 118).

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 malveillants 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 malveillants 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 malveillants, à l'exception des rootkits, mais ne permet pas d'analyser la mémoire, les registres et les cookies.
Analyse automatique à l'ouverture de session	Analyse les éléments qui sont exécutés quand un utilisateur se connecte à Windows. Par défaut, l'analyse à l'ouverture de session est désactivée. Si vous voulez utiliser cette tâche, faites un clic-droit dessus, sélectionnez **Planifier** et définissez la tâche à exécuter **au démarrage du système**. Spécifiez combien de temps après le démarrage la tâche doit s'exécuter (en minutes).

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.

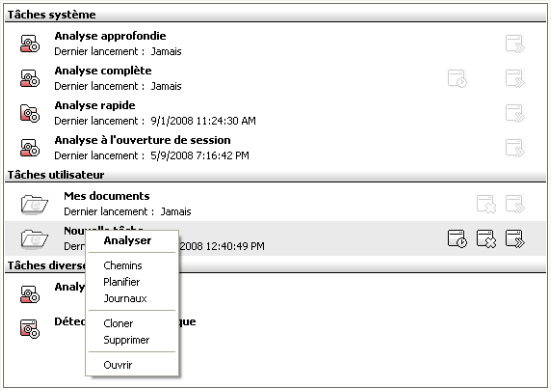
- **Analyser** - lance la tâche selectionnée, démarrant ainsi une analyse immédiate.

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.

16.2.2. 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.
- **Chemins** - ouvre la fenêtre **Propriétés** et l'onglet Chemins 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** - ouvre la fenêtre **Propriétés** et l'onglet Planificateur permettant de planifier la tâche sélectionnée.
- **Journaux** - ouvre la fenêtre **Propriétés**, l'onglet Journaux, où vous pouvez consulter les rapports générés après l'éxécution des tâches sélectionnées.
- **Cloner** - reproduit la tâche sélectionnée. Très utile lors de la création de nouvelles tâches car cette fonction vous permet aussi d'en modifier les propriétés si besoin.
- **Effacer** - efface la tâche sélectionnée.

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

- **Ouvrir** - ouvre la fenêtre **Propriétés** et l'onglet Vue d'ensemble permettant de modifier les paramètres de la tâche sélectionnée.

Note
À cause de la nature particulière de la catégorie **Tâches diverses**, seules les options **Journaux** et **Ouvrir** sont disponibles dans ce cas.

16.2.3. 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.

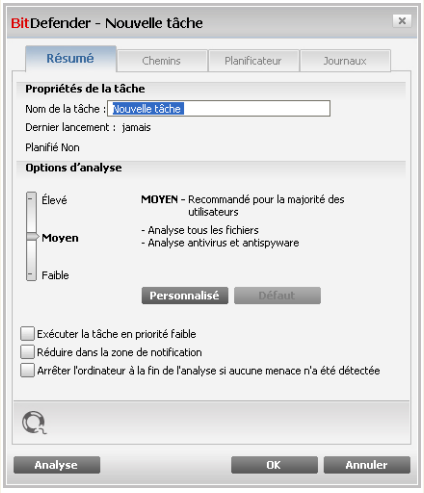
16.2.4. Configuration des tâches d'analyse

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. 137).

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
Moyen	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:

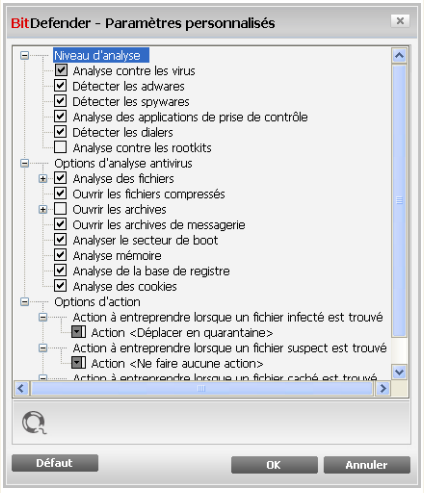
- **Exécuter la tâche d'analyse avec une priorité basse.** Diminue la priorité du processus d'analyse. Vous allez permettre aux autres logiciels de s'exécuter à une vitesse supérieure en augmentant le temps nécessaire pour que l'analyse soit finie.
- **Réduire la fenêtre d'analyse au démarrage dans la 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.
- **Arrêter l'ordinateur lorsque l'analyse est terminée si aucune menace n'a été détecté**

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 regroupées en trois catégories:

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

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

Option	Description
	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	Analyser les applications légitimes qui pourraient être utilisées pour cacher des outils d'espionnage ou d'autres applications malicieuses.
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.

- **Options d'analyse des virus.** Spécifiez le type d'objets à analyser (types de fichiers, archives, etc.) en sélectionnant les options appropriées dans la catégorie **Options d'analyse des virus**.

Option		Description
Analyser les fichiers	**Analyse de tous les fichiers**	Tous les fichiers 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`.

Option	Description
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. L'analyse des fichiers archive augmente le temps d'analyse et demande plus de ressource système. Vous pouvez cliquer sur le champ **Taille limite des archives** et saisir la taille maximum des archives à être analysées (en Ko).
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.

- **Options d'action.** Définissez l'action à entreprendre pour chaque catégorie de fichiers détectés en utilisant les options dans la catégorie **Options d'action**.

Note
Pour définir une nouvelle action, cliquez sur l'action actuelle et sélectionnez l'option désirée à partir du menu.

  - 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	Supprimer le code malveillant des fichiers infectés.

Action	Description
Effacer	Supprime immédiatement les fichiers infectés, sans avertissement.
Déplacer en quarantaine	Déplace les fichiers infectés dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.

- 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. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.

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. Les fichiers mis en quarantaine ne

Action	Description
	peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.
Rendre visible	Affiche les fichiers cachés pour vous permettre de les visualiser.

- **Options d'action à prendre pour les fichiers archivés.** L'analyse et la manipulation des fichiers dans des fichiers archives peut être soumise à des restrictions Les archives protégées par mot de passe ne peuvent pas être analysées à moins que vous ne communiquiez le mot de passe. En fonction du type de fichier archive utilisé (Extension), il est possible que BitDefender ne puisse pas désinfecter, isoler ou supprimer des fichiers archivés. Configurez les actions à entreprendre sur les fichiers archivés détectés en utilisant les options appropriées dans la catégorie**Options d'action pour les fichiers archivés**.
  - Sélectionnez l'action à mener sur les fichiers infectés détectés. Les options suivantes sont disponibles:

Action	Description
Ne pas entreprendre d'action	Ne conserver que les enregistrement de fichiers archives infectés dans le journal d'analyse. Une fois l'analyse terminée, vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.
Désinfecter	Supprimer le code malveillant des fichiers infectés. La désinfection peut échouer dans certains cas, par exemple quand le fichier infecté se trouve dans une archive courrier spécifique.
Effacer	Supprime immédiatement les fichiers infectés, sans avertissement.
Déplacer en quarantaine	Déplacer les fichiers infectés de leur emplacement d'origine vers le dossier de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.

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

Action	Description
Ne pas entreprendre d'action	Ne conserver que les enregistrements de fichiers archive suspects dans le journal d'analyse. Une fois l'analyse terminée, vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.
Effacer	Supprime immédiatement les fichiers suspects, sans avertissement.
Déplacer en quarantaine	Déplace les fichiers suspects dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.

○ Sélectionnez l'action à entreprendre sur les fichiers protégés par mot de passe détectés. Les options suivantes sont disponibles:

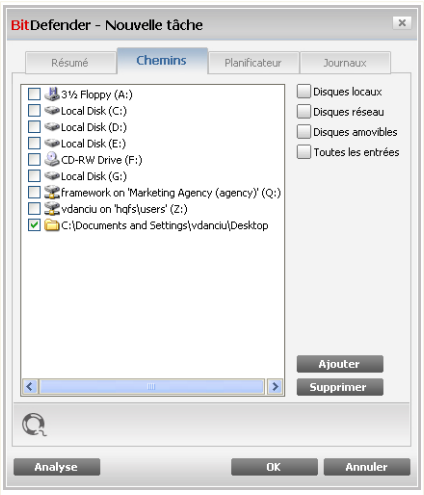
Action	Description
Noter comme non analysé"	Ne conserver que les enregistrements des fichiers protégés par mot de passe dans le journal d'analyse. Une fois l'analyse terminée, vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.
Demander pour le mot de passe	Quand un fichier protégé par mot de passe est détecté, demander à l'utilisateur le mot de passe afin de pouvoir analyser le fichier.

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.

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, faites un clic droit sur la tâche et sélectionnez **Chemins**. 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.

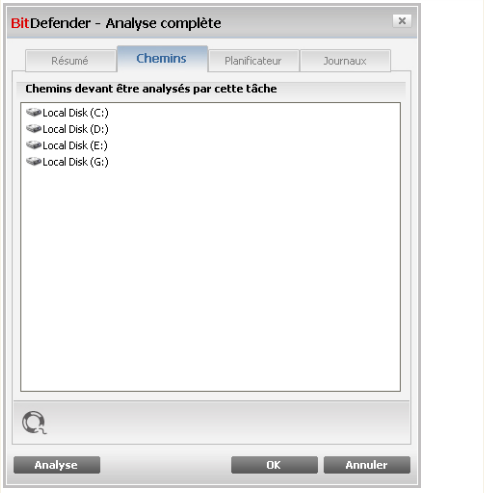
Note
Si vous voulez analyser l'ensemble de votre ordinateur, cochez la case **Toutes les entrées**.

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

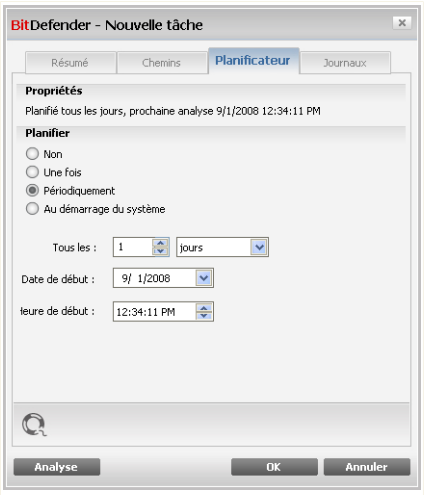
Analyse complète du système et **Analyse approfondie du système** analysera tous les disques locaux, alors que **Analyse rapide du système** analysera uniquement le répertoire `Windows` et `Program Files`.

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**.
- **Au démarrage système** - démarre l'analyse au moment défini après que l'utilisateur se soit connecté à Windows.

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

16.2.5. 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 2009.
- 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.

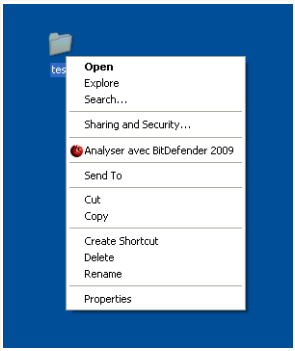
Pour exécuter une tâche d'analyse, utilisez l'une des méthodes suivantes:

- 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. 133).

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

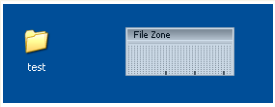
Faîtes un clic-droit sur le fichier ou répertoire que vous souhaitez analyser et sélectionnez l'option **BitDefender Antivirus 2009**.

Lorsque le moteur d'analyse BitDefender apparaît, l'analyse est lancée. Pour plus d'informations, reportez-vous à « *Moteur d'analyse BitDefender* » (p. 133).

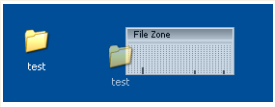
Vous pouvez modifier les options d'analyse et voir les fichiers de rapport à partir de la fenêtre **Propriétés** de la tâche **Analyse via le menu contextuel**.

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

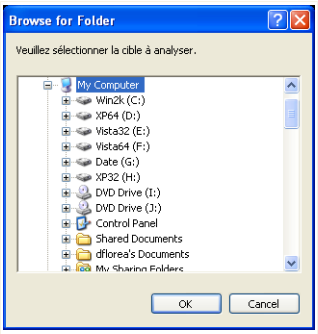
Lorsque le moteur d'analyse BitDefender apparaît, l'analyse est lancée. Pour plus d'informations, reportez-vous à « *Moteur d'analyse BitDefender* » (p. 133).

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 objets que BitDefender doit analyser, suivez le chemin suivant depuis le menu Démarrer de Windows: **Démarrer** → **Programmes** → **BitDefender 2009** → **Analyse manuelle BitDefender**. La fenêtre suivante apparaît:



Analyse manuelle

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

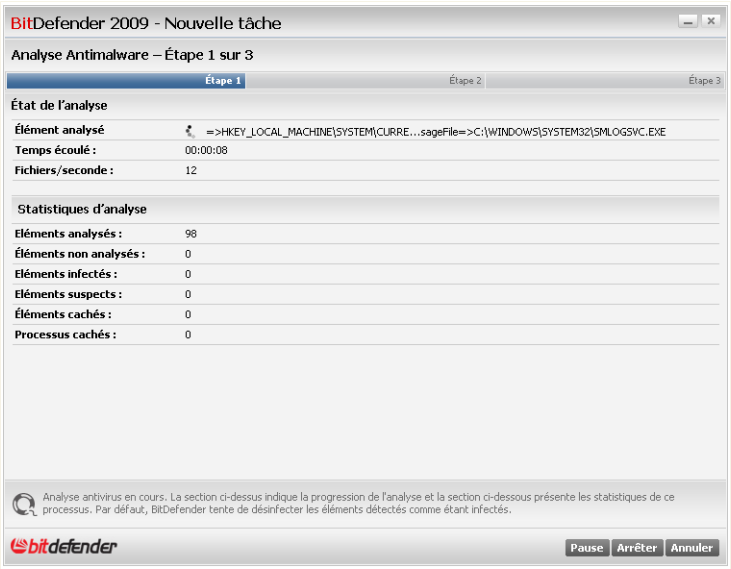
Lorsque le moteur d'analyse BitDefender apparaît, l'analyse est lancée. Pour plus d'informations, reportez-vous à « *Moteur d'analyse BitDefender* » (p. 133).

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.

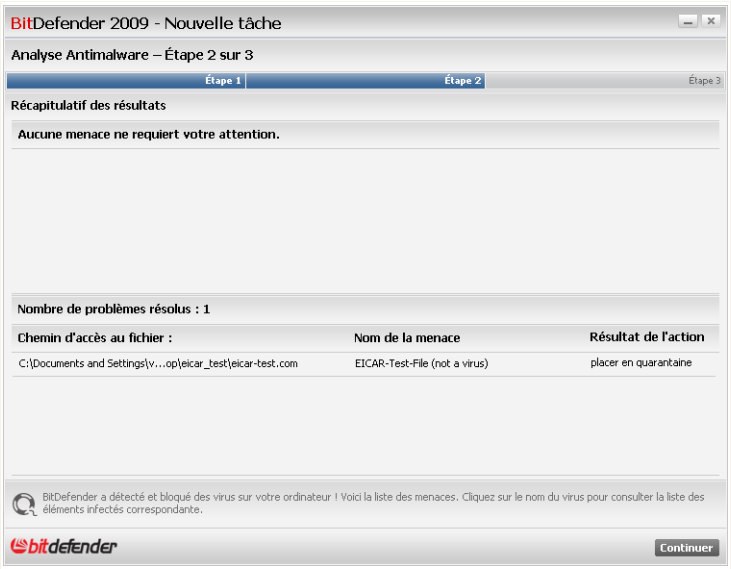
Pour suspendre temporairement le processus d'analyse, cliquez sur **Pause**. Pour reprendre l'analyse, cliquez sur **Reprendre**.

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 l'ensemble des problèmes de sécurité ou sélectionner des actions spécifiques pour chaque groupe de problèmes.

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.
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.

Résumé

Le récapitulatif des résultats s'affiche. Cliquez sur **Afficher le journal** pour voir le journal des analyses.

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

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

BitDefender n'a pas pu corriger certains problèmes

Dans la plupart des cas, BitDefender désinfecte ou isole l'infection des fichiers infectés qu'il détecte. 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.

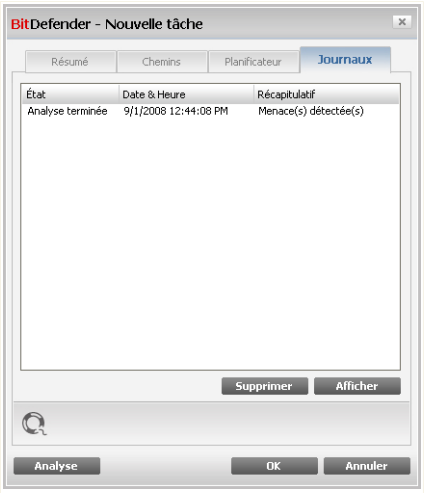
BitDefender a détecté des fichiers suspects

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.

16.2.6. 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 :

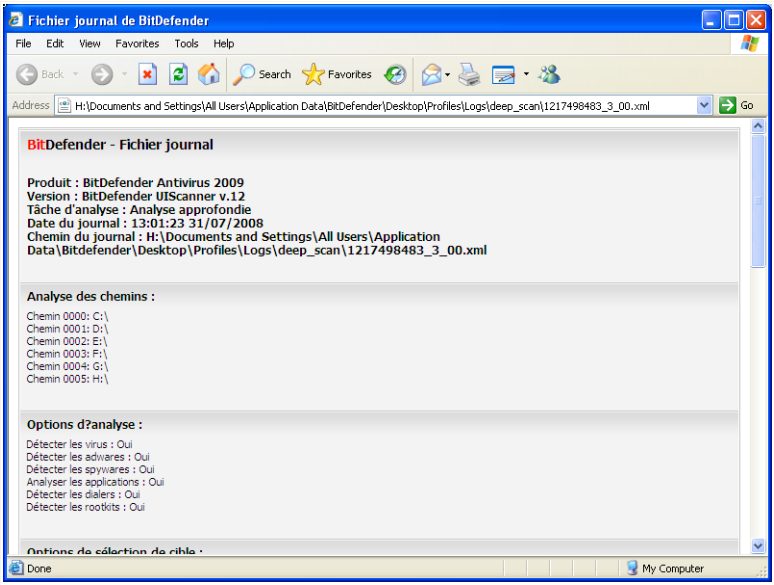
- **Supprimer** - pour supprimer le journal d'analyse sélectionné.
- **Afficher** - pour voir le journal d'analyse sélectionné. Le journal d'analyse s'affichera dans votre navigateur Internet par défaut.

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.

16.3. 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.

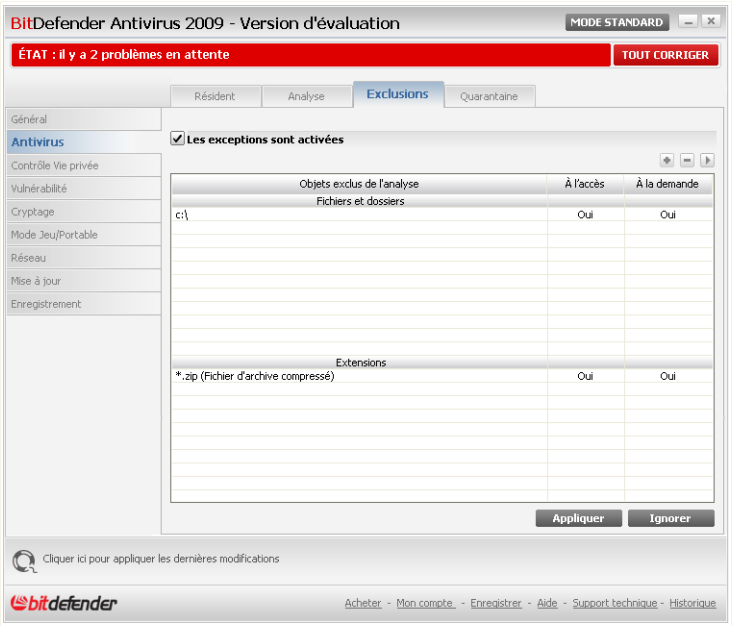
BitDefender vous permet d'exclure des objets d'une analyse à l'accès ou d'une analyse sur demande ou des deux. Cette fonction permet de réduire la durée d'une analyse et d'éviter d'interférer dans votre travail.

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 l'interface avancée.



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**.

16.3.1. 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.

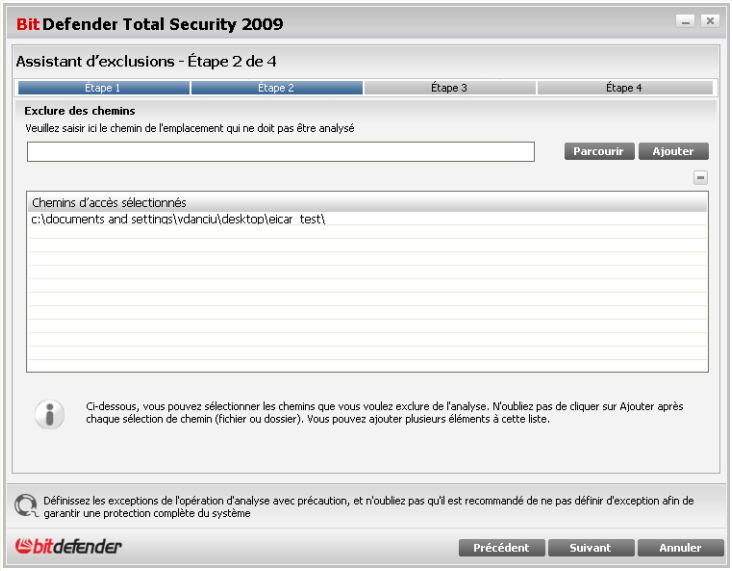
Étape 1/4 - Sélectionner le type d'objet

Type d'objet

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

Cliquez sur **Suivant**.

Étape 2/4 - 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**.

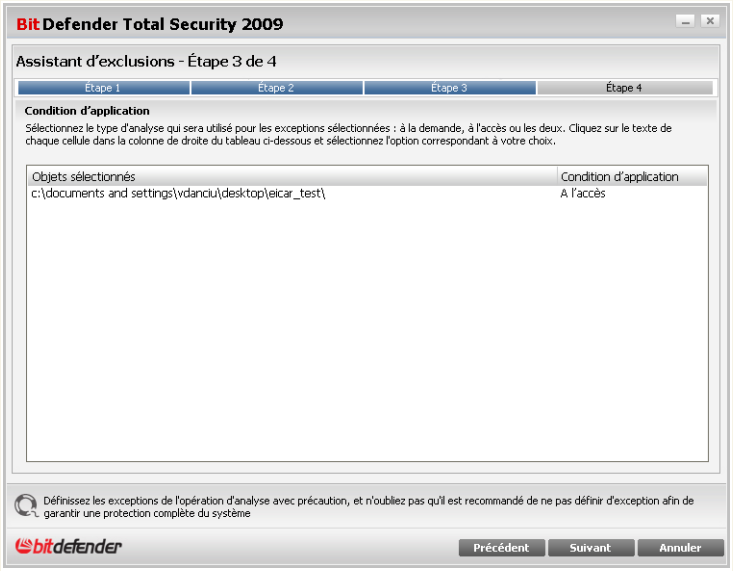
> ***Note***
> Si le chemin indiqué n'existe pas, un message d'erreur apparaît. Cliquez sur **OK** et vérifiez la validité du chemin.

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 3/4 - 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 **Suivant**.

Étape 4/4 - Analyser les fichiers exclus

Analyser les fichiers exclus

Il vous est fortement conseillé d'analyser les fichiers dans les chemins spécifiés pour vous assurer qu'ils ne soient pas infectés. Cochez la case pour analyser ces fichiers avant de les exclure de l'analyse.

Cliquez sur **Terminer**.

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

16.3.2. 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.

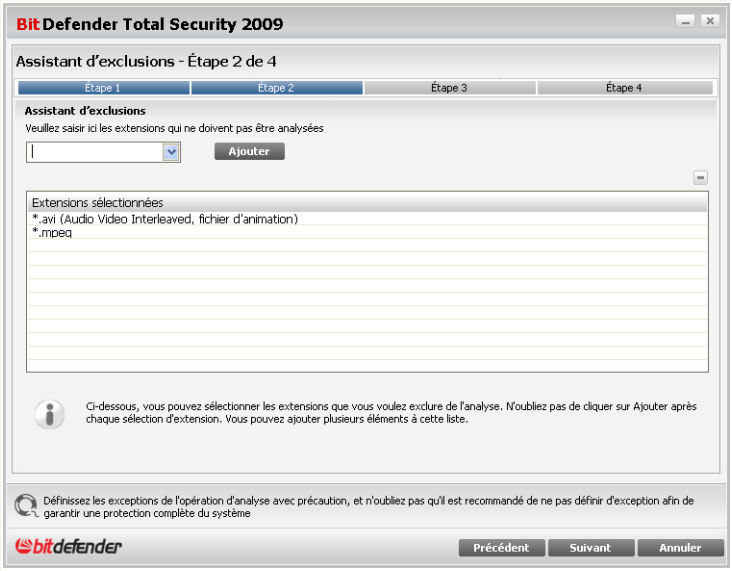
Étape 1/4 - Sélectionner le type d'objet

Type d'objet

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

Cliquez sur **Suivant**.

Étape 2/4 - Spécifier les extensions exclues



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.

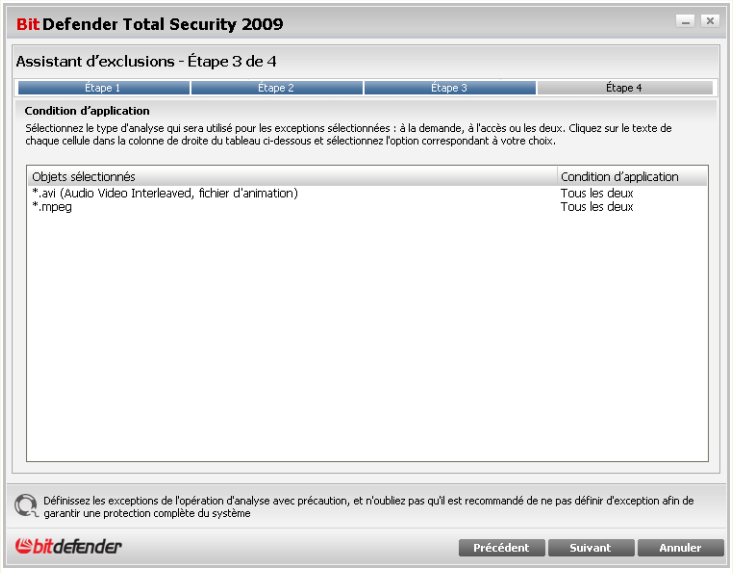
- Saisissez l'extension à exclure de l'analyse dans la zone de texte, puis cliquez sur **Ajouter**.

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 3/4 - 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 **Suivant**.

Étape 4/4 - Sélectionner le type d'analyse

Type d'analyse

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

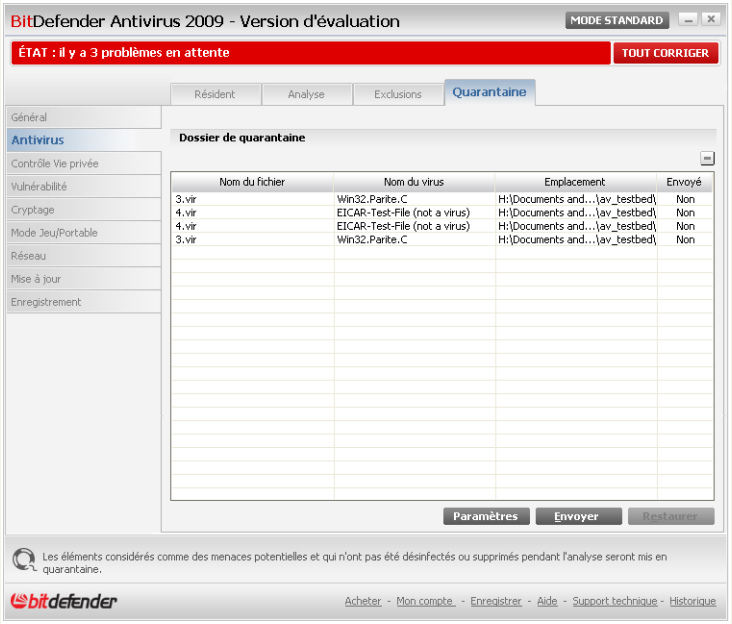
Cliquez sur **Terminer**.

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

16.4. 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 l'interface avancée.



Quarantaine

La partie Quarantaine affiche tous les fichiers actuellement isolés dans le dossier Quarantaine. Pour chaque fichier en quarantaine, vous pouvez voir son nom, le nom du virus détecté, le chemin de son emplacement d'origine et sa date de soumission.

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

16.4.1. Gérer les fichiers en quarantaine

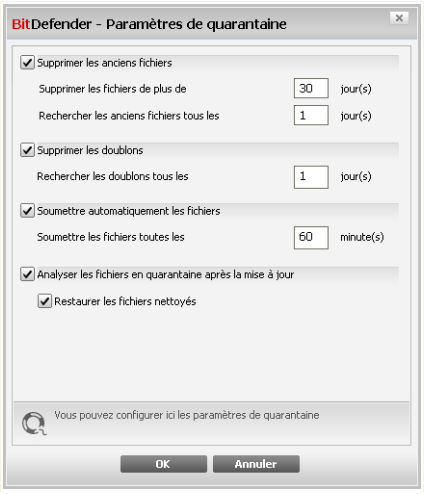
Pour effacer un fichier sélectionné dans la zone de quarantaine, cliquez sur le bouton **Déplacer**. Si vous voulez restaurez un fichier sélectionné dans son emplacement d'origine, cliquez sur **Restaurer**.

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.

16.4.2. 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 30 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.

Analyser les fichiers en quarantaine après une mise à jour. Pour analyser automatiquement les fichiers en quarantaine après chaque mise à jour effectuée, cochez l'option correspondante. Vous pouvez choisir de remettre automatiquement vos fichiers sains dans leur emplacement d'origine en sélectionnant **Restaurer les fichiers sains**.

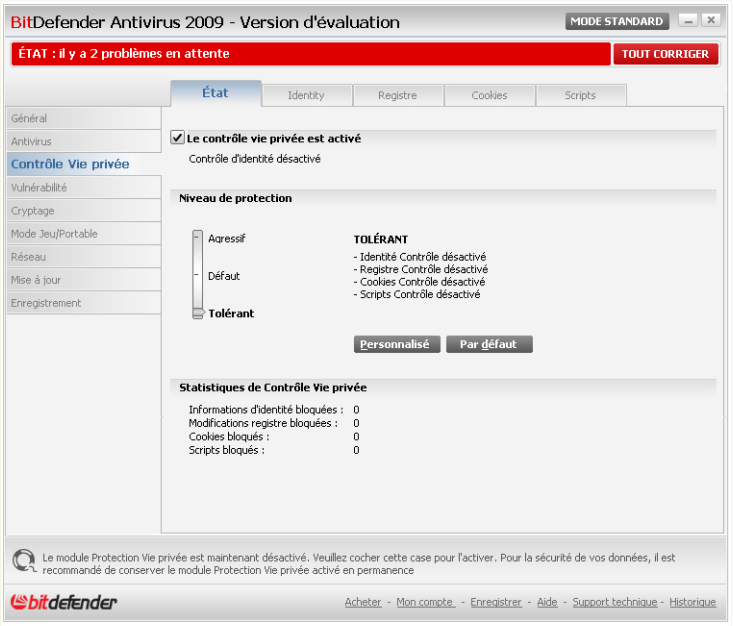
Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

17. 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.

17.1. Statut du Contrôle Vie privée

Pour configurer le Contrôle Vie privée et consulter des informations sur son activité, rendez-vous dans **Contrôle Vie privée>État** dans le Mode avancé.



Statut du Contrôle Vie privée

Vous pouvez vérifier si le Contrôle Vie privée est activé ou désactivé. Si vous voulez modifier l'état du Contrôle Vie privée, cochez ou décochez la case correspondante.

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 ces contrôles de protection essentiels :

- Contrôle d'identité - protège vos données confidentielles en filtrant tout le trafic sortant Internet (HTTP), e-mail (SMTP) et de messagerie instantanée selon les règles que vous avez créées dans la section Identité.
- Contrôle de la base de registre - demande votre autorisation dès lors qu'un programme tente de modifier une entrée de registre afin de s'exécuter au démarrage de Windows.
- Contrôle des cookies - demande votre autorisation dès lors qu'un nouveau site Web tente de créer un cookie sur votre ordinateur.
- Contrôle des scripts - demande votre autorisation dès lors qu'un site Web tente d'exécuter un script ou un autre contenu actif.

En bas de la section, vous pouvez consulter les **statistiques du Contrôle Vie privée**.

17.1.1. 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	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.

17.2. Contrôle d'identité

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

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

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

Vous pouvez créer des règles pour protéger toutes les informations que vous considérez comme personnelles ou confidentielle, votre numéro de téléphone, votre adresse e-mail ou votre Numéro de compte bancaire... Le support multi-utilisateurs est fourni pour que les utilisateurs connectés sur des comptes Windows différents puissent configurer et utiliser leurs propres règles de protection. Les règles que vous créez sont appliquées et accessibles uniquement lorsque vous êtes connecté sur votre compte utilisateur Windows.

Pourquoi utiliser le Contrôle d'identité?

- Le Contrôle d'identité est très efficace dans le blocage des spywares keylogger. Ce type d'applications malicieuses enregistre vos frappe clavier et les envoit par Internet à des pirates. Le pirate peut récupérer des informations sensibles à partir des données volées, comme vos numéros de comptes bancaires ou vos mots de passe pour les utiliser à son propre profit.

  Dans l'hypothèse où une application de ce type réussirait à contourner la protection antivirus, elle ne pourra pas envoyer les données subtilisées par email, par le web

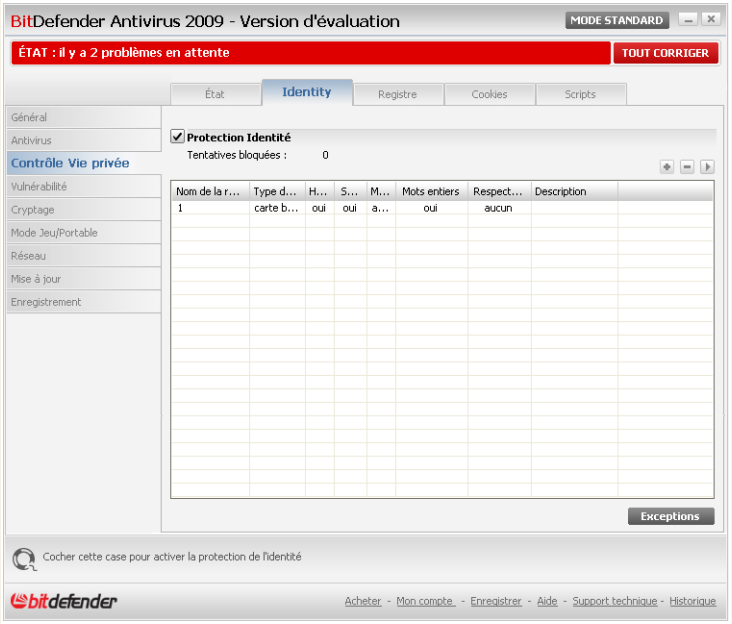
ou par messagerie instantanée si vous avez créé les règles de protection d'identité adaptées.

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

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

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

Pour configurer le contrôle d'identité, rendez-vous dans **Contrôle Vie privée>Identité** dans le Mode avancé.



Contrôle d'identité

Suivez les étapes suivantes pour utiliser le contrôle d'identité :

1. Cochez la case **Contrôle d'identité**.
2. Définissez les règles nécessaires à la protection de vos données sensibles. Pour plus d'informations, reportez-vous à « *Création de règles d'Identité* » (p. 156).
3. Définissez si nécessaire des exceptions pour les règles que vous venez de créer. Pour plus d'informations, reportez-vous à « *Définition des exceptions* » (p. 160).

17.2.1. Création de règles d'Identité

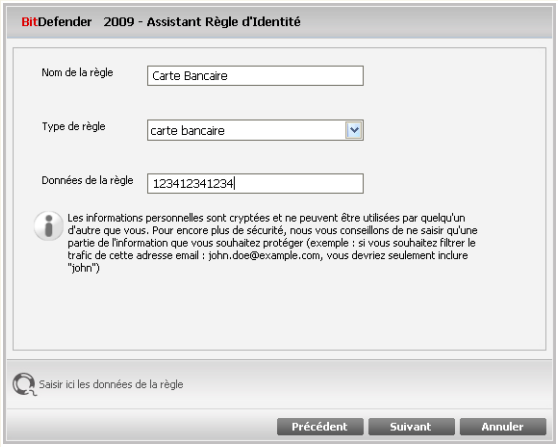
Pour créer une règle de protection de l'identité, clique sur le bouton **Ajouter** et suivez les instructions de l'assistant de configuration.

Etape 1/4- Fenêtre d'accueil

Fenêtre de bienvenue

Cliquez sur **Suivant**.

Étape 2/4 - Définir le type de règle et les données



Définition des types de règles et de données

Vous devez définir les paramètres suivants:

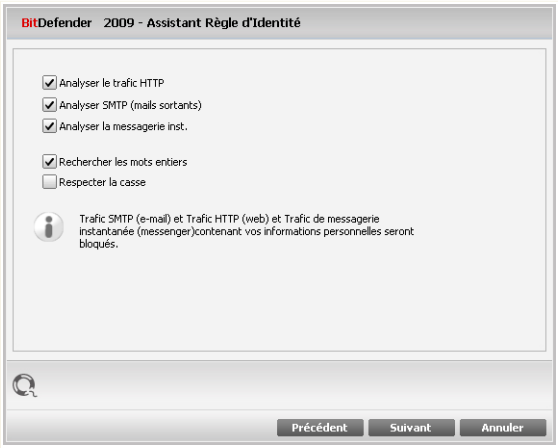
- **Nom de la règle** - saisissez le nom de la règle dans ce champ de saisie.
- **Type de règle** - détermine le type de règle (addresse, nom, carte de crédit, code PIN, etc.)
- **Données de la règle** - saisissez les données que vous voulez protéger dans ce champ de saisie. Si par exemple vous voulez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

> ***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**.

Étape 3/4 - Sélectionner le trafic



Sélection du trafic

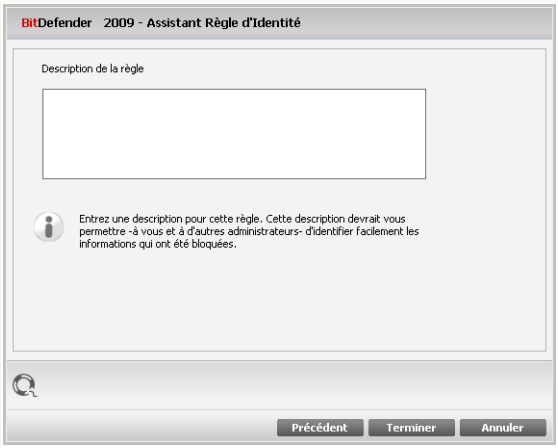
Sélectionnez le type de trafic que BitDefender doit analyser. Les options suivantes sont disponibles:

- **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.
- **Analyser la messagerie instantanée** - Analyse le trafic de messagerie instantanée et bloque les échanges sortants qui contiennent les éléments déterminés dans la règle de gestion des données.

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

Cliquez sur **Suivant**.

Étape 4/4 - Décrire la règle



Description de la règle

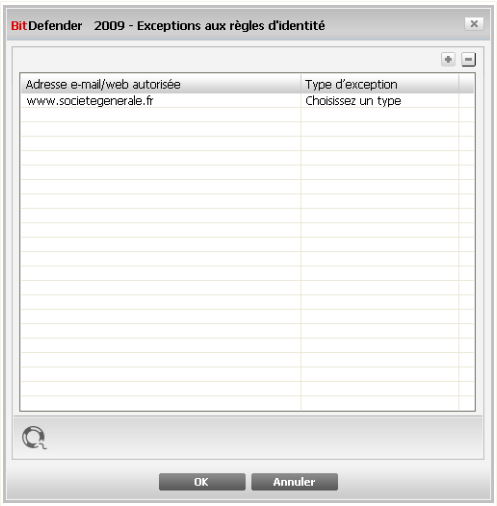
Entrez une description courte de la règle dans le champ correspondant. Puisque les données bloquées (chaines de caractères) ne sont pas affichées sous forme de texte clair quand vous accédez à la règle, la description devrait vous aider à l'identifier rapidement.

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

17.2.2. 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 l'adresse autorisée** et indiquez l'adresse du site Internet, de l'e-mail ou du contact de messagerie instantanée 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**.
   - Si vous avez indiqué un contact de messagerie instantanée, sélectionnez **Messagerie instantanée**.

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

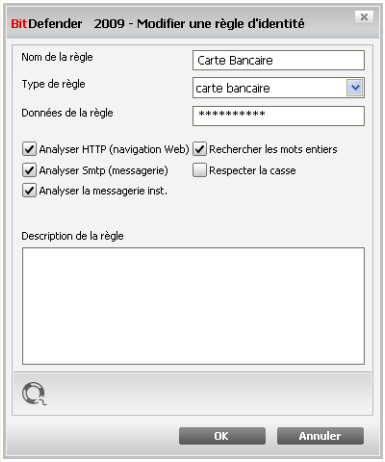
Cliquez**OK** pour sauvegarder les changements.

17.2.3. Gestion des règles

Vous pouvez voir les règles existantes dans le tableau correspondant.

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

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

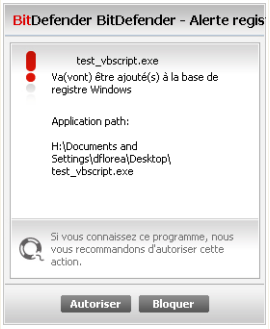
Dans cette rubrique, vous pouvez modifier le nom, la description et les paramètres de la règle (type, données et trafic). Cliquez sur **OK** pour enregistrer les modifications.

17.3. Contrôle de la base de registre

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

La **Base de registres** est également utilisée pour définir quels programmes devraient être lancés automatiquement lorsque Windows démarre. 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 voir le programme essayant de modifier le registre de Windows.

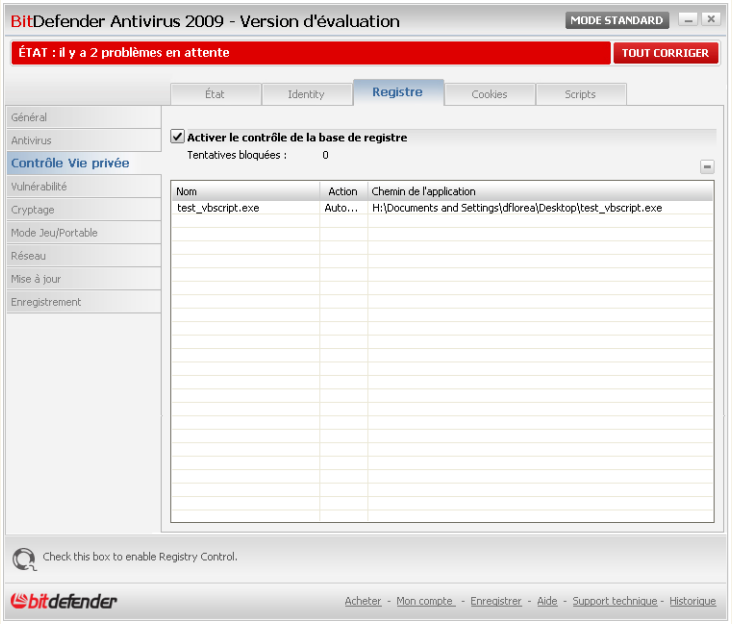
Si vous ne reconnaissez pas le programme et qu'il vous semble suspect, cliquez sur **Bloquer** pour l'empêcher de modifier le registre Windows. Autrement, cliquez sur **Autoriser** pour permettre la modification.

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

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.

Pour configurer le contrôle de la base de registre, rendez-vous dans **Contrôle Vie privée>Base de registre** dans le Mode avancé.



Contrôle de la base de registre

Vous pouvez voir les règles existantes dans le tableau correspondant.

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

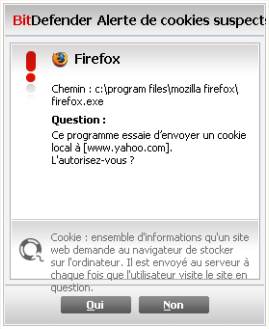
17.4. Contrôle des cookies

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.

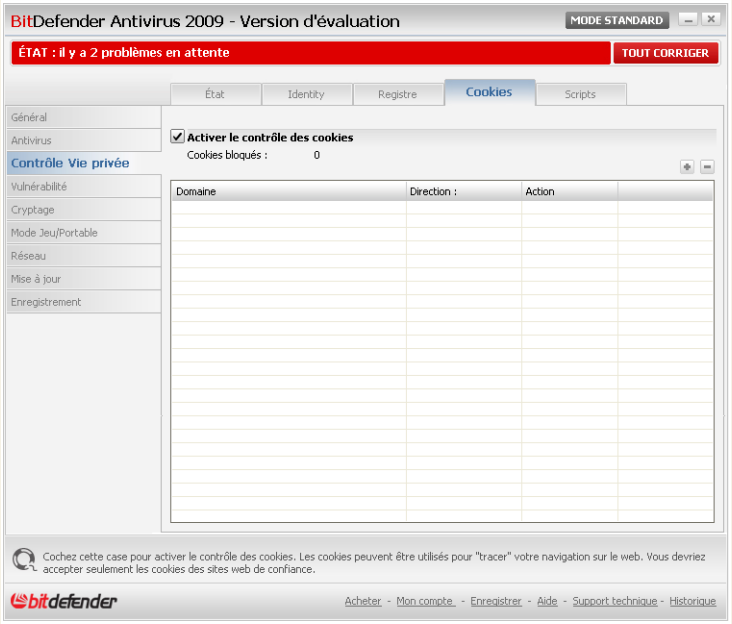
Sélectionnez **Retenir cette réponse** et cliquez sur **Oui** ou **Non** et une règle sera créée, appliquée et listée dans le tableau des règles.

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.

Pour configurer le contrôle des cookies, rendez-vous dans **Contrôle Vie privée>Cookie** dans le Mode avancé.



Contrôle des cookies

Vous pouvez voir les règles existantes dans le tableau correspondant.

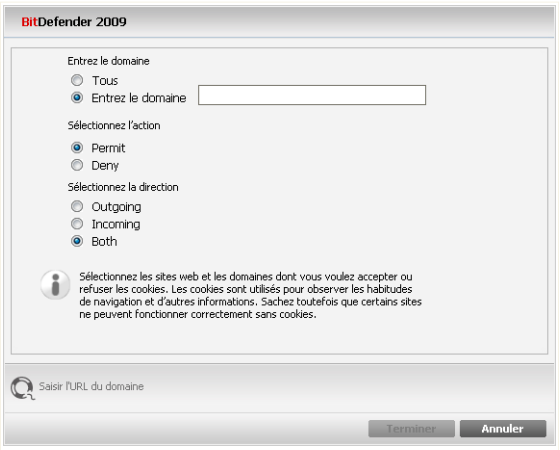
Important
Les règles sont listées dans l'ordre de priorité en commençant par le haut de la liste, la première règle a la priorité la plus élevée. Glisser & déposer les règles afin de changer leur priorité.

Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton **Supprimer**. Pour modifier les paramètres de la règle, double cliquez dessus et faites les changements désirés dans la fenêtre de configuration.

Pour ajouter manuellement une règle, cliquez sur le bouton **Ajouter** et configurer les paramètres de la règle dans la fenêtre de configuration.

17.4.1. Fenêtre de configuration

Lorsque vous modifiez ou ajoutez manuellement une règle, une fenêtre de configuration apparaît.



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.

Type	Description
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.

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

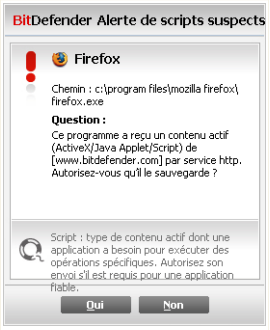
Cliquez sur **Terminer**.

17.5. Contrôle des scripts

Les Scripts et d'autres codes comme les contrôles ActiveX et Applets Java, qui sont utilisés pour créer des pages web interactives, peuvent être programmés pour avoir des effets néfastes. Les éléments ActiveX, par exemple, peuvent obtenir un accès total à vos données et peuvent lire des données depuis votre ordinateur, supprimer des informations, capturer des mots de passe et intercepter des messages lorsque vous êtes en ligne. 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:

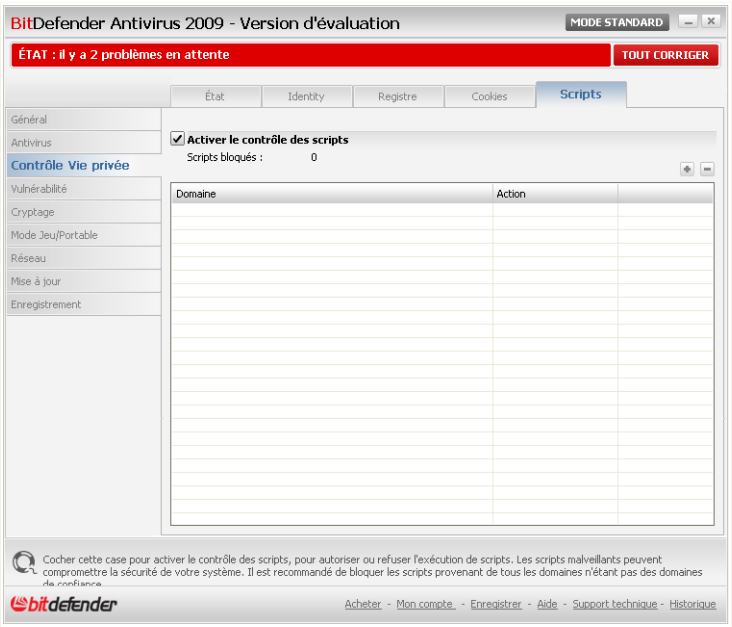


Alerte de scripts

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.

Pour configurer le contrôle des scripts, rendez-vous dans **Contrôle Vie privée>Script** dans le Mode avancé.



Contrôle des scripts

Vous pouvez voir les règles existantes dans le tableau correspondant.

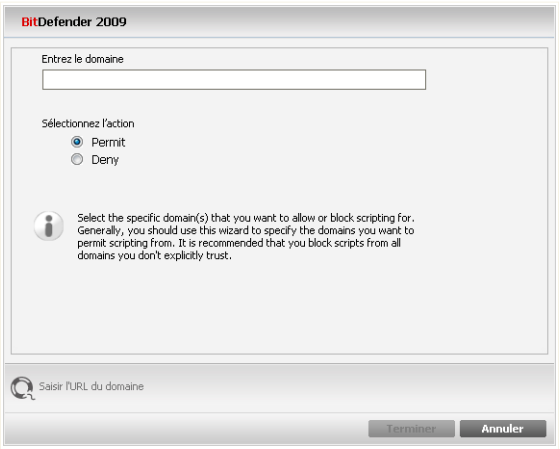
Important
Les règles sont listées dans l'ordre de priorité en commençant par le haut de la liste, la première règle a la priorité la plus élevée. Glisser & déposer les règles afin de changer leur priorité.

Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton **Supprimer**. Pour modifier les paramètres de la règle, double cliquez dessus et faites les changements désirés dans la fenêtre de configuration.

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

17.5.1. Fenêtre de configuration

Lorsque vous modifiez ou ajoutez manuellement une règle, une fenêtre de configuration apparaît.



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**.

18. Cryptage de messagerie instantanée

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

- votre correspondant ait installé sur son ordinateur une version de BitDefender qui prenne en charge le cryptage de messagerie instantanée et que ce dernier soit activé pour l'application de messagerie instantanée utilisée pour converser ;
- vous et votre correspondant utilisiez soit Yahoo Messenger, soit Windows Live (MSN) Messenger.

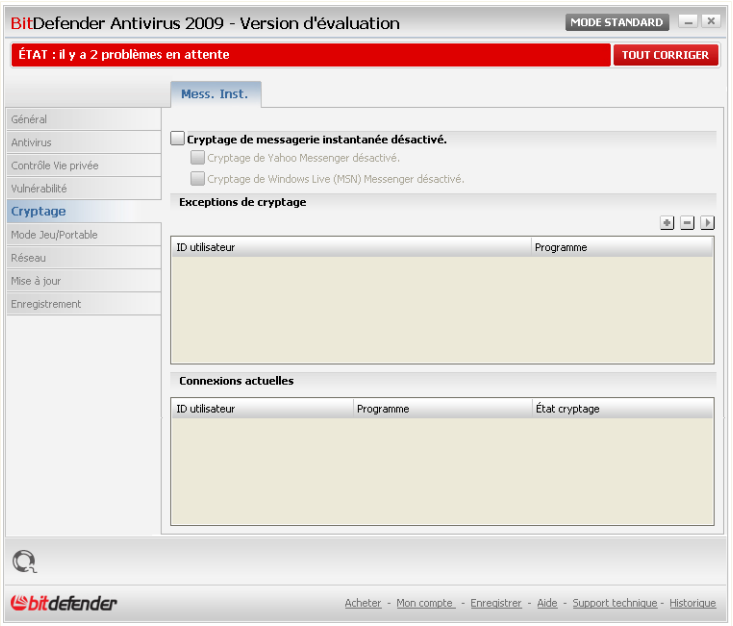
Important

BitDefender ne cryptera pas la conversation si le correspondant utilise une application à interface Web, telle que Meebo, ou une autre application de chat compatible Yahoo Messenger ou MSN.

Pour configurer le cryptage de messagerie instantanée, rendez-vous dans **Cryptage>Cryptage de messagerie instantanée** dans le Mode avancé.

Note

Vous pouvez aisément configurer le cryptage de messagerie instantanée en utilisant la barre d'outils BitDefender dans la fenêtre de chat. Pour plus d'informations, reportez-vous à « *Intégration dans Messenger* » (p. 36).



Cryptage de messagerie instantanée

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

Deux tableaux sont affichés :

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

- Votre contact n'a pas de version BitDefender installée supportant le cryptage des messageries instantanées.

18.1. Désactiver le cryptage pour des utilisateurs spécifiques

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

1. Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre de configuration.

Ajout de contacts

2. Tapez dans le champ de saisie l'identifiant utilisateur de votre contact.
3. Sélectionnez l'application de messagerie instantanée associée au contact.
4. Cliquez sur **OK**.

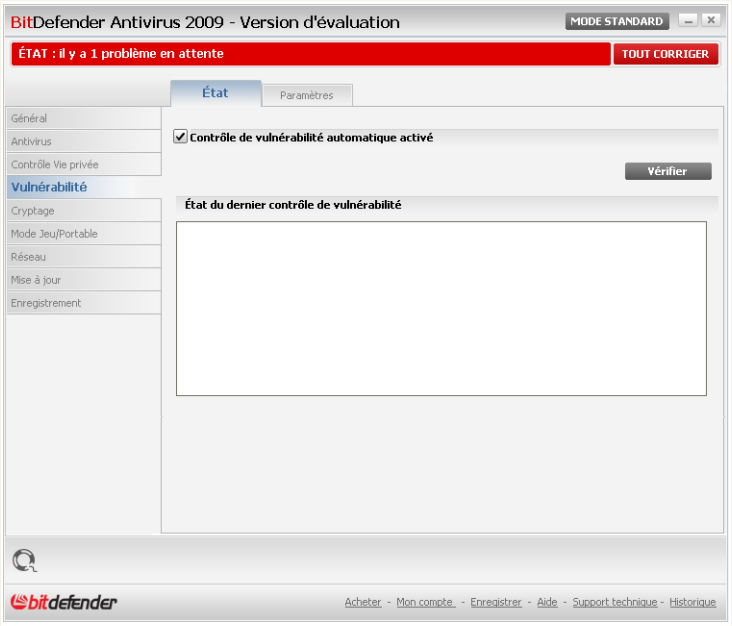
19. Vulnérabilité

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

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

19.1. Etat

Pour configurer l'analyse automatique des vulnérabilités ou lancer une analyse des vulnérabilités, allez dans **État> Vulnerabilité** dans l'interface avancée.



État de la vulnérabilité

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

Important
Pour être automatiquement averti sur les vulnérabilités du système ou des applications, veuillez garder l'option **Analyse automatique des vulnérabilités** activée.

19.1.1. Réparation des vulnérabilités

Pour réparer une vulnérabilité particulière, double-cliquez dessus et selon le problème, procédez comme suit :

- Si des mises à jour Windows sont disponibles, cliquez sur**Installer toutes les mises à jour système** pour installer toutes les mises à jour disponibles.
- Si une application n'est pas à jour, cliquez sur le lien **Page d'accueil**fourni pour télécharger et installer la dernière version de cette application.
- Si un compte utilisateur Windows utilise un mot de passe faible, vous pouvez forcer l'utilisateur à changer de mot de passe à sa prochaine connexion ou le changer vous même.

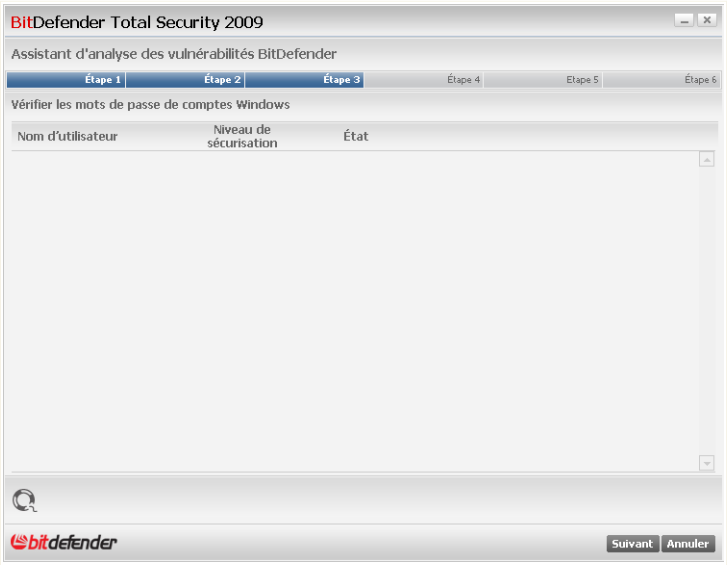
Pour rechercher des vulnérabilités sur votre ordinateur, cliquez sur **Vérifier maintenant** et suivez les instructions de l'assistant.

Etape 1/6 - Sélectionnez les vulnérabilités à vérifier

Vulnérabilités

Cliquez sur **Suivant** pour lancer l'analyse des vulnérabilités sélectionnées.

Etape 2/6 - Vérifier les vulnérabilités



Analyse de vulnérabilité

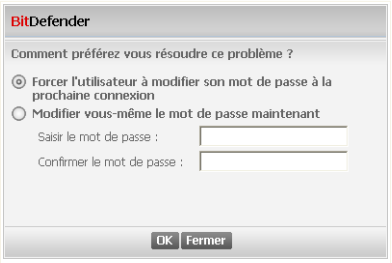
Patientez jusqu'à ce que BitDefender ait terminé l'analyse des vulnérabilités.

Étape 3/6 - Modifier les mots de passe vulnérables

Mots de passe utilisateur

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

Cliquez sur **Réparer** pour modifier les mots de passe vulnérables. Une nouvelle fenêtre s'affiche.



Changer le mot de passe

Choisir la méthode à utiliser pour régler ce problème :

- **Obliger l'utilisateur à changer son mot de passe à la prochaine connexion.** BitDefender demandera à l'utilisateur de modifier son mot de passe lors de sa prochaine connexion à Windows
- **Changer le mot de passe utilisateur.** Vous devez saisir le nouveau mot de passe dans les champs de modification.

Note
Pour avoir un mot de passe Fort, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple `#`, `$` ou `@`).

Cliquez sur **OK** pour changer le mot de passe.

Cliquez sur **Suivant**.

Étape 4/6 - Mettre à jour les applications

Applications

Vous pouvez voir la liste des applications vérifiées par BitDefender et savoir si ces dernières sont à jour. Si une application n'est pas à jour, cliquez sur le lien fourni pour télécharger la dernière version.

Cliquez sur **Suivant**.

Étape 6/6 - Mettre à jour Windows

Mises à jours Windows

Vous pouvez voir la liste des mises à jour Windows (critiques et non-critiques) qui ne sont pas installées actuellement sur votre ordinateur. Cliquez sur **Installer toutes les mises à jour système** pour installer toutes les mises à jour disponibles.

Cliquez sur **Suivant**.

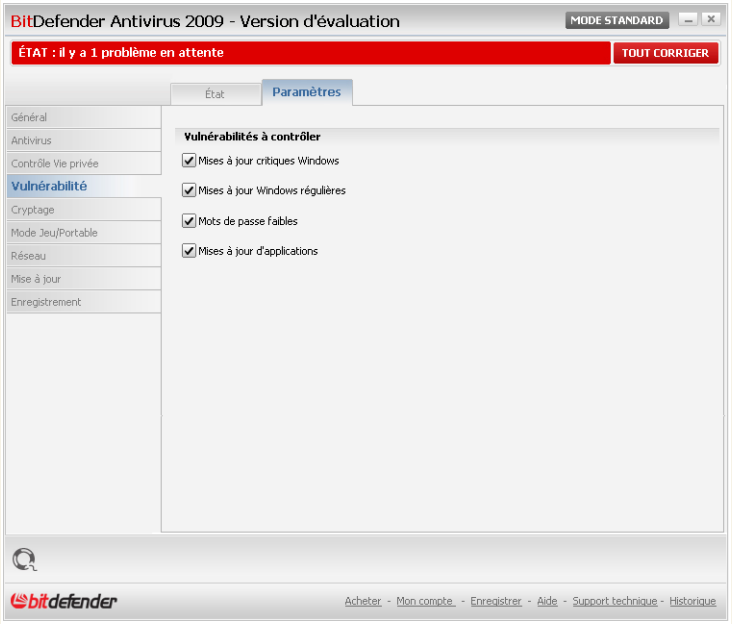
Étape 6/6 - Voir les résultats

Résultats

Cliquez sur **Fermer**.

19.2. Paramètres

Pour configurer les paramètres de l'analyse automatique des vulnérabilités, allez dans **Vulnérabilité>Paramètres** dans l'interface avancée.



Paramètres de l'analyse automatique des vulnérabilités.

Cochez les cases correspondantes aux vulnérabilités système que vous voulez analyser régulièrement :

- **Mises à jour Windows critiques**
- **Mises à jour Windows régulières**
- **Mots de passe vulnérables**
- **Mises à jour d'applications**

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

20. Mode Jeu / Portable

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

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

20.1. Mode Jeu

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

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

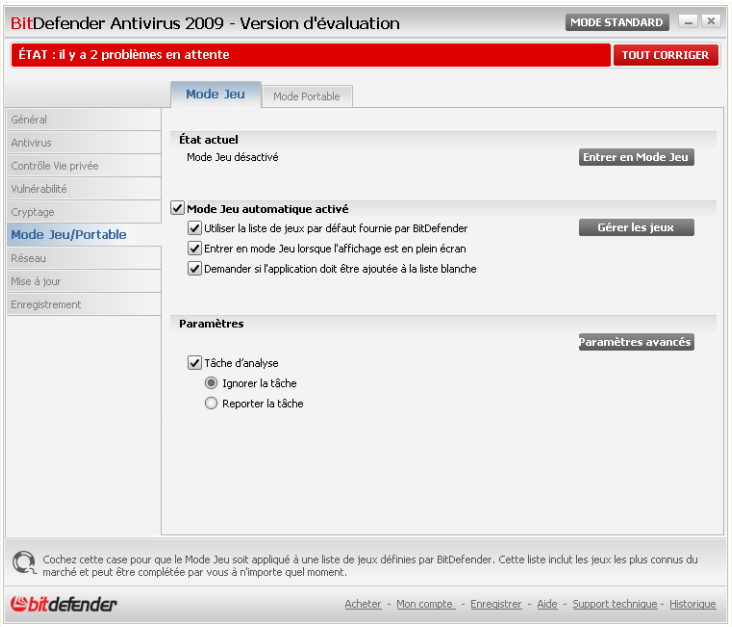
> ***Note***
> Pour modifier ce paramètre, rendez-vous dans Mise à jour>Paramètres et décochez la case **Ne pas mettre à jour si le Mode Jeu est actif**.

- Les tâches d'analyse planifiées sont désactivées par défaut.

Par défaut, BitDefender passe automatiquement en Mode Jeu lorsque vous lancez un jeu figurant dans la liste des jeux connus de BitDefender, ou lorsqu'une application s'exécute en mode plein écran. Vous pouvez passer manuellement en Mode Jeu en utilisant le raccourci clavier par défaut `Ctrl+Alt+Shift+G`. Nous vous recommandons fortement de quitter le Mode Jeu lorsque vous avez fini de jouer (vous pouvez pour ce faire utiliser le même raccourci clavier par défaut `Ctrl+Alt+Shift+G`).

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

Pour configurer le Mode Jeu, rendez-vous dans **Mode Jeu/Portable** dans le Mode avancé.



Mode Jeu

Vous pouvez vérifier l'état du Mode Jeu dans la partie supérieure de la section. Vous pouvez cliquer sur **Entrer en Mode Jeu** ou **Quitter le Mode Jeu** pour modifier l'état en cours.

20.1.1. Configuration du Mode Jeu automatique

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

- **Utiliser la liste de jeux par défaut fournie par BitDefender** - permet de passer automatiquement en Mode Jeu lorsque vous lancez un jeu figurant dans la liste de

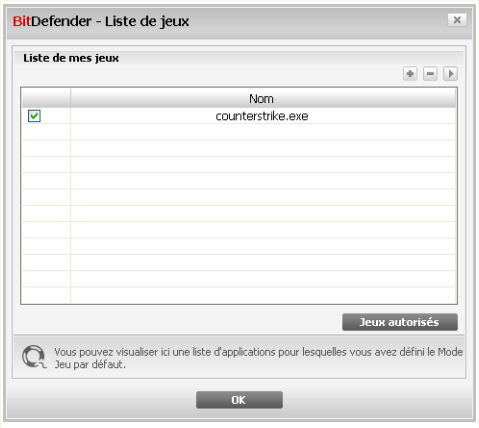
jeux connus de BitDefender. Pour consulter cette liste, cliquez sur **Gérer les jeux** puis sur **Afficher les jeux autorisés**.

- **Passer en Mode Jeu lors du passage en plein écran** - permet de passer automatiquement en Mode Jeu lorsqu'une application s'exécute en mode plein écran.
- **Ajouter l'application à la liste de jeux ?** - permet d'être notifié pour l'ajout d'une nouvelle application à la liste de jeux, à la fermeture du mode plein écran. Si vous ajoutez une nouvelle application à la liste de jeux, la prochaine fois que vous lancerez celle-ci, BitDefender passera automatiquement en Mode Jeu.

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

20.1.2. Gestion de la liste de jeux

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



Liste de jeux

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

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

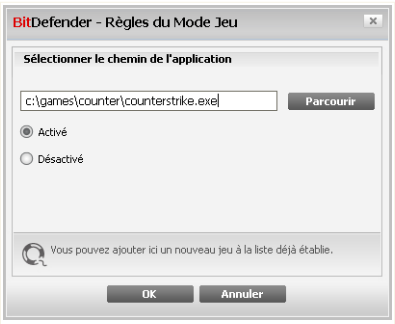
Si vous voulez désactiver le Mode Jeu automatique pour une application spécifique de la liste, décochez la case correspondante. Vous avez tout intérêt à désactiver le Mode Jeu automatique pour les applications standard qui utilisent le mode plein écran, telles que les navigateurs Web et les lecteurs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

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

- Cliquez sur **Ajouter** pour ajouter une nouvelle application à la liste de jeux.
- Cliquez sur **Supprimer** - pour supprimer une application de la liste des jeux.
- Cliquez sur **Gérer les jeux** pour visualiser une entrée existante dans la liste de jeux.

Ajout ou édition de jeux

Lorsque vous ajoutez ou éditez une entrée de la liste de jeux, la fenêtre suivante apparaît :



Ajouter un jeu

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

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

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

20.1.3. Configuration des paramètres du Mode Jeu

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

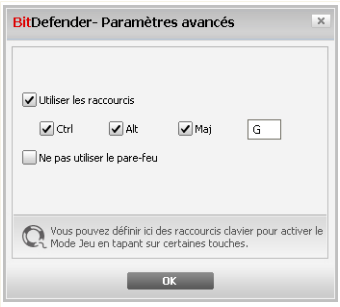
- **Tâche d'analyse** - permet d'éviter l'exécution de tâches d'analyse planifiées lorsque le Mode Jeu est activé. Vous pouvez choisir une des options suivantes :

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

20.1.4. Changer le raccoruci clavier du Mode Jeu

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

1. Cliquez sur **Paramètres avancés**. Une nouvelle fenêtre s'affiche.



Paramètres avancés

2. Sous l'option **Utiliser le raccourci**, définissez le raccourci clavier désiré :

- Choisissez la touche que vous souhaitez utiliser en cochant l'une des suivantes : touche Contrôle (`Ctrl`), Touche Shift(`Shift`) ou touche Alt (`Alt`).
- Dans le champ éditable, entrez la lettre que vous souhaitez utiliser.

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

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

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

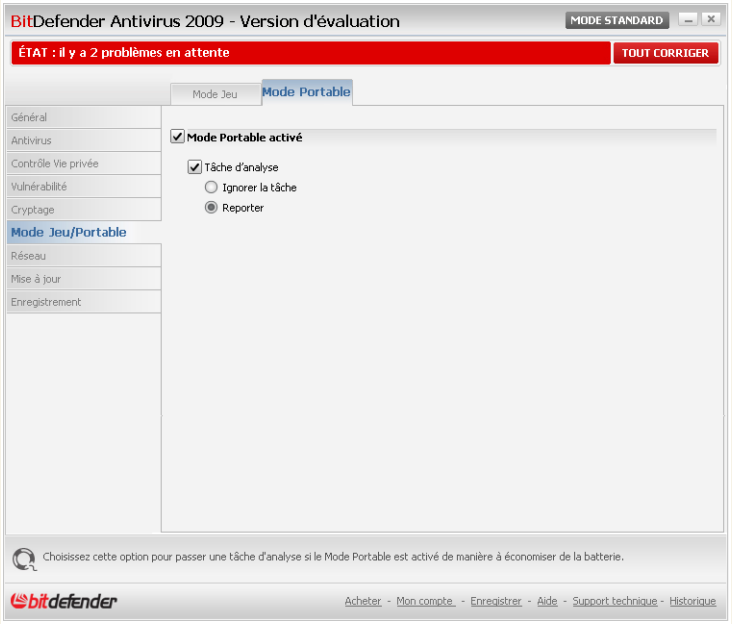
20.2. Mode Portable

Le Mode Portable est spécialement conçu pour les utilisateurs d'ordinateurs portables et de notebooks. Son objectif est de minimiser l'impact de BitDefender sur la consommation énergétique lorsque ces périphériques sont alimentés par leur batterie.

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

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

Pour configurer le Mode Portable, rendez-vous dans **Réglages du produit>Mode Portable** dans le Mode avancé.



Mode Portable

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

20.2.1. Configuration des paramètres du Mode Portable

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

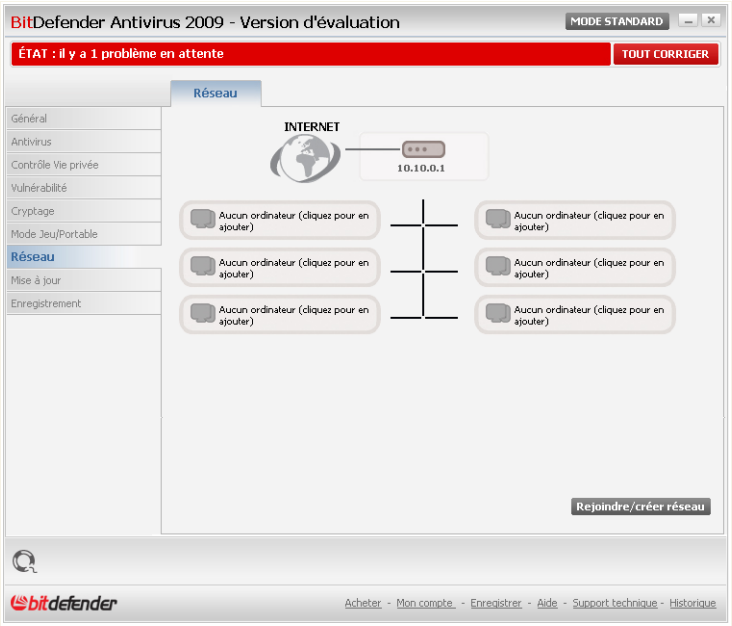
- **Tâche d'analyse** - permet d'éviter l'exécution de tâches d'analyse planifiées lorsque le Mode Portable est activé. Vous pouvez choisir une des options suivantes :

Option	Description
Ignorer la tâche	Annule complètement l'exécution de la tâche planifiée.

Option	Description
Reporter la tâche	Exécute la tâche planifiée juste après la désactivation du Mode Portable.

21. Réseau

Le module Réseau vous permet de gérer les produits BitDefender installés sur tous les ordinateurs de votre foyer à partir d'un seul et même ordinateur.



Carte réseau

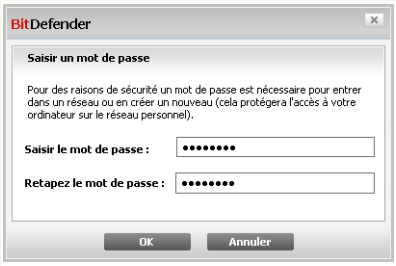
Vous devez suivre ces étapes pour pouvoir gérer les produits BitDefender installés sur tous les ordinateurs de votre foyer :

1. Rejoindre le réseau domestique BitDefender via votre ordinateur. Rejoindre le réseau consiste à configurer un mot de passe d'administration pour la gestion de réseau domestique.
2. Allumez chaque ordinateur que vous voulez gérer et rejoignez le réseau à partir de ceux-ci (en saisissant le mot de passe).
3. Revenez sur votre ordinateur et ajoutez les ordinateurs que vous voulez gérer.

21.1. Rejoindre le réseau BitDefender

Procédez comme suit pour rejoindre le réseau domestique BitDefender :

1. Cliquez sur **Rejoindre/créer un réseau**. Vous serez invité à définir le mot de passe de gestion de réseau domestique.



Définir le mot de passe

2. Entrez le même mot de passe dans chacun des champs de saisie.
3. Cliquez sur **OK**.

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

21.2. Ajout d'ordinateurs au réseau BitDefender

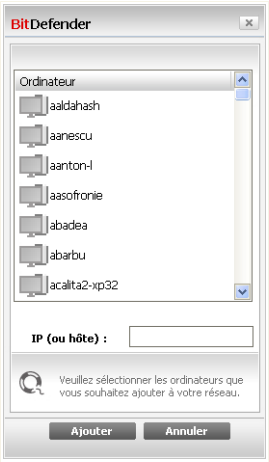
Avant de pouvoir ajouter un ordinateur au réseau domestique BitDefender, vous devez définir le mot de passe de gestion de réseau domestique BitDefender sur l'ordinateur à ajouter.

Procédez comme suit pour ajouter un ordinateur au réseau domestique BitDefender :

1. Cliquez sur **Gérer le réseau**. Vous serez invité à saisir le mot de passe local de gestion de réseau domestique.

Saisir le mot de passe

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



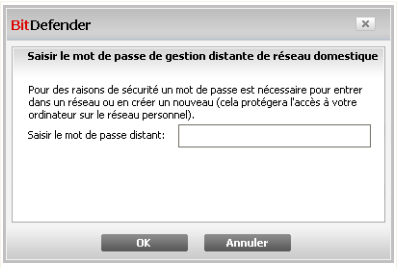
Ajouter un ordinateur

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

- Indique un ordinateur en ligne sans aucun produit BitDefender installé.
- Indique un ordinateur en ligne avec BitDefender installé.

- Indique un ordinateur hors connexion avec BitDefender installé.

3. Choisissez une des possibilités suivantes :
   - Sélectionnez dans la liste le nom de l'ordinateur à ajouter.
   - Tapez l'adresse IP ou le nom de l'ordinateur à ajouter dans le champ correspondant.
4. Cliquez sur **Ajouter**. Vous serez invité à saisir le mot de passe de gestion de réseau domestique de l'ordinateur concerné.



Authentification

5. Tapez le mot de passe de gestion de réseau domestique défini sur l'ordinateur concerné.
6. Cliquez sur **OK**. Si vous avez spécifié le bon mot de passe, le nom de l'ordinateur sélectionné apparaît sur la carte réseau.

Note
Vous pouvez ajouter jusqu'à cinq ordinateurs sur la carte réseau.

21.3. Gestion du réseau BitDefender

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

Carte réseau

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

Si vous faites un clic-droit sur un ordinateur présent sur la carte du réseau, vous pourrez voir les tâches administratives que vous pouvez lancer sur cet ordinateur distant.

- **Enregistrer cet ordinateur**
- **Définir le mot de passe des paramètres**
- **Lancer une tâche d'analyse**
- **Réparer les problèmes sur cet ordinateur**
- **Afficher l'historique de cet ordinateur**
- **Lancer une mise à jour sur cet ordinateur**

- **Appliquer le profil**
- **Lancer une tâche d'optimisation sur cet ordinateur**
- **Définir cet ordinateur comme serveur de mise à jour sur ce réseau**

Avant de lancer une tâche sur un ordinateur spécifique, vous serez invité à saisir le mot de passe local de gestion de réseau domestique.

Saisir le mot de passe

Tapez le mot de passe de gestion de réseau domestique et cliquez sur **OK**.

Note

Si vous prévoyez de lancer plusieurs tâches, il peut s'avérer utile de sélectionner l'option **Ne plus afficher ce message durant cette session**. En sélectionnant cette option, vous n'aurez plus à saisir le mot de passe pour la session en cours.

22. 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 a été trouvée, elle sera installée automatiquement ou il vous sera demandé de confirmer son installation, selon les paramètres de mise à jour automatique.

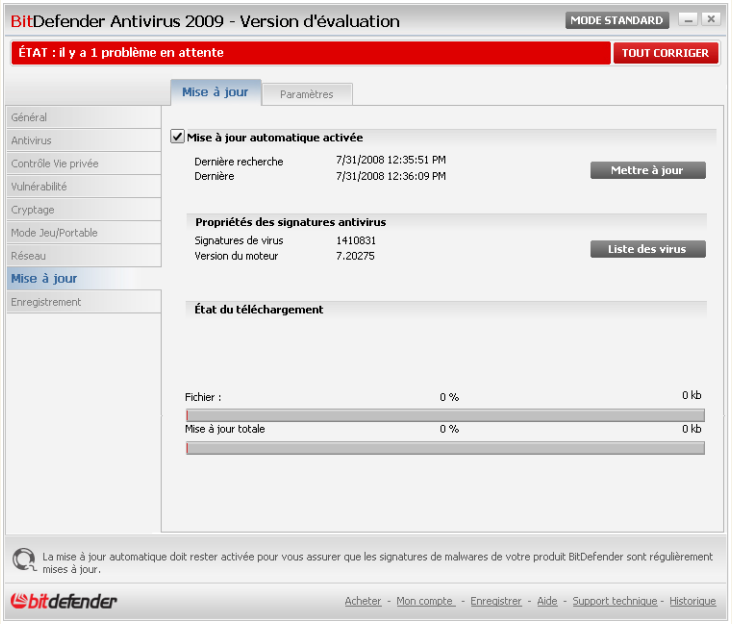
Le processus de mise à jour est exécuté à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, le processus de mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.

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 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**.

22.1. Mise à jour automatique

Pour consulter des informations relatives aux mises à jour et définir des mises à jour automatiques, rendez-vous dans **Mise à jour>Mise à jour** dans le Mode avancé.



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.

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.

Vous pouvez accéder aux signatures de codes malveillants de votre application BitDefender en cliquant sur **Afficher la liste des virus**. Un fichier HTML contenant toutes les signatures disponibles est créé et s'ouvre dans un navigateur Internet. 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.

22.1.1. Demandes de mise à jour

La mise à jour automatique peut aussi etre effectuée n'importe quand en cliquant sur **Mettre à jour**. Cette mise à jour est connue aussi sous l'appellation **Mettre à jour a la demande de l'utilisateur**.

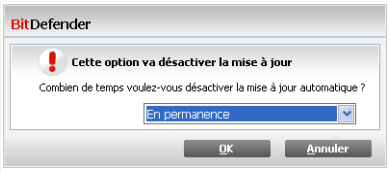
Le module **Mise à jour**se connecte au serveur de mise à jour BitDefender et recherche les mises à jour disponibles. Si une mise à jour est détectée, vous serez invité à la confirmer ou elle sera effectuée automatiquement en fonction des options que vous aurez définies dans la section Paramètres de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

22.1.2. 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

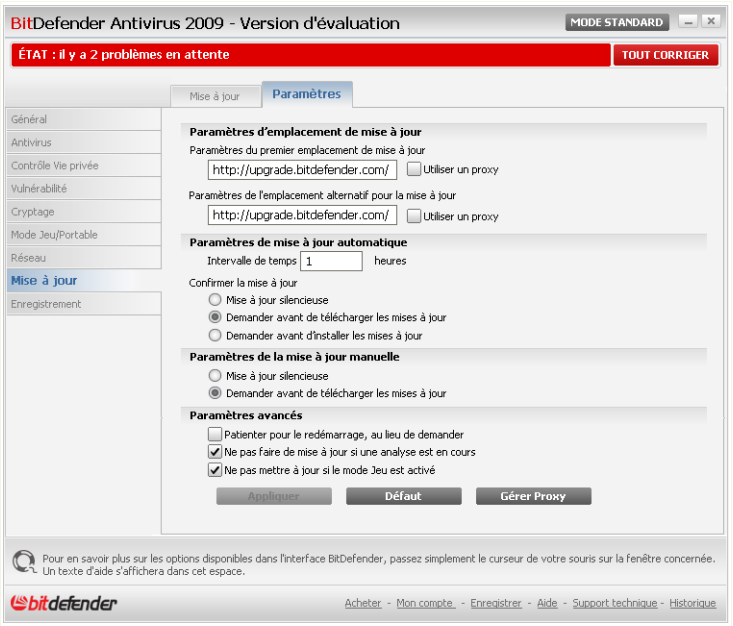
Vous devez confirmer votre choix en sélectionnant dans le menu la durée pendant laquelle vous souhaitez désactiver la mise à jour automatique. Vous pouvez désactiver la mise à jour automatique pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.

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.

22.2. 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 proxys, rendez-vous dans **Mise à jour>Paramètres** dans le Mode avancé.



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.

22.2.1. Paramétrage des emplacements de mise à jour

Pour configurer les emplacements de mise à jour, utilisez les options de la catégorie **Paramètres d'emplacement de mise à jour**.

Note
Ne configurez ces paramètres que si vous êtes connecté à un réseau local qui stocke les signatures de codes malveillants BitDefender localement ou si vous êtes connecté à Internet via un serveur proxy.

Pour effectuer des mises à jour plus fiables et plus rapides, vous pouvez configurer deux emplacements de mise à jour: un **premier emplacement de mise à jour** et un **emplacement alternatif de mise à jour** . Par défaut, ces emplacements sont identiques: `http://upgrade.bitdefender.com`.

Pour modifier l'un des emplacements de mise à jour, indiquez l'URL du site miroir local dans le champ **URL** correspondant à l'emplacement que vous souhaitez modifier.

Note
Nous vous recommandons de configurer le miroir local en tant 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. Pour plus d'informations, reportez-vous à « *Gestion des serveurs proxy* » (p. 204)

22.2.2. 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.
- **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.

22.2.3. 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.

22.2.4. 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.

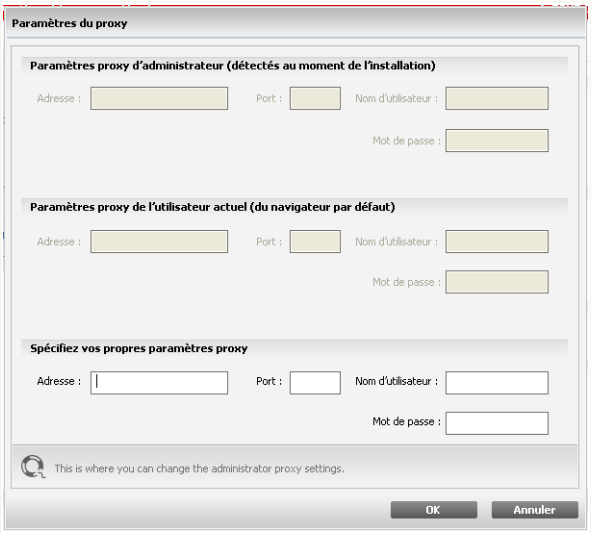
- **Ne pas mettre à jour si le mode jeu est actif** - BitDefender n'effectuera pas de mise à jour si le mode jeu est activé. Ainsi, vous limitez l'influence du produit sur les performances du système lorsque vous jouez.

22.2.5. 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.

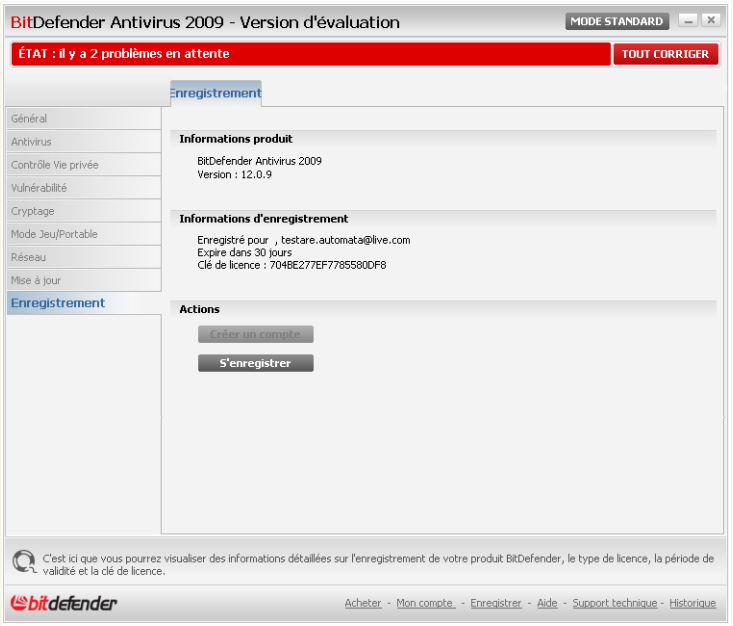
Tout d'abord, la catégorie contenant vos propres paramètres de proxy est utilisée pour la connexion Internet. Si elle ne fonctionne pas, ce sont alors les paramètres de proxy détectés lors de l'installation qui sont utilisés. Finalement, s'ils ne fonctionnent pas non plus, les paramètres du proxy de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

23. Enregistrement

Pour avoir accès à des informations complètes sur votre produit et votre enregistrement, allez à **Enregistrement** dans l'interface avancée.



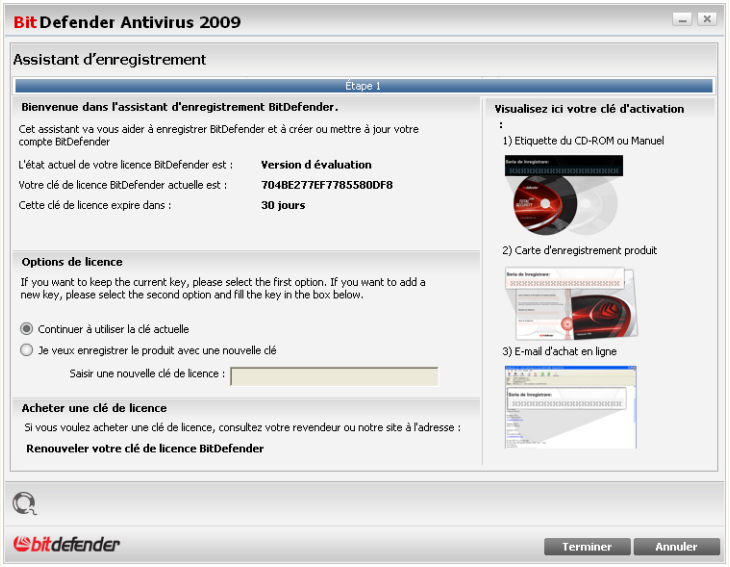
Enregistrement

Cette section affiche:

- **Informations produit** : le produit et la version BitDefender.
- **Informations d'enregistrement** : l'adresse e-mail utilisée pour vous connecter à votre compte BitDefender (si ce dernier est configuré), la clé d'activation actuelle et dans combien de jours la licence arrivera à son terme.

23.1. Enregistrement de BitDefender Antivirus 2009

Cliquez sur **Enregistrer maintenant** pour ouvrir la fenêtre d'enregistrement du produit.



Enregistrement

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

Pour enregistrer BitDefender Antivirus 2009 :

1. Sélectionnez **Je veux enregistrer le produit avec une nouvelle clé**.
2. Entrez la clé d'activation dans le champ de saisie.

Note

Vous trouverez votre clé d'activation :

- sur l'étiquette du CD.
- sur la carte d'enregistrement du produit.
- sur l'e-mail d'achat en ligne.

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

Cliquez sur **Terminer**.

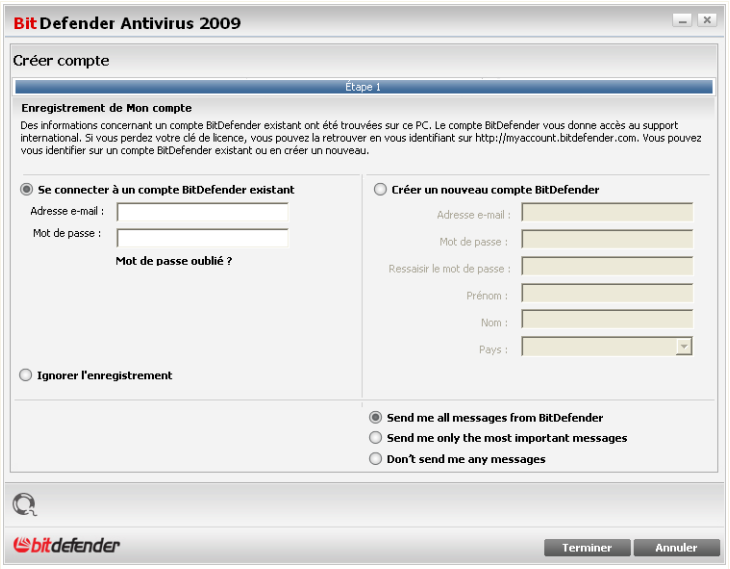
23.2. Création d'un compte BitDefender

La création d'un compte BitDefender est OBLIGATOIRE pour finaliser l'enregistrement de votre produit BitDefender. Le compte BitDefender vous donne accès au support technique, à des offres spéciales et à des promotions. Si vous perdrez votre clé d'activation BitDefender, vous pouvez la retrouver en vous connectant sur votre compte à l'adresse http://myaccount.bitdefender.com.

Important

Vous devez créer un compte dans les 15 jours après l'installation de BitDefender (si vous vous enregistrez, l'expiration est repoussée à 30 jours). Dans le cas contraire, BitDefender ne se mettra plus à jour.

Si vous n'avez pas encore créé de compte BitDefender, cliquez sur **Créer un compte** pour ouvrir la fenêtre d'enregistrement du compte.



Création de compte

Si vous ne souhaitez pas créer un compte BitDefender, sélectionnez **Passer l'enregistrement** et cliquez sur **Terminer**. Autrement, procédez selon votre situation actuelle :

- « Je n'ai pas de compte BitDefender » (p. 209)
- « J'ai déjà un compte BitDefender » (p. 210)

Je n'ai pas de compte BitDefender

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. Le mot de passe doit comporter au moins six 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.

Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte. Sélectionnez l'une des actions disponibles :

- **Envoyez moi tous les messages provenant de BitDefender**
- **Envoyez moi uniquement les messages les plus importants**
- **Je ne veux recevoir aucun message**

Cliquez sur **Terminer**.

J'ai déjà un compte BitDefender

BitDefender détectera automatiquement si vous avez déjà un compte BitDefender actif sur cet ordinateur. Dans ce cas, veuillez fournir le mot de passe de votre compte.

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.

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

Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte. Sélectionnez l'une des actions disponibles :

- **Envoyez moi tous les messages provenant de BitDefender**
- **Envoyez moi uniquement les messages les plus importants**
- **Je ne veux recevoir aucun message**

Cliquez sur **Terminer**.

Demander de l'aide

24. 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 logiciel:

1. **Mise à disposition d'une foire aux questions:**

   Accessible dans la rubrique Assistance > Particuliers/Bureau à domicile > Nom de votre logiciel sur le site : http://www.bitdefender.fr.

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 dédié disponible en cliquant sur le bouton « Contacter BitDefender » de la page de questions-réponses détaillée ci-dessus.

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

   Pour la France et DOM-TOM : 08.92.561.161 (0,34 € TTC / min)

   Pour la Belgique : 070.35.83.04

   Pour la Suisse : 0900.000.118 (0,60 F TTC / min)

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

   Cette possibilité requiert de contacter le support téléphonique. Si le problème que vous rencontrez le nécessitait, le technicien vous proposera cette option de support complémentaire.

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

   Ce service permet de vous mettre en relation directe 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 module est un service international, assuré majoritairement en Anglais.

CD de secours BitDefender

25. Vue d'ensemble

BitDefender Antivirus 2009 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/

25.1. 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.

25.2. 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.

26. 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.

26.1. 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.

Note
Choisissez la langue que vous voulez utiliser pour le CD de Secours.

Page d'accueil au démarrage

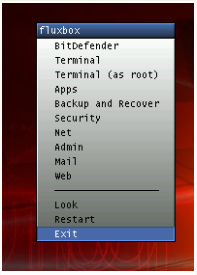
Au démarrage, la mise à jour des signatures de virus est effectuée automatiquement. Cela peut prendre un certain temps.

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

L'interface

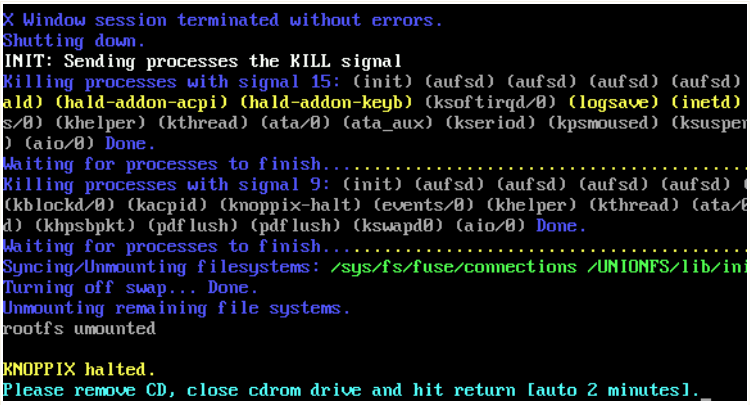
26.2. Arrêter le CD de secours BitDefender

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.

26.3. 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**.

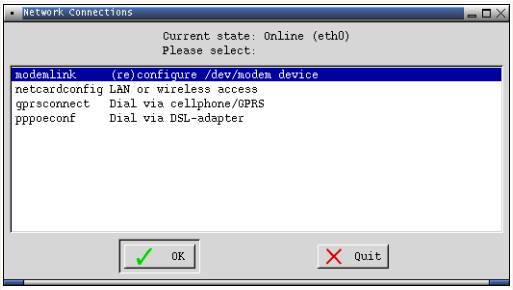
Vous pouvez également lancer les commandes suivantes depuis un terminal. Le moteur d'analyse **BitDefender Antivirus Scanner** considérera le fichier ou dossier sélectionné comme étant l'endroit à analyser par défaut.

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

26.4. Comment configurer la connexion Internet?

Si vous utilisez un réseau DHCP et une carte réseau ethernet, la connexion Internet devrait déjà être reconnue et configurée. Pour la configurer manuellement, suivez les étapes suivantes:

1. Double-cliquez sur le raccourci de connexions Réseau, disponible sur le bureau Windows, la fenêtre suivante apparaîtra.



Connexions réseau

2. Choisissez le type de connexion que vous utilisez et cliquez sur OK.

Connexion	Description
modemlink	Choisissez le type de connexion lorsque vous utilisez un modem et une ligne téléphonique pour accéder à Internet.
netcardconfig	Choisissez le type de connexion lorsque vous utilisez un Reséau local (LAN) pour accéder à Internet. Ceci s'applique également dans le cas d'une connexion Wi-Fi.
gprsconnect	Choisissez ce type de connexion quand vous accédez à Internet via un réseau de téléphonie mobile en utilisant le protocole GPRS (General Packet Radio Service). Ceci s'applique aussi à l'utilisation de modem GPRS.
pppoeconf	Choisissez ce type de connexion quand vous utilisez un Modem xDSL (Digital Subscriber Line) pour accéder à Internet.

3. Suivez les instructions à l'écran. En cas de doute sur vos réponses, contacter votre administrateur réseau pour plus d'informations.

Important
Merci de noter que les options ci-dessus ne permettent d'activer que le Modem. Pour configurer la connexion Réseau suivez les étapes suivantes.

1. Faîtes un clic-droit sur le bureau. Le menu contextuel du CD de Secours BitDefender apparaîtra.
2. Sélectionnez **Terminal (as root)**.
3. Saisissez les lignes de commande suivantes :

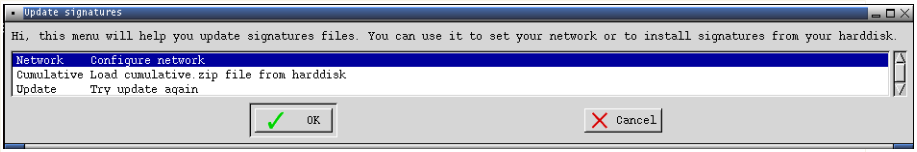
```
# pppconfig
```

4. Suivez les instructions à l'écran. En cas de doute sur vos réponses, contacter votre administrateur réseau pour plus d'informations.

26.5. Comment actualiser BitDefender?

Au démarrage, la mise à jour des signatures de virus est effectuée automatiquement. Si vous avez choisi de passer cette étape, voici comment mettre à jour BitDefender.

1. Double-cliquez sur le raccourci Mise à jour de Signatures. La fenêtre suivante apparaîtra:



Mettre à jour les Signatures

2. Choisissez une des possibilités suivantes :
   - Choisissez **Cumulative** pour parcourir votre disque dur et installer les signatures déjà sauvegardées sur votre disque dur en chargeant le fichier`cumulative.zip`.
   - Choisissez **Mettre à Jour** pour vous connecter immédiatement à Internet et téléchargez la dernière base de signatures.
3. Cliquez sur **OK**.

26.5.1. 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**.

26.6. 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.

   Note
   Si vous branchez une clé USB à un autre moment, il vous faudra monter le disque amovible en suivant ces étapes :
   a. Double-cliquez sur le raccourci Terminal Emulator sur le bureau Windows.
   b. Saisissez la commande suivante :

```
# mount  /media/sdb1
```

Merci de noter que selon la configuration de votre ordinateur cela peut être `sda1` au lieu de `sdb1`.

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.

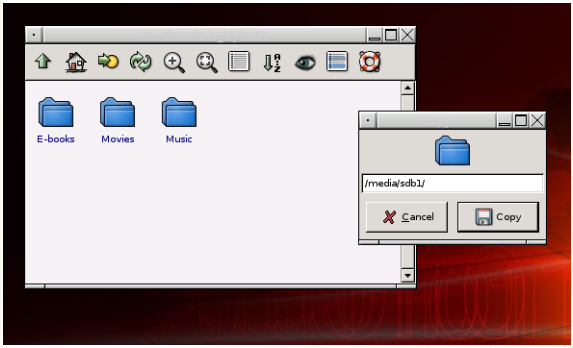
Important

Si l'ordinateur n' a pas été éteint correctement il est possible que certaines partitions n'aient pas été montées automatiquement. Pour monter une partition, suivez les étapes suivantes :

a. Double-cliquez sur le raccourci Terminal Emulator sur le bureau Windows.
b. Saisissez la commande suivante :

```
# mount  /media/partition_name
```

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**.

   Merci de noter que selon la configuration de votre ordinateur cela peut être `sda1` au lieu de `sdb1`.

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 malveillants par nature. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler des codes malveillants ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des codes malveillants, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, corrompre des fichiers et des logs et éviter leur détection.

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.