Defend what you create

Manuel Utilisateur

Dr.Web Agent
Version 6.0.4
Manuel Utilisateur
27/08/2013

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Consultez le site web official pour en savoir plus sur les bureaux régionaux ou internationaux.

Doctor Web

Doctor Web développe et distribue les solutions de sécurité de l'information Dr.Web® qui fournissent une protection efficace contre les logiciels malveillants et le spam.
Les clients de Doctor Web sont des utilisateurs particuliers dans le monde entier, ainsi que des institutions gouvernementales, des petites entreprises et des entreprises nationales.
Les solutions antivirus Dr.Web sont connues depuis 1992 pour leur excellence en matière de détection des malwares et leur conformité aux standards de sécurité de l'information internationaux. Les certificats d'Etat et les prix attribués aux solutions Dr.Web ainsi que l'utilisation de nos produits dans le monde entier sont les meilleurs témoins de la confiance qui leur est accordée.

Nous remercions tous nos clients pour leur soutien et leur fidélité aux produits Dr.Web !

Contenu

Chapitre 1. Introduction

1.1. Légende

Légende

Les symboles utilisés dans ce guide sont présentés dans le tableau récapitulatif 1.

Tableau 1. Légende

Symboles	Commentaires
 Notice	Une notice/indication importante.
 Attention	Un avertissement sur des erreurs éventuelles et sur les points auxquels faire attention.
Dr.Web Agent	Nom de produit/composant **Dr.Web**.
Réseau antivirus	Un terme.
<adresse IP>	Les champs destinés à remplacer les noms fonctionnels par leurs valeurs.
Appliquer	Les noms des boutons, fenêtres, éléments du menu et autres éléments de l'interface utilisateur.
CTRL	Les touches du clavier.
`C:\Windows\`	Les noms de fichiers/dossiers ou fragments de programme.
Annexe A	Les liens croisés vers des chapitres de la documentation ou les hyperliens vers les ressources externes.

Abréviations

Dans le texte du guide les abréviations suivantes sont utilisées :

- FDD – Floppy Disk Drive (disque souple – un support magnétique amovible),
- GUI – Graphical User Interface (interface graphique utilisateur), la version du programme dotée des outils de GUI,
- UAC – User Account Control (contrôle des comptes utilisateur – le composant de Microsoft Windows qui requiert la confirmation des actions demandant des privilèges d'administrateur aux fins de la protection d'ordinateur d'accès non-sanctionné),
- URL – Uniform Resource Locator (localisateur uniforme de ressources – le moyen standard d'écrire l'addresse d'une ressource sur l'Internet),
- **SGMAJ Dr.Web – Système global de mises à jour Dr.Web,**
- OS – operating system (système d'exploitation).

1.2. Antivirus Dr.Web® Enterprise Security Suite

Le logiciel **Dr.Web Enterprise Security Suite** est destiné à établir et à contrôler une protection antivirus cohérente des ordinateurs de votre entreprise.

Les postes protégés sont unis dans le réseau antivirus géré par l'administrateur depuis le **Serveur Enterprise**. La protection des postes est complètement automatique et gérée de façon centralisée afin d'assurer un niveau de sécurité maximum avec une intervention minimum du personnel.

Dr.Web Enterprise Security Suite fournit les fonctionnalités suivantes :

- installation centralisée (sans intervention du personnel) des packages antivirus sur les postes protégés,

- configuration centralisée des packages antivirus sur les postes protégés,
- mises à jour centralisées des bases virales et des modules de programmes sur les postes protégés,
- surveillance de la situation virale, du statut des packages antivirus et des systèmes d'exploitation sur tous les postes protégés.

Dr.Web Agent s'installe sur les postes protégés. Ce logiciel gère la protection du poste et assure la connexion au **Serveur Enterprise**, depuis lequel les mises à jour des programmes antivirus et des composants sont effectuées, il permet également de paramétrer le fonctionnement de l'antivirus sur les postes protégés.

Aucun autre produit antivirus, y compris un produit **Dr.Web,** ne doit être installé sur un ordinateur ayant **Dr.Web Agent**.

Vous trouverez la description des paramètres disponibles dans la rubrique Gestion de Dr.Web Agent.

Chapitre 2. Composant Dr.Web Agent

2.1. Fonctions principales et paramètres de Dr.Web Agent

La protection des ordinateurs contre les virus et le spam est assurée par des logiciels inclus dans le package antivirus **Dr.Web Enterprise Security Suite**.

La gestion de la protection et la connexion au **Serveur Enterprise** sont effectuées via **l'Agent Dr.Web Enterprise Security Suite** (ci-après - **Dr.Web Agent**).

Dr.Web Agent assure les fonctions suivantes :

- installation, mise à jour, configuration du package antivirus **Dr.Web**, lancement du processus de scan, exécution d'autres tâches configurées par le **Serveur Enterprise**,
- accès aux composants du package antivirus **Dr.Web** depuis une interface spécialisée,
- transmission des résultats d'exécution des tâches au **Serveur**,
- communication au **Serveur** des notifications sur les événements, prévues dans la configuration du package antivirus.

Dr.Web Agent permet à l'utilisateur d'effectuer les opérations listées ci-dessous :

- configuration de la planification de l'analyse antivirus,
- lancement du processus de scan,
- modification des paramètres des composants du logiciel **Dr.Web,** y compris certains paramètres de l'**Agent**,
- visualisation des statistiques sur les événements viraux survenus sur le PC ainsi que d'autres informations sur le fonctionnement du logiciel **Dr.Web**.

Pour modifier les paramètres de l'**Agent** ou ceux des composants du logiciel, des droits sont requis. Pour en savoir plus, merci de consulter la description des paramètres des composants concernés.

2.2. Pré-requis système

Aucun autre antivirus y compris d'autres versions de l'antivirus **Dr.Web** ne peut être installé sur les postes du réseau antivirus géré par **Dr.Web**.

Le fonctionnement de Dr.Web Agent et le package antivirus requièrent :

1. Pré-requis minimum :
   - un processeur Intel Pentium IV, 1.6 GHz ;
   - RAM 512 Mo.
2. Pré-requis recommandés :
   - un processeur Intel Pentium IV, 2.4 GHz ou supérieur ;
   - RAM au moins 1 Go.
3. Espace libre sur le disque dur : au moins 250 Mo pour les exécutables + de l'espace pour les fichiers de log et les fichiers temporaires.
4. Systèmes d'exploitation (voir Annexe B. Liste complète des OS supportés) :
   a) Microsoft® Windows® 98, Windows Me, Windows NT4 (SP6) ou supérieur. Selon le système d'exploitation, les composants suivants peuvent être installés :

Composant	OS
SpIDer Gate, **SelfPROtect**, **Office Control**,	Windows 2000 avec SP4 et supérieur.

Composant	OS
Dr.Web Plug-in pour Outlook	
SpIDer Guard NT4, **Dr.Web Scanner NT4**	• Windows 98, • Windows ME, • Windows NT4 (SP6a), • Windows 2000 avec SP4, sans Update Rollup1, • Windows XP sans SP ainsi qu'avec SP1, • Windows 2003 sans SP.
FireWall, **SpIDer Guard G3**, **Dr.Web Scanner**	• Windows 2000 avec SP4 et Update Rollup1, • Windows XP avec SP2 et supérieur, • Windows 2003 avec SP1 et supérieur, • Windows Vista et supérieur.
SpIDer Mail NT4	• Windows 98, • Windows NT4 avec SP6a.
SpIDer Mail	tous les OS supportés supérieurs aux OS listés ci-dessus pour la version **SpIDer Mail NT4**.

b) Microsoft® Windows Mobile® ;

c) Novell® NetWare® ;

d) OS de la famille UNIX® : OS Linux®, OS FreeBSD® ou OS Solaris™ ;

e) Android ;

f) Mac OS® X.

5. Le module ajoutable **Dr.Web pour Outlook** requiert l'installation d'un client Microsoft Outlook du package MS Office :
   - Outlook 2000 (Outlook 9),

- Outlook 2002 (Outlook 10 ou Outlook XP),
- Office Outlook 2003 (Outlook 11),
- Office Outlook 2007,
- Office Outlook 2010.

6. Le fonctionnement de la rubrique d'aide contextuelle **Dr.Web Agent pour Windows** requiert Windows® Internet Explorer® 6.0 ou supérieur.

Les fonctions de l'**Agent** sous OS Windows Mobile et Novell NetWare sont décrites dans les manuels respectifs **Dr.Web Agent pour Windows Mobile** et **Dr.Web Agent pour Novell NetWare**.

2.3. Installation et désinstallation de l'antivirus

2.3.1. Installation de l'Agent Dr.Web

Avant de procéder à l'installation, merci de consulter la rubrique Pré-requis système.

L'installation de l'**Agent Dr.Web** doit être effectuée par l'utilisateur ayant les droits d'administrateur sur le poste.

Il existe 2 moyens pour installer/désinstaller **Dr.Web Agent** et le package antivirus :

1. Mode distant - depuis le **Serveur** via le réseau. L'opération peut être effectuée par l'administrateur du réseau antivirus. Aucune intervention de l'utilisateur n'est requise (pour en savoir plus sur la *création* d'un poste antivirus et sur l'installation distante du logiciel antivirus, merci de consulter le Guide de l'administrateur **Antivirus Dr.Web Enterprise Security Suite**).

L'installation distante de **Dr.Web Agent** peut être effectuée uniquement sur les postes tournant sous les systèmes d'exploitation Windows NT4 ou supérieur.

2. Mode local - sur la machine de l'utilisateur. La procédure peut être effectuée par l'administrateur ou par l'utilisateur de la machine. Vous pouvez utiliser l'un des biais suivants :
   - Package d'installation `esinst.exe`.
   - Installateur réseau de l'**Agent** `drwinst.exe`.

   Ce mode d'installation de l'antivirus est décrit ci-dessous.

2.3.1.1. Installation de l'Agent Dr.Web avec le package d'installation

Si un antivirus est déjà installé sur le poste, l'installateur va d'abord essayer de le désinstaller. Si la tentative échoue, vous devez désinstaller manuellement l'antivirus se trouvant sur le poste.

La marche à suivre afin d'installer l'Agent et le package antivirus sur le poste de travail :

1. Téléchargez un package d'installation de l'**Agent**. Pour cela, cliquez sur le lien fourni par l'administrateur du réseau antivirus.
2. Lancez le fichier téléchargé `esinst.exe`. Une fenêtre de l'assistant d'installation de l'antivirus **Dr.Web** va s'ouvrir.
3. Avant l'installation, l'assistant vous demandera de confirmer qu'aucun logiciel antivirus n'est installé sur le poste. Veuillez vous assurer qu'aucun logiciel antivirus n'est utilisé sur votre poste (y compris d'autres versions de l'antivirus **Dr.Web**), puis cochez la case **Aucun antivirus n'est présent sur mon PC**. Puis cliquez sur **Suivant**.
4. La prochaine fenêtre vous propose de choisir un mode d'installation :

- **Rapide (recommandé)** - l'installation la plus facile. Tous les paramètres sont spécifiés automatiquement. Puis passez à l'étape **8**.
- **Sélective** - l'installation permettant de sélectionner des composants antivirus à installer sur votre PC.
- **Mode Administrateur** - l'installation la plus complète, permettant de spécifier/modifier tout paramètre d'installation et tout paramètre du logiciel antivirus installé.

5. En cas de mode **Sélective** ou en **Mode Administrateur,** il vous sera ensuite demandé de choisir les composants antivirus **Dr.Web** à installer. Cochez les cases en face des composants à installer.

   La rubrique **Chemin d'installation** permet de spécifier le chemin pour l'installation de l'antivirus sur le poste de l'utilisateur. Par défaut, c'est le répertoire `Dr.Web Enterprise Suite` se trouvant dans le dossier `Program files` sur le disque système (il peut être spécifié avec une variable système `%ProgramFiles%`). Pour spécifier/modifier le chemin donné par défaut, cliquez sur **Parcourir** et entrez ensuite le chemin nécessaire.

   Puis cliquez sur **Suivant**.

   Pour réaliser l'installation **Sélective**, passez à l'étape **8**.

6. En cas d'installation en **Mode Administrateur**, veuillez configurer l'**installateur réseau** dans la fenêtre suivante :
   - Dans le champ **Dr.Web Enterprise Server,** entrez l'adresse réseau du serveur **ES** depuis lequel **l'Agent** et le package antivirus seront installés. Si vous avez déjà spécifié l'adresse du **Serveur** lors du démarrage de l'installateur, l'adresse sera automatiquement entrée dans ce champ.

En cas d'installation de l'**Agent Dr.Web** avec l'installateur créé dans le **Centre de Gestion**, le champ **Dr.Web Enterprise Server** sera rempli automatiquement.

Si vous ne connaissez pas l'adresse du **Serveur**, cliquez sur le bouton **Rechercher**. Une fenêtre permettant de rechercher les **Enterprise Serveurs** actifs dans le réseau sera ouverte. Configurez les paramètres nécessaires (au format *<nom_du_serveur>*@*<adresseIP>*/*<suffix_réseau>*:*<port>*) et cliquez sur le bouton **Rechercher**. Dans la liste des Serveurs, sélectionnez le serveur depuis lequel vous voulez installer l'antivirus, cliquez ensuite sur le bouton **OK**.

- Dans le champ **Clé publique de Dr.Web Enterprise Server** vous pouvez spécifier le chemin complet vers la clé publique `(drwcsd.pub)` se trouvant sur votre poste (si l'installateur est lancé depuis le **Serveur** via le réseau, la clé est copiée vers les fichiers temporaires du système. Après l'installation, la clé sera déplacée vers le répertoire d'installation).
- Dans la rubrique **Utiliser la compression durant le téléchargement**, sélectionnez une variante de compression : **Oui** - utiliser la compression, **Non** - ne pas utiliser la compression, **Possible** - utiliser la compression en fonction de la configuration sur le **Serveur**.
- La case cochée **Ajouter Dr.Web Agent à la liste des exclusions du pare-feu Windows** assure l'ajout des ports et des interfaces utilisés par l'Agent dans la liste des exclusions du pare-feu (excepté le système Windows 2000). Il est recommandé de cocher la case afin d'éviter d'éventuelles erreurs, par exemple, lors de la mise à jour automatique des composants antivirus et des bases virales.
- Si nécessaire, vous pouvez cochez la case **Enregistrer l'Agent dans la liste des programmes installés**.

Cette option permet, entre autres, de supprimer l'**Agent** et le package antivirus en utilisant les outils standard Windows (voir Désinstallation de l'Agent Dr.Web).

7. En cas d'installation en **Mode Administrateur** : configurez **l'Agent** dans la fenêtre suivante:

- Dans la rubrique **Authentification**, veuillez spécifier les paramètres d'authentification de l'**Agent** sur le **Serveur**. En cas de mode **Automatique (par défaut)**, le mode d'accès au poste sera déterminé sur le **Serveur**. Lorsque le mode d'authentification **Manuelle** est choisi, il faudra spécifier les paramètres d'authentification du poste : son **Identificateur** sur le **Serveur** et un **Mot de passe** pour y accéder. Dans ce cas, le poste aura l'accès sur le **Serveur** sans approbation manuelle par l'administrateur.

Lors de l'installation de l'**Agent Dr.Web** avec l'installateur créé sur la **Centre de Gestion**, les champs **Identificateur** et **Mot de passe** seront automatiquement remplis conformément au mode d'authentification **Manuelle**.

- Les rubriques **Compression** et **Chiffrage** permettent de configurer la bande passante entre le **Serveur** et l'**Agent** (pour plus d'information, consultez le paragraphe **Utilisation du chiffrage et de la compression de la bande passante** du guide de l'administrateur de l'**Antivirus Dr.Web Enterprise Security Suite**).

Puis cliquez sur **Suivant**.

8. L'installation de l'**Agent** et des composants antivirus commence (sans aucune intervention de l'utilisateur).
9. Après la fin de l'installation, l'assistant d'installation vous proposera de redémarrer la machine. Cliquez sur le bouton **Terminer** pour quitter l'assistant d'installation.
10. Redémarrez le poste.

Lors de l'installation du package antivirus contenant le composant **Dr.Web Firewall**, pour terminer l'installation, il faut redémarrer le poste deux fois.

Dans ce cas, sous OS Windows Vista et Windows Server 2008, après le deuxième redémarrage, le service de **Planificateur de tâches** Windows ne sera pas lancé, étant bloqué par le composant **Dr.Web Firewall**. Cette fonctionnalité sera rétablie après la création automatique d'une règle préconfigurée par le composant **Dr.Web Firewall** qui autorise le démarrage du service de

Planificateur de tâches, ainsi que le redémarrage ultérieur du **Planificateur**, par exemple, après un redémarrage du poste.

2.3.1.2. Installation de l'Agent Dr.Web avec l'Installateur réseau

Si l'installateur réseau a été lancé dans le mode d'installation standard (sans clé `-uninstall`) sur le poste sur lequel l'**Agent** a déjà été installé, aucune action ne sera évoquée.

Avant procéder à une nouvelle installation, il est nécessaire de supprimer l'**Agent** installé.

L'installaton avec l'Installateur réseau peut être effectuée dans les deux modes principaux :

1. En tâche de fond.
2. En mode graphique.

Installation de l'Agent Dr.Web avec l'installateur en tâche de fond

Afin d'installer l'Agent Dr.Web en tâche de fond, faites comme suit :

1. Sur l'ordinateur sur lequel vous allez installer l'antivirus, lancez le programme `drwinst.exe` que vous pouvez trouver sur l'un des chemins ci-dessous :
   - Dans le dossier réseau d'installation de l'**Agent**. En cas d'installation du **Serveur**, c'est le sous-dossier `Installer` (par défaut, c'est une ressource cachée partagée) du dossier d'installation du **Serveur** que vous pouvez déplacer ultérieurement.
   - A la page d'installation du **Centre de Gestion** accessible sur n'importe quel ordinateur ayant accès réseau au **Serveur Enterprise**, à l'adresse :
     `http://`*<Adresse_du_Serveur>*`:`*<numéro_du_port>*`/install/`
     comme *<Adresse_du_Serveur>*, spécifiez l'adresse IP ou le nom DNS de l'ordinateur sur lequel est installé le **Serveur Enterprise**. En tant que *<numéro_du_port>*, spécifiez le port `9080` (ou `9081` pour https).

   Par défaut, le programme `drwinst`, lancé sans aucune clé, utilise le mode **Multicast** afin de scanner le réseau pour rechercher des **Serveurs Enterprise** actifs.

Lors de l'utilisation du mode **Multicast** pour rechercher des **Serveurs** actifs, l'installation de l'**Agent** sera réalisée depuis le premier **Serveur** détecté. Dans ce cas, si la clé existante pub ne correspond pas à la clé de **Serveur**, l'installation sera terminée avec une erreur. Si c'est le cas, spécifiez l'adresse du **Serveur** de manière explicite au démarrage de l'installateur (voir ci-dessous).

La commande `drwinst` peut également être lancée avec les clés complémentaires suivantes :

- Dans le cas où le mode **Multicast** n'est pas utilisé, lors de l'installation de l'**Agent,** il est recommandé d'utiliser le nom du **Serveur** (pré-enregistré dans le service DNS) :

```
drwinst <DNS_nom_du_serveur>
```

Ceci facilite le processus de configuration du réseau antivirus relatif à la procédure de réinstallation du **Serveur Enterprise** sur un autre ordinateur.

- Vous pouvez aussi spécifier l'adresse du **Serveur** de façon explicite :

```
drwinst 192.168.1.3
```

- La clé `-regagent` permet d'enregistrer l'**Agent** dans la liste d'ajout/suppression de programmes lors de l'installation.
- Afin de lancer l'installateur en mode graphique, veuillez utiliser la clé `-interactive`.

Vous pouvez consulter la liste complète des paramètres de l'**Installateur réseau** dans l'Annexe **H4. Installateur réseau** du Manuel Administrateur de **Dr.Web Antivirus Enterprise Security Suite**.

2. Lorsque l'installation est finie, le logiciel de l'**Agent Dr.Web** est installé sur le poste (ce n'est pas encore le package antivirus).
3. Dès que le poste est approuvé sur le **Serveur** (dans le cas où l'approbation est requise par la configuration du **Serveur**), le package antivirus sera automatiquement installé.
4. Après la requête de l'**Agent**, veuillez redémarrer le poste.

Lors de l'installation du package antivirus contenant le composant **Dr.Web Firewall**, pour terminer l'installation, il faut redémarrer le poste deux fois.

Dans ce cas, sous OS Windows Vista et Windows Server 2008, après le deuxième redémarrage, le service de **Planificateur de tâches** Windows ne sera pas lancé, étant bloqué par le composant **Dr.Web Firewall**. Cette fonctionnalité sera rétablie après la création automatique d'une règle préconfigurée par le composant **Dr.Web**

Firewall qui autorise le démarrage du service de **Planificateur de tâches**, ainsi que le redémarrage ultérieur du **Planificateur**, par exemple, après un redémarrage du poste.

Installation de l'Agent Dr.Web avec l'installateur en mode graphique

Afin d'installer l'Agent Dr.Web en mode graphique, faites comme suit :

1. Sur l'ordinateur sur lequel vous allez installer l'antivirus, lancez le programme `drwinst.exe` avec la clé `-interactive`. Vous pouvez trouver le programme `drwinst.exe` sur l'un des chemins suivants:
   - Dans le dossier réseau d'installation de l'**Agent**. En cas d'installation du **Serveur**, c'est le sous-dossier `Installer` (par défaut, c'est une ressource cachée partagée) du dossier d'installation du **Serveur** que vous pouvez déplacer ultérieurement.
   - A la page d'installation du **Centre de Gestion** accessible sur n'importe quel ordinateur ayant accès réseau au **Serveur Enterprise**, à l'adresse :
     `http://`*<Adresse_du_Serveur>*`:`*<numéro_du_port>*`/install/`
     comme *<Adresse_du_Serveur>*, spécifiez l'adresse IP ou le nom DNS de l'ordinateur sur lequel est installé le **Serveur Enterprise**. En tant que *<numéro_du_port>*, spécifiez le port `9080` (ou `9081` pour https).

   La fenêtre de l'assistant d'installation de l'antivirus **Dr.Web** va s'ouvrir.

2. Avant l'installation, l'assistant vous demandera de confirmer qu'aucun logiciel antivirus n'est installé sur le poste. Veuillez vous assurer qu'aucun logiciel antivirus n'est utilisé sur votre poste (y compris d'autres versions de l'antivirus **Dr.Web**), puis cochez la case **Aucun antivirus n'est présent sur mon PC**. Puis cliquez sur **Suivant**.
3. La prochaine fenêtre vous propose de choisir un mode

d'installation :

- **Rapide (recommandé)** - l'installation la plus facile. Tous les paramètres sont spécifiés automatiquement. Puis passez à l'étape **7**.
- **Sélective** - l'installation permettant de sélectionner les composants antivirus à installer sur votre PC.
- **Mode administrateur** - l'installation la plus complète, permettant de spécifier/modifier tout paramètre d'installation et tout paramètre du logiciel antivirus installé.

4. En cas de mode **Sélective** ou **Mode administrateur,** il vous sera ensuite demandé de choisir les composants antivirus **Dr.Web** à installer. Cochez les cases correspondantes aux composants à installer.

   La rubrique **Chemin d'installation** permet de spécifier le chemin pour l'installation de l'antivirus sur le poste de l'utilisateur. Par défaut, c'est le répertoire `Dr.Web Enterprise Suite` se trouvant dans le dossier `Program files` sur le disque système (il peut être spécifié avec une variable système `%ProgramFiles%`). Pour spécifier/modifier le chemin donné par défaut, cliquez sur **Parcourir** et entrez ensuite le chemin nécessaire.

   Puis cliquez sur **Suivant**.

   Pour réaliser l'installation **Sélective**, passez à l'étape **7**.

5. En cas d'installation en **Mode administrateur**, veuillez configurer l'**installateur réseau** dans la fenêtre suivante :

   - Dans le champ **Dr.Web Enterprise Server,** entrez l'adresse réseau du **Serveur Enterprise** depuis lequel l'**Agent** et le package antivirus seront installés. Si vous avez déjà spécifié l'adresse du **Serveur** lors du démarrage de l'installateur, l'adresse sera automatiquement entrée dans ce champ. Si vous ne connaissez pas l'adresse du **Serveur**, cliquez sur le bouton **Rechercher**. Une fenêtre permettant de rechercher les **Enterprise Serveur** actifs dans le réseau va s'ouvrir. Configurez les paramètres nécessaires (au format *<nom_du_serveur>*@*<adresseIP>*/

<suffix_réseau>:*<port>*) et cliquez sur le bouton **Rechercher**. Dans la liste des Serveurs, sélectionnez le serveur depuis lequel vous voulez installer l'antivirus, cliquez ensuite sur le bouton **OK**.

- Dans le champ **Clé publique de Dr.Web Enterprise Server** vous pouvez spécifier le chemin complet vers la clé publique (`drwcsd.pub`) se trouvant sur votre poste (si l'installateur est lancé depuis le **Serveur** via le réseau, la clé est copiée vers les fichiers temporaires du système. Après l'installation, la clé sera déplacée vers le répertoire d'installation).
- Dans la rubrique **Utiliser la compression durant le téléchargement**, sélectionnez une variante de compression : **Oui** - utiliser la compression, **Non** - ne pas utiliser la compression, **Possible** - utiliser la compression en fonction de la configuration sur le **Serveur**.
- La case cochée **Ajouter le Dr.Web Agent à la liste d'exclusion du pare-feu windows** assure l'ajout des ports et des interfaces utilisés par l'**Agent** dans la liste des exclusions du pare-feu (excepté le système Windows 2000). Il est recommandé de cocher la case afin d'éviter d'éventuelles erreurs, par exemple, lors de la mise à jour automatique des composants antivirus et des bases virales.
- Si nécessaire, vous pouvez cochez la case **Enregistrer l'Agent dans la liste des programmes installés**.

Cette option permet, entre autres, de supprimer l'**Agent** et le package antivirus en utilisant les outils standard Windows (voir Désinstallation de l'Agent Dr.Web).

6. En cas d'installation en **Mode administrateur** : configurez l'**Agent** dans la fenêtre suivante :
   - Dans la rubrique **Authentification**, veuillez spécifier les paramètres d'authentification de l'**Agent** sur le **Serveur**. En cas de mode **Automatique (par défaut)**, le mode d'accès au poste sera déterminé sur le **Serveur**. Lorsque le mode d'authentification **Manuelle** est choisi, il faudra spécifier les paramètres d'authentification du poste : son **Identificateur** sur le **Serveur** et un **Mot de passe** pour y accéder. Dans ce cas, le poste aura l'accès sur le

Serveur sans approbation manuelle par l'administrateur.

- Les rubriques **Compression** et **Chiffrage** permettent de configurer la bande passante entre le **Serveur** et l'**Agent** (pour plus d'information, consultez le paragraphe **Utilisation du chiffrage et de la compression de la bande passante** du guide de l'administrateur de l'**Antivirus Dr.Web Enterprise Security Suite**).

Puis cliquez sur **Suivant**.

7. L'installation de l'**Agent Dr.Web** commence. Après la fin du processus d'installation de l'**Agent**, cliquez sur **Terminer** pour quitter l'assistant d'installation.
8. Après l'approbation du poste sur le **Serveur** (dans le cas où ceci est prévu par la configuration du **Serveur** et à condition que le mode d'authentification **Manuelle** ne soit sélectionné à l'étape **6** de l'installation en **Mode administrateur**), le package antivirus sera installé automatiquement.
9. Veuillez redémarrer votre PC sur demande de l'**Agent**.

Lors de l'installation du package antivirus contenant le composant **Dr.Web Firewall**, pour terminer l'installation, il faut redémarrer le poste deux fois.

Dans ce cas, sous OS Windows Vista et Windows Server 2008, après le deuxième redémarrage, le service de **Planificateur de tâches** Windows ne sera pas lancé, étant bloqué par le composant **Dr.Web Firewall**. Cette fonctionnalité sera rétablie après la création automatique d'une règle préconfigurée par le composant **Dr.Web Firewall** qui autorise le démarrage du service de **Planificateur de tâches**, ainsi que le redémarrage ultérieur du **Planificateur**, par exemple, après un redémarrage du poste.

2.3.2. Désinstallation de l'Agent Dr.Web

Pour effectuer la suppression de **l'Agent** et du package antivirus sur un poste, cette option doit être autorisée par l'administrateur sur le **Serveur**.

Après la désinstallation de l'antivirus, votre ordinateur ne sera plus protégé contre les virus et d'autres programmes malveillants.

Il existe deux marches à suivre pour supprimer l'antivirus depuis le poste (**Dr.Web Agent** et package antivirus) :

1. Avec les outils standard d'OS Windows.
2. Avec l'installateur de l'Agent.

Désinstallation avec les outils standard de Windows

Ce mode de désinstallation n'est disponible que dans le cas où, lors de l'installation de l'Agent avec l'installateur graphique, la case **Enregistrer l'Agent dans la liste des programmes installés** a été cochée.

Si l'**Agent** est installé avec l'installateur en tâche de fond, la suppression de l'antivirus avec les outils standards de Windows ne sera possible que dans le cas où, lors de l'installation, la clé `-regagent` a été appliquée.

Pour désinstaller, sélectionnez la marche à suivre correspondant à votre système d'exploitation :

- Sous les OS Windows 98, Windows NT, Windows ME, Windows 2000 : **Démarrer** → **Paramètres** → **Panneau de configuration** → **Ajout et suppression de programmes**.
- Sous OS Windows XP, Windows 2003 (en fonction de l'apparence du menu **Démarrer**) :

- Menu "Démarrer" : **Démarrer** → **Panneau de configuration** → **Ajout et suppression de programmes.**
- Apparence classique du menu "Démarrer" : **Démarrer** → **Paramètres** → **Panneau de configuration** → **Ajout et suppression de programmes**.

◆ Sous OS Windows Vista et Windows 7 (en fonction de l'apparence du menu **Démarrer**) :

- Menu "Démarrer" : **Démarrer** → **Panneau de configuration** → **Programmes et fonctionnalités**, puis en fonction de l'affichage du Panneau de configuration :
  - Affichage classique : **Programmes et fonctionnalités**.
  - Page d'accueil : **Programmes** → **Programmes et fonctionnalités**.
- Affichage classique du menu "Démarrer" : **Démarrer** → **Paramètres** → **Panneau de configuration** → **Programmes et fonctionnalités**.

◆ Sous OS Windows 8 :

- Ouvrez le **Panneau de configuration** de toute manière convenable, par exemple, via l'élément **Panneau de configuration** se trouvant dans le menu contextuel que vous pouvez afficher par un clic droit de la souris dans le coin inférieur gauche de l'écran ou via l'élément **Charms Bar** → **Paramètres** → **Panneau de configuration**. Puis, en fonction du type de configuration - **Affichage** pour le Panneau de configuration :
  - Petites icônes/grandes icônes : **Programmes et fonctionnalités**.
  - Catégorie : **Programmes** → **Suppression de programmes**.

Dans la liste qui sera ouverte, sélectionnez la ligne **Dr.Web Agent** et cliquez ensuite sur **Supprimer** (ou sur **Remplacer/Supprimer** pour les versions antérieures de Windows). Ainsi l'antivirus sera désinstallé sur le poste.

Désinstallation avec l'installateur

Suppression avec l'installateur réseau

Pour supprimer le logiciel d'**Agent** et le package antivirus depuis le poste avec l'installateur réseau de l'**Agent**, il est nécessaire d'exécuter, dans le dossier d'installation de l'**Agent** (par défaut – `C:\Program Files\DrWeb Enterprise Suite`), la commande `drwinst` accomagnée du paramètre `-uninstall` (ou avec les clés `-uninstall -interactive` afin de pouvoir suivre la progression de la désinstallation).

Suppression avec le package d'installation

Afin de supprimer le logiciel d'**Agent** et le package antivirus à l'aide du package d'installation, lancez le fichier d'installation `esinst.exe` en version du produit correspondant à celle qui est installée sur votre machine. Une fenêtre de l'assistant de désinstallation de l'antivirus **Dr.Web** va s'ouvrir. Pour commencer la désinstallation de l'antivirus, cliquez sur le bouton **Suivant**.

2.4. Lancement et arrêt de l'interface Dr.Web Agent

Dr.Web Agent démarre automatiquement après l'installation, puis il sera lancé à chaque démarrage de Windows.

Lancé sous Windows, **Dr.Web Agent** affiche l'icône  dans la zone de notifications de la barre des tâches.

L'exécution de la commande **Quitter** depuis le menu contextuel de l'**Agent** ne fait que supprimer l'icône dans la zone de notifications de la **Barre des tâches**. L'**Agent** continue à fonctionner.

Au démarrage du système d'exploitation Windows, l'icône de l'**Agent** s'affiche automatiquement dans la zone de notifications de la **Barre des tâches** lors du lancement de l'**Agent**.

Pour afficher l'icône de **l'Agent**, (Si l'icône a été supprimée avec la commande **Quitter**) sans redémarrage de l'ordinateur, il suffit de lancer l'interface de **l'Agent** comme suit :

- Sous les OS plus anciens que Windows 8 : **Démarrer** → **Programmes** → **Dr.Web Enterprise Suite** → élément **Start AgentUI**.
- Sous OS Windows 8: menu **Applications** (peut être ouvert via l'élément Toutes les applications sur la barre d'applications de l'écran d'accueil) → section **Dr.Web Enterprise Suite** → élément **Start AgentUI**.

Pour démarrer l'interface d'agent en tant qu'utilisateur avec des privilèges administratifs :

- sous OS plus ancien que Windows Vista :
  1. Cliquez sur l'élément **Start AgentUI** (Voir ci-dessus), faites un clic droit dans le menu contextuel, puis sélectionnez **Exécuter en tant que**.
  2. Dans la fenêtre qui apparaît, entrez les données d'authentification (login et mot de passe) du compte souhaité, puis cliquez sur **OK**.
  3. L'Interface de **l'Agent** sera lancée au nom de l'utilisateur spécifié.
- sous OS Windows Vista et supérieurs :
  1. Dans le menu contextuel de l'icône de **l'Agent**, cliquez sur **Administrateur**.
  2. A condition que l'UAC soit activé, confirmez la demande de lancement de l'application en tant qu'administrateur.
  3. L'Interface de **l'Agent** sera lancée au nom d'administrateur.

2.5. Gestion de Dr.Web Agent

Lancé sous Windows, **Dr.Web Agent** affiche l'icône  dans la zone de notification de la **Barre des tâches**.

Lors du passage du curseur sur l'icône de l'**Agent**, une infobulle s'affiche pour visualiser des données récapitulatives sur les événements viraux, le statut des composants antivirus et sur la dernière mise à jour (voir aussi Messages d'information).

Les fonctions de **Dr.Web Agent** disponibles pour affichage et modification peuvent être lancées depuis le menu contextuel de l'icône de **Dr.Web Agent**. Pour cela, cliquez droit sur l'icône et sélectionnez l'élément nécessaire.

Figure 2-1. Menu contextuel de l'Agent Dr.Web.

Le menu contextuel comprend les éléments suivants :

- **Quitter** - enlever l'icône de **Dr.Web Agent** depuis la zone de notifications dans la **Barre des tâches** (voir le paragraphe Lancement et arrêt de l'interface de Dr.Web Agent).

- **Support** - consulter la page du service support technique **Doctor Web**.
- **Préparation des fichiers de log** - créer une archive (au format zip) contenant un jeu de fichiers de log et des informations sur le système pour l'envoyer au service support technique.
- **Doctor Web, Ltd.** - consulter le site **Doctor Web**.
- **Aide** - rubrique d'aide sur **Dr.Web Agent**.
- **A propos** - affiche les informations sur l'application et sa version. Cette fenêtre permet également de consulter le site web de **Doctor Web** ainsi que la page du service support technique **Doctor Web**.
- **SpIDer Mail** - activer/désactiver le moniteur de courrier **SpIDer Mail**.

  SpIDer Mail analyse de façon automatique toutes les consultations des serveurs de messagerie effectuées depuis des clients de messagerie installés sur votre ordinateur.

- **SpIDer Guard** - activer/désactiver le moniteur de fichiers **SpIDer Guard**.

  SpIDer Guard analyse à la volée tous les fichiers consultés et surveille de façon permanente l'activité des processus en cours d'exécution afin de contrôler si elle s'apparente à une activité virale.

- **SpIDer Gate** - activer/désactiver le moniteur HTTP **SpIDer Gate**.

  SpIDer Gate assure la protection de votre ordinateur contre les programmes malveillants pouvant se propager via des réseaux selon le protocole HTTP.

- **SelfPROtect** - activer/désactiver le moniteur système **SelfPROtect**.

  Ce composant assure la protection des fichiers et dossiers **Dr.Web** contre toute tentative d'accès, autorisée ou non autorisée. Par exemple, contre la suppression par des virus. Lorsque le moniteur système est actif, seules les applications **Dr.Web** peuvent accéder aux ressources spécifiées.

- La liste déroulante **Prévention des actions suspectes** comprend les options suivantes :
  - **Protéger le fichier système HOSTS** - bloque toute tentative d'apporter des modifications dans le fichier HOSTS utilisé par le système d'exploitation afin de faciliter l'accès à Internet : pour transformer les noms de sites en plein texte vers les adresses IP appropriées. La modification du fichier HOSTS peut témoigner d'une activité malveillante.
  - **Protéger les objets système critiques** - bloque la modification des objets critiques du système d'exploitation (la base de registre etc.).
- **Accès réseau** - la case cochée active l'accès au réseau local et à Internet, sinon l'accès est bloqué.
- **Plug-in de Outlook** - activer/désactiver le module ajoutable **Dr.Web pour Outlook**.

  Dr.Web pour Outlook vérifie le courrier entrant/sortant via le client de messagerie Microsoft Outlook.

- **Firewall** - activer/désactiver le pare-feu **Dr.Web Firewall**.

  Le pare-feu **Dr.Web Firewall** assure la protection de votre ordinateur contre l'accès non autorisé de l'extérieur ainsi que contre la fuite de données confidentielles via le réseau.

Pour en savoir plus sur les éléments du menu, merci de consulter les paragraphes suivants de ce Guide. Pour consulter un paragraphe, cliquez sur l'élément correspondant du menu conextuel dans la figure 2-1.

Le jeu des paramètres disponibles dans le menu contextuel de l'icône de **Dr.Web Agent** peut varier en fonction de la configuration du poste. L'administrateur du réseau antivirus a le droit de limiter les droits de l'utilisateur en matière de gestion et de configuration des outils antivirus installés sur son poste.

Dans le cas où certains éléments du menu sont désactivés, 2 variantes sont possibles :

1. Les droits permettant de modifier les configurations sont désactivés sur le **Serveur** par l'administrateur du réseau antivirus.
2. L'utilisateur n'a pas de droits d'administrateur sur ce poste.

Le menu contextuel de **l'Agent** lancé sans droits d'administrateur sous le système Windows Vista ou supérieur, contient un élément complémentaire **Administrateur** (Voir fig. 2-2). Cet élément du menu permet de lancer le **Dr.Web Agent** au nom de l'administrateur du poste ayant un accès complet à toutes les fonctions de **l'Agent** : tous les éléments du menu autorisés sur le **Serveur Enterprise** seront actifs.

Le menu contextuel de **l'Agent** lancé sous droits d'administrateur, sous le système d'exploitation Windows Vista ou supérieur, à condition que UAC soit activé, comprend l'élément **Utilisateur**. Cet élément permet de lancer **l'Agent** sans avoir les droits d'administrateur (sous utilisateur).

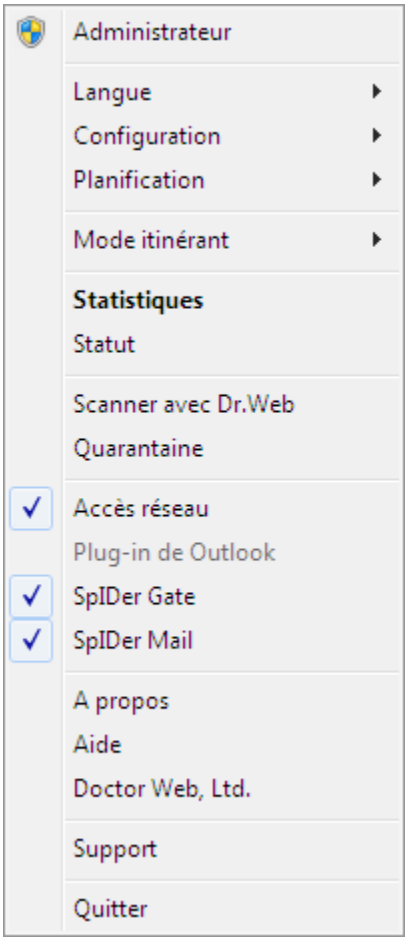


Figure 2-2. Menu contextuel de l'Agent Dr.Web sous utilisateur Windows 7.

Pour afficher la rubrique d'aide sur une fenêtre active, dans toutes les boîtes de dialogue de **Dr.Web Agent,** pressez la touche F1. Pour la rubrique d'aide contextuelle sur un élément de la fenêtre, cliquez droit sur cet élément.

L'apparence de l'icône de **Dr.Web Agent** varie en fonction du statut de la connexion du poste au **Serveur** ainsi que des statuts d'autres paramètres. Les variantes possibles du statut des composants et l'apparence respective de l'icône sont présentées sur le tableau 2.

Tableau 2. L'apparence de l'icône et le statut respectif des composants

Apparence	Description	Action
	Araignée noire sur un fond vert.	**l'Agent** est opérationnel et connecté au **Serveur**.
	Les flèches rouge sur un fond vert.	Pas de connexion au **Serveur**.
	Point d'exclamation dans un triangle jaune sur un fond vert.	**l'Agent** requiert le redémarrage de l'ordinateur ou les composants **SelfPROtection** ou **Spider Guard** sont inactifs.
	La couleur de fond passe du vert au rouge.	Une erreur est survenue lors de la mise à jour des composants.
	La couleur de fond reste en permanence rouge.	**l'Agent** est arrêté ou n'est pas opérationnel.
	La couleur de fond reste jaune.	**l'Agent** fonctionne en mode itinérant.

Chapitre 3. Fonctionnalités de Dr.Web Agent

3.1. Configuration de la langue d'interface

Le changement de la langue de l'interface de tous les composants antivirus se fait uniquement via **Dr.Web Agent**.

Pour changer la langue de l'interface de **Dr.Web Agent** et des composants antivirus **Dr.Web,** veuillez sélectionner l'élément **Langue** dans le menu contextuel de l'icône de **l'Agent**. Choisissez une langue dans la liste déroulante qui s'affiche.

3.2. Mise à jour de l'antivirus

Dès que les mises à jour de l'antivirus **Dr.Web** sont prêtes, elles sont immédiatement téléchargées et installées de façon automatique. Cependant, dans des situations critiques, vous pouvez mettre à jour les composants antivirus manuellement (une consultation auprès de votre administrateur est conseillée).

La mise à jour de l'antivirus installé sur votre poste démarre à l'aide de l'élément **Synchroniser maintenant** depuis le menu contextuel.

- Si la couleur du fond de l'icône de **l'Agent** passe du vert au rouge, vous devez forcer la mise à jour des composants en échec. Pour cela, cliquez sur l'élément **Seuls les composants en échec** dans l'élément **Synchroniser maintenant** du menu contextuel.

- Dans le cas où vous voulez mettre à jour tous les composants installés de l'antivirus (par exemple lorsque **l'Agent** n'est pas connecté au **Serveur** pendant longtemps), sélectionnez **Tous les composants** depuis l'élément **Synchroniser maintenant** du menu contextuel.

En cas de synchronisation forcée de tous les composants, deux redémarrages du poste sont requis. Veuillez suivre les instructions de l'**Agent**.

3.3. Configuration de Dr.Web Agent

L'élément **Configuration** du menu contextuel de **l'Agent** assure l'accès aux paramètres de **Dr.Web Agent**.

Dans le menu déroulant de l'élément **Configuration,** vous pouvez paramétrer le type de notifications virales à recevoir sur votre poste. Pour cela, cochez la case correspondante à l'élément sélectionné (clic gauche) :

- **Notifications importantes** - recevoir uniquement les notifications importantes qui comprennent les notifications suivantes :
  - sur les erreurs lors du démarrage des composants antivirus ;
  - sur les erreurs lors des mises à jour de l'antivirus et des composants antivirus, ce type de notification s'affiche dès la fin de la procédure de mise à jour échouée ;
  - sur un redémarrage requis après la mise à jour, la notification s'affiche dès que la mise à jour s'achève ;
  - sur la nécessité de patienter pendant qu'une invitation à redémarrer le poste pour terminer l'installation des composants s'affiche.
- **Notifications insignifiantes** - recevoir uniquement les notifications insignifiantes :
  - sur le lancement du scan à distance ;
  - sur la fin de la procédure de scan à distance ;

- sur le lancement d'une mise à jour de l'antivirus ou des composants antivirus ;
- sur la mise à jour réussie de l'antivirus ou des ses composants (sans nécessité de redémarrer la machine).

◆ **Notifications virales** - recevoir uniquement les notifications virales. Ce type de notifications comprend les notifications sur un(des) virus détecté(s) par un des composants antivirus.

Afin de recevoir toutes les notifications, cochez les trois éléments. Sinon, seuls les types de notifications sélectionnés seront affichés (voir également le paragraphe Messages d'information).

Afin d'activer le mode synchronisation de l'horloge système avec le **Serveur**, cochez la case **Synchroniser l'heure**. Si la fonction est activée, **l'Agent** contrôle périodiquement l'horloge système de votre PC en la synchronisant avec l'horloge du **Serveur**.

Pour afficher ou modifier les paramètres de connexion au **Serveur**, sélectionnez l'élément **Connexion** (voir la rubrique Configuration de la connexion au Serveur).

Pour afficher ou modifier les paramètres de journalisation des événements viraux sur vote PC, sélectionnez l'élément **Niveau de détail du journal** (voir la rubrique Niveau de détail du journal).

L'item **Synchroniser l'heure** n'est disponible dans le menu **Configuration** qu'à condition que l'utilisateur dispose :

1. Les droits permettant de modifier la configuration. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur le PC.

3.3.1. Configuration de la connexion au Serveur

L'affichage et la modification des paramètres de connexion au **Serveur Enterprise** sont disponibles depuis l'élément **Configuration** → **Connexion** du menu contextuel.

L'élément **Connexion** est disponible depuis le menu **Configuration** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier la configuration. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur le PC.

La boîte de dialogue de la configuration de la connexion au **Serveur Enterprise** (voir fig. 3-1) permet de modifier les paramètres de connexion au **Serveur** actif ou de configurer une connexion à un nouveau **Serveur Enterprise**.

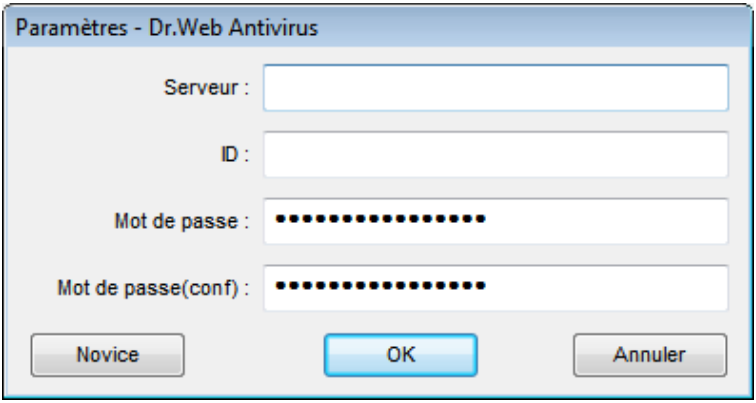


Fig. 3-1. Configuration de la connexion au Serveur

Dans toutes les boîtes de dialogue de **Dr.Web Agent**, pour afficher la rubrique d'aide sur une fenêtre active, pressez F1. Pour la rubrique d'aide sur un élément de la fenêtre, cliquez droit sur cet élément dans l'illustration.

La modification de la connexion au **Serveur Enterprise** doit être approuvée par l'administrateur du réseau antivirus. Si cette règle n'est pas respectée, votre poste sera déconnecté du réseau.

Vous pouvez modifier les paramètres suivants :

- **Serveur** - entrez ici le nom du **Serveur Enterprise** ou son adresse IP.
- **ID** - spécifiez ici l'identificateur de **l'Agent Dr.Web** attribué à votre poste pour l'enregistrement sur le **Serveur**.
- **Mot de passe** - entrez le mot de passe de **l'Agent Dr.Web** pour vous connecter au **Serveur Enterprise**. Veuillez confirmer votre mot de passe dans le champ **Mot de passe (conf)**.

Pour quitter la boîte de dialogue et sauvegarder les modifications, cliquez qur **OK**.

Pour quitter la boîte de dialogue sans sauvegarder les modifications, cliquez sur **Annuler**.

Pour réinitialiser tous les paramètres de connexion au **Serveur**, cliquez sur **Novice**. Dans ce cas, l'**Agent** sera déconnecté du **Serveur Enterprise** et le package antivirus ne pourra plus assurer la protection maximum de votre PC. Afin de configurer la connexion au **Serveur** ultérieurement, vous devez entrer dans cette boîte de dialogue de nouvelles données sur l'enregistrement sur le **Serveur**. Après la confirmation de l'enregistrement par l'administrateur du réseau antivirus, votre PC sera de nouveau connecté au **Serveur Enterprise**.

3.3.2. Niveau de détail du journal

Le niveau de détail du journal sur votre PC peut être changé depuis le menu contextuel **Configuration** → **Niveau de détail du journal**.

L'élément **Niveau de détail du journal** est disponible depuis le menu **Configuration** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier ces paramètres. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur le PC.

Dans la liste déroulante, sélectionnez un élément nécessaire (**Débogage 3** - maximum de détails, **Erreurs critiques** - le journal avec un minimum de détails, seuls les messages d'erreur sont sauvegardés) :

- **Débogage 3** ... **Débogage** - les messages de débogage avec un niveau de détail spécifié,
- **Trace 3** ... **Trace** - le traçage des actions avec un niveau de détail spécifié,
- **Information** - les messages d'information,
- **Notice** - les messages d'information importants,
- **Alerte** - les alertes sur des erreurs éventuelles,
- **Erreur** - les messages sur des erreurs de fonctionnement,
- **Erreur critique** - les messages sur des erreurs critiques de fonctionnement.

3.4. Mode d'interaction entre l'Agent et le Serveur

La modification des paramètres d'interaction entre **Dr.Web Agent** et le **Serveur** s'effectue à l'aide de l'élément **Mode de lancement** du menu contextuel de **l'Agent**.

L'élément **Mode de lancement** est disponible depuis le menu de **l'Agent** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier ces paramètres. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur le PC.

Dans la liste déroulante de l'élément **Mode de lancement**, les éléments suivants sont disponibles :

- **Connexion au Dr.Web Enterprise Server** - pour envoyer à l'administrateur des statistiques et pour recevoir depuis le **Serveur** des instructions et des mises à jour **Dr.Web**.
- **Accepter les tâches** - pour recevoir périodiquement des tâches de scan antivirus de votre PC de la part de l'administrateur.
- **Accepter les mises à jour** - pour recevoir périodiquement des mises à jour des composants antivirus et des bases virales.
- **Mémoriser les événements** - pour activer ou désactiver l'envoi des statistiques sur les événements viraux survenus sur vote ordinateur.

  Lorsque l'option est activée, l'**Agent** continue à interagir avec le **Serveur** mais les informations listées ci-après ne seront pas envoyées au **Serveur** :

  - statistiques périodiques,
  - informations sur le virus,
  - modification de la configuration de l'**Agent** et de la configuration des composants antivirus,

- informations sur le démarrage et l'arrêt des composants antivirus.

Ces informations ne sont pas critiques et n'ont pas d'impact sur le fonctionnement de l'**Agent**.

Il est à noter que les informations ci-dessus sont sauvegardées et seront envoyées lors de la connexion prochaine au **Serveur** dès que l'option **Mémoriser les événements** est désactivée.

L'option peut être utile en cas de capacité faible du canal.

3.5. Configuration de la planification

En fonction des paramètres spécifiés sur le **Serveur**, vous pouvez éditer et afficher la planification du **Scanner** antivirus :

- spécifier ou modifier la planification locale de l'analyse,
- consulter la planification centralisée de l'analyse.

Pour cela, vous devez sélectionner un élément depuis le menu déroulant de l'élément **Planification** du menu contextuel de **l'Agent**.

3.5.1. Planification locale. Liste des tâches locales

En fonction des paramètres spécifiés sur le **Serveur**, vous pouvez créer votre planification et y ajouter différents paramètres d'analyse sur votre PC.

L'élément **Locale** est disponible depuis l'élément **Planification** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier ces paramètres. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur le PC.

Lorsque vous cliquez sur **Locale** depuis l'élément **Planification** du menu contextuel, une fenêtre affichant votre planification sera ouverte.

Pour spécifier un paramètre d'analyse sur votre PC, cliquez sur le bouton **Ajouter** et dans le menu qui s'affiche sélectionnez un type de paramètre :

- Chaque heure
- Chaque jour
- Chaque semaine
- Chaque mois
- Toutes les N minutes
- Au démarrage

Vous pouvez modifier ultérieurement les tâches spécifiées. Pour cela, sélectionnez une tâche et cliquez sur le bouton **Editer**.

Pour supprimer une tâche, sélectionnez-la dans la liste et cliquez sur le bouton **Enlever**.

Vous pouvez lancer le processus de scan immédiatement avec la commande **Scanner** dans le menu contextuel de l'icône Dr.Web Agent.

Dans toutes les boîtes de dialogue de **Dr.Web Agent**, pour afficher la rubrique d'aide sur une fenêtre active, pressez la touche F1. Pour la rubrique d'aide sur un élément de la fenêtre, cliquez droit sur cet élément dans l'illustration.

3.5.1.1. Tâches exécutées chaque heure

Les tâches de ce type sont exécutées chaque heure, à la minute spécifiée.

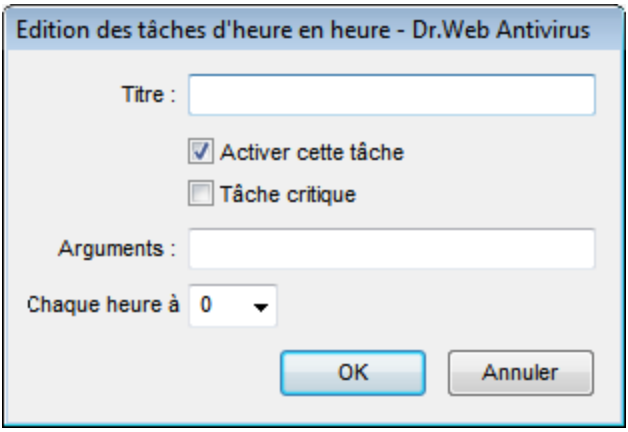


Figure 3-2. Boîte de dialogue des tâches d'heure en heure

Pour afficher la rubrique d'aide sur une fenêtre active, dans toutes les boîtes de dialogue de **Dr.Web Agent** pressez la touche F1. Pour la rubrique d'aide contextuelle sur un élément de la fenêtre, cliquez droit sur cet élément.

La boîte de dialogue des tâches de chaque heure (voir fig. 3-2) vous permet de spécifier les paramètres suivants :

- **Titre** - entrez ici le nom de la tâche.
- Cochez la case **Activer cette tâche** pour autoriser son exécution.

  Pour bloquer l'exécution de la tâche, décochez la case. La tâche sera présente dans la liste mais elle ne sera pas exécutée.

- La case cochée **Tâche critique** active l'exécution de la tâche lors du prochain démarrage de **Dr.Web Agent**, au cas où elle n'a pas été exécutée (**Dr.Web Agent** désactivé au moment de l'exécution de la tâche). Si l'exécution de la tâche a échoué

plusieurs fois, au prochain démarrage de **Dr.Web Agent,** elle sera exécutée une seule fois.

- **Arguments** - vous pouvez entrer ici des paramètres complémentaires de lancement de la tâche. Pour cela, utilisez les clés de la ligne de commande listées dans l'Annexe Clés de la ligne de commande pour le Scanner.
- **Chaque heure à** - entrez les minutes pour exécuter la tâche toutes les heures à un moment précis.

Pour quitter la fenêtre et sauvegarder les paramètres de la tâche, cliquez sur **OK**.

Pour quitter la fenêtre sans sauvegarder les modifications/la nouvelle tâche, cliquez sur **Annuler**.

3.5.1.2. Tâches exécutées chaque jour

Les tâches de ce type sont exécutées chaque jour, à l'heure spécifiée.

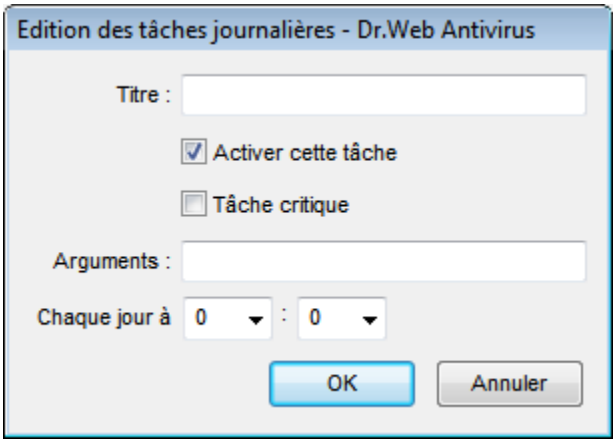


Figure 3-3. Boîte de dialogue des tâches journalières

Pour afficher la rubrique d'aide sur une fenêtre active, dans toutes les boîtes de dialogue de **Dr.Web Agent** pressez la touche F1. Pour la rubrique d'aide contextuelle sur un élément de la fenêtre, cliquez droit sur cet élément.

La boîte de dialogue des tâches journalières (voir fig. 3-3) vous permet de spécifier les paramètres suivants :

- **Titre** - entrez ici le nom de la tâche.
- Cochez la case **Activer cette tâche** pour autoriser son exécution.

  Pour bloquer l'exécution de la tâche, décochez la case. La tâche sera présente dans la liste mais elle ne sera pas exécutée.

- La case cochée **Tâche critique** active l'exécution de la tâche lors du prochain démarrage de **Dr.Web Agent**, dans le cas où elle n'a pas été exécutée (**Dr.Web Agent** désactivé au moment de l'exécution de la tâche). Si l'exécution de la tâche a échoué plusieurs fois, au prochain démarrage de **Dr.Web Agent,** elle sera exécutée une seule fois.
- **Arguments** - vous pouvez entrer ici des paramètres complémentaires de lancement de la tâche. Pour cela, utilisez les clés de la ligne de commande listées dans l'Annexe Clés de la ligne de commande pour le Scanner.
- **Chaque jour à** - entrez l'heure et la minute pour l'exécution de la tâche journalière.

Pour quitter la fenêtre et sauvegarder les paramètres de la tâche, cliquez sur **OK**.

Pour quitter la fenêtre sans sauvegarder les modifications/la nouvelle tâche, cliquez sur **Annuler**.

3.5.1.3. Tâches exécutées chaque semaine

Les tâches de ce type sont exécutées chaque semaine, au jour et à l'heure spécifiés.

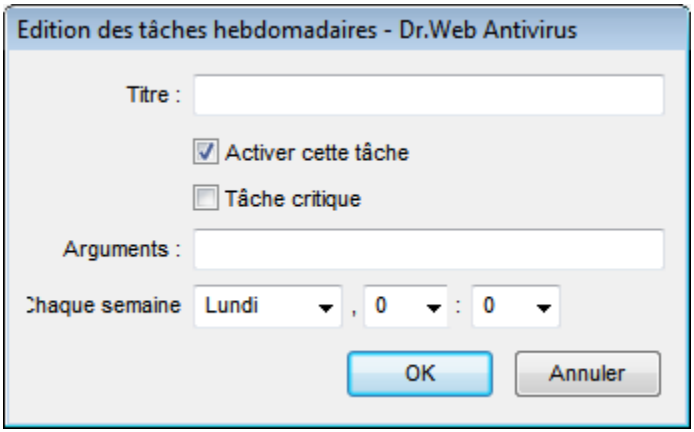


Figure 3-4. Boîte de dialogue des tâches hebdomadaires

Pour afficher la rubrique d'aide sur une fenêtre active, dans toutes les boîtes de dialogue de **Dr.Web Agent** pressez la touche F1. Pour la rubrique d'aide contextuelle sur un élément de la fenêtre, cliquez droit sur cet élément.

La boîte de dialogue des tâches hebdomadaires (voir fig. 3-4) vous permet de spécifier les paramètres suivants :

- **Titre** - entrez ici le nom de la tâche.
- Cochez la case **Activer cette tâche** pour autoriser son exécution.

  Pour bloquer l'exécution de la tâche, décochez la case. La tâche sera présente dans la liste mais elle ne sera pas exécutée.

- La case cochée **Tâche critique** active l'exécution de la tâche lors du prochain démarrage de **Dr.Web Agent**, dans le cas où elle n'a pas été exécutée (**Dr.Web Agent** désactivé au moment de l'exécution de la tâche). Si l'exécution de la tâche a échoué plusieurs fois, au prochain démarrage de **Dr.Web Agent,** elle sera exécutée une seule fois.
- **Arguments** - vous pouvez entrer ici des paramètres complémentaires de lancement de la tâche. Pour cela, utilisez les clés de la ligne de commande listées dans l'Annexe Clés de la

ligne de commande pour le Scanner.

- **Chaque semaine** - entrez ici le jour de la semaine, l'heure et les minutes pour l'exécution de la tâche hebdomadaire.

Pour quitter la fenêtre et sauvegarder les paramètres de la tâche, cliquez sur **OK**.

Pour quitter la fenêtre sans sauvegarder les modifications/la nouvelle tâche, cliquez sur **Annuler**.

3.5.1.4. Tâches exécutées chaque mois

Les tâches de ce type sont exécutées chaque mois au jour et à l'heure spécifiés.

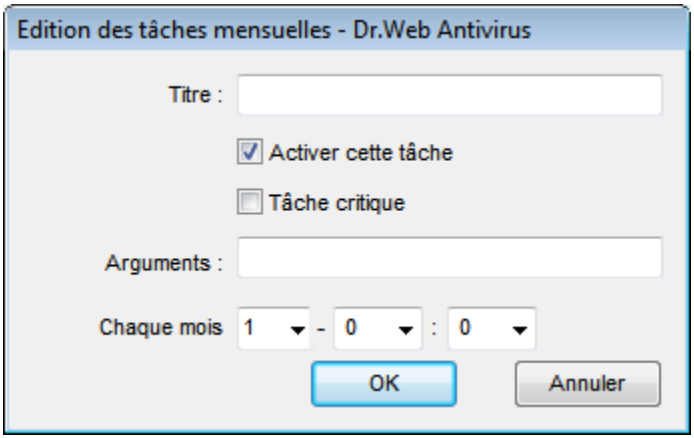


Figure 3-5. Boîte de dialogue des tâches mensuelles

Pour afficher la rubrique d'aide sur une fenêtre active, dans toutes les boites de dialogue de **Dr.Web Agent** pressez la touche F1. Pour la rubrique d'aide contextuelle sur un élément de la fenêtre, cliquez droit sur cet élément.

La boîte de dialogue des tâches mensuelles (voir. fig. 3-5) vous permet de spécifier les paramètres suivants :

- **Titre** - entrez ici le nom de la tâche.
- Cochez la case **Activer cette tâche** pour autoriser son exécution.

  Pour bloquer l'exécution de la tâche, décochez la case. La tâche sera présente dans la liste mais elle ne sera pas exécutée.

- La case cochée **Tâche critique** active l'exécution de la tâche lors du prochain démarrage de **Dr.Web Agent**, dans le cas où elle n'a pas été exécutée (**Dr.Web Agent** désactivé au moment de l'exécution de la tâche). Si l'exécution de la tâche a échoué plusieurs fois, au prochain démarrage de **Dr.Web Agent** elle sera exécutée une seule fois.
- **Arguments** - vous pouvez entrer ici des paramètres complémentaires de lancement de la tâche. Pour cela, utilisez les clés de la ligne de commande listées dans l'Annexe Clés de la ligne de commande pour le Scanner.
- **Chaque mois** - entrez ici le jour, l'heure et les minutes pour l'exécution de la tâche mensuelle.

Pour quitter la fenêtre et sauvegarder les paramètres de la tâche, cliquez sur **OK**.

Pour quitter la fenêtre sans sauvegarder les modifications/la nouvelle tâche, cliquez sur **Annuler**.

3.5.1.5. Tâches exécutées toutes les N minutes

Les tâches de ce type sont exécutées toutes les N minutes.

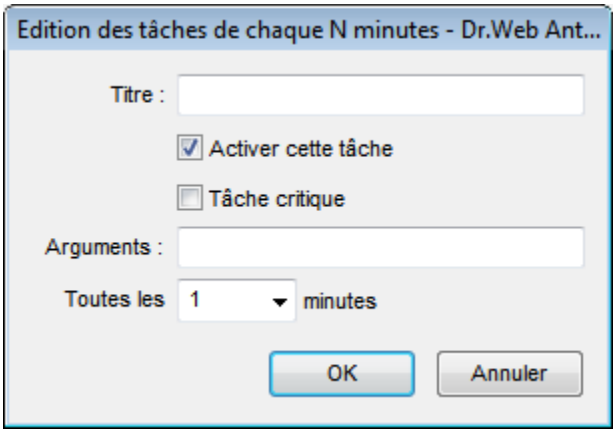


Figure 3-6. Boîte de dialogue des tâches de chaque N minutes

Pour afficher la rubrique d'aide sur une fenêtre active, dans toutes les boîtes de dialogue de **Dr.Web Agent** pressez la touche F1. Pour la rubrique d'aide contextuelle sur un élément de la fenêtre, cliquez droit sur cet élément.

La boîte de dialogue des tâches (voir fig. 3-6) vous permet de spécifier les paramètres suivants :

- **Titre** - entrez ici le nom de la tâche.
- Cochez la case **Activer cette tâche** pour autoriser son exécution.

  Pour bloquer l'exécution de la tâche, décochez la case. La tâche sera présente dans la liste mais elle ne sera pas exécutée.

- La case cochée **Tâche critique** active l'exécution de la tâche lors du prochain démarrage de **Dr.Web Agent**, dans le cas où elle n'a pas été exécutée (**Dr.Web Agent** désactivé au moment de l'exécution de la tâche). Si l'exécution de la tâche a échoué plusieurs fois, au prochain démarrage de **Dr.Web Agent** elle sera exécutée une seule fois.
- **Arguments** - vous pouvez entrer ici des paramètres complémentaires de lancement de la tâche. Pour cela, utilisez les clés de la ligne de commande listées dans l'Annexe Clés de la

ligne de commande pour le Scanner.

- **Toutes les <...> minutes** - entrez l'espacement entre les exécutions de la tâche, en minutes.

Pour quitter la fenêtre et sauvegarder les paramètres de la tâche, cliquez sur **OK**.

Pour quitter la fenêtre sans sauvegarder les modifications/la nouvelle tâche, cliquez sur **Annuler**.

3.5.1.6. Tâches exécutées au démarrage

Les tâches de ce type sont exécutées au démarrage de l'ordinateur (au démarrage du système d'exploitation).

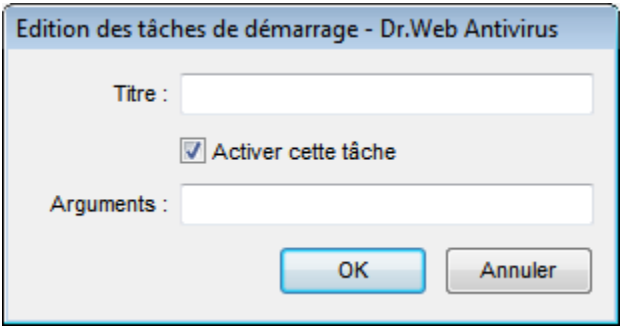


Figure 3-7. Boîte de dialogue des tâches de démarrage

Pour afficher la rubrique d'aide sur une fenêtre active, dans toutes les boîtes de dialogue de **Dr.Web Agent** pressez la touche F1. Pour la rubrique d'aide contextuelle sur un élément de la fenêtre, cliquez droit sur cet élément.

La boîte de dialogue des tâches (voir fig. 3-7) vous permet de spécifier les paramètres suivants :

- **Titre** - entrez ici le nom de la tâche.
- Cochez la case **Activer cette tâche** pour autoriser son exécution.

Pour bloquer l'exécution de la tâche, décochez la case. La tâche sera présente dans la liste mais elle ne sera pas exécutée.

- **Arguments** - vous pouvez entrer ici des paramètres complémentaires de lancement de la tâche. Pour cela, utilisez les clés de la ligne de commande listées dans l'Annexe Clés de la ligne de commande pour le Scanner.

Pour quitter la fenêtre et sauvegarder les paramètres de la tâche, cliquez sur **OK**.

Pour quitter la fenêtre sans sauvegarder les modifications/la nouvelle tâche, cliquez sur **Annuler**.

3.5.2. Planification centralisée

La fenêtre de la planification centralisée vous permet de consulter les tâches de l'analyse sur les postes du réseau paramétrées sur le **Serveur Enterprise**.

Dans toutes les boîtes de dialogue de **Dr.Web Agent**, pour afficher la rubrique d'aide sur une fenêtre active, pressez la touche F1. Pour la rubrique d'aide sur un élément de la fenêtre, cliquez droit sur cet élément dans l'illustration.

3.6. Configuration du mode itinérant

Si votre PC ou PC portable n'est pas connecté au **Serveur Enterprise** pendant une longue période, il est conseillé d'activer le mode itinérant de **Dr.Web Agent** afin de recevoir les mises à jour depuis des serveurs de **SGMAJ Dr.Web**.

Pour cela, sélectionnez l'élément **Mode itinérant** → **Activé** dans le menu contextuel de l'icône de **l'Agent**. La couleur de l'icône de **l'Agent** passera au jaune.

Tournant en mode itinérant, **l'Agent** tente de se connecter au **Serveur**, si la connexion a échoué après trois reprises, il effectue une mise à jour via le protocole HTTP depuis des serveurs du **SGMAJ Dr.Web**. Les tentatives de se connecter au **Serveur** sont régulières et espacées d'environ une minute.

L'élément **Mode itinérant** est disponible dans le menu contextuel à condition que le mode itinérant d'utilisation de **SGMAJ Dr.Web** soit autorisé dans les droits du poste sur le **Serveur**.

Pour configurer le mode itinérant, sélectionnez **Mode itinérant** → **Paramètres**. Une fenêtre affichant les paramètres du mode itinérant de **l'Agent** s'ouvrira.

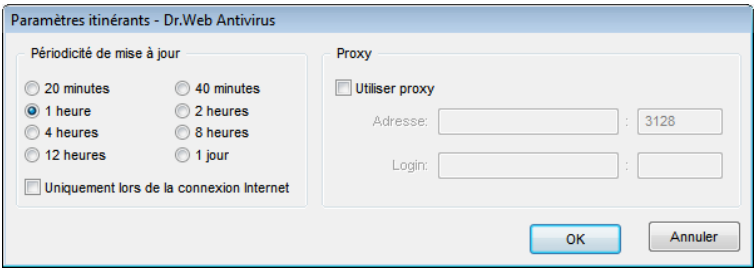


Fig. 3-8. Boîte de dialogue de configuration du mode itinérant

Dans toutes les boîtes de dialogue de **Dr.Web Agent**, pour afficher la rubrique d'aide sur une fenêtre active, pressez la touche F1. Pour la rubrique d'aide sur un élément de la fenêtre, cliquez droit sur cet élément dans l'illustration.

Vous pouvez paramétrer une périodicité de la vérification des mises à jour depuis **SGMAJ** dans le panneau **Périodicité de mises à jour** :

- **20 minutes** - vérifier les mises à jour toutes les 20 minutes.
- **40 minutes** - vérifier les mises à jour toutes les 40 minutes.
- **1 heure** - vérifier les mises à jour chaque heure.
- **2 heures** - vérifier les mises à jour toutes les 2 heures.

- **4 heures** - vérifier les mises à jour toutes les 4 heures.
- **8 heures** - vérifier les mises à jour toutes les 8 heures.
- **12 heures** - vérifier les mises à jour toutes les 12 heures.
- **1 jour** - vérifier les mises à jour une fois par jour.

Cochez la case **Uniquement lors de la connexion Internet**, si vous souhaitez que la vérification des mises à jour se fasse uniquement lors de la connexion à Internet.

Pour utiliser un serveur proxy, cochez la case **Utiliser proxy**. Si la case est cochée, les champs suivants sont activés :

- **Adresse** - pour spécifier l'adresse et le port du serveur proxy.
- **Login** - pour spécifier les paramètres d'authentification sur le serveur proxy : un login et un mot de passe.

Pour lancer une mise à jour en mode itinérant immédiatement, sélectionnez dans le menu contextuel de l'**Agent** l'élément **Mode itinérant** → **Lancer la mise à jour**.

Durant le fonctionnement de l'**Agent** en mode itinérant, la connexion de l'**Agent** au **Enterprise Serveur** est désactivée. Toutes les modifications paramétrées sur le Serveur pour le poste seront prises en compte dès que le mode itinérant sera désactivé et la connexion de l'**Agent** au Serveur sera reprise. Seules les bases virales seront mises à jour lorsque le mode itinérant est activé.

Pour désactiver le mode itinérant, dans le menu contextuel de l'**Agent,** sélectionnez l'élément **Mode itinérant** et décochez ensuite la case **Activé**. La couleur de l'icône de l'**Agent** passera du jaune au vert et la connexion de l'**Agent** au **Serveur** sera reprise.

3.7. Affichage des statistiques

Pour afficher les statistiques sur le poste, sélectionnez l'élément **Statistiques** dans le menu contextuel de l'**Agent**. Vous pouvez également double-cliquer sur l'icône de l'**Agent**. Une fenêtre affichant toutes les statistiques sur le fonctionnement de l'antivirus sera affichée.

La première colonne du tableau statistiques affiche les composants **Dr.Web** installés sur votre poste. Les autres colonnes affichent le nombre d'objets vérifiés (scannés) par les composants respectifs.

Les catégories d'objets suivants sont présentes :

- les objets infectés détectés par l'antivirus,
- les modifications de virus,
- les objets suspects,
- les activités virales.

Le nombre d'objets listés ci-dessous est également affiché :

- réparés,
- supprimés,
- renommés,
- déplacés,
- verrouillés.

La fenêtre affiche aussi le nombre d'erreurs et la vitesse de l'analyse.

Pour en savoir plus sur les catégories de statistiques, consultez la rubrique Onglet Statistiques du chapitre Dr.Web Scanner pour Windows.

Dans toutes les boîtes de dialogue de **Dr.Web Agent**, pour afficher la rubrique d'aide sur une fenêtre active, pressez la touche F1. Pour la rubrique d'aide sur un élément de la fenêtre, cliquez droit sur cet élément dans l'illustration.

3.8. Affichage du statut de l'antivirus

Pour afficher le statut du logiciel antivirus installé sur le poste, sélectionnez l'élément **Statut** dans le menu contextuel **de l'Agent**.

La partie haute de la fenêtre affiche :

- le total de définitions virales dans la base,
- la date de la dernière mise à jour,
- la version de l'**Agent** en fonction,
- l'activité du scan (si le scanner est actif ou pas).

La fenêtre du statut comprend les onglets suivants :

- **Bases**. L'onglet contient des informations détaillées sur toutes les bases virales installées :
  - le nom de fichier contenant la base virale,
  - la version de la base virale,
  - le nombre d'entrées dans la base,
  - la date de création de la base virale.
- **Composants**. L'onglet contient des informations sur tous les composants antivirus **Dr.Web** installés sur le poste :
  - le nom du composant,
  - le statut du composant : actif (en cours d'exécution) ou inactif (non lancé).
- **Modules**. L'onglet comprend des informations détaillées sur tous les modules de l'antivirus **Dr.Web** :
  - le fichier associé au module correspondant du produit,
  - la version complète du module,
  - la description du module - le nom du module.

La partie basse de la fenêtre du statut affiche :

- la barre de statut de l'antivirus. Elle contient des notifications importantes (voir la rubrique Configuration de Dr.WebAgent). Lorsque l'**Agent** fonctionne correctement, le message suivant s'affiche - **Aucune action requise**,

- ID (l'identificateur unique) de l'**Agent**.

Dans toutes les boîtes de dialogue de **Dr.Web Agent**, pour afficher la rubrique d'aide sur une fenêtre active, pressez la touche F1. Pour la rubrique d'aide sur un élément de la fenêtre, cliquez droit sur cet élément dans l'illustration.

3.9. Messages d'information

Le système de notifications consiste en bulles d'information (tool tips) qui s'affichent contre l'icône de **Dr.Web Agent**.

Les messages contenus dans les bulles d'information peuvent être classés selon les informations affichées :

- Notifications - des informations détaillées sur les actions exécutées ou nécessaires qui concernent l'antivirus ou le fonctionnement de votre PC.
- Résumé de **Dr.Web Agent** - des données récapitulatives sur l'état et le fonctionnement de l'antivirus.
- Messages envoyés par l'administrateur.

Notifications

Les notifications contiennent de l'information sur les événements viraux et sur les actions de l'antivirus sur votre PC (pour plus d'information, merci de consulter la rubrique Configuration de Dr.Web Agent).

A part les fonctions d'information, les bulles peuvent être dotées de fonctions de gestion. Par exemple, la fenêtre avertissant du redémarrage nécessaire du PC après une mise à jour des composants antivirus (voir fig.3-9) est dotée de boutons permettant de remettre ou d'exécuter un redémarrage de la machine. Pour cela, sélectionnez un délai dans la liste déroulante et cliquez ensuite sur **Ultérieurement**.

Figure 3-9. Notification de Dr.Web Agent

Résumé de Dr.Web Agent

Lors du passage du curseur sur l'icône de **Dr.Web Agent**, une bulle contenant les informations ci-dessous s'affiche :

- les statistiques des événements viraux (voir aussi Consultation des statistiques),
- le statut des composants antivirus,
- la date de la dernière mise à jour.

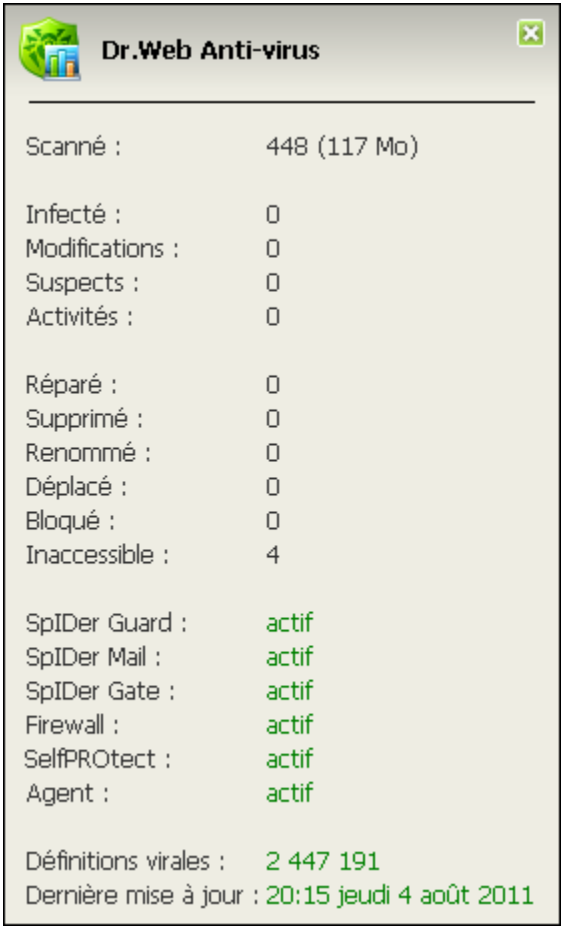


Figure 3-10. Bulle d'information de Dr.Web Agent

Messages envoyés par l'administrateur

L'utilisateur peut recevoir des messages de la part de l'administrateur système du réseau antivirus, ces messages contiennent :

- le texte du message,

- des liens hypertexte vers des ressources web,
- le logo de la société (ou d'autres informations graphiques),
- l'en-tête du message contient l'heure précise de la réception du message.

Les messages s'affichent sous forme de bulles d'information (voir fig. 3-11).

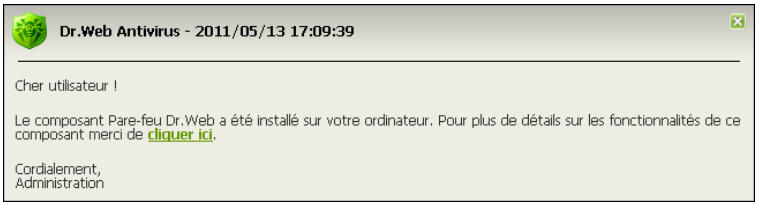


Figure 3-11. Bulle d'information de l'administrateur

A la différence des bulles d'information contenant des notifications ou des résumés de **Dr.Web Agent** qui se ferment après une certaine période d'inactivité, les messages de l'administrateur seront affichés jusqu'au moment où l'utilisateur les ferme explicitement.

Chapitre 4. Dr.Web Scanner pour Windows

Avec la commande **Scanner** depuis le menu contextuel de l'**Agent**, vous pouvez lancer le **Scanner antivirus Dr.Web pour Windows** pour scanner périodiquement votre ordinateur à la recherche des virus et d'autre malware.

Le **Dr.Web Scanner pour Windows** est destiné à effectuer l'analyse antivirus des secteurs d'amorçage, de la mémoire et des fichiers particuliers ainsi que des objets au sein des structures composées (les archives, conteneurs, messages e-mail avec des pièces-jointes).

La version installée de **Dr.Web Scanner pour Windows** est fonction du système d'exploitation. Il existe deux versions de **Dr.Web Scanner :**

- Dr.Web Scanner,
- Dr.Web Scanner NT4.

Avant l'installation du **Scanner**, la version d'OS est automatiquement détectée, et puis la version appropriée du **Dr.Web Scanner pour Windows** est installée (voir Pré-requis système).

Pour passer à la rubrique d'aide **Dr.Web Antivirus pour Windows**, pressez la touche F1 dans toute fenêtre du **Scanner**.

4.1. Dr.Web Scanner

Vous pouvez consultez la description des modes d'anayse avec le **Dr.Web Scanner** dans le Manuel **Dr.Web Antivirus pour Windows**, paragraphe **Modes d'analyse**.

Pour plus d'information sur les actions du **Dr.Web Scanner** en cas de détection d'objets contaminés ou suspects, consultez le Manuel **Dr.Web Antivirus pour Windows**, paragraphe **Actions en cas de détection de virus**.

Pour la description des paramètres du fonctionnement du **Dr.Web Scanner**, consultez le Manuel **Dr.Web Antivirus pour Windows**, paragraphe **Configurer le Scanner Dr.Web**.

4.2. Dr.Web Scanner NT4

4.2.1. Analyse antivirus

4.2.1.1. Modes d'analyse

Le **Dr.Web Scanner NT4** (ci-après - **Scanner**) supporte plusieurs modes d'analyse.

Analyse rapide

Dans ce mode, les objets suivants sont analysés :

- mémoire vive ;
- secteurs d'amorçage de tous les disques ;
- objets d'auto-démarrage ;
- dossier racine du disque de démarrage ;
- disque racine contenant le dossier d'installation de Windows ;

- dossier système Windows ;
- dossier des Documents de l'utilisateur (`Mes documents`) ;
- répertoire système temporaire ;
- répertoire d'utilsateur temporaire.

Analyse complète

Dans ce mode, la mémoire vive, tous les disques durs et les supports amovibles (y compris les secteurs d'amorçage) sont scannés.

Analyse sélective

Ce mode permet de choisir tout dossier ou fichier à scanner.

Lorsque ce mode est sélectionné, dans la partie centrale de l'onglet **Analyse**, l'arborescence du système de fichiers sera affichée. Si nécessaire, vous pouvez la dérouler pour passez à un niveau plus détaillé et visualiser les dossiers et fichiers.

Dans l'arborescence, sélectionnez les objets que vous souhaitez scanner. Les secteurs d'amorçage de tous les disques seront également scannés.

La figure ci-dessous présente la situation où dans le mode **Analyse sélective**, un répertoire se trouvant sur le disque C est sélectionné pour l'analyse.

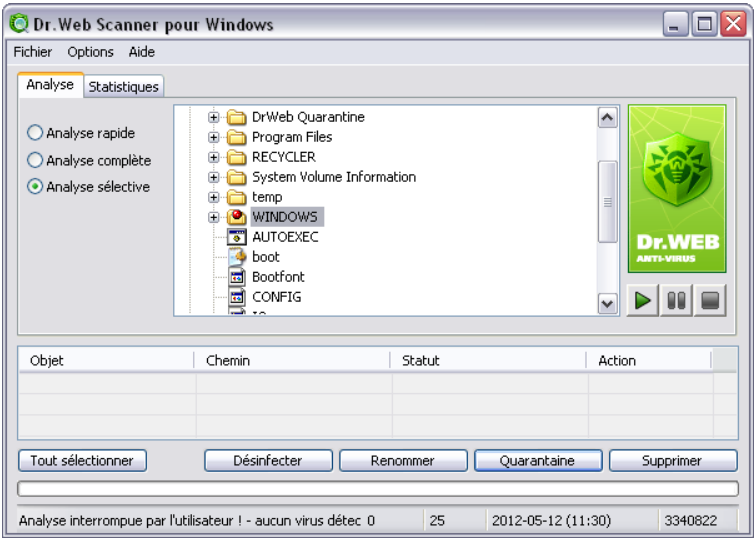


Figure 4-1. Fenêtre principale du Dr.Web Scanner. Onglet Analyse.

Par défaut, outre les objets sélectionnés, les sous-répertoires de tous les répertoires sélectionnés et tous les disques logiques ainsi que les secteurs d'amorçage de tous les disques logiques sur lesquels au moins un répertoire ou un fichier est sélectionné, les secteurs d'amorçages principaux sur les disques physiques sont scannés.

En cas d'analyse rapide ou complète, le **Scanner** définira si le fichier-HOSTS (fichier texte qui contient une base de noms de domaines et qui est utilisé lors de la transformation de noms vers les adresses de noeuds réseau) a été modifié. Le fichier-HOSTS peut être modifié par des logiciels malveillants (par exemple, dans le but de rediriger l'utilisateur vers un site web spécifique).

Au cas où le fichier HOSTS a été modifié, le **Scanner** suggèrera de le restaurer dans son état initial. Ceci permettra d'éliminer les modifications non approuvées du fichier par des malwares.

4.2.1.2. Lancement du scan antivirus

Par défaut, lors du scan, toutes les méthodes de détection des objets malveillants sont utilisés et les actions suivantes sont effectuées :

- les fichiers exécutables emballés par des outils de compression spécifiques sont décompressés et analysés ;
- les fichiers au sein des archives de tous les types répandus sont également analysés (ACE (jusqu'à la version 2.0), ALZIP, AR, ARJ, BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP etc.) ;
- les fichiers au sein des conteneurs de fichiers (1C, CHM, MSI, RTF, ISO, CPIO, DEB, RPM etc.) sont analysés ;
- les messages e-mail (dont le format doit correspondre au standard RFC822) sauvegardés dans les boîtes aux lettres des clients de messagerie sont analysés.

Lancement du scan antivirus

1. Dans le menu contextuel de l'icône de l'**Agent**, sélectionnez l'élément **Scanner**. La fenêtre principale du **Scanner** sera ouverte.

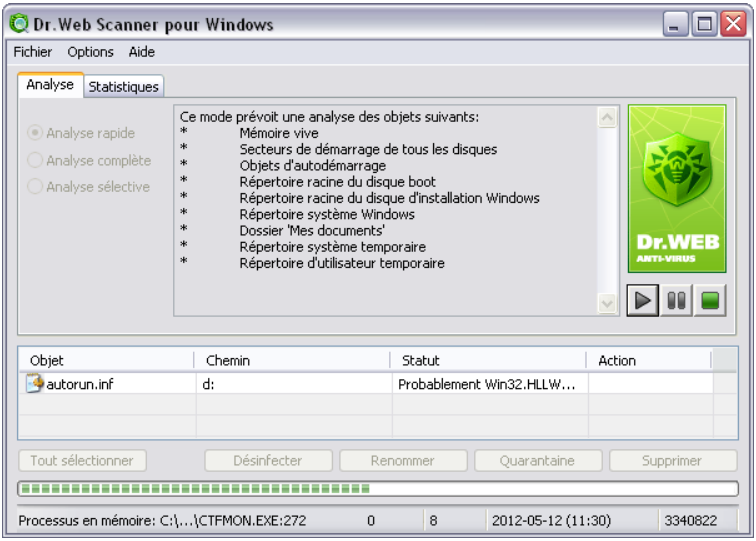


Figure 4-2. Fenêtre principale du Dr.Web Scanner pour Windows.

2. Avant de lancer le scan, sélectionnez l'un des modes d'analyse affichés sur l'onglet Analyse :
   - Analyse rapide ;
   - Analyse complète ;
   - Analyse sélective .

   Ultérieurement, vous pourrez suspendre le processus d'analyse lancé et si nécessaire, spécifier un autre mode d'analyse.

3. Si besoin est, spécifiez les paramètres de l'analyse dans la rubrique Options.

   Vous pouvez également modifier la méthode utilisée par défaut pour spécifier les actions à réaliser en cas de détection de ménaces (pour en savoir plus, consultez le paragraphe Actions en cas de détection de menaces) dans la rubrique **Actions**.

4. Pour gérer le processus de scan, utilisez les boutons se trouvant dans la partie droite de la fenêtre :

-  **Lancer l'analyse** - pour lancer le processus de scan ;
-  **Mettre en pause** - pour suspendre le processus de scan. Afin de reprendre l'analyse, cliquez à nouveau sur  **Lancer l'analyse** ;
-  **Arrêter l'analyse** - pour arrêter ke processus de scan.

5. Les résultats du scan sont affichés en bas de l'onglet **Analyse** et sur l'onglet Statiqtiques. Le tableau de rapport contient les informations suivantes :

Colonne	Description
Objet	liste les noms des objets contaminés ou suspects, des secteurs d'amorçage ou des processus dans la mémoire. Si des objets malveillants ou suspects sont détectés dans des objets complexes (archive, fichier email ou conteneur de fichiers), le rapport contient les noms de tels objets.
Chemin	liste les chemins complets vers les objets malveillants (pour les fichiers et les secteurs d'amorçage) ou affiche des informations sur les archives contaminées.
Statut	Pour les fichiers et les secteurs d'amorçage : liste les noms des programmes malveillants ou de leurs modifications (une modification d'un virus connu est un code du virus modifié de telle manière que l'antivirus le détecte mais que les algorithmes de désinfection correspondant au virus initial ne sont pas applicables à ce code modifié) selon la classification interne de **Doctor Web**. Pour les menaces au sein des objets composés, des informations sur tels objets sont affichées. Pour les objets suspects, il y a une mention que l'objet est *probablement contaminé* et le type supposé du programme malveillant selon le classification de l'analyseur heuristique est également affiché.

Colonne	Description
Action	Des informations sur les actions réalisées par le **Scanner** dans le but de neutralisation des programmes malveillants (désinfection, suppression, renommage, déplacement). Dans le cas où l'objet détecté est en cours d'utilisation par une application Windows, l'action sélectionnée ne peut pas être menée immédiatement. Pour de tels objets, dans le champ de rapport du **Scanner**, la colonne **Action** affiche les messages : **Sera désinfecté après redémarrage**, **Sera supprimé après redémarrage** ou **Sera renommé après redémarrage**, en fonction de l'action sélectionnée. Ainsi, l'action nécessaire ne sera réalisée qu'après le prochain redémarrage de la machine. En cas de détection de tels objets, il est recommandé de redémarrer le système immédiatement après la fin du scan.

En plus des boutons et des éléments du menu permettant d'accéder aux fenêtres, paramètres et fonctions, vous pouvez utiliser les raccourcis clavier

F1 – afficher la rubrique d'aide ;

F3 – ouvrir la fenêtre principale du **Scanner Dr.Web** sur l'onglet **Analyse** ;

F4 – ouvrir la fenêtre principale du **Scanner Dr.Web** sur l'onglet **Statistiques** ;

F5 – ouvrir la fenêtre de configuration du chemin et du masque pour l'analyse ;

F7 – lancer l'analyse rapide (scan de la mémoire vive et des objets d'auto démarrage) ;

F8 – lancer la mise à jour ;

F9 – ouvrir la fenêtre de configuration du **Scanner Dr.Web** ;

F10 – retour au menu de la fenêtre courante ;

CTRL+F5 – lancer le scan ;

CTRL+F6 – arrêter le scan ;

CTRL+F2 – effacer le rapport du **Scanner Dr.Web** ;

ALT+X – quitter le **Scanner Dr.Web**.

4.2.1.3. Actions en cas de détection de menaces

Si un virus connu est détecté ou que vous soupçonnez un objet d'être contaminé par un virus, les actions suivantes peuvent être menées :

1. Par défaut, le **Scanner** informe l'utilisateur sur les menaces détectées via le champ de rapport spécialisé en bas de l'onglet **Analyse**. Les processus infectés détectés sont automatiquement arrêtés, les trojans trouvés sont supprimés. L'utilisateur peut choisir des actions ultérieures en fonction des objets détectés (pour en savoir plus, consultez la rubrique Configuration des actions sur les menaces détectées).
2. Si l'option **Demander confirmation** se trouvant sur l'onglet **Actions** dans la fenêtre de configuration du **Scanner**, est désactivée, le **Scanner** applique les actions spécifiées sur l'onglet **Actions** de manière automatique sans demander une confirmation de l'utilisateur (pour en savoir plus, consultez le paragraphe Onglet Actions).

Configuration des actions sur les menaces détectées

Configuré par défaut, le **Scanner** vous alerte en cas de détection d'une menace (excepté les canulars, les riskwares et les hacktools dont la détection est ignorée par défaut). Les résultats de l'analyse sont réunis dans le tableau vous permettant de choisir des actions nécessaires à appliquer aux objets détectés.

Le rapport contient des informations sur les objets contaminés ou suspects détectés lors du scan ainsi que sur les actions menées par le **Scanner**. Si les objets contaminés ont été trouvés dans des archives ou dans des conteneurs de fichiers, les archives contenant tels objets seront listés ainsi que les objets infectés.

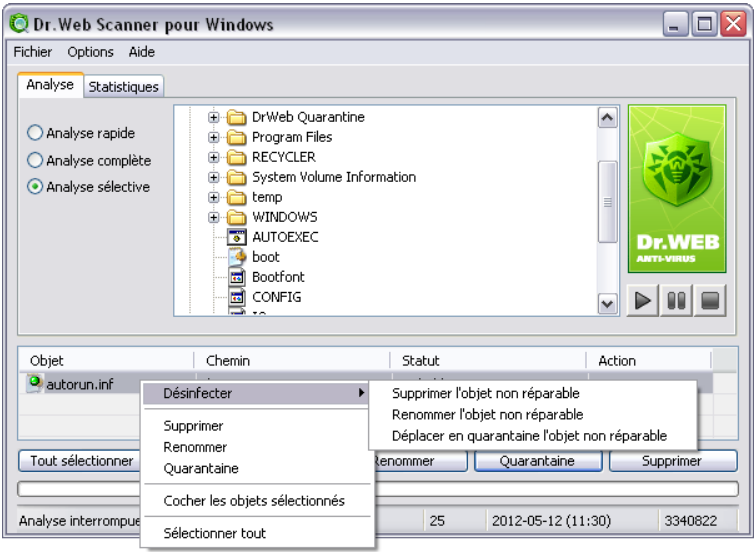


Figure 4-3. Fenêtre principale du Dr.Web Scanner. Onglet Analyse.

Les actions listées ci-après peuvent être appliquées aux objets détectés :

Action	Description
Désinfecter	Restaure l'objet dans son état d'origine, avant l'infection. Lorsque vous sélectionnez cette action, un menu supplémentaire apparaît qui vous invite à sélectionner une réaction du **Scanner** si la désinfection de l'objet échoue. Cette action est valable uniquement pour les objets contaminés par des virus connus et curables, exceptés les trojans et les fichiers contenus dans des objets complexes (archives, fichiers email ou conteneurs de fichiers). C'est la seule action disponible pour les secteurs d'amorçage contaminés.
Supprimer	Supprime l'objet. Cette action est impossible pour les secteurs d'amorçage.

Action	Description
Renommer	Modifie l'extension du nom de fichier de l'objet selon les paramètres du **Scanner**. Par défaut, le primier symbole de l'extension est remplacé par #. Cette action n'est pas applicable aux secteurs d'amorçage.
Déplac	Déplace l'objet dans le dossier Quarantaine dont le chemin est est spécifié dans les paramètres du **Scanner**. Cette action n'est pas applicable aux secteur d'amorçage.

Pour effectuer une action

1. Sélectionnez un objet dans le tableau de rapport. Pour sélectionnez plusieurs objets en une seule fois, maintenez appuyées les touches SHIFT ou CTRL. Vous pouvez également utiliser les raccourcis suivants :
   - INSERT – pour sélectionner un objet et déplacer le courseur vers la position suivante ;
   - CTRL+A – pour sélectionner tout ;
   - la touche * sur le clavier numérique – tout sélectionner ou tout désélectionner.
2. Réalisez l'une des actions suivantes :
   - Cliquez droit sur l'objet sélectionné et dans le menu contextuel, choisissez l'action que vous souhaitez appliquer.
   - Cliquez sur le bouton approprié sous le tableau Rapport.

Aucune action ne peut être appliquée aux fichiers se trouvant au sein des objets complexes (archives, fichiers email ou conteneurs de fichiers). Dans ce cas, l'action sera appliquée à l'objet dans son ensemble. De plus, si dans ce cas-là, vous sélectionnez de **Supprimer** un objet complexe, le **Scanner** affiche un message d'alerte indiquant que les données peuvent être perdues.

En plus des boutons et des éléments de menu permettant d'accéder aux différentes fenêtres, menus et fonctionnalités, vous pouvez également utiliser les raccourcis clavier

F1 – afficher la rubrique d'aide ;

F3 – ouvrir la fenêtre principale du **Scanner Dr.Web** sur l'onglet **Analyse** ;

F4 – ouvrir la fenêtre principale du **Scanner Dr.Web** sur l'onglet **Statistiques** ;

F5 – ouvrir la fenêtre de configuration du chemin et du masque pour l'analyse ;

F7 – lancer l'analyse rapide (scan de la mémoire vive et des objets d'auto démarrage) ;

F8 – lancer la mise à jour ;

F9 – ouvrir la fenêtre de configuration du **Scanner Dr.Web** ;

F10 – retour au menu de la fenêtre courante ;

CTRL+F5 – lancer le scan ;

CTRL+F6 – arrêter le scan ;

CTRL+F2 – effacer le rapport du **Scanner Dr.Web** ;

ALT+X – quitter le **Scanner Dr.Web**.

4.2.2. Fenêtre principale du Dr.Web Scanner

La fenêtre principale du **Scanner** comporte les onglets suivants :

- l'onglet Analyse sur lequel les tâches de scan sont configurées ;
- l'onglet Statistiques permettant accéder aux résultats de l'activité du **Scanner**.

4.2.2.1. Onglet Analyse

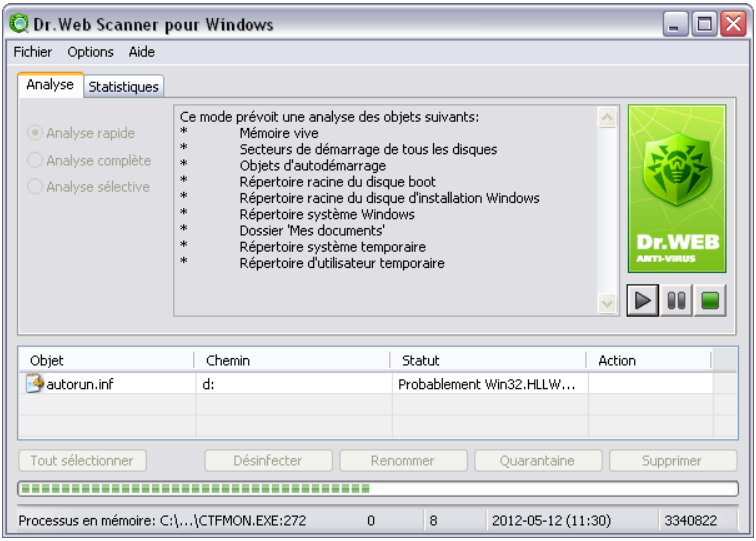


Figure 4-4. Fenêtre principale du Dr.Web Scanner. Onglet Analyse.

Pour afficher la rubrique d'aide sur un paramètre situé dans un autre onglet, cliquez sur l'onglet correspondant dans l'illustration

Dans l'onglet **Analyse** vous pouvez configurer, lancer et gérer les analyses antivirus des objets Windows. Par défaut, le **Scanner** utilise toutes les méthodes de détection pour détecter les virus et autres logiciels malicieux.

En fonction du mode d'analyse sélectionné, la partie centrale de la fenêtre affiche soit une liste d'objets à scanner, soit l'arborescence du système de fichiers. En bas de la fenêtre, vous avez un tableau affichant des informations sur les objets contaminés ou suspects trouvés lors de l'analyse ainsi que les actions réalisées par le **Scanner**.

En plus des boutons et des éléments de menu permettant d'accéder aux différentes fenêtres, menus et fonctionnalités, vous pouvez également utiliser les raccourcis clavier

F1 – afficher la rubrique d'aide ;

F3 – ouvrir la fenêtre principale du **Scanner Dr.Web** sur l'onglet **Analyse** ;

F4 – ouvrir la fenêtre principale du **Scanner Dr.Web** sur l'onglet **Statistiques** ;

F5 – ouvrir la fenêtre de configuration du chemin et du masque pour l'analyse ;

F7 – lancer l'analyse rapide (scan de la mémoire vive et des objets d'auto démarrage) ;

F8 – lancer la mise à jour ;

F9 – ouvrir la fenêtre de configuration du **Scanner Dr.Web** ;

F10 – retour au menu de la fenêtre courante ;

CTRL+F5 – lancer le scan ;

CTRL+F6 – arrêter le scan ;

CTRL+F2 – effacer le rapport du **Scanner Dr.Web** ;

ALT+X – quitter le **Scanner Dr.Web**.

4.2.2.2. Onglet Statistiques

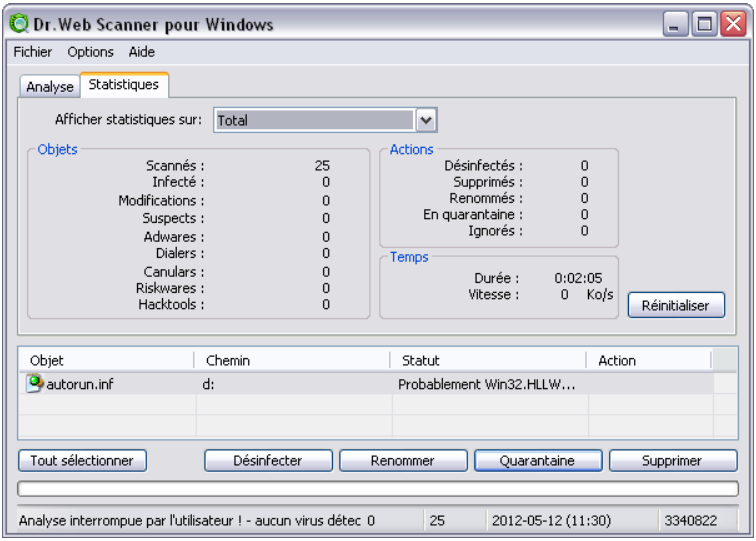


Figure 4-5. Fenêtre principal du Dr.Web Scanner. Onglet Statistiques

Pour afficher la rubrique d'aide sur un paramètre situé dans un autre onglet, cliquez sur l'onglet correspondant dans l'illustration

L'onglet **Statistiques** fournit toutes les données sur les opérations du **Scanner** qui incluent le nombre total d'objets scannés, le nombre d'objets infectés par des virus connus ou des modifications de virus connus, le nombre d'objets suspects et les actions menées par le logiciel sur les objets infectés ou suspects.

Vous pouvez également recevoir des statistiques pour tout disque logique de la machine. Pour cela, sélectionnez le disque dans le menu déroulant en haut de la fenêtre.

Pour effacer les données statistiques, cliquez sur **Réinitialiser**.

En plus des boutons et des éléments de menu permettant d'accéder aux différentes fenêtres, menus et fonctionnalités, vous pouvez également utiliser les raccourcis clavier

F1 – afficher la rubrique d'aide ;

F3 – ouvrir la fenêtre principale du **Scanner Dr.Web** sur l'onglet **Analyse** ;

F4 – ouvrir la fenêtre principale du **Scanner Dr.Web** sur l'onglet **Statistiques** ;

F5 – ouvrir la fenêtre de configuration du chemin et du masque pour l'analyse ;

F7 – lancer l'analyse rapide (scan de la mémoire vive et des objets d'auto démarrage) ;

F8 – lancer la mise à jour ;

F9 – ouvrir la fenêtre de configuration du **Scanner Dr.Web** ;

F10 – retour au menu de la fenêtre courante ;

CTRL+F5 – lancer le scan ;

CTRL+F6 – arrêter le scan ;

CTRL+F2 – effacer le rapport du **Scanner Dr.Web** ;

ALT+X – quitter le **Scanner Dr.Web**.

4.2.3. Configuration du Dr.Web Scanner

Dans la plupart des cas, les paramètres du **Scanner Dr.Web** définis par défaut sont optimaux. Ne les modifiez pas si cela n'est pas nécessaire.

Modification des paramètres du Scanner Dr.Web

1. Si le **Scanner** n'est pas lancé, lancez-le. Pour ce faire, depuis le menu contextuel de l'icône de l'**Agent**, sélectionnez l'élément **Scanner**. La fenêtre principale du **Scanner** apparaît.
2. Dans le menu de la fenêtre principale du **Scanner**, sélectionnez **Options**, puis dans le sous-menu, cliquez sur **Changer la configuration**. Une fenêtre contenant les onglets

suivants sera ouverte :

- l'onglet Scanner, où vous pouvez spécifier les fichiers et dossiers à exclure de l'analyse ;
- l'onglet Types de fichiers, où vous pouvez précisier des restrictions supplémentaires concernant les types de fichiers à scanner ;
- l'onglet Actions, où vous pouvez configurer les réactions du **Scanner** lors de la détection de fichiers infectés ou suspects, des programmes malveillants et des archives contaminées ;
- l'onglet Rapport vous permettant de paramètrer l'écriture dans le fichier de log du **Scanner** ;
- l'onglet Général, où vous pouvez configurer l'interaction entre le **Scanner** et le système d'exploitation ainsi que les alertes sonores pour les différents événements.

3. Apportez des modifications comme vous le souhaitez. Si nécessaire, cliquez sur **Appliquer** avant de passer vers un autre onglet.
4. Pour obtenir des informations sur les paramètres se trouvant sur l'onglet ouvert, pressez la touche F1.
5. Après avoir effectué vos paramètres, cliquez sur **OK** pour sauvegarder les modifications apportées ou sur **Annuler** pour les annuler.
6. Vous pouvez conserver les paramètres pour les sessions de scan ultérieures (les processus d'analyse qui seront lancés lors du prochain démarrage du **Scanner**), pour cela, si dans l'onglet Général, la case **Enregistrement automatique de la configuration** n'est pas cochée, allez dans les **Options** du menu principal et cliquez sur **Enregistrer la configuration**.

4.2.3.1. Onglet Scanner

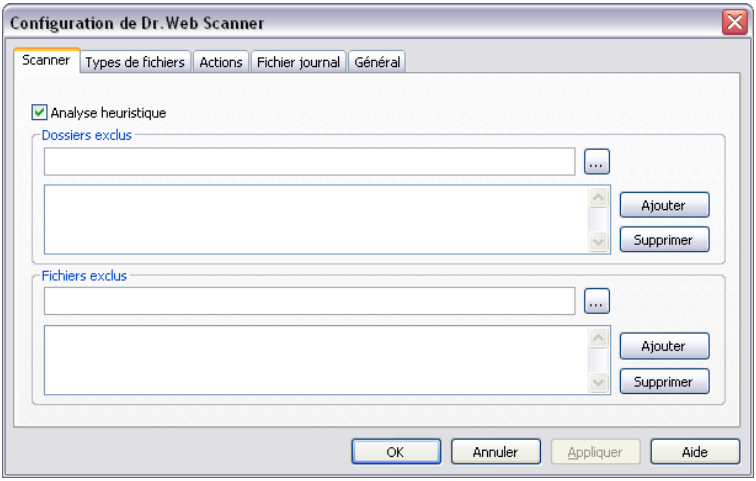


Figure 4-6. Fenêtre de configuration du Dr.Web Scanner. Onglet Scanner.

Pour afficher la rubrique d'aide sur un paramètre situé dans un autre onglet, cliquez sur l'onglet correspondant dans l'illustration

L'onglet **Scanner** offre des options suivantes :

- L'utilisation de l'analyseur heuristique (méthode permettant de déteter les objets suspects à forte probabilité contaminés par des virus inconnus).

  Cette option est activée par défaut. Il est recommandé d'utiliser l'analyse heuristique pendant le scan et de ne pas désactiver cette option.

  Une particularité de ce type de recherche de virus est que la probabilité de contamination est prise en compte. Ceci permet de détecter non pas les objets infectés mais les objets suspects d'être infectés. Un certain nombre de logiciels (par exemple, les chargeurs d'amorçage) peuvent provoquer des fausses alertes de l'analyseur heuristique puisqu'ils utilisent le code semblable à un code viral. De plus, ce type d'analyse peut ralentir l'analyse sur

les ordinateurs obsolètes. C'est une raison pour désactiver l'analyse heuristique. Cependant, l'analyse heuristique renforce la protection antivirus.

- Les listes de fichiers et de dossiers exclus de l'analyse.

Liste des dossiers à exclure de l'analyse

Dans cette rubrique, vous pouvez spécifier les dossiers à exclure de l'analyse. Par exemple, les dossiers de **Quarantaine**, des dossiers relatifs au certains programmes etc.

Pour éditer la liste des chemins à exclure :

1. Pour ajouter un dossier dans la liste :
   a) Saisissez le chemin vers le dossier contenant les fichiers que vous souhaitez exclure de l'analyse. Vous pouvez également utiliser le bouton **Parcourir**  et sélectionner un dossier particulier à l'aide de l'explorateur.
   b) Cliquez sur le bouton **Ajouter** se trouvant à droite. Le dossier sera ajouté dans la liste affichée plus bas.
2. Pour supprimer un dossier dans la liste,sélecionnez-le et cliquez ensuite sur **Supprimer**. Le contenu du dossier sera analysé lors du prochain session de scan.

Liste des fichiers à exclure de l'analyse

Ici vous pouvez rédiger une liste des fichiers (masques de fichiers) à ne pas faire analyser (tous les fichiers ayant les noms listés seront exclus de l'analyse). Par exemple, vous pouvez exclure de l'analyse les fichiers temporaires et fichiers d'échange ou swap.

Pour éditer la liste des fichiers à exclure :

1. Pour ajouter un fichier dans la liste :

a) entrez le nom du fichier que vous souhaitez exclure de l'analyse. Vous pouvez également utiliser le bouton**Parcourir**  et sélectionner l'objet à l'aide de l'explorateur. Vous pouvez aussi utiliser des masques.

Un masque est un modèle permettant de définir un objet. Le masque peut contenir des symboles autorisés à être utilisés dans les noms de fichiers ainsi que des symboles spécifiques :

- * remplace toute séquence (y compris une séquence vide) de n'importe quel symbole ;
- ? remplace un symbole dans la position définie.

Exemples :

- **rapport*.doc** est un masque déterminant tous les documents de Microsoft Word dont le nom commence par la séquence `rapport`, par exemple, il spécifie les fichiers suivants : rapport-fevrier`.doc`, rapport`121209.doc` etc. ;
- ***.exe** est un masque déterminant tous les exécutables ayant l'extension `EXE`, par exemple `setup.exe`, `iTunes.exe` etc. ;
- **photo????09.jpg** est un masque déterminant tous les fichiers au format `JPG` dont le nom commence par la séquence `photo` et se termine par la sequence numérique `09` et qui contiennent entre les deux encore 4 symboles non déterminés,par exemple `photo121209.jpg`, `photomama09.jpg` ou `photo----09.jpg`.

b) Cliquez sur le bouton **Ajouter** se trouvant à droite. Le fichier (masque de fichier) sera ajouté dans la liste située plus bas.

2. Pour enlever un objet de la liste, sélectoinnez-le dans la liste et cliquez sur **Supprimer**. Le fichier sera analysé lors du prochain processus de scan.

Pour exclure un fichier spécifique de l'analyse, ajoutez le chemin complet vers ce fichier y compris son nom dans la liste **Dossier exclus** (vous pouvez utiliser le bouton **Parcourir** pour sélectionner le dossier dans lequel se trouve le fichier, et puis tapez le nom du fichier après le chemin).

4.2.3.2. Onglet Types de fichiers

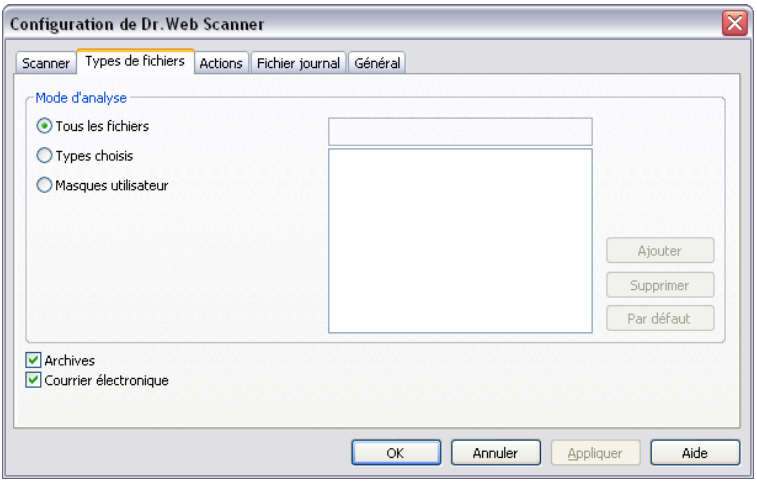


Figure 4-7. Fenêtre de configuration du Dr.Web Scanner. Onglet Types des fichiers.

Pour afficher la rubrique d'aide sur un paramètre situé dans un autre onglet, cliquez sur l'onglet correspondant dans l'illustration

Sur l'onglet **Types de fichiers**, vous pouvez définir certaines restrictions concernant les fichiers analysés en fonction de la tâche d'analyse.

Dans le groupe **Mode d'analyse**, sélectionnez les types de fichiers à scanner par le **Scanner** :

- L'option définie par défaut - **Tous les fichiers** commande de vérifier tous les fichiers selon la tâche d'analyse. Cette variante fournit une protection maximale.
- Les options **Types choisis** et **Masques utilisateur** commandent de contrôler uniquement les fichiers dont les dont les noms ou extensions sont listés dans la partie droite de l'onglet. Pour activer cette liste, cochez la case correspondante.

  Par défaut, la liste comprend les extensions principales des fichiers pouvant transporter des virus ainsi que les principaux types d'archive. Vous pouvez également éditer cette liste.

Configuration de la liste des fichiers à analyser

1. Pour ajouter un élément dans la liste des fichiers analysés :

   a) Sélectionnez l'un des rubriques suivantes et spécifiez le mode d'analyse avec les paramètres listés ci-après :

   - pour établir la liste d'extensions des fichiers analysés, sélectionnez l'option **Types choisis** et saisissez les extensions dans le champ se trouvant au-dessus de la liste ;
   - pour spécifier les fichiers de type spécifique pour l'analyse, sélectionnez l'option **Masques utilisateur** et saisissez un masque déterminant les fichiers en question dans le champ se trouvant au-dessus de la liste.

   ▸ Pour en savoir plus sur les masques

   Un masque est un modèle permettant de définir un objet. Le masque peut contenir des symboles autorisés à être utilisés dans les noms de fichiers ainsi que des symboles spécifiques :

   - * remplace toute séquence (y compris une séquence vide) de n'importe quel symbole ;
   - ? remplace un symbole dans la position définie.

   Exemples :

- **rapport*.doc** est un masque déterminant tous les documents de Microsoft Word dont le nom commence par la séquence `rapport`, par exemple, il spécifie les fichiers suivants : rapport-fevrier`.doc`, rapport`121209.doc` etc. ;
- ***.exe** est un masque déterminant tous les exécutables ayant l'extension `EXE`, par exemple `setup.exe`, `iTunes.exe` etc. ;
- **photo????09.jpg** est un masque déterminant tous les fichiers au format `JPG` dont le nom commence par la séquence `photo` et se termine par la sequence numérique `09` et qui contiennent entre les deux encore 4 symboles non déterminés,par exemple `photo121209.jpg`, `photomama09.jpg` ou `photo----09.jpg`.

b) Cliquez sur **Ajouter**.

c) Si nécessaire, reproduisez les étapes a) et b) pour ajouter d'autres types de fichiers ou masques utilisateur.

2. Pour enlever un élément de la liste des fichiers analysés, sélectionnez-le dans la liste et cliquez sur **Supprimer**.
3. Pour restaurer la liste définie par défaut, cliquez sur le bouton **Par défaut**.

Ici, vous pouvez également programmer l'analyse des archives et du courrier électronique :

- Cochez la case **Archives** pour déballer les archives et analyser les fichiers qui y sont contenus.

Si cette option est activée, ceci augmente considérablement la charge sur l'ordinateur.

- Cochez la case **Courrier électronique** pour vérifier les fichiers des clients de messagerie qui conservent les messages en texte brut. Si vous n'utilisez pas ce type de client de messagerie, décochez la case.

L'analyse des fichiers email peut augmenter considérablement la charge sur la machine.

Pour prévenir toute intrusion des virus avec les messages e-mail, utilisez le moniteur de courrier **SpIDer Mail**.

4.2.3.3. Onglet Actions

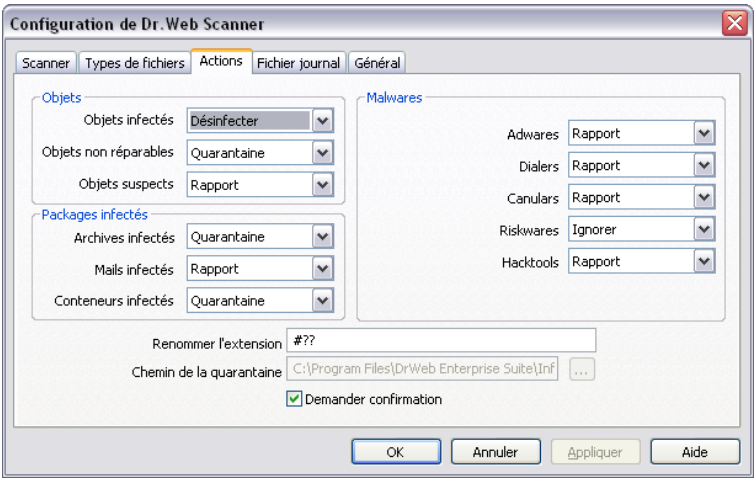


Figure 4-8. Fenêtre de configuration du Dr.Web Scanner. Onglet Actions.

Pour afficher la rubrique d'aide sur un paramètre situé dans un autre onglet, cliquez sur l'onglet correspondant dans l'illustration

Sur l'onglet **Actions**, vous pouvez configurer les réactions du **Scanner** lors de la détection des fichiers contaminés ou suspects, des programmes malicieux et des archives infectées.

Pour chaque catégorie, une réaction est spécifiée séparément :

- **Objets** :
  - infectés par des virus connus et (supposé) désinfectables ;
  - infectés par des virus incurables ;

- potentiellement infectés (objets suspects).

◆ **Malwares**.

◆ **Packages contaminés** (archives, fichiers email, conteneurs).

Par défaut, le **Scanner** vous informe uniquement lorsqu'il détecte un virus connu ou lorsqu'il y a une suspicion d'infection (voir aussi Actions en cas de détection de menaces). Les données concernant tous les objets infectés ou suspects s'affichent dans le champ de rapport, dans lequel vous pouvez sélectionner manuellement une action.

Les réactions ci-dessous peuvent être appliquées aux objets malveillants détectés :

Action	Description
Désinfecter	Commande au **Scanner** de tenter de restaurer l'état d'origine d'un objet avant son infection. Si l'objet est incurable ou que la tentative de désinfection a échoué, l'action dédiée aux virus incurables est appliquée. Cette action est possible pour les virus connus seulement, sauf les Trojan qui sont supprimés lors de leur détection et les fichiers infectés au sein des objets complexes (archives, fichiers email ou conteneurs de fichiers). C'est la seule action applicable aux secteurs d'amorçage contaminés.
Supprimer	Commande au **Scanner** de supprimer l'objet. Cette action n'est pas applicable aux secteurs d'amorçage.
Renommer	Commande au **Scanner** de renommer l'extension d'un fichier infecté ou suspect en fonction du masque spécifié dans le champ **Renommer l'extension** (par défaut, c'est #??, i.e. que le premier caractère de l'extension est remplacé par #). Cette action n'est pas applicable aux secteurs d'amorçage.
Quarantaine	Commande au **Scanner** de déplacer un objet vers le dossier quarantaine spécifié dans le champ **Chemin de la quarantaine** (par défaut, le sous-dossier `infected.!!!` dans le dossier d'installation de **Dr.Web**). Cette action n'est pas applicable aux secteurs d'amorçage.

Action	Description
Ignorer	Commande au **Scanner** d'ignorer l'objet sans lui appliquer aucune action ni afficher aucune information dans le rapport d'analyse. (Valable unqiuement pour les malwares dont adware, dialers, canulars, hacktools et riskware).

Si un objet malicieux est détecté dans une archive, une réaction définie pour les archives sera appliquées. L'action est appliquée à tout l'archive et non seulement à l'objet infecté qu'elle contient.

Pour achever la désinfection de certains fichiers contaminés, un redémarrage de Windows est requis.

L'invite de redémarrage configurée par l'administrateur sur le **Serveur** antivirus peut avoir plusieurs options : un redémarrage automatique, une demande à l'utilisateur de redémarrer la machine ou un refus de redémarrage.

4.2.3.4. Onglet Fichier journal

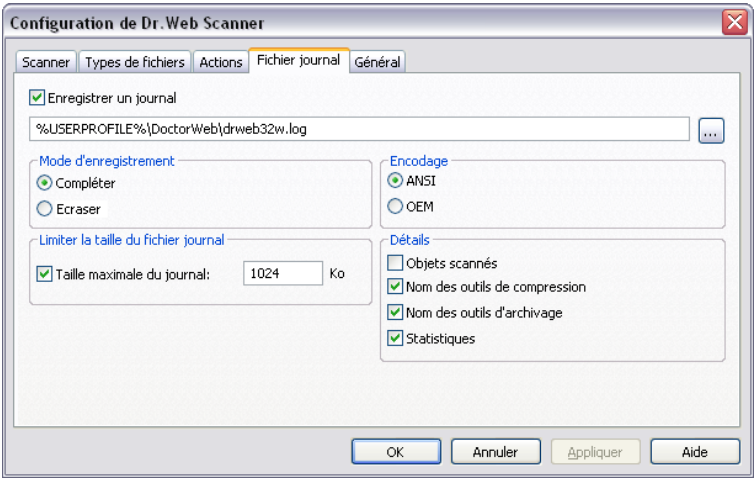


Figure 4-9. Fenêtre de configuration du Dr.Web Scanner. Onglet Fichier Journal.

Pour afficher la rubrique d'aide sur un paramètre situé dans un autre onglet, cliquez sur l'onglet correspondant dans l'illustration

Sur l'onglet **Fichier Journal** vous pouvez configurer les paramètres relatifs à l'écriture dans le fichier de log du **Scanner**.

Cochez la case **Enregistrer un journal** pour activer la journalisation.

Par défaut, l'écriture dans le journal est activée et le fichier de log `DRWEB32W.log` se trouve dans le dossier `%USERPROFILE%\DoctorWeb`.

Vous pouvez configurer les paramètres d'écriture dans le fichier de log :

- La rubrique **Mode d'enregistrement** permet de définir un mode d'écriture dans le fichier de log :
  - **Compléter** – commande au **Scanner** d'ajouter de nouvelles entrées à la fin du fichier journal ;

- **Ecraser** – commande d'écraser le fichier journal à chaque démarrage du **Scanner**.

◆ Cochez la case **Taille maximale du journal** pour spécifier une limitation pour la taille du fichier de log. La taille du fichier sera inférieure ou égale à la valeur mise dans le champ **Ko**.

Lorsque la taille dépasse la valeur maximale spécifiée, le fichier est écrasé.

◆ Dans la rubrique **Encodage**, vous pouvez choisir un codage pour le fichier de log :

- **ANSI** – utiliser le codage ANSI (Windows);
- **OEM** – utiliser le codage OEM (DOS).

◆ La rubrique **Détails** permet de choisir des informations complémentaires à écrire dans le fichier de log.

Lorsque l'enregistrement du fichier journal est activé, même si aucune autre case n'est activée, les messages sur la détection des objets suspects ou contaminés sont enregistrés y compris les noms des virus et des modifications virales (pour les objets suspects, la classification des codes suspects selon l'analyseur heuristiques), ainsi que les actions réalisées.

Pour écrire dans le fichier de log des informations détallées, cochez les cases suivantes :

- **Objets scannés** - enregistrer les noms de tous les objets scannés, pour les objets sains, ajouter une note **Ok** (ce mode peut augmenter considérablement le volume du fichier). Par défaut, cette option est désactivée.
- **Nom des outils de compression** - enregistrer les messages sur la détection des fichiers exécutables compressés par des outils spécifiques ainsi que les noms des outils de compression correspondants. Par défaut, cette option est désactivée.
- **Nom des outils d'archviage** - enregistrer les messages sur les archives scannées et sur les outils d'archivage correspondants ainsi que sur les erreurs liées avec ces archives (par exemple, en cas de déballage échoué d'une archive protégée par un mot de passe). Par défaut, cette option est désactivée.

- **Statistiques** - enregistrer des statistiques relatives au fonctionnement du logiciel lors du processus de scan et durant la session courante du **Scanner**.

4.2.3.5. Onglet Général

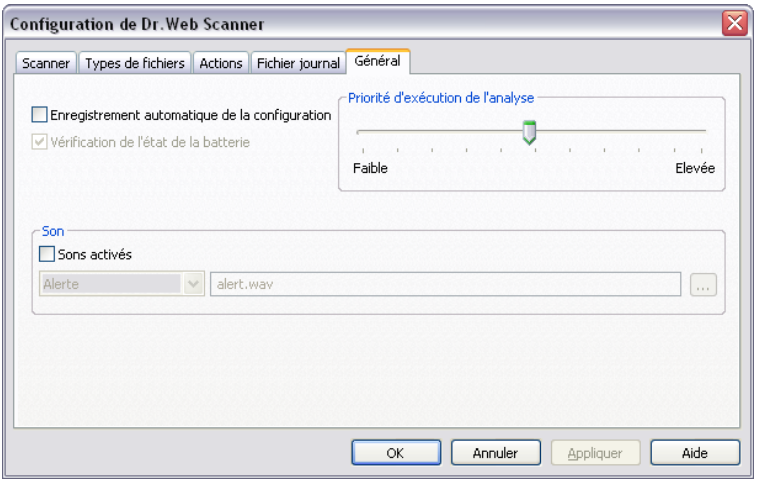


Figure 4-10. Fenêtre de configuration du Dr.Web Scanner. Onglet Général.

Pour afficher la rubrique d'aide sur un paramètre situé dans un autre onglet, cliquez sur l'onglet correspondant dans l'illustration

Sur l'onglet **Général**, vous pouvez configurer les paramètres d'interaction du logiciel avec le système d'exploitation ainsi que les effets sonores pour des événements différents.

- La case **Enregistrement automatique de la configuration** lorsqu'elle est cochée, commande au **Scanner** de sauvegarder les modifications de paramètres en quittant. Sinon, les changements sont appliqués uniquement lors de la session courante du **Scanner** et seront remis en l'état initial a son prochaine démarrage.

  Vous pouvez également spécifier de manière explicite de sauvegarder la configuration, en sélectionnant l'option

Enregistrer la configuration à l'onglet **Options** de la fenêtre principal du **Scanner**.

- La case **Vérification de l'état de la batterie**, lorsqu'elle est sélectionnée, commande au **Scanner** de verifier si votre ordinateur peut être alimenté de la batterie pour commencer le scan. L'option est valable uniquement pour les ordinateurs portables.
- Le curseur **Priorité d'exécution de l'analyse** permet de modifier la priorité du processus de scan dans le système.
- Dans la rubrique **Sons**, vous pouvez configurer les alertes sonores ou associer des sons à des évenements. Par défaut, les alertes sonores sont désactivées.
  - Cochez la case **Sons activés** afin d'activer les alertes sonores du **Scanner**.
  - Si vous souhaitez modifier un son défini par défaut, sélectionnez dans la liste déroulante un événement nécessaire et spécifiez le fichier sonore souhaité dans le champ à droite.

4.2.4. Scan en mode ligne de commande

Vous pouvez lancer **Dr.Web Scanner pour Windows** en mode ligne de commande. Ce mode vous permet de configurer les paramètres nécessaires pour la session courante de scan ainsi qu'une liste des objets à scanner spécifiés avec les clés correspondantes. C'est en mode ligne de commande que vous pouvez réaliser le démarrage du **Scanner** selon la planification de manière automatique.

La commande de démarrage a la syntaxe suivante :

`[<chemin_vers_le_programme>]drweb32w [<objets>] [<clés>]`

La liste des objets à scanner peut être vide ou peut contenir plusieurs éléments séparés par des espaces.

Les variantes des objets à scanner listées ci-dessous sont les plus fréquemment utilisées :

- `*` – scanner tous les disques durs ;

- `C:` – scanner le disque `C:` ;
- `D:\games` – scanner les fichiers dans le répertoire spécifié ;
- `C:\games\*` – scanner tous les fichiers et sous -dossiers dans le répertoire `C:\games` ;

Les paramètres sont les clés de la ligne de commande déterminant la configuration du programme. Si aucune clé n'est présente, le scan sera réalisé avec les paramètres enregistrés précédemment (ou avec les paramètres définis par défaut s'ils n'ont pas été modifiés).

Chaque paramètre de ce type commence par le symbole /, les clés sont séparées par des espaces.

Les clés les plus souvent utilisées sont listées ci-dessous. Pour la liste complète des clés, consultez l'Annexe A.

- `/cu` – désinfecter les objets infectés ;
- `/icm` – déplacer les fichiers incurables (dans le dossier défini par défaut) ;
- `/icr` – renommer (par défaut) ;
- `/qu` – fermer la fenêtre du **Scanner** après la fin de session ;
- `/go` – n'afficher aucune requête.

Les deux derniers paramètres sont surtout utiles en cas de lancement automatique du **Scanner** (par exemple, selon la planification).

Les mêmes paramètres peuvent être utilisés avec le **Dr.Web Scanner en ligne de commande pour Windows DrWebWcl**. Dans ce cas, à la place de `drweb32w`, il faut taper la commande `drwebwcl`.

Par défaut, le **Scanner en ligne de commande DrWebWcl** utilise les mêmes paramètres que la version GUI du **Scanner**. Les paramètres spécifiés avec des outils de l'interface graphique du **Scanner** (voir Configuration du Scanner Dr.Web) sont également utilisés lors du processus du scan en mode ligne de commande à condition que d'autres valeurs des paramètres ne soient pas spécifiées sous forme des clés.

4.2.5. Le Scanner en ligne de commande

Le jeu de composants de **Dr.Web Antivirus** inclut également le **Scanner en ligne de commande DWScancl**. A la différence du **Scanner en ligne de commande DrWebWcl**, ce scanner offre à l'utilisateur des possibilités avancées de configuration (jeu étendu de paramètres) et il est destiné aux systèmes à plusieurs processeurs.

Le **Scanner en ligne de commande DWScancl** ne met pas les fichiers suspects d'être malveillants dans le dossier `infected.!!!`, mais il les place dans la **Quarantaine**.

Afin de lancer le **Scanner en ligne de commande DWScancl**, utilisez la commande suivante :

[<*chemin_vers_le_programme*>]`dwscancl` [<*clés*>] [<*objets*>]

Chaque clé commence par le symbole `/`, pluiseurs clés sont séparées par des espaces. La liste des objets à scanner peut être vide ou peut contenir plusieurs éléments séparés par des espaces.

Pour la liste des clés du **Scanner en ligne de commande DWScancl**, consultez l'Annexe A.

Codes de retour :

0 – le scan est achevé avec succès, aucun objet infecté n'a pas été détecté.

1 – le scan est achevé avec succès, des objets infectés ont été trouvés.

10 – des clés invalides sont spécifiées.

11 – le fichier clé est introuvable ou ne supporte pas le **Scanner en ligne de commande DWScancl**.

12 – le **Scanning Engine** n'est pas lancé.

255 – le processus de scan a été interrompu par l'utilisateur.

Chapitre 5. Quarantaine

Pour afficher ou modifier le contenu de la **Quarantaine**, sélectionnez l'élément **Quarantaine** depuis le menu contextuel **de l'Agent**. Une fenêtre contenant un récapitulatif sur le statut de la **Quarantaine** va s'ouvrir.

La **Quarantaine** de l'antivirus **Dr.Web** sert à isoler les fichiers suspectés d'être malveillants.

Les dossiers de **Quarantaine** sont crées sur chaque disque logique sur lequel des fichiers suspects ont été détectés. Un dossier de **Quarantaine** portant le nom `DrWeb Quarantine` est crée dans la racine du disque sous forme de dossier caché. L'utilisateur n'a pas de droits d'accès aux fichiers contenus dans le dossier de **Quarantaine**.

En cas de détection d'un objet contaminé sur un support amovible sur lequel l'écriture est autorisée, un dossier `DrWeb Quarantine` sera crée sur ce support et l'objet détecté sera déplacé vers ce dossier.

Les fichiers de **Quarantaine** se trouvant sur le disque dur sont sauvegardés sous forme encryptée.

Les fichiers de **Quarantaine** se trouvant sur un support amovible seront enregistrés en clair.

Les postes avec le module de **Quarantaine** installé doivent fonctionner sous les OS permettant d'installer **SpIDer Guard G3** (voir Pré-requis système).

Sinon la **Quarantaine** ne pourra pas gérer les fichiers dans le dossier `Infected.!!!` (se trouvant dans le dossier d'installation de l'**Antivirus**) et les informations sur le contenu de la **Quarantaine** ne seront pas envoyées au **Serveur**.

Des informations sur les objets contaminés déplacés vers le répertoire de **Quarantaine** sur un support amovible sont accessibles uniquement dans la **Quarantaine** locale sur le poste (à condition que le support amovible soit connecté au

poste) et elles sont inaccessibles pour la gestion à distance depuis le **Serveur**.

5.1. Configuration de l'interface

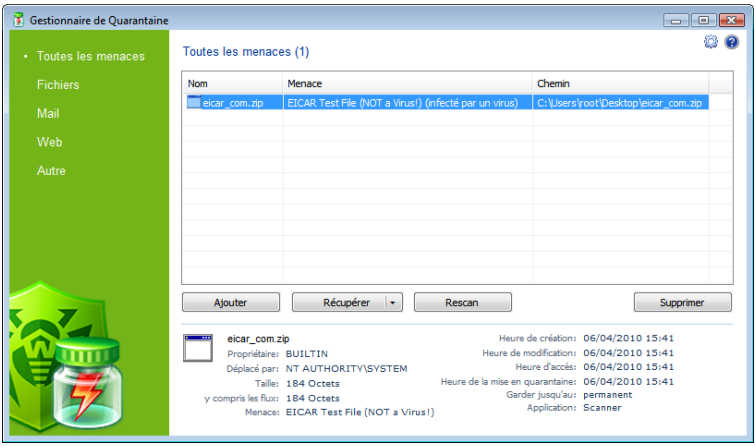


Figure 5-1. Fenêtre de la Quarantaine

La partie centrale de la fenêtre affiche un récapitulatif contenant les informations sur le statut de la Quarantaine et notamment les champs suivants :

- **Nom** - la liste des objets se trouvant dans la **Quarantaine**,
- **Menace** - une catégorie de programme malveillant attribuée par l'**Antivirus** lors du déplacement automatique d'un objet vers la **Quarantaine**,
- **Chemin** - le chemin détaillé vers l'objet avant son déplacement vers la **Quarantaine**.

Il est également possible d'afficher des informations détaillées sur l'objet comme dans la partie basse de la fenêtre de la **Quarantaine**.

La marche à suivre pour paramétrer l'affichage des informations dans les colonnes :

1. Faites afficher le menu contextuel des en-têtes du tableau des objets, pour cela, cliquez droit sur un en-tête.
2. Depuis le menu contextuel sélectionnez **Personnaliser les colonnes**.
3. Dans la fenêtre qui apparaît, cochez les cases contre les éléments à inclure dans le tableau des objets. Afin de supprimer des colonnes du tableau des objets, décochez les cases contre les éléments respectifs.
    a) Pour cocher toutes les cases, cliquez sur le bouton **Cocher tout**.
    b) Pour désélectionner tous les éléments, cliquez sur **Décocher tout**.
4. Pour modifier l'ordre des colonnes dans le tableau, sélectionnez une colonne à déplacer et cliquez ensuite sur un des boutons décrits ci-dessous :
    a) **Déplacer vers le haut** – pour déplacer la colonne vers le haut du tableau (plus haut dans la liste des paramètres et vers la gauche dans le tableau des objets).
    b) **Déplacer vers le bas** – pour déplacer la colonne vers la fin du tableau (plus bas dans la liste des paramètres et vers la droite dans le tableau des objets).
5. Pour sauvegarder les modifications apportées aux paramètres des colonnes, cliquez sur le bouton **OK**, pour fermer la fenêtre sans sauvegarder les modifications, cliquez sur **Annuler**.

En bas de la fenêtre de la **Quarantaine**, des informations détaillées sur les objets sélectionnés de la **Quarantaine** seront affichées.

5.2. Configuration des propriétés de la quarantaine

Pour paramétrer les propriétés de la Quarantaine :

1. Cliquez sur le bouton  **Paramètres** dans la fenêtre de la **Quarantaine**.
2. La fenêtre **Propriétés de la Quarantaine** vous permet de modifier les paramètres suivants :
   - La rubrique **Spécifier la taille de la Quarantaine** permet de gérer l'espace destiné au dossier de **Quarantaine**. Utilisez le curseur pour modifier la taille maximum de la **Quarantaine**, la taille maximum est calculée par rapport à l'espace total du disque (en cas de plusieurs disques logiques, la taille sera calculée séparément pour chaque disque sur lequel se trouvent des dossiers de **Quarantaine**). La valeur `100%` correspond à une taille maximum illimitée du dossier de **Quarantaine.**
   - Dans la rubrique **Aperçu**, cochez la case **Afficher les copies de backup** afin d'afficher dans le tableau des objets les copies de backup des fichiers se trouvant dans la **Quarantaine**.
3. Après la fin du paramétrage, cliquez sur **OK** pour sauvegarder les modifications apportées ou sur le bouton **Annuler**, pour annuler les modifications.

Les copies de backup seront automatiquement créées lors des déplacements des fichiers vers la **Quarantaine**. Même si les fichiers sont sauvegardés dans la **Quarantaine** **de façon permanente**, leurs copies de backup ne seront conservées que **temporairement** (voir aussi la rubrique Vidage de la Quarantaine).

Pour afficher la rubrique d'aide, cliquez sur le bouton  .

5.3. Gestion du contenu de la quarantaine

Le panneau latéral de gauche sert au filtrage des objets de la **Quarantaine** à afficher. Après avoir cliqué sur un élément, dans la partie centrale de la fenêtre seront affichés soit tous les objets de la **Quarantaine**, soit des groupes d'objets spécifiés : fichiers, objets de mail, pages web ou d'autres objets non listés dans les catégories définies.

La fenêtre de la **Quarantaine** permet aux utilisateurs d'afficher les fichiers conformément à leurs droits d'accès.

Afin de pouvoir afficher les objets cachés, veuillez lancer en tant qu'administrateur soit le fichier de **Quarantaine** `dwqrui.exe` se trouvant dans le répertoire d'installation, soit l'interface de **Dr.Web Agent** (voir le paragraphe Lancement et arrêt de l'interface Dr.Web Agent).

La fenêtre de la **Quarantaine** permet d'accéder aux boutons suivants :

- **Ajouter** - ajouter un fichier dans la **Quarantaine**. Avec le navigateur de fichiers qui s'ouvre, sélectionnez le fichier nécessaire.
- **Récupérer** - déplacer un fichier depuis la **Quarantaine** et restaurer l'emplacement d'origine du fichier sur le poste (le restaurer sous le nom d'origine et dans le dossier dans lequel il était avant son déplacement vers la **Quarantaine**).

Utilisez cette option uniquement si vous êtes sûr que l'objet n'est pas dangereux.

Dans le menu déroulant, vous pouvez choisir l'option **Restaurer vers** - déplacer un fichier sous le nom spécifié vers le dossier donné par l'administrateur.

- **Rescan** - rescanner un fichier se trouvant dans la

Quarantaine. Si lors du rescan, le fichier s'avère sain, la **Quarantaine** proposera de récupérer ce fichier.

- **Supprimer** - supprimer un fichier dans la **Quarantaine** et dans le système.

Pour appliquer une action à un groupe d'objets, sélectionnez les objets dans la fenêtre de la **Quarantaine**, en tenant pressée la touche SHIFT ou CTRL, puis cliquez droit sur une ligne du tableau, puis, dans le menu déroulant, sélectionnez une action à effectuer.

5.4. Vidage de la quarantaine

Vidage automatique de la Quarantaine

En cas de dépassement de la capacité du disque, le vidage automatique de la **Quarantaine** est effectué :

1. En premier lieu, les copies de backup des fichiers de **Quarantaine** seront supprimées.
2. S'il manque de l'espace sur le disque, les fichiers de **Quarantaine** dont la durée de conservation a expiré seront également supprimés.

Si la **Quarantaine** est débordée et que le vidage automatique n'est pas disponible, le déplacement des fichiers vers la **Quarantaine** ne sera pas possible. Dans ce cas, vous pouvez élargir la taille de la **Quarantaine** dans la rubrique **Propriétés de la quarantaine** → **Spécifier la taille de la Quarantaine** ou supprimer les fichiers depuis la **Quarantaine** manuellement.

Vidage complet de la Quarantaine

Il existe deux possibilités pour supprimer tout le contenu de la **Quarantaine** :

1. Ouvrez le gestionnaire de **Quarantaine** à l'aide du menu contextuel **de l'Agent** et sélectionnez l'élément **Quarantaine**. Sélectionnez tous les fichiers dans la fenêtre de la **Quarantaine** et cliquez sur le bouton **Supprimer**.
2. Utilisez la fonction système **Disk Cleanup** pour nettoyer le disque.

   a) Cette fonction peut être exécutée de la manière suivante :

   - sous OS plus ancien que Windows Vista :
     - menu **Démarrer** → **Programmes** → **Accessoires** → **Outils système** → **Nettoyage de disque**.
     - Via l'explorateur de fichiers : dans le menu contextuel du disque sur lequel vous voulez effacer la **Quarantaine**, sélectionnez **Propriétés** → **Nettoyage de disque**.
   - Sous OS Windows Vista et Windows 7 : menu **Démarrer** → **Programmes** → **Accessoires** → **Outils système** → **Nettoyage de disque**.
   - Sous OS Windows 8: menu **Applications** (peut être ouvert via l'élément Toutes les applications sur la barre d'applications de l'écran d'accueil) → section **Administration** → élément **Nettoyage de disque**.

   S'il y a plusieurs lecteurs logiques, sélectionnez le lecteur sur lequel vous voulez effacer la **Quarantaine**.

   b) Dans la fenêtre **Nettoyage de disque** qui va s'ouvrir, dans la liste **Fichiers à supprimer**, cochez la case contre l'élément **Quarantaine Dr.Web**, puis cliquez sur **OK**. Le contenu de la **Quarantaine** sera supprimé.

Chapitre 6. Dr.Web Firewall

Le pare-feu **Dr.Web Firewall** est conçu pour protéger vote ordinateur contre l'accès non autorisé de l'extérieur ainsi que contre la fuite de données importantes depuis votre ordinateur via le réseau. Ce composant vous permet de contrôler la connexion et la transmission de données via Internet et de bloquer des connexions suspectes au niveau des packages et des applications.

Durant une certaine période après l'installation, **Dr.Web Firewall** fonctionne en mode d'apprentissage. Le mode d'apprentissage du pare-feu est décrit dans le Guide **Antivirus Dr.Web pour Windows**, dans la rubrique **Apprentissage du Pare-feu Dr.Web**.

Pour consulter la rubrique d'aide **Antivirus Dr.Web pour Windows**, cliquez sur la touche F1 dans toute fenêtre du Pare-feu.

Le menu contextuel de **l'Agent** vous permet :

1. D'accéder à la configuration du Pare-feu.
2. De consulter le journal du Pare-feu.

6.1. Configuration de Dr.Web Firewall

Pour afficher ou modifier les paramètres du pare-feu **Dr.Web Firewall**, sélectionnez l'élément **Configuration du Firewall** dans le menu contextuel de **l'Agent**.

L'élément **Configuration du Firewall** est disponible depuis le menu contextuel de **l'Agent** à condition que l'utilisateur dispose des droits d'administrateur sur l'ordinateur.

La fenêtre de la configuration de **Dr.Web Firewall** va s'ouvrir. Pour en savoir plus sur la gestion du composant **Dr.Web Firewall**, merci de consulter le Guide **Antivirus Dr.Web pour Windows**, au

paragraphe **Paramètres du pare-feu**.

Pour afficher la rubrique d'aide **Antivirus Dr.Web pour Windows**, pressez la touche F1 dans toute fenêtre du Pare-feu.

6.2. Journal de Dr.Web Firewall

Pour afficher le log du pare-feu **Dr.Web Firewall**, sélectionnez l'élément **Journal du Firewall** dans le menu contextuel de **l'Agent**.

L'élément **Journal du Firewall** est disponible depuis le menu contextuel de **l'Agent** à condition que l'utilisateur dispose des droits d'administrateur sur l'ordinateur.

La fenêtre du log du Pare-feu **Dr.Web Firewall** va s'ouvrir. Pour en savoir plus sur le log de **Dr.Web Firewall**, merci de consulter le Guide **Antivirus Dr.Web pour Windows**, au paragraphe **Log des événements**.

Pour consulter la Rubrique d'aide **Antivirus Dr.Web pour Windows**, pressez la touche F1 dans toute fenêtre du Pare-feu.

Chapitre 7. Office Control

Le module **Dr.Web Office Control** permet de restreindre l'accès des utilisateurs aux ressources locales et sites web spécifiés. Cette fonction assure non seulement le contrôle de l'intégrité des fichiers importants et leur protection contre la contamination par des virus, mais également la protection des données confidentielles sauvegardées sur votre ordinateur.

Il existe une possibilité de protéger des fichiers spécifiés ainsi que les dossiers se trouvant sur les disques locaux ou sur des lecteurs externes connectés à la machine. Il est possible de bloquer toute consultation des informations sur les supports externes.

Par défaut, le moniteur bloque l'accès aux dossiers de l'antivirus **Dr.Web**. Utilisez les paramètres pour configurer le module.

En fonctions des paramètres spécifiés sur le **Serveur**, vous pouvez paramétrer le module **Office Control**.

Même si l'utilisateur est autorisé à contrôler l'accès aux ressources, l'administrateur peut modifier les paramètres sur le **Serveur**. Les paramètres spécifiés sur le **Serveur** seront mis à jour automatiquement sur le poste de l'utilisateur.

Pour modifier les paramètres du module :

1. Depuis le menu contextuel de **l'Agent** sélectionnez l'élément **Configuration d'Office Control**.

L'élément **Configuration d'Office Control** est disponible dans le menu contextuel de l'**Agent** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier ces paramètres. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur le PC.

2. Entrez le mot de passe pour le module **Office Control**.

La liste des ressources est protégée contre l'édition par un mot de passe spécifié lors de la configuration initiale du module de **Office Control**. Vous pouvez changer de mot de passe dans la fenêtre de la configuration du module ou contacter pour cela votre administrateur.

Pour changer de mot de passe, pressez le bouton **Changer de mot de passe** se trouvant dans la fenêtre de la configuration.

3. Pour la rubrique d'aide sur les paramètres se trouvant sur l'onglet, cliquez sur le bouton  (**Aide**).
4. Apportez les modifications nécessaires sur les onglets de paramètres :
   - **Filtre d'URL** (consultez les informations détaillées dans la Rubrique d'aide **Antivirus Dr.Web pour Windows**, **Rubrique Filtre d'URL**).
   - **Accès local** (consultez les informations détaillées dans la Rubrique d'aide **Antivirus Dr.Web pour Windows**, **Rubrique Accès local**).

   Pour consulter la Rubrique d'aide **Antivirus Dr.Web pour Windows**, pressez la touche F1 dans toute fenêtre d'**Office Control**.
5. Cliquez sur le bouton **Appliquer** pour sauvegarder les modifications apportées sans fermer la fenêtre des paramètres.
6. A la fin de l'édition des paramètres, cliquez sur **OK** pour sauvegarder toutes les modifications apportées ou sur le bouton **Annuler** - pour annuler les modifications et fermer ensuite la fenêtre des paramètres.

Chapitre 8. SpIDer Gate

Le moniteur HTTP **SpIDer Gate** permet de protéger votre PC contre les malwares qui sont propagés via le protocole HTTP. Le protocole HTTP est utilisé par les navigateurs web, les gestionnaires de téléchargement et par d'autres applications recevant des données depuis le réseau Internet. De tels programmes sont également appelés clients HTTP.

Par défaut, **SpIDer Gate** est inclus dans le jeu de composants installés et reste en permanence en mémoire, il redémarre en cas de redémarrage de Windows.

Les paramètres de **SpIDer Gate** vous permettent de désactiver l'analyse du trafic entrant ou sortant, vous pouvez également créer une liste d'applications dont le trafic HTTP (informations transmises via le protocole HTTP) sera toujours analysé complètement. Il existe une possibilité d'exclure de l'analyse le trafic de certaines applications, à spécifier.

La modification de la configuration du moniteur HTTP **SpIDer Gate** peut être autorisée ou interdite par l'administrateur de **Dr.Web Enterprise Security Suite**. Pour consulter ou modifier la configuration du moniteur **SpIDer Gate**, sélectionnez dans le menu contextuel de l'**Agent** l'élément **Configuration de SpIDer Gate**.

L'élément **Configuration de SpIDer Gate** est disponible depuis le menu de l'**Agent** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier ces paramètres. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur le PC.

Paramétré par défaut, le moniteur HTTP analyse tout le trafic HTTP. Vous pouvez modifier les paramètres du module.

Pour plus d'information sur la gestion du gardien **SpIDer Gate**, merci de consulter le Guide **Dr.Web Antivirus pour Window,** le chapitre **Configurer SpIDer Gate**.

Pour afficher la rubrique d'aide **Dr.Web Antivirus pour Windows**, pressez la touche F1 dans n'importe quelle fenêtre du moniteur.

Chapitre 9. SpIDer Guard

SpIDer Guard est un gardien antivirus (nommé aussi moniteur de fichiers). L'application reste en permanence en mémoire vive et effectue le scan à la volée des fichiers, elle détecte également toute activité virale.

SpIDer Guard démarre automatiquement à chaque démarrage du système d'exploitation. Le moniteur en cours d'exécution ne peut pas être déchargé durant la session ouverte du système. Au besoin (par exemple en cas d'exécution d'une tâche sensible à la charge du processeur en temps réel) vous pouvez mettre en pause l'analyse des fichiers à la volée.

Paramétré par défaut, le gardien **SpIDer Guard** analyse à la volée tous les fichiers modifiés ou créés ainsi que les secteurs de démarrage, il vérifie également tous les fichiers ouverts sur les supports amovibles et sur les disques réseau. Le processus de scan ressemble au fonctionnement du **Scanner Dr.Web**, mais les critères d'analyse sont moins stricts. De plus, le gardien **SpIDer Guard** surveille de façon permanente les processus en cours d'exécution afin de détecter des activités ressemblantes à l'activité virale et en cas de détection de menaces, il bloque les processus concernés.

En cas de détection d'objets infectés, le gardien **SpIDer Guard** applique à ces objets des actions définies par les paramètres spécifiés. Les paramètres permettent de configurer une réaction automatique du gardien si des événements viraux surviennent.

Configuration du gardien

La rubrique des paramètres du gardien **SpIDer Guard** varie en fonction de la version installée. Il existe deux versions du gardien **SpIDer Guard** :

- SpIDer Guard G3,
- SpIDer Guard NT.

Avant l'installation, la version du système d'exploitation sera automatiquement reconnue et une version respective de **SpIDer Guard** sera installée (voir le paragraphe Pré-requis système).

9.1. Configuration de SpIDer Guard G3

La configuration du programme est optimale dans la plupart des cas, il est déconseillé de la modifier sans nécessité.

En option, les paramètres disponibles de SpIDer Guard :

1. Depuis le menu contextuel de **l'Agent** sélectionnez l'élément **Configuration de SpIDer Guard**.

L'élément **Configuration de SpIDer Guard** est disponible depuis le menu contextuel de l'**Agent** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier ces paramètres. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur le PC.

2. La fenêtre de la configuration sera ouverte en vous proposant les onglets suivants :
   - l'onglet Général permet de configurer le mode d'analyse des fichiers et des processus sur le poste protégé,
   - l'onglet Actions permet de paramétrer des réactions du gardien **SpIDer Guard** en cas de détection de fichiers suspects ou infectés ou de programmes malveillants,
   - l'onglet Exclusions permet de configurer une liste de dossiers et de fichiers à exclure de l'analyse par le gardien **SpIDer Guard**,
   - l'onglet Log permet de paramétrer le mode d'écriture dans le fichier de log du gardien **SpIDer Guard**.
3. Apportez les modifications nécessaires.

4. A la fin de l'édition des paramètres, cliquez sur le bouton **OK** pour sauvegarder les modifications apportées ou sur le bouton **Annuler** pour annuler les modifications.

Pour afficher la rubrique d'aide sur la fenêtre active de configuration de **SpIDer Guard**, pressez la touche F1. Pour la rubrique d'aide contextuelle sur un élément de la fenêtre, cliquez droit sur cet élément.

9.1.1. Onglet Général

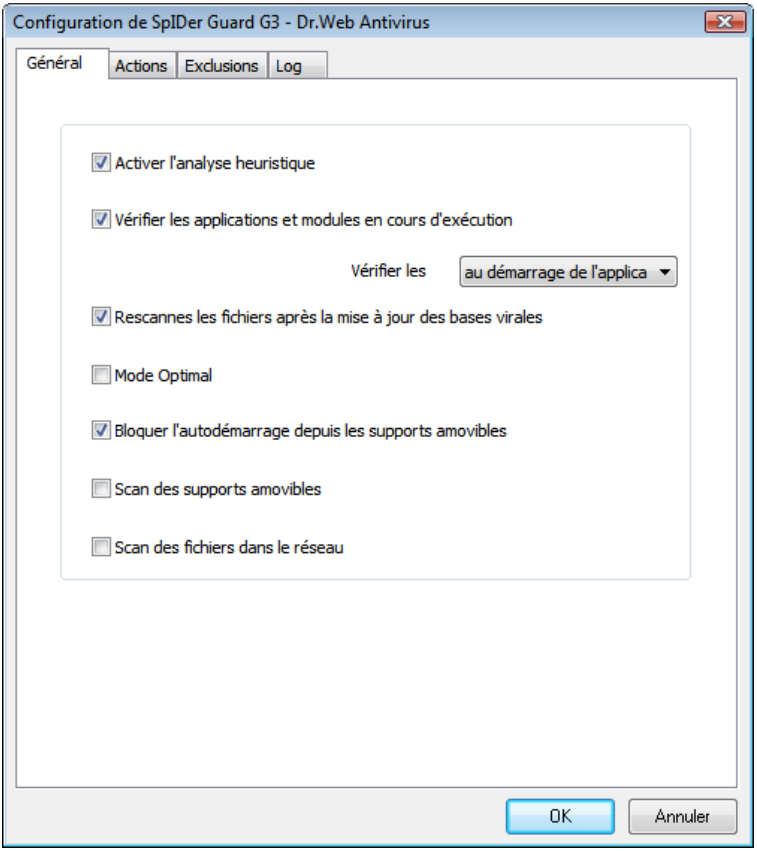


Figure 9-1. Fenêtre de configuration de SpIDer Guard. Onglet Général.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet **Général** permet de configurer le mode d'analyse des fichiers et des processus sur un poste protégé :

- Cochez la case **Activer l'analyse heuristique** pour effectuer une analyse avec le moteur heuristique.

  Décochez la case pour effectuer une analyse par signatures des virus connus seulement (voir aussi la rubrique **Méthodes de détection des virus** dans le Guide **Antivirus Dr.Web pour Windows**).

- La case cochée **Vérifier les applications et modules en cours d'exécution** active l'analyse des fichiers et applications lancées. Pour paramétrer le mode d'analyse des fichiers des processus lancés, sélectionnez un élément dans la liste déroulante :
  - **en tâche de fond** - pour vérifier les modules en tâche de fond, après leur démarrage lorsque les modules sont déjà en cours d'exécution.
  - **au démarrage de l'application** - pour vérifier les modules avant leur démarrage.
- La case cochée **Rescanner les fichiers après la mise à jour des bases virales** assure une reprise du processus d'analyse de tous les modules actifs chargés et des fichiers infectés immédiatement après la mise à jour des bases virales. Si la case est décochée, seuls les fichiers infectés seront vérifiés dès que les bases virales seront à jour.
- La case **Mode Optimal** active le mode d'analyse déterminant le scan d'objets par le gardien **SpIDer Guard** en fonction des actions appliquées à un objet :
  - Si la case **Mode Optimal** est cochée, les fichiers sur les disques durs seront scannés uniquement lors de certaines consultations de fichiers : à l'exécution, à la création, lors des tentatives d'écrire (lire) dans (depuis) des fichiers ou dans des secteurs de démarrage.

- Si la case **Mode Optimal** n'est pas cochée, l'analyse des fichiers sur les disques durs sera effectuée lors de tous types d'accès aux fichiers : à l'exécution, à la création, lors de l'écriture (tentatives d'écrire) dans les fichiers existants ou dans des secteurs de démarrage ainsi que lors de toute ouverture des fichiers y compris l'ouverture en lecture seule.

La désactivation du **Mode Optimal** assure un maximum de protection mais entraîne une augmentation importante de la charge sur l'ordinateur.

Les modes d'analyse des fichiers se trouvant sur les supports amovibles ou sur les lecteurs réseau sont paramétrés séparément avec les cases **Scan des supports amovibles** et **Scan des fichiers dans le réseau**.

▸ Précisions et recommandations

Il est recommandé d'activer le **Mode Optimal** après avoir réalisé une analyse méticuleuse de tous les disques durs avec le **Scanner Dr.Web**. Ceci permet d'éliminer tout possibilité d'intrusion sur l'ordinateur de nouveaux virus ou d'autres programmes malveillants depuis des supports amovibles. Ainsi, les objets sains et déjà vérifiés ne seront pas rescannés.

La réaction du gardien **SpIDer Guard** en cas de détection d'objets malveillants peut être paramétrée dans l'onglet Actions.

Certains lecteurs externes (notamment les disques dotés d'une interface usb) peuvent se présenter dans le système en tant que disques durs. Il est recommandé d'utiliser de tels lecteurs avec précaution et d'effectuer une analyse antivirus avec le **Scanner Dr.Web** des lecteurs connectés à l'ordinateur.

◆ La case cochée **Bloquer l'autodémarrage depuis les supports amovibles** bloque le démarrage automatique des applications depuis des supports amovibles. Ceci permet de protéger votre ordinateur contre le lancement de programmes

malveillants pouvant se trouver sur des supports amovibles.

- Cochez la case **Scan des supports amovibles** pour activer l'analyse des fichiers se trouvant sur des supports amovibles (disques CD/DVD, FDD, lecteurs flash et d'autres supports pouvant se connecter via le port USB) à chaque consultation de tels fichiers, y compris l'ouverture en lecture seule.

  Si la case **Scan des supports amovibles** est décochée, les fichiers sur les supports amovibles ne seront scannés que lors de leur exécution.

- Cochez la case **Scan des fichiers dans le réseau** pour vérifier les objets sur les lecteurs réseau lors de leur exécution ainsi qu'à chaque consultation, y compris l'ouverture en lecture seule.

  Si la case **Scan des fichiers dans le réseau** est décochée, les fichiers sur les lecteurs réseau ne seront scannés que lors de leur exécution sur votre poste de travail.

9.1.2. Onglet Actions

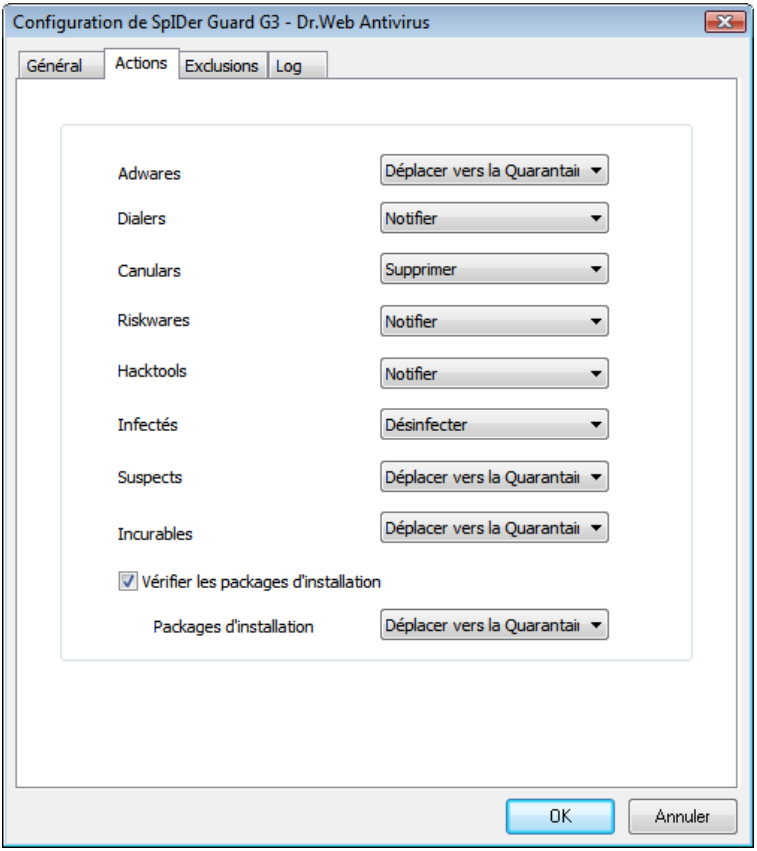


Figure 9-2. Fenêtre de configuration de SpIDer Guard. Onglet Actions.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet **Actions** permet de paramétrer la réaction du gardien **SpIDer Guard** en cas de détection de fichiers suspects ou infectés ainsi que de programmes malveillants. Le jeu de réactions disponibles est

fonction du type de l'événement viral.

Les actions listées ci-dessous peuvent être paramétrées pour être appliquées aux objets détectés :

- **Désinfecter** - réparer l'objet infecté afin de le restaurer dans son état initial, avant la contamination. En cas de désinfection impossible, l'action sélectionnée pour les objets incurables sera appliquée.

  Cette action ne peut être appliquée qu'aux objets infectés par un virus connu et curable, excepté les trojans et les fichiers infectés contenus dans des objets composés (archives, fichiers de mail, conteneurs de fichiers).

- **Supprimer** - supprimer les objets infectés.
- **Déplacer vers la Quarantaine** - déplacer les objets infectés vers le dossier de Quarantaine.
- **Notifier** - notifier sur la détection de virus (la procédure de paramétrage des notifications est décrite ci-après).
- **Ignorer** - laisser passer l'objet sans réaction, aucune notification ne sera affichée.

L'option **Ignorer** ne prévoit aucune action à réaliser : aucun avertissement ne sera affiché à l'utilisateur comme par exemple en cas de détection d'un objet malveillant si l'option **Notifier** est activée.

Tableau 3. Actions de SpIDer Guard applicables aux objets malicieux détectés

Objet	Action				
	Désinfecter	Supprimer	Quarantaine	Notifier	Ignorer
Adwares		+	+/*	+	+
Dialers		+	+	+/*	+
Canulars		+/*	+	+	+
Riskwares		+	+	+/*	+
Hacktools		+	+	+/*	+

Objet	Action				
	Désinfecter	Supprimer	Quarantaine	Notifier	Ignorer
Infectés	+/*	+	+		
Suspects		+	+/*	+	+
Incurables		+	+/*		
Packages d'installation		+	+/*	+	+

Légende

+	l'action est autorisée pour ce type d'objets
+/*	l'action est spécifiée en tant que réaction par défaut pour ce type d'objets

Utilisez les paramètres listés ci-dessous pour configurer les actions à appliquer aux objets malveillants déctectés :

- La liste déroulante **Adwares** permet de paramétrer une réaction de **SpIDer Guard** en cas de détection de ce type de programmes.
- La réaction de **SpIDer Guard** peut être paramétrée de façon analogue pour s'appliquer à d'autres types de malwares :
  - dialers,
  - canulars,
  - riskwares,
  - hacktools.
- La liste déroulante **Infectés** permet de configurer une réaction de **SpIDer Guard** en cas de détection d'un fichier infecté par un virus connu.
- La liste déroulante **Suspects** permet de configurer une réaction de **SpIDer Guard** en cas de détection d'un fichier suspecté d'être contaminé par un virus (selon le moteur heuristique).
- La liste déroulante **Incurables** permet de configurer une réaction de **SpIDer Guard** en cas de détection d'un fichier infecté par un virus incurable (ou dans le cas où une tentative de réparer le fichier a échoué).
- L'option **Vérifier les packages d'installation** permet de spécifier l'analyse à la volée des fichiers d'installation.

Lors du paramétrage de cette option, dans la liste déroulante **Packages d'installation**, sélectionnez une action à effectuer en cas de détection d'objets malveillants dans des packages d'installation.

Configuration des notifications

A la fin de l'action spécifiée, le gardien **SpIDer Guard** affiche par défaut une notification dans la zone de notification de la barre des tâches Windows. Vous pouvez activer ou désactiver l'affichage des notifications.

Pour paramétrer les notifications du gardien **SpIDer Guard**, dans le menu contextuel de **l'Agent,** sélectionnez l'élément **Configuration**, puis cochez ou décochez la case **Notifications virales** afin de recevoir ou de ne pas recevoir les notifications.

9.1.3. Onglet Exclusions

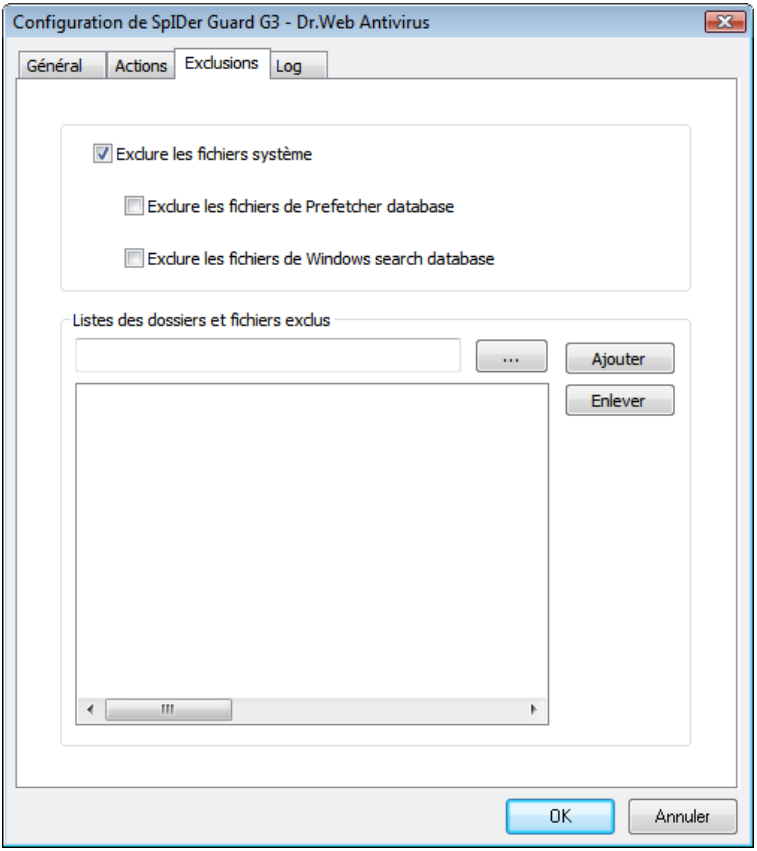


Figure 9-3. Fenêtre de configuration de SpIDer Guard. Onglet Exclusions.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet **Exclusions** permet de spécifier la liste des dossiers et fichiers à ne pas faire analyser par le gardien **SpIDer Guard**.

La case **Exclure les fichiers système** enjoint d'exclure de l'analyse les fichiers système répertoriés dans la liste interne du composant **SpIDer Guard**. Cette liste est rédigée pour chaque version de Windows selon les recommandations de Microsoft® relatives à l'utilisation des logiciels antivirus.

Cochez la case **Exclure les fichiers système** pour accéder aux éléments suivants :

- La case **Exclure les fichiers de Prefetcher database** permet d'exclure de l'analyse les fichiers de la bases de données du composant système Prefetcher (le composant du système d'exploitation Microsoft Windows, qui accelère son premier démarrage et raccourcit le temps de lancement des programmes par l'enregistrement de l'information utilisée au cours du lancement).
- La case **Exclure les fichiers de Windows search database** permet d'exclure de l'analyse les fichiers de la base de données du service de recherche Windows.

La rubrique **Listes des dossiers et fichiers exclus** contient une liste des dossiers et fichiers à ne pas faire analyser par **SpIDer Guard.** Ces listes peuvent contenir les dossiers de **Quarantaine** de l'antivirus, des dossiers de programmes, des fichiers temporaires (fichiers d'échange ou swap) etc.

Les listes sont vides par défaut. Vous pouvez ajouter aux exclusions des dossiers et fichiers ou utiliser des masques pour ne pas analyser un groupe d'objets spécifiés.

Création des listes d'exclusions

1. Pour ajouter un dossier ou un fichier dans la liste des exclusions, suivez une des instructions ci-dessous :
   - pour spécifier un dossier ou un fichier existant, cliquez sur le bouton  et sélectionnez ensuite le dossier ou le fichier avec l'explorateur de fichiers qui s'ouvre. Vous pouvez également saisir le chemin complet vers le fichier ou vers le dossier dans le champ de saisie ;

- afin d'exclure de l'analyse tous les fichiers ou dossiers portant un nom défini, entrez ce nom dans le champ de saisie. Il n'est pas nécessaire de spécifier le chemin vers le dossier ou fichier ;
- afin d'exclure de l'analyse un type de fichier ou de dossier, entrez dans le champ de saisie le masque respectif.

▸ Pour en savoir plus sur les masques

Un masque est un modèle permettant de définir un objet. Le masque peut contenir des symboles autorisés à être utilisés dans les noms de fichiers ainsi que des symboles spécifiques :

- `*` remplace toute séquence (y compris une séquence vide) de n'importe quel symbole ;
- `?` remplace un symbole dans la position définie.

Exemples :

- **rapport*.doc** est un masque déterminant tous les documents de Microsoft Word dont le nom commence par la séquence `rapport`, par exemple, il spécifie les fichiers suivants : `rapport-fevrier.doc`, `rapport121209.doc` etc. ;
- ***.exe** est un masque déterminant tous les exécutables ayant l'extension `EXE`, par exemple `setup.exe`, `iTunes.exe` etc. ;
- **photo????09.jpg** est un masque déterminant tous les fichiers au format `JPG` dont le nom commence par la séquence `photo` et se termine par la sequence numérique `09` et qui contiennent entre les deux encore 4 symboles non déterminés,par exemple `photo121209.jpg`, `photomama09.jpg` ou `photo----09.jpg`.

2. Cliquez sur le bouton **Ajouter**.
3. Si nécessaire, reprenez les étapes 1 et 2 pour ajouter d'autres fichiers ou dossiers.
4. Pour supprimer un fichier ou un dossier de la liste des exclusions, sélectionnez l'élément correspondant dans la liste et cliquez sur le bouton **Supprimer**.

9.1.4. Onglet Log

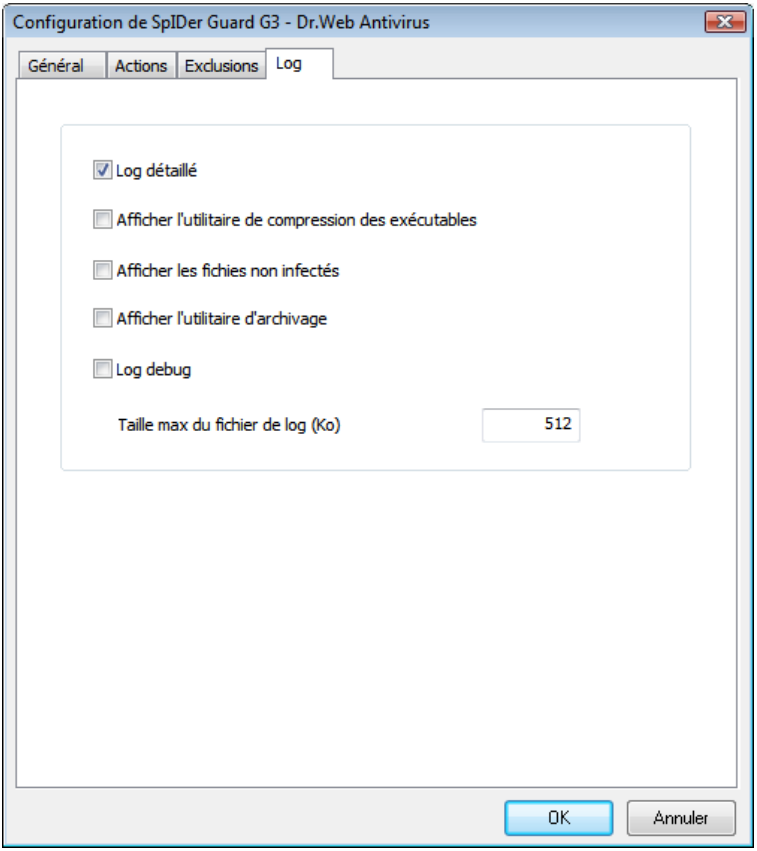


Figure 9-4. Fenêtre de configuration de SpIDer Guard. Onglet Log.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet **Log** permet de paramétrer le mode d'écriture dans le fichier de log et de spécifier les informations à enregistrer dans le fichier de log.

Le journal du gardien **SpIDer Guard** est sauvegardé dans le fichier `spiderg3.log` se trouvant dans le répertoire d'installation **Dr.Web Enterprise Security Suite**.

Il est recommandé d'analyser périodiquement le fichier de log.

Afin de paramétrer le niveau de détail du journal, cochez les cases respectives associées au niveau de détail du journal et aux types d'informations à écrire dans le fichier de log.

Les cases suivantes servent à paramétrer le mode de journalisation :

- **Log détaillé** – à part des événements généraux, ce mode de journalisation assure l'écriture d'informations détaillées sur les objets analysés. Ce mode est recommandé pour déterminer les objets les plus fréquemment vérifiés par le gardien **SpIDer Guard**. Si nécessaire, vous pouvez ajouter ces objets dans la liste des exclusions pour diminuer la charge sur l'ordinateur ;
- **Log debug** – ce mode permet d'enregistrer le maximum d'information sur le fonctionnement du gardien **SpIDer Guard**, ceci peut augmenter considérablement la taille du fichier de log. Il est recommandé de n'utiliser ce mode que lorsque des problèmes de fonctionnement de **SpIDer Guard** surviennent ou en cas de demande du support technique de **Doctor Web**.

Les cases listées ci-dessous permettent de paramétrer le type d'informations à enregistrer dans le log :

- **Afficher l'utilitaire de compression des exécutables** - pour enregistrer les messages sur la détection des fichiers exécutables compressés par des utilitaires de compression ainsi que les noms de ces utilitaires. La case est décochée par défaut.
- **Afficher les fichiers non infectés** - pour enregistrer les noms de tous les objets vérifiés y compris les objets sains pour lesquels la note `Ok` sera affichée (ce mode peut augmenter considérablement la taille du fichier de log). La case est décochée par défaut.

- **Afficher l'utilitaire d'archivage** - pour enregistrer les messages sur les archives vérifiées ainsi que sur les utilitaires d'archivage par lesquels elles ont été traitées, pour enregistrer des erreurs associées (par exemple sur un échec d'extraction de l'archive protégée par un mot de passe). La case est décochée par défaut.

La case **Taille max du fichier de log** permet de limiter la taille du fichier de log d'une valeur maximale spécifiée en Ko.

9.2. Configuration de SpIDer Guard NT4

La configuration du programme est optimale dans la plupart des cas, il est déconseillé de la modifier sans nécessité.

La marche à suivre pour paramétrer le moniteur de fichiers SpIDer Guard :

L'élément **Configuration de SpIDer Guard** est disponible depuis le menu contextuel de l'**Agent** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier ces paramètres. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur le PC.

1. Afin d'afficher ou de modifier les paramètres du scan, sélectionnez dans le menu contextuel de **l'Agent** l'élément **Configuration de SpIDer Guard** → **Options de l'analyse**. Pour en savoir plus, merci de consulter la rubrique Options de l'analyse.
2. Pour consulter ou modifier les paramètres de démarrage du gardien, sa configuration et les notifications sur les événements, veuillez sélectionner dans le menu contextuel de **l'Agent** l'élément **Configuration de SpIDer Guard** → **Contrôle**. Pour en savoir plus sur le système de contrôle du moniteur, consultez la rubrique Contrôle.

3. A la fin de l'éditon des paramètres, cliquez sur **OK** pour sauvegarder les modifications apportées ou sur le bouton **Annuler** pour les annuler.

Pour afficher la rubrique d'aide sur une fenêtre active, dans toutes les boîtes de dialogue pressez la touche F1. Pour la rubrique d'aide contextuelle sur un élément de la fenêtre, cliquez droit sur cet élément.

9.2.1. Configuration du scan

La configuration du programme est optimale dans la plupart des cas, il est déconseillé de la modifier sans nécessité.

La marche à suivre pour configurer le moniteur de fichiers SpIDer Guard :

1. Depuis le menu contextuel de **l'Agent** sélectionnez l'élément **Configuration de SpIDer Guard** → **Options de l'analyse**.

L'élément **Configuration de SpIDer Guard** est disponible depuis le menu contextuel de l'**Agent** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier ces paramètres. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur le PC.

2. La fenêtre de la configuration s'ouvrira et vous permettra d'accéder aux onglets suivants :
   - l'onglet Options de l'analyse permet de paramétrer le mode d'analyse des fichiers et des processus sur le poste protégé ;
   - l'onglet Types de fichiers permet de paramétrer l'ensemble des fichiers à vérifier par le gardien conformément aux conditions spécifiées à l'onglet Options de l'analyse ;

- l'onglet Actions permet de paramétrer une réaction du gardien **SpIDer Guard** en cas de détection d'objets infectés ou suspects ainsi que de programmes malveillants ;
- l'onglet Fichier journal permet de paramétrer le mode d'écriture dans le fichier de log du gardien **SpIDer Guard** ;
- l'onglet Exclusions permet de paramétrer une liste des dossiers et des fichiers à ne pas faire analyser par le gardien **SpIDer Guard**.

3. Apporter les modifications nécessaires.
4. A la fin de l'édition, cliquez sur le bouton **OK** pour sauvegarder les modifications ou sur le bouton **Annuler** pour les annuler.

9.2.1.1. Onglet Options de l'analyse

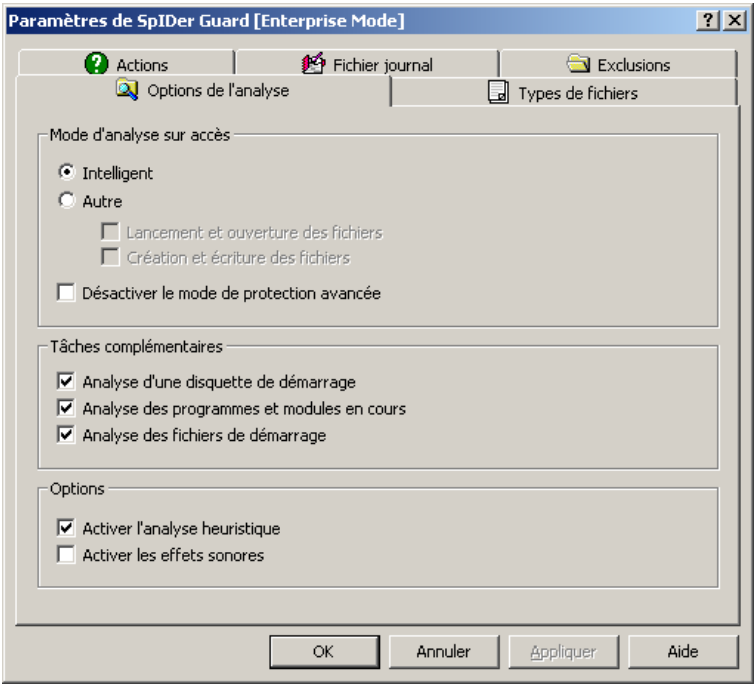


Figure 9-5. Fenêtre de configuration de SpIDer Guard. Onglet Options de l'analyse.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet **Options de l'analyse** permet de configurer le mode d'analyse des fichiers et dossiers sur un poste protégé.

Mode d'analyse "à la volée" (sur accès)

La rubrique **Mode d'analyse sur accès** permet de configurer un mode d'analyse de sorte que le scan d'objets par le gardien **SpIDer Guard** soit fonction des actions appliquées à un objet :

- Si la case **Intelligent** est cochée, le scan des fichiers et secteurs de démarrage sur les disques durs ne sera effectué que lors de certaines consultations de ces fichiers : à l'exécution, à la création d'un fichier, lors de l'écriture (tentative d'écriture) dans des fichiers existants ou dans des secteurs de démarrage.

  Cependant, le scan des fichiers se trouvant sur des supports amovibles ou sur des lecteurs réseau sera effectué lors de tout type d'accès aux fichiers : à l'exécution, à la création d'un fichier, lors de l'écriture (tentative d'écriture) dans des fichiers existants, ainsi que lors de toute ouverture des fichiers y compris l'ouverture en lecture seule.

- Si la case **Autre** est cochée, les variantes suivantes sont disponibles :
  - **lancement et ouverture des fichiers** - si la case est cochée, tous les fichiers seront analysés lors de leur exécution et de leur ouverture y compris l'ouverture en lecture seule.
  - **Création et écriture des fichiers** - si la case est cochée, tous les fichiers seront analysés à leur création et lors de l'écriture (tentative d'écriture) dans des fichiers existants ou dans des secteurs de démarrage.

  Les options envisagées vous permettent de configurer un niveau de protection nécessaire sur votre ordinateur.

Si vous cochez les deux cases **Lancement et ouverture des fichiers** et **Création et écriture des fichiers** en même temps, le niveau maximum de protection sera assuré mais la charge sur l'ordinateur sera considérablement augmentée.

▸ Précisions et recommandations

Il est recommandé d'activer le mode **Intelligent** après l'analyse de tous les disques durs avec le **Scanner Dr.Web**. Ceci permet d'éliminer toute intrusion de nouveaux virus ou d'autres programmes malveillants sur l'ordinateur via des supports amovibles, en revanche, le rescan des objets sains ne sera pas effectué.

La réaction du gardien **SpIDer Guard** en cas de détection d'objets malicieux peut être configurée dans l'onglet Actions.

Certains lecteurs externes (notamment les disques durs dotés d'une interface usb) peuvent se présenter dans le système en tant que disques durs. Il est recommandé d'utiliser de tels lecteurs avec précaution et d'effectuer une analyse antivirus avec le **Scanner Dr.Web** des lecteurs connectés à l'ordinateur.

- La case **Désactiver le mode de protection avancée** permet de désactiver le mode de protection avancée. Ce mode est activé par défaut. Si le mode est activé, le gardien vérifie en temps réel tous les fichiers, dont l'analyse est spécifiée dans les paramètres de l'application. Tous les autres fichiers seront mis en file d'attente pour analyse ultérieure (les fichiers ouverts en lecture dans les modes **Intelligent** et **Création et écriture des fichiers**). Ces fichiers seront analysés par le gardien dès que des ressources système seront libérées.

Options supplémentaires

- la case **Analyse d'une disquette de démarrage** permet de vérifier si une disquette est insérée dans le lecteur, si oui, cette disquette sera scannée (une disquette infectée peut contaminer l'ordinateur lors de son démarrage).
- la case **Analyser des programmes et modules en cours** active l'analyse des fichiers et applications en cours d'exécution.
- la case **Analyse des fichiers de démarrage** active le scan de tous les fichiers du dossier Démarrage (le dossier Démarrage, fichiers système .ini, la base de registre Windows).

Paramètres

- Cochez la case **Activer l'analyse heuristique** pour activer le moteur heuristique.

Décochez la case pour réaliser l'analyse par signatures des virus connus seulement (voir aussi le paragraphe **Méthodes de détection des virus** dans le Guide **Antivirus Dr.Web pour Windows**).

- La case **Activer les effets sonores** active l'utilisation de réactions sonores du gardien. Les sons sont désactivés par défaut.

9.2.1.2. Onglet Types de fichiers

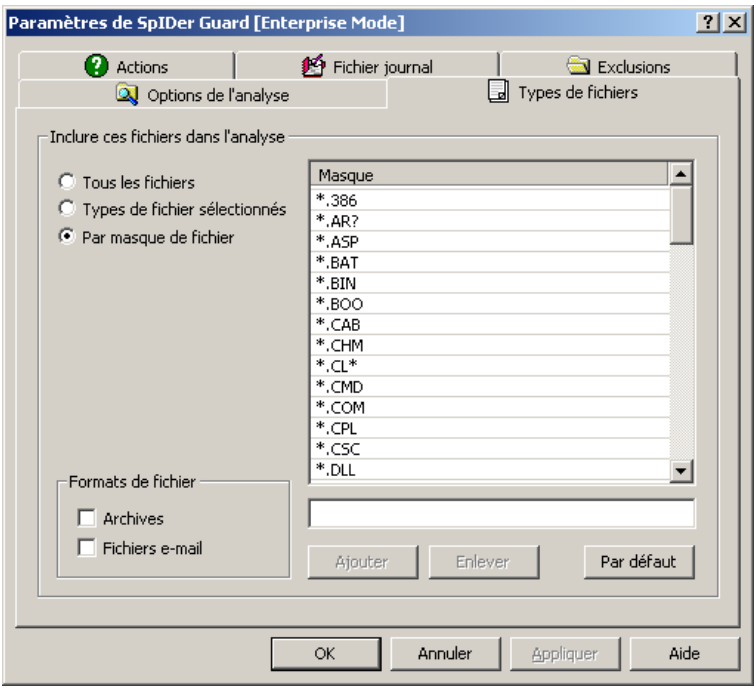


Figure 9-6. Fenêtre de configuration de SpIDer Guard. Onglet Types de fichiers.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet **Types de fichiers** permet de configurer le jeu de fichiers à analyser selon les critères spécifiés dans l'onglet Options de l'analyse.

La rubrique **Inclure ces fichiers dans l'analyse** vous permet de sélectionner les types de fichiers à scanner par le gardien :

- La case **Tous les fichiers** est cochée par défaut et active l'analyse de tous les fichiers selon les critères définis dans l'onglet Options de l'analyse. Cette variante assure le maximum de protection.
- Les cases **Types de fichiers sélectionnés** et **Par masque de fichier** activent le scan des fichiers dont les noms ou les extensions sont mentionnés dans la liste se trouvant dans la partie droite de l'onglet. La liste sera activée si une de ces cases est cochée.

  Par défaut, la liste comprend les extensions des principaux types de fichiers pouvant être porteurs de virus, elle contient également les principaux types d'archives de fichiers. Vous pouvez éditer cette liste.

Création de la liste des fichiers à analyser

1. Pour ajouter un élément dans la liste des fichiers analysés :

   a) Sélectionnez l'un des rubriques suivantes et spécifiez le mode d'analyse avec les paramètres listés ci-après :

   - pour établir la liste d'extensions des fichiers analysés, sélectionnez l'option **Types de fichiers sélectionnés** et saisissez les extensions dans le champ se trouvant au-dessous de la liste ;
   - pour spécifier les fichiers de type spécifique pour l'analyse, sélectionnez l'option **Par masque de fichier** et saisissez un masque déterminant les fichiers en question dans le champ se trouvant au-dessous de la liste.

   ▸ Pour en savoir plus sur les masques

   Un masque est un modèle permettant de définir un objet. Le masque peut contenir des symboles autorisés à être utilisés dans les noms de fichiers ainsi que des symboles spécifiques :

- * remplace toute séquence (y compris une séquence vide) de n'importe quel symbole ;
- ? remplace un symbole dans la position définie.

Exemples :

- **rapport*.doc** est un masque déterminant tous les documents de Microsoft Word dont le nom commence par la séquence `rapport`, par exemple, il spécifie les fichiers suivants : rapport-fevrier`.doc`, rapport`121209.doc` etc. ;
- ***.exe** est un masque déterminant tous les exécutables ayant l'extension `EXE`, par exemple `setup.exe`, `iTunes.exe` etc. ;
- **photo????09.jpg** est un masque déterminant tous les fichiers au format `JPG` dont le nom commence par la séquence `photo` et se termine par la sequence numérique `09` et qui contiennent entre les deux encore 4 symboles non déterminés,par exemple `photo121209.jpg`, `photomama09.jpg` ou `photo----09.jpg`.

b) Cliquez sur **Ajouter**.

c) Si nécessaire, reproduisez les étapes a) et b) pour ajouter d'autres types de fichiers ou masques utilisateur.

2. Pour enlever un élément de la liste des fichiers analysés, sélectionnez-le dans la liste et cliquez sur **Supprimer**.
3. Pour restaurer la liste définie par défaut, cliquez sur le bouton **Par défaut**.

Dans la rubrique **Formats de fichier** vous pouvez paramétrer le mode d'analyse des archives et des fichiers de mail :

- Cochez la case **Archives** afin d'activer l'analyse des fichiers archivés. Les fichiers inclus dans les archives ne sont pas analysés par défaut, même si le type ou le masque de fichier est mentionné dans la liste des types ou des masques à analyser (s'il y a un fichier infecté dans une archive, le virus sera détecté par le gardien lors de l'extraction du fichier de l'archive, avant que l'infection puisse se propager).

Etant activée, cette option augmente considérablement la charge système.

- Cochez la case **Fichiers e-mail** pour activer l'analyse des fichiers de courrier électronique. Par défaut, les boîtes aux lettres ne sont pas scannées (s'il y a un fichier infecté dans la pièce jointe, le virus sera détecté par le gardien lors de son extraction avant que l'infection puisse se propager).

Etant activée, cette option augmente considérablement la charge du processeur.

Pour la protection contre les virus propagés via le courriel, utilisez le gardien du courriel **SpIDer Mail**.

9.2.1.3. Onglet Actions

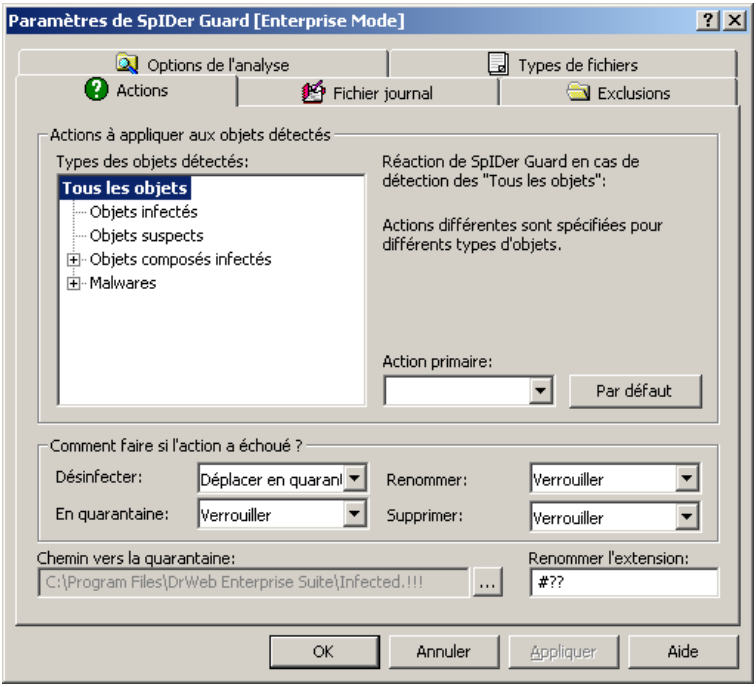


Figure 9-7. Fenêtre de configuration de SpIDer Guard. Onglet Actions.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet **Actions** permet de paramétrer la réaction du gardien **SpIDer Guard** lors de la détection de fichiers infectés ou suspects et de malwares. Le jeu de réactions disponibles est fonction du type d'événement viral.

Paramétrage des actions

Tous les types d'objet malveillants sont affichés dans l'arborescence dans la partie gauche de la fenêtre. Dès qu'un objet est sélectionné dans la liste, la partie droite de la fenêtre affiche la réaction par défaut du logiciel en cas de détection d'un tel objet. L'action paramétrée par les options actuelles ainsi que les actions à appliquer si l'action primaire à échoué seront également affichées dans cette fenêtre.

Vous pouvez modifier les réactions du programme en cas de détection de chaque type d'objet séparément.

La marche à suivre pour paramétrer les actions à appliquer aux objets malveillants détectés :

1. Pour modifier les paramètres de l'action primaire, sélectionnez dans la liste déroulante **Action primaire** une réaction primaire du programme.
2. Dans la rubrique **Comment faire si l'action a échoué** vous pouvez paramétrer les actions à exécuter en cas d'échec des actions principales suivantes : désinfecter, déplacer vers la **Quarantaine**, renommer, supprimer.

Actions disponibles

Les actions suivantes peuvent être appliquées aux objets détectés :

- **Désinfecter** - réparer l'objet infecté afin de restaurer son état antérieur à la contamination.

  Cette action ne peut être appliquée qu'aux objets infectés par un virus connu et curable, excepté les trojans et les fichiers infectés contenus dans les objets composés (archive, fichiers de mail, conteneurs de fichiers).

- **Supprimer** - supprimer les objets infectés ou suspects (aucune action ne sera appliquée aux secteurs de démarrage).

Par défaut, le logiciel n'analyse pas et ne permet pas de supprimer les archives de fichiers. Si l'analyse des archives est activée (l'activation de l'option augmente considérablement la charge système), vous pouvez autoriser la sélection de l'action **Supprimer** pour l'appliquer aux archives. Pour cela, ouvrez dans l'éditeur de texte le fichier de configuration du logiciel (`drweb32.ini` dans le répertoire d'installation) et ajoutez dans la section `[SpIDerGuardNT]` une ligne `EnableDeleteArchiveAction=Yes` (si cette ligne existe déjà, mettez `Yes` à la place de `No`) et sauvegardez ensuite le fichier.

Aucune action ne peut être appliquée directement aux fichiers contenus dans les archives. Si l'action **Supprimer** est sélectionnée, tout l'ensemble de l'archive sera supprimé.

- **Déplacer vers la Quarantaine** - déplacer les objets infectés vers le dossier de Quarantaine paramétré dans le champ **Chemin vers la Quarantaine** (par défaut le dossier `infected.!!!` est spécifié dans le répertoire d'installation).
- **Notifier** - envoyer une notification sur la détection d'un virus (dans la fenêtre Boîte de dialogue en cas de détection d'un objet infecté).
- **Verrouiller** - bloquer l'accès au fichier dont l'analyse provoque une réaction d'alerte du gardien. Le fichier sera débloqué après le redémarrage de l'ordinateur ou lorsque le contrôle sera mis en pause temporairement.
- **Ignorer** - laisser passer l'objet sans réaction, aucune notification ne sera affichée.

L'option **Ignorer** ne prévoit aucune action à réaliser : aucun avertissement ne sera affiché à l'utilisateur comme, par exemple, en cas de détection d'un objet malveillant si l'option **Notifier** est activée.

- **Renommer** - pour remplacer l'extension de l'objet infecté ou suspect selon le masque spécifié dans le champ **renommer l'extension** (par défaut les symboles `#??` seront utilisés pour remplacer le premier caractère de l'extension par le symbole `#`).

Tableau 4. Actions de SpIDer Guard applicables aux objets infectés ou suspects

Action	Objet	
	Infectés	Suspects
Désinfecter	+/*	
Supprimer	+	+
Déplacer vers la Quarantaine	+	+/*
Notifier	+	+
Verrouiller	+	+
Ignorer		+
Renommer	+	+

Tableau 5. Actions de SpIDer Guard applicables aux objets composés

Action	Objet composé		
	Archives	Fichiers de mail	Conteneurs
Déplacer vers la Quarantainte	+/*	+	+/*
Notifier	+	+/*	+
Verrouiller	+	+	+
Ignorer	+	+	+
Renommer	+	+	+

Tableau 6. Actions de SpIDer Guard applicables aux programmes malveillants

Action	Objet malicieux				
	Adwares	Dialers	Canulars	Riskwares	Hacktools
Supprimer	+	+	+	+	+

Action	Objet malicieux				
	Adwares	Dialers	Canulars	Riskwares	Hacktools
Déplacer vers la Quarantaine	+	+	+	+	+
Notifier	+/*	+/*	+/*	+	+/*
Verrouiller	+	+	+	+	+
Ignorer	+	+	+	+/*	+
Renommer	+	+	+	+	+

Légende

+	l'action est autorisée à être appliquée à ce type d'objets
+/*	l'action est spécifiée en tant que réaction primaire par défaut à appliquer à ce type d'objets

En cas de détection d'objets contenant des **adwares** et **dialers**, la réaction **Déplacer vers la Quarantaine** sera définie par défaut pour le gardien dans le package **Dr.Web pour serveurs**, pour le gardien dans le package **Dr.Web pour postes de travail,** la réaction **Notifier** sera définie par défaut.

Réaction en cas de détection

En cas de détection d'un objet infecté ou suspect, en fonction de la version du gardien les réactions suivantes sont disponibles :

- Paramétré par défaut, **SpIDer Guard** intégré dans le package **Dr.Web pour postes de travail** demande une réaction de la part de l'utilisateur. Le gardien affiche la Boîte de dialogue en cas de détection d'un objet infecté qui permet à l'utilisateur de choisir une action manuellement.
- **SpIDer Guard** intégré dans le package **Dr.Web pour serveurs** réalise automatiquement les actions définies par défaut afin de prévenir une menace virale.

9.2.1.4. Onglet Fichier journal

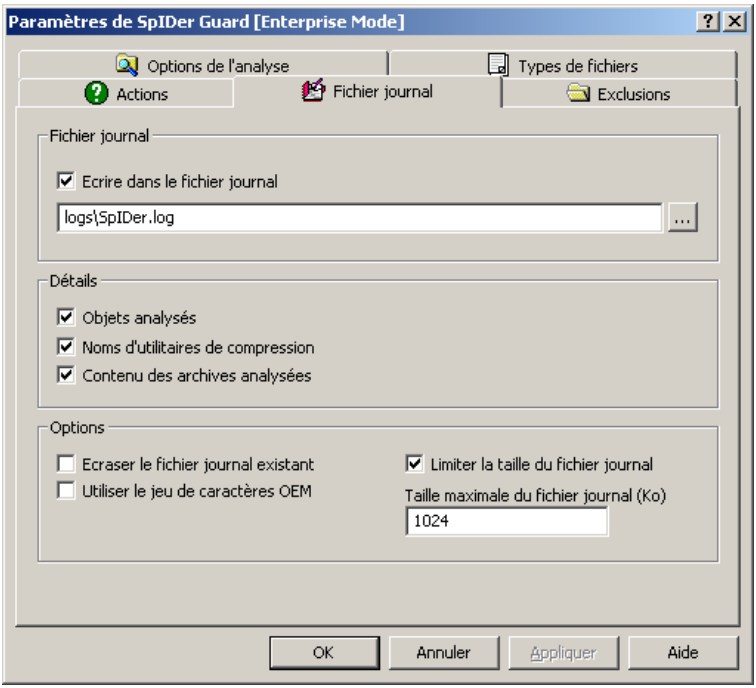


Figure 9-8. Fenêtre de configuration de SpIDer Guard. Onglet Fichier journal.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet **Fichier journal** permet de configurer le mode de journalisation et de spécifier les informations à écrire dans le fichier de log.

Il est recommandé d'effectuer l'écriture dans le fichier de log et de l'analyser périodiquement.

Fichier journal

La rubrique **Fichier journal** permet de configurer les paramètres généraux du fichier de log.

Cochez la case **Ecrire dans le fichier journal** pour enregistrer dans le fichier de log des données sur le fonctionnement du gardien **SpIDer Guard**.

Vous pouvez également spécifier le nom et l'emplacement du fichier de log dans le champ approprié. Par défaut, le journal de **SpIDer Guard** sera sauvegardé vers `logs/SpIDer.log` se trouvant dans le répertoire d'installation **Dr.Web Enterprise Security Suite**.

Détails

La rubrique **Détails** sert à paramétrer les informations supplémentaires à écrire dans le journal.

Le niveau de détails du journal peut être configuré avec les cases suivantes :

- **Objets analysés** - pour enregistrer les noms de tous les objets vérifiés y compris les objets sains pour lesquels la note `Ok` sera affichée (ce mode peut augmenter considérablement la taille du fichier de log). La case est décochée par défaut.
- **Noms d'utilitaires de compression** - pour enregistrer les messages sur la détection des exécutables compressés par des outils spécifiques de compression et pour enregistrer les nom de tels outils.
- **Contenu des archives analysées** - pour enregistrer les messages sur les archives vérifiées ainsi que sur les utilitaires d'archivage par lesquels elles ont été traitées, pour enregistrer des erreurs associées (par exemple sur un échec d'extraction de l'archive protégée par un mot de passe). La case est décochée par défaut.

Options

La rubrique **Options** offre des paramètres supplémentaires d'écriture dans le fichier de log :

- Cochez la case **Ecraser le fichier journal existant** pour écraser le fichier journal périmé et écrire un nouveau journal au début de chaque session. Si la case est décochée, les informations seront enregistrées à la fin du fichier approprié.
- Cochez la case **Utiliser le jeu de caractères OEM** pour écrire dans le codage DOS.
- Si vous souhaitez limiter la taille du fichier journal, cochez la case **Limiter la taille du fichier journal** et spécifiez une taille maximale du fichier de log en Ko dans le champ **Taille maximale du fichier journal** (Ko).

9.2.1.5. Onglet Exclusions

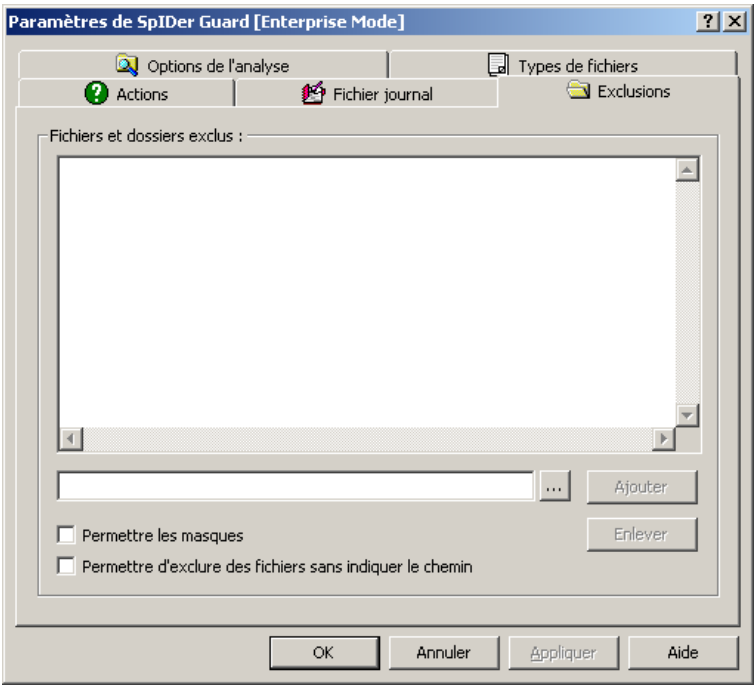


Figure 9-9. Fenêtre de configuration de SpIDer Guard. Onglet Exclusions.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet **Exclusions** permet de spécifier la listes des dossiers et fichiers à ne pas faire analyser par le gardien **SpIDer Guard**.

La rubrique **Fichiers et dossiers exclus** permet de configurer une liste des dossiers et fichiers à ne pas faire analyser par le gardien **SpIDer Guard**. La liste peut contenir les dossiers de Quarantaine de l'antivirus, des dossiers de programmes, des fichiers temporaires (fichiers d'échange ou swap) etc.

La liste est vide par défaut. Vous pouvez ajouter aux exclusions des dossiers et fichiers ou utiliser des masques pour ne pas analyser un groupe d'objets spécifiés.

Création d'une liste d'exclusions

1. Pour ajouter un dossier ou un fichier dans la liste des exclusions, suivez une des instructions ci-dessous :
   - pour spécifier un dossier ou un fichier existant, cliquez sur le bouton  et sélectionnez ensuite le dossier ou le fichier avec l'explorateur de fichiers qui s'ouvre. Vous pouvez également saisir le chemin complet vers le fichier ou vers le dossier dans le champs de saisie ;
   - afin d'exclure de l'analyse tous les fichiers ou dossiers portant un nom défini sans spécifier le chemin, cochez la case **Permettre d'exclure des fichiers sans indiquer le chemin**, puis entrez le nom dans le champ de saisie ;
   - afin d'exclure de l'analyse un type de fichier ou de dossier, cochez la case **Permettre les masques** puis entrez le masque dans le champ de saisie.

   ▸ Pour en savoir plus sur les masques

   Un masque est un modèle permettant de définir un objet. Le masque peut contenir des symboles autorisés à être utilisés dans les noms de fichiers ainsi que des symboles spécifiques :

   - `*` remplace toute séquence (y compris une séquence vide) de n'importe quel symbole ;
   - `?` remplace un symbole dans la position définie.

   Exemples :

   - **rapport*.doc** est un masque déterminant tous les documents de Microsoft Word dont le nom commence par la séquence `rapport`, par exemple, il spécifie les fichiers suivants : rapport-fevrier`.doc`, rapport`121209.doc` etc. ;
   - ***.exe** est un masque déterminant tous les exécutables ayant l'extension `EXE`, par exemple `setup.exe`, `iTunes.exe` etc. ;
   - **photo????09.jpg** est un masque déterminant tous les

fichiers au format `JPG` dont le nom commence par la séquence `photo` et se termine par la sequence numérique `09` et qui contiennent entre les deux encore 4 symboles non déterminés,par exemple `photo121209.jpg`, `photomama09.jpg` ou `photo----09.jpg`.

2. Cliquez sur le bouton **Ajouter**.
3. Si nécessaire, reprenez les étapes 1 et 2 pour ajouter de nouveaux fichiers et dossiers.
4. Pour supprimer un fichier ou un dossier de la liste des exclusions, sélectionnez l'élément correspondant dans la liste et cliquez ensuite sur le bouton **Supprimer**.

9.2.2. Contrôle

La configuration du programme est optimale dans la plupart des cas, il est déconseillé de la modifier sans nécessité.

La marche à suivre pour paramétrer le moniteur de fichiers SpIDer Guard :

1. Depuis le menu contextuel de **l'Agent,** sélectionnez l'élément **Configuration de SpIDer Guard** → **Contrôle**, sinon vous pouvez cliquer sur l'élément **SpIDer Guard** depuis le **Panneau de configuration** Windows.

L'élément **Configuration de SpIDer Guard** est disponible depuis le menu contextuel de l'**Agent** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier ces paramètres. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur le PC.

2. La fenêtre de la configuration sera ouverte en vous proposant les onglets suivants :

- Contrôle,
- Options,
- Alertes,
- Notifications.

3. Apportez les modifications nécessaires.
4. A la fin de l'édition des paramètres, cliquez sur **OK** pour sauvegarder les modifications apportées ou sur le bouton **Annuler** pour les annuler.

9.2.2.1. Onglet Contrôle

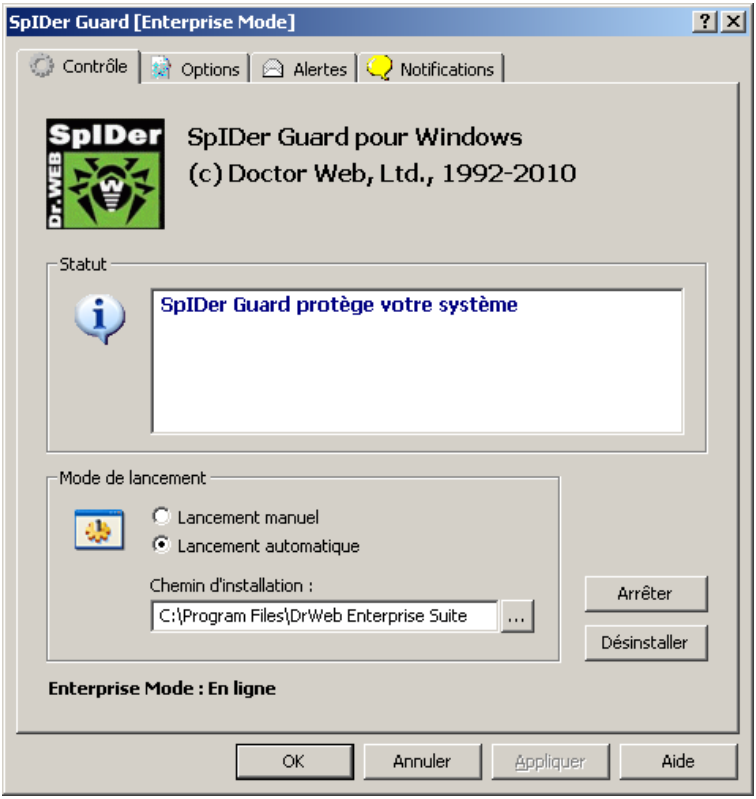


Figure 9-10. Fenêtre de Contrôle de SpIDer Guard. Onglet Contrôle.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet **Contrôle** permet de paramétrer le mode de lancement de **SpIDer Guard** ainsi que de lancer la procédure d'installation ou de désinstallation du composant dans le système d'exploitation.

La rubrique **Mode de lancement** permet de choisir un mode de démarrage du programme :

- Si le mode **Lancement manuel** est sélectionné, cliquez sur **Lancer** pour démarrer le gardien. Une fois lancé, le gardien peut être arrêté avec le bouton **Arrêter**.
- Si le mode **Lancement automatique** est sélectionné, le gardien démarre automatiquement à chaque démarrage du système.

Pour installer le gardien dans le système d'exploitation, cliquez sur le bouton **Installer**, pour annuler l'enregistrement du composant dans le système, cliquez sur le bouton **Désinstaller**.

Après l'installation de l'**Antivirus** selon les paramètres standard, l'installation du gardien sera effectuée automatiquement dès que le système démarre. Cependant, vous pouvez modifier le mode de lancement de **SpIDer Guard** si vous désactivez le mode de lancement automatique.

Pour désactiver le mode de lancement automatique de SpIDer Guard :

1. Allez sur l'onglet Contrôle dans la fenêtre de Contrôle de **SpIDer Guard**.

L'élément **Configuration de SpIDer Guard** → **Contrôle** est disponible depuis le menu contextuel de l'**Agent** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier ces paramètres. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur le PC.

2. Dans la rubrique **Mode de lancement**, sélectionnez **Mode de lancement manuel**.
3. Cliquez sur le bouton **OK**.

Ainsi, lors des démarrages ultérieurs de Windows, le programme ne sera pas lancé automatiquement. Si nécessaire, vous pouvez

le lancer manuellement. Pour cela, cliquez dans la fenêtre décrite ci-dessus sur le bouton **Installer**. Le gardien lancé manuellement peut être arrêté à l'aide du bouton **Arrêter**.

9.2.2.2. Onglet Options

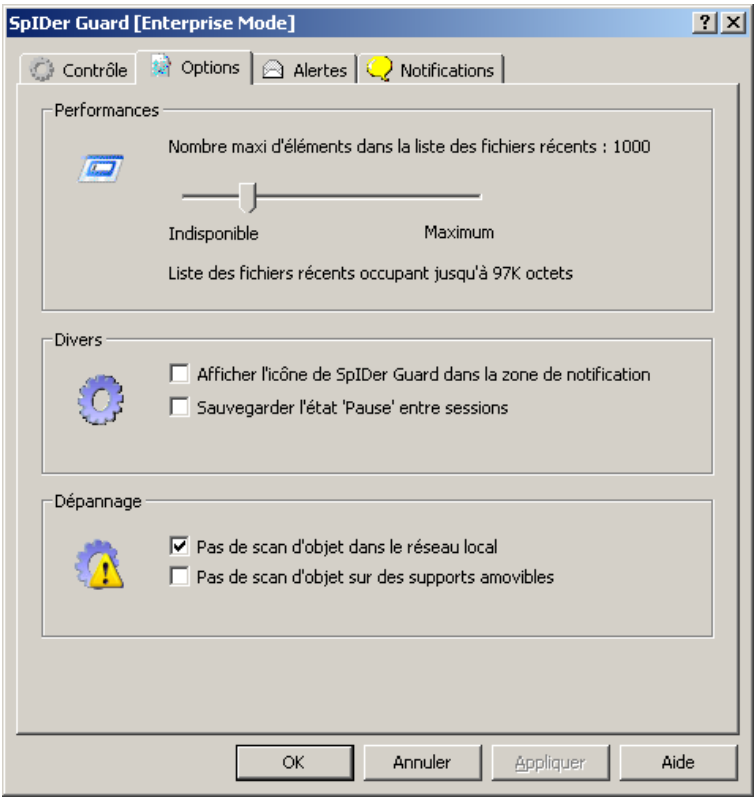


Figure 9-11. Fenêtre de Contrôle de SpIDer Guard. Onglet Options.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

Cet onglet de la fenêtre de Contrôle de **SpIDer Guard** permet de configurer certains paramètres du gardien.

Performances

La rubrique **Performances** sert à configurer la taille de la liste des chemins des fichiers déjà vérifiés. Cette liste est enregistrée dans la mémoire cache.

Vous pouvez paramétrer la taille de la liste à l'aide du curseur.

Les fichiers contenus dans la liste seront exclus des analyses ultérieures à moins qu'ils ne soient modifiés. Par défaut, le paramètre prend la valeur moyenne 100, ce qui correspond à 9 Ko de la mémoire utilisée par chaque disque logique. Si le système dispose de ressources suffisantes de mémoire libre, il est recommandé d'augmenter la valeur jusqu'à 500–1000. Le paramètre ne sera pris en compte qu'en mode d'analyse **lancement et ouverture des fichiers** ou lors de l'analyse des fichiers sur les disques réseau et supports amovibles en mode **Intelligent**.

Divers

La rubrique **Divers** vous donne l'accès aux paramètres suivants :

- Cochez la case **Afficher l'icône de SpIDer Guard dans la zone de notification** pour afficher l'icône dans la zone de notification de la barre des tâches (un élément du bureau Microsoft Windows affichant les icônes des applications en cours d'exécution et se trouvant dans la partie droite de la barre des tâches. Par défaut la barre des tâche se trouve en bas de l'écran) Windows.
- Cochez la case **Sauvegarder l'état 'Pause' entre sessions** pour maintenir **SpIDer Guard** en pause après le redémarrage au cas où le moniteur a été désactivé lors de la session courante.

Dépannage

La rubrique **Dépannage** comprend les paramètres suivants :

- Cochez la case **Pas de scan d'objet sur des supports amovibles** pour n'effectuer le scan des fichiers se trouvant sur des supports amovibles que lors de leur exécution.

  Si la case **Pas de scan d'objet sur des supports amovibles** est décochée, le scan des fichiers se trouvant sur des lecteurs amovibles (disques CD/DVD, FDD), lecteurs-flash et d'autres supports pouvant être connectés via des ports USB) sera effectué lors de toute consultation de tels fichiers y compris l'ouverture en lecture seule.

- Cochez la case **Pas de scan d'objet dans le réseau local** pour effectuer le scan des fichiers se trouvant sur des lecteurs réseau uniquement à l'exécution de tels fichiers sur votre poste de travail.

  Si la case **Pas de scan d'objet dans le réseau local** est décochée, l'analyse des objets se trouvant sur des lecteurs réseau sera effectuée à l'exécution de tels fichiers ainsi qu'à chaque consultation de tels fichiers y compris l'ouverture en lecture seule.

Certains lecteurs externes (notamment les disques durs amovibles dotés d'une interface usb) peuvent se présenter dans le système en tant que disques durs. Il est recommandé d'utiliser de tels lecteurs avec précaution et d'effectuer une analyse antivirus avec le **Scanner Dr.Web** des lecteurs connectés à l'ordinateur.

9.2.2.3. Onglet Alertes

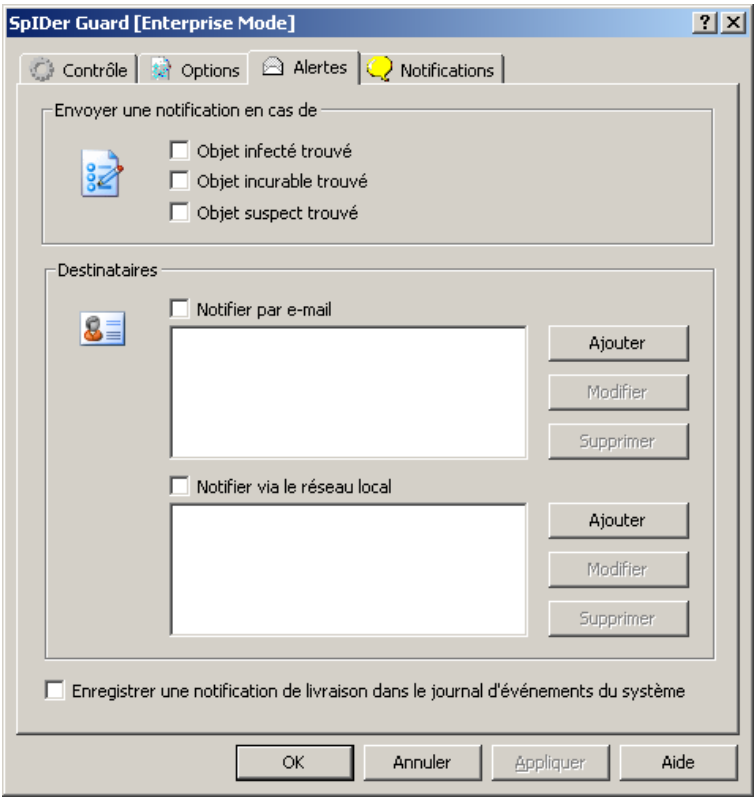


Figure 9-12. Fenêtre de Contrôle de SpIDer Guard. Onglet Alertes.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet **Alertes** permet de paramétrer les alertes sur des événements viraux : la liste des événements à notifier, le mode d'envoi et la listes des destinataires.

Dans la rubrique **Afficher une notification en cas de**, cochez les cases contre les types d'événements à notifier.

Vous pouvez paramétrer le mode d'envoi dans la rubrique **Destinataires** :

- Cochez la case **Notifier par e-mail** pour envoyer les notifications sur les événements sélectionnés par e-mail.
- Cochez la case **Notifier via le réseau local** pour envoyer les notifications sur les événements sélectionnés via le réseau local.

Les cases **Notifier par e-mail** et **Notifier via le réseau local** fonctionnent séparément et toutes les deux peuvent être cochées en même temps.

Rédigez (éditez) ensuite des listes de destinataires des notifications pour les modes d'envoi sélectionnés :

1. Pour ajouter un nouveau destinataire dans la liste par e-mail, cliquez sur le bouton **Ajouter** contre la liste des adresses e-mail. La Fenêtre de configuration de l'adresse e-mail sera ouverte.
2. Pour ajouter un nouveau destinataire dans la liste via le réseau local, cliquez sur le bouton **Ajouter** contre la liste des adresses réseau. La Fenêtre de configuration de l'adresse réseau sera ouverte.
3. Pour supprimer un élément dans une liste, sélectionnez-le et cliquez ensuite sur le bouton **Supprimer**.
4. Pour éditer un élément dans une liste, sélectionnez-le et cliquez ensuite sur le bouton **Modifier**. La Fenêtre de configuration de l'adresse e-mail ou la Fenêtre de configuration de l'adresse réseau va s'ouvrir.

9.2.2.4. Onglet Notifications

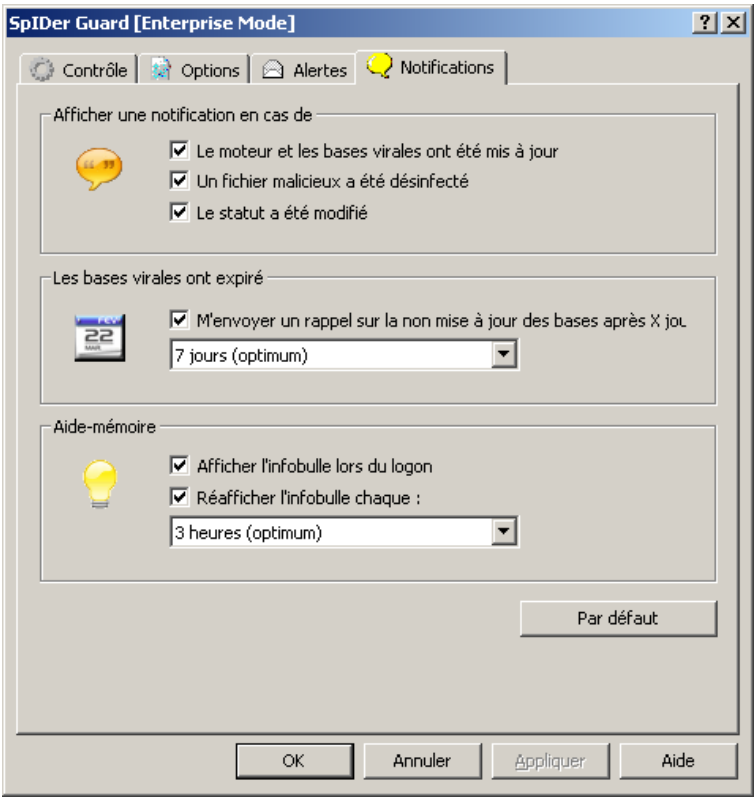


Figure 9-13. Fenêtre de Contrôle de SpIDer Guard. Onglet Notifications.

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet **Notifications** permet de configurer les notifications popup. Ces notifications apparaissent sous forme d'infobulle au-dessus de l'icône de **SpIDer Guard** dans la zone de notification Windows, à condition que l'affichage de l'icône soit activé.

La rubrique **Afficher une notification en cas de** propose la liste des événements à notifier par l'affichage des infobulles :

- **Le moteur et les bases virales ont été mis à jour** - notifier en cas de mise à jour du moteur et des bases virales.
- **Un fichier malicieux a été désinfecté** - notifier en cas de détection et neutralisation d'un objet infecté.
- **Le statut a été modifié** - notifier sur des changements dans le fonctionnement du gardien **SpIDer Guard** (lancement, arrêt).

La case cochée **M'envoyer un rappel sur la non mise à jour des bases de données virales après x jours** active l'affichage des notifications si les bases virales n'ont pas été mises à jour durant la période affichée dans la liste déroulante.

La rubrique **Aide-mémoire** permet de paramétrer l'affichage des infobulles sur les événements spécifiés :

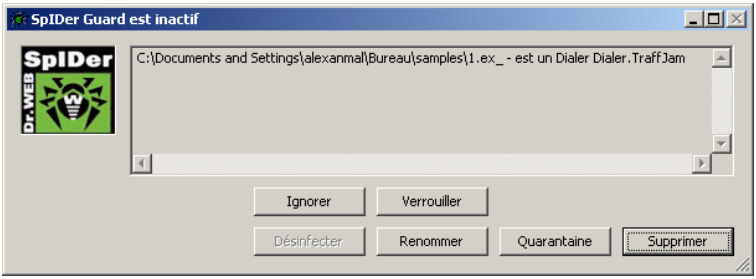
- **Afficher l'infobulle lors du logon** - pour afficher l'infobulle à chaque démarrage du système d'exploitation.
- **Réafficher l'infobulle chaque** - activer le ré-affichage de l'infobulle durant la période spécifiée dans la liste déroulante.

Cliquez sur le bouton **Par défaut** pour restaurer les paramètres initiaux recommandés par le logiciel.

9.2.3. Boîtes de dialogues utilisateur supplémentaires

9.2.3.1. Boîte de dialogue en cas de détection d'un objet infecté

Cette boîte de dialogue apparaît en cas de détection d'un objet infecté ou suspect par le gardien, à condition que l'action **Notifier** soit spécifiée dans la configuration des réactions de l'application.

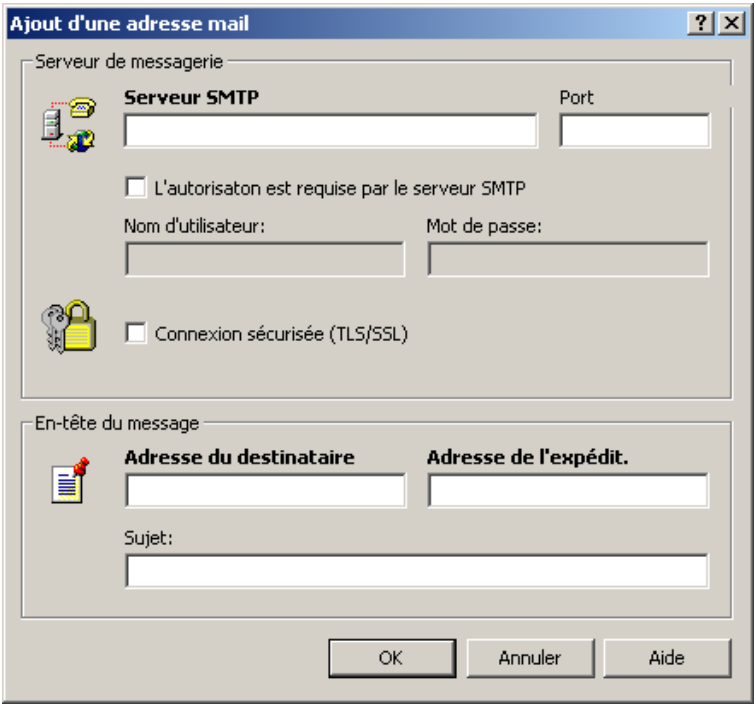


Boite de dialogue en cas de détection d'un objet infecté

Le jeu des boutons disponibles est fonction du type d'événement viral ou du type d'objet infecté (certaines réactions ne s'appliquent pas en cas d'archives, fichiers e-mail, conteneurs de fichiers).

- Cliquez sur le bouton **Ignorer** pour ne réaliser aucune action en cas de détection d'un objet suspect.
- Cliquez sur le bouton **Verrouiller** pour bloquer l'accès au fichier dont l'analyse a entraîné la réaction du gardien. Le fichier sera déverrouillé au démarrage de l'ordinateur ainsi que dans le cas où le contrôle est mis temporairement en pause.
- Cliquez sur le bouton **Désinfecter** (le bouton n'est disponible que lors de la détection d'un virus réparable à priori et n'est pas disponible en cas d'archives de tout type) pour essayer de réparer l'objet infecté par un virus connu. Si le virus est incurable ou la tentative de le réparer a échoué, la boîte de dialogue se rouvrira mais cette fois le bouton Désinfecter ne sera pas disponible.
- Cliquez sur le bouton **Renommer** pour renommer l'extension du fichier infecté ou suspect selon les paramètres spécifiés par défaut.
- Le bouton **Quarantaine** sert à déplacer un fichier infecté ou suspect vers le dossier de Quarantaine défini par défaut.
- Cliquez sur le bouton **Supprimer** pour supprimer un fichier infecté ou suspect (aucun action ne sera appliquée aux secteurs de démarrage). Par défaut, ce bouton n'est pas disponible pour supprimer des archives de tout type.

9.2.3.2. Fenêtre de configuration de l'adresse e-mail



Cette fenêtre permet de configurer l'adresse et les paramètres de messagerie à utiliser pour vous envoyer des notifications sur les événements viraux.

Serveur de messagerie

La rubrique **Serveur de messagerie** permet de configurer les paramètres du serveur SMTP nécessaires aux envois du courrier électronique.

Les paramètres obligatoires sont les suivants :

- **Serveur SMTP** - une adresse IP ou un nom de domaine pour le serveur de courrier sortant.
- **Port** - un numéro de port utilisé par le serveur SMTP.

Si le serveur SMTP requiert une autorisation, cochez la case **Autorisation sur le serveur SMTP** et remplissez les champs **Nom utilisateur** et **Mot de passe** pour accéder au serveur de courrier sortant.

Pour utiliser une connexion sécurisée via les protocoles TLS et SSL, cochez la case **Connexion sécurisée (TLS/SSL)**.

En-tête du message

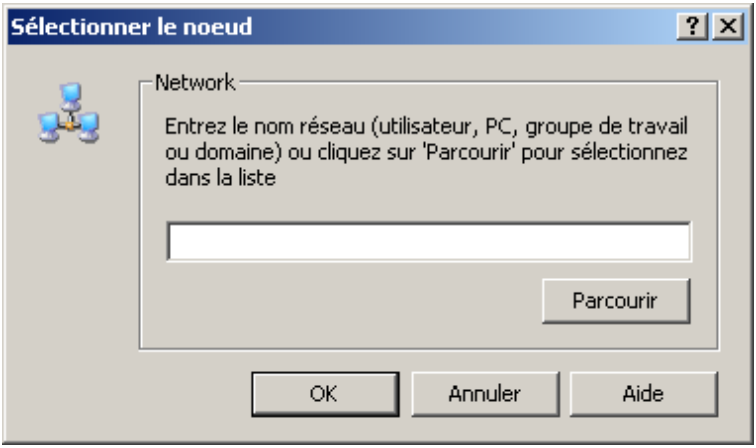
La rubrique En-tête du message permet de configurer les attributs du message.

Veuillez spécifier les adresses e-mail suivantes :

- Dans le champ **Adresse du destinataire**, configurez l'adresse e-mail à laquelle les notifications sur les événements viraux seront envoyées.
- Dans le champ **Adresse de l'expéditeur**, configurez l'adresse e-mail à indiquer en tant qu'adresse de l'expéditeur dans le message sur la situation virale.

Vous pouvez attribuer un sujet au message dans le champ **Sujet**. Si le champ n'est pas rempli, le sujet spécifié par défaut sera appliqué.

9.2.3.3. Fenêtre de configuration de l'adresse réseau



Entrez ici l'adresse de l'ordinateur dans le réseau Microsoft pour l'inclure à la liste d'après laquelle seront envoyées les notifications.

Dans le champ **Nom de l'ordinateur**, entrez le nom réseau du poste ou cliquez sur le bouton **Parcourir** pour trouver l'ordinateur avec l'Explorateur réseau.

Chapitre 10. SpIDer Mail

Le gardien de courrier **SpIDer Mail** est inclus par défaut dans le jeu de composants installés. Il réside en permanence en mémoire et démarre de manière automatique au démarrage du système d'exploitation.

En cas de licence relative au package Antivirus+Antispam (conformément au fichier clé), le gardien de courrier peut également effectuer l'analyse antispam du courrier avec **Dr.Web Antispam**.

La configuration de **SpIDer Mail** définie par défaut est optimale et assure un maximum de protection avec une intervention minimale de l'utilisateur. Cependant, elle empêche d'utiliser certaines fonctionnalités des clients de messagerie (par exemple, l'envoi d'un message à de multiples adresses peut être classé comme envoi massif, le spam reçu n'est pas classé), l'option permettant d'obtenir des informations utiles des messages supprimés automatiquement (depuis la partie texte non infectée) n'est pas utilisée. Les utilisateurs exérimentés peuvent modifier les options de l'analyse du courrier et la configuration de réaction du gardien de courrier **SpIDer Mail** en cas d'événements divers.

Traitement des messages

Paramétré par défaut, le gardien de courrier **SpIDer Mail** intercepte de façon automatique toutes les requêtes envoyées par n'importe quel client de messagerie tournant sur votre ordinateur vers des serveurs de messagerie, exécutées via les ports standard liés aux protocoles correspondants. Les ports standard sont les suivants :

- pour le protocole POP3 - port 110 ;
- pour le protocole SMTP - port 25 ;
- pour le protocole IMAP4 - port 143 ;
- pour le protocole NNTP - port 119.

Dans certains cas, l'interception automatique des connexions POP3, SMTP, IMAP4 et NNTP n'est pas possible. Dans ce cas, vous pouvez paramétrer l'interception manuelle des connexions.

Le gardien de courrier **SpIDer Mail** réceptionne chaque message entrant à la place du logiciel de messagerie et le contrôle avec un niveau de détail maximum. Si aucun virus ou objet suspect n'est détecté, le message est transféré au logiciel de messagerie de manière "transparente" comme s'il était reçu directement depuis le serveur. Les messages sortants sont contrôlés de la même façon avant d'être envoyés au serveur.

Dr.Web Antispam

La fonction d'analyse antispam n'est disponible que dans le cas où **Dr.Web Agent** fonctionne conformément à la licence Antivirus+Antispam.

Les technologies de filtrage antispam **Dr.Web** exploitent plusieurs milliers de règles qui peuvent être divisées en différents groupes :

- **analyse heuristique** est une technologie très intelligente qui analyse de façon empirique toutes les parties d'un message : en-tête, corps du message, etc. ainsi que les pièces jointes ;
- **filtrage de contre mesure** est une technique qui consiste à contrer et à déjouer les techniques utilisées par les spammeurs pour contourner la détection ;
- **analyse basée sur les palettes HTML** – les messages contenant des codes HTML sont comparés à une liste de palettes reconnues par la bibliothèque antispam ;
- **analyse sémantique** est une analyse au cours de laquelle les mots et phrases d'un message sont comparés aux mots et phrases typiquement utilisés dans le spam. Un dictionnaire spécifique est utilisé afin d'analyser aussi bien les éléments visibles qu'invisibles, comme par exemple des mots, expressions et symboles cachés par des techniques spéciales des spammeurs ;
- **technologie anti-scamming** consiste à utiliser un module

spécialisé pour filtrer les messages scam (comme les messages pharming – une variante des messages –scam) qui intègrent les « Nigerian » scams, loan scams, lottery et casino scams et les faux messages de banques ou organismes de crédit ;

- **filtrage de spam technique** – il s'agit des messages dits Bounce qui peuvent être considérés soit comme une réaction sur des virus, soit comme une activité virale. Un module antispam spécialisé classe de tels messages comme indésirables.

Réactions de SpIDer Mail

Par défaut, la réaction du gardien **SpIDer Mail** sur des messages entrants infectés ou suspects, ainsi qu'en cas de messages non vérifiés (par exemple les messages ayant une structure très compliquée) est la suivante :

- les informations malveillantes seront enlevées des messages infectés (cette action est désignée comme *désinfection* du message), puis ces messages sont délivrés de façon ordinaire ;
- les messages contenant des objets suspects seront déplacés sous forme de fichiers séparés vers la Quarantaine, une notification sera envoyée vers le client de messagerie (cette action est désignée comme *déplacement* du message) ;
- les messages non infectés ainsi que ceux non vérifiés seront délivrés sans modification (ils sont désignés comme *laissés passer*) ;
- tous les messages supprimés ou déplacés sont également enlevés depuis les serveurs POP3 ou IMAP4.

Les messages infectés ou suspects ne sont pas transmis au serveur, l'utilisateur sera notifié sur le refus d'envoi du message (en général, le client de messagerie sauvegarde ce type de message).

En cas de virus inconnu pouvant se propager via le courrier électronique, le gardien de courrier **SpIDer Mail** peut détecter les signes d'un comportement typiquement viral (envois massifs). Cette option est activée par défaut.

Le gardien de courrier **SpIDer Mail** offre une possibilité de vérifier les messages entrants pour lutter contre le spam avec Antispam Dr.Web. Par défaut l'option est activée.

Analyse des messages par d'autres moyens

Le gardien **SpIDer Guard** et le **Scanner Dr.Web** peuvent aussi détecter des virus dans les boîtes aux lettres de certains formats, cependant le gardien **SpIDer Mail** offre quelques avantages :

- Tous les formats de BAL ne sont pas supportés par le gardien **SpIDer Guard** et le **Scanner Dr.Web** ; en cas d'utilisaton du gardien **SpIDer Mail**, les messages infectés n'arrivent pas dans les BAL ;
- Par défaut, **SpIDer Guard** ne vérifie pas les BAL, l'activation de cette option diminue considérablement les performances du système ;
- **Le Scanner Dr.Web** vérifie les BAL soit à la demande de l'utilisateur, soit selon une planification, mais pas au moment de la réception du courrier, de plus cette procédure consomme beaucoup de ressources et prend du temps.

Ainsi, parmi tous les composants de **Enterprise Security Suite** paramétrés par défaut, le gardien de courrier **SpIDer Mail** est le premier à détecter des virus et objets suspects propagés via le courrier électronique et les empêche de pénétrer l'ordinateur. Son fonctionnement consomme très peu de ressources système, ainsi l'utilisation des autres compostans pour l'analyse des fichiers email n'est pas indispensable.

Configuration du gardien

La configuration du gardien **SpIDer Mail** varie en fonction de la version du gardien installée. Il existe deux versions du gardien **SpIDer Mail** :

- SpIDer Mail,
- SpIDer Mail NT4.

Avant l'installation du gardien, la version du système d'exploitation est reconnue de façon automatique, puis une version appropriée de **SpIDer Mail** est installée (voir Pré-requis système).

Si nécessaire (par exemple en cas d'exécution d'une tâche très sensible à la charge du processeur en temps réel) vous pouvez désactiver temporairement le fonctionnement du gardien.

10.1. Configuration de SpIDer Mail

La configuration du programme est optimale dans la plupart des cas, il est déconseillé de la modifier sans nécessité.

La marche à suivre pour configurer le moniteur de courrier SpIDer Mail :

1. Depuis le menu contextuel de l'**Agent** sélectionnez l'élément **Configuration de SpIDer Mail**.

L'élément **Configuration de SpIDer Mail** est disponible depuis le menu contextuel de l'**Agent** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier ces paramètres. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur la machine.

2. La fenêtre contenant les rubriques décrites ci-dessous apparaît :
   - La rubrique **Analyse** permet de configurer le mode d'analyse du courrier électronique (pour en savoir plus, consultez la rubrique d'aide **Antivirus Dr.Web pour Windows**, **Rubrique Analyse**).

- La rubrique **Antispam** permet de configurer le mode d'analyse antispam du courrier avec l'**Antispam Dr.Web** (vous trouverez la description détaillée dans la rubrique d'aide **Antivirus Dr.Web pour Windows**, **Rubrique Antispam**).
- La rubrique **Exclusions** permet de configurer une liste des applications exclues de l'analyse par le gardien de courrier **SpIDer Mail** (pour en savoir plus, consultez la rubrique d'aide **Antivirus Dr.Web pour Windows**, **Rubrique Exclusions**).
- La rubrique **Interception** permet de configurer l'interception des connexions aux serveurs de messagerie (pour en savoir plus, consultez la rubrique d'aide **Antivirus Dr.Web pour Windows**, **Rubrique Interception**).
- La rubrique **Log** permet de spécifier le mode d'écriture dans le fichier de log du gardien de courrier **SpIDer Mail** (pour en savoir plus, consultez la rubrique d'aide **Antivirus Dr.Web pour Windows**, **Rubrique Log**).

Pour afficher la rubrique d'aide sur une fenêtre active, dans toutes les boîtes de dialogue pressez la touche F1.

3. Apportez des modifications nécessaires.
4. A la fin d'édition, cliquez sur **OK** pour sauvegarder les modifications apportées ou sur le bouton **Annuler** pour refuser les modifications.

10.2. Configuration de SpIDer Mail NT4

La configuration du programme est optimale dans la plupart des cas, il est déconseillé de la modifier sans nécessité.

La marche à suivre pour configurer le moniteur de courrier SpIDer Mail NT4:

1. Depuis le menu contextuel de l'**Agent** sélectionnez l'élément **Configuration de SpIDer Mail**.

L'élément **Configuration de SpIDer Mail** est disponible depuis le menu contextuel de l'**Agent** à condition que l'utilisateur dispose des droits appropriés :

1. Les droits permettant de modifier ces paramètres. Les droits peuvent être paramétrés sur le **Serveur** par l'administrateur du réseau antivirus.
2. Les droits d'administrateur sur la machine.

2. La fenêtre contenant les rubriques décrites ci-dessous apparaît :
   - La rubrique Analyse permet de configurer le mode d'analyse du courrier électronique ;
   - La rubrique Actions permet de configurer une réaction du gardien **SpIDer Mail** en cas de détection de fichiers infectés ou suspects dans le courrier ;
   - La rubrique Moteur permet de configurer le fonctionnement du moteur antivirus ;
   - La rubrique Journal permet de configurer le mode d'écriture dans le fichier de log du gardien **SpIDer Mail** ;
   - La rubrique Interception permet de configurer l'interception des connexions aux serveurs POP3/SMTP/IMAP4/NNTP ;
   - La rubrique Applications exclues permet de configurer une liste des dossiers et fichiers à exclure de l'analyse par le gardien **SpIDer Mail**.
3. Apportez des modifications nécessaires.
4. A la fin d'édition de la configuration, cliquez sur **OK** pour sauvegarder les modifications apportées ou sur le bouton **Annuler** pour refuser les modifications.

10.2.1. Onglet Scan (Analyse)

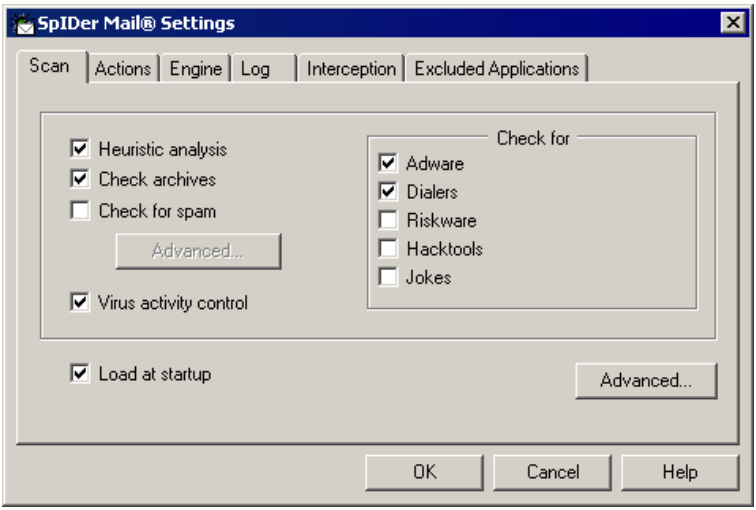


Figure 10-1. Fenêtre de Configuration de SpIDer Mail. Onglet Scan (Analyse).

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

Cet onglet permet de configurer le mode d'analyse du courrier électronique.

Le jeu de paramètres décrits ci-dessous permet de configurer le mode d'analyse du courrier électronique. Les paramètres importants listés ci-après sont spécifiés par défaut, il est déconseillé de les modifier :

- Cochée par défaut, la case **Heuristic analysis** (**Analyse heuristique**) active l'utilisation du moteur heuristique lors de l'analyse du courrier électronique par le gardien de courrier. Ce mode utilise les mécanismes spécialisés permettant de détecter dans le courrier les objets suspects fort probablement infectés par des virus inconnus.
- Cochée par défaut, la case **Check archives** (**Contrôler les fichiers dans les archives**) active l'analyse du contenu des archives transmises via le courrier électronique. Pour accélérer le

fonctionnement du gardien de courrier **SpIDer Mail**, décochez la case **Check archives** (**Contrôler les fichiers dans les archives**) afin de désactiver l'option.

Si l'option de vérification des fichiers dans les archives est désactivée, cela ne facilite pas l'intrusion des virus sur la machine à condition que le gardien **SpIDer Guard** fonctionne de manière permanente. Ceci ne fait que reporter la détection des virus. Lors de l'extraction d'une archive infectée, le système d'exploitation va tenter d'écrire l'objet infecté sur le disque et c'est à ce moment-là que l'objet malveillant sera détecté par le gardien **SpIDer Guard**.

- La case **Virus activity control** (**Contrôle de l'activité virale)** est cochée par défaut. Si l'option est activée, l'application va détecter des signes caractéristiques des envois massifs qui témoignent souvent de contamination de l'ordinateur par des virus. En opérant dans ce mode, le gardien de courrier **SpIDer Mail** peut bloquer votre envoi d'un message à de multiples adresses. Si c'est bien le cas, il est recommandé de décocher la case.

Cet onglet vous permet également de paramétrer la vérification de votre courrier contre le spam :

- La case cochée **Check for spam** (**Contrôler le spam**) active l'analyse des messages entrants avec le gardien de courrier par le fitlre antispam.

L'option de contrôle du spam n'est disponible que dans le cas où **Dr.Web Agent** fonctionne sous licence Antivirus + Antispam.

Afin de modifier la configuration du filtre antispam, cliquez sur le bouton **Advanced** (**Avancé**) se trouvant en bas. La fenêtre de Configuration de l'analyse antispam des messages s'ouvrira.

A part les messages contenant des fichiers infectés, le gardien de courrier peut détecter le courrier pouvant comprendre d'autres types de programmes indésirables :

- **Adware** (**Adwares**),
- **Dialers** (**Dialers payants**),
- **Riskware** (**Riskwares**),
- **Hacktools** (**Hacktools**),
- **Jokes** (**Canulars**).

Pour modifier le jeu de programmes indésirables à détecter, cochez les cases contre les types de programmes à détecter et déchochez les cases contres les types de programmes à ne pas détecter.

Paramétré par défaut, le gardien de courrier ne détecte que les **Adware** (**Adwares**) et **Dialers** (**Dialers payants**).

La réaction du gardien de courrier en cas de détection des programmes indésirables est la même que celle sur des messages infectés, configurée dans l'onglet Actions.

La case **Load at startup** (**Lancer au démarrage**) est cochée par défaut. Dans ce cas, **SpIDer Mail** démarre de façon automatique au démarrage du système Windows. Vous pouvez décocher la case, alors vous aurez à lancer le programme manuellement.

Pour configurer les paramètres supplémentaires relatifs à l'analyse du courrier électronique, cliquez sur le bouton Avancé se trouvant dans le coin inférieur droit de la fenêtre.

10.2.1.1. Configuration du filtre antispam

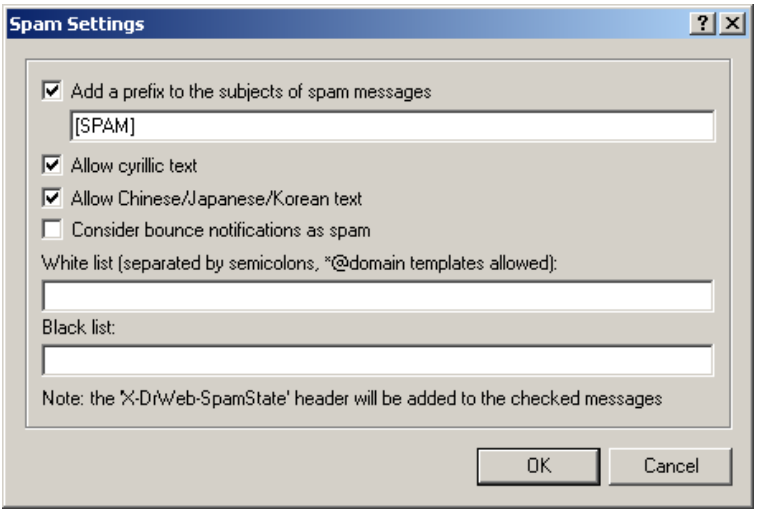


Figure 10-2. Fenêtre de Configuration de SpIDer Mail.

Si vous utilisez les protocoles IMAP/NNTP pour réceptionner votre courrier, configurez votre client de messagerie de sorte que les messages soient téléchargés entièrement depuis le serveur de messagerie - sans affichicher préalablement les en-têtes. Ceci est indispensable pour le fonctionnement correct du filtre antispam.

Si la case **Add prefix to the subjects of the spam messages (Ajouter un préfixe au sujet des messages spam**) est cochée, le gardien **SpIDer Mail** ajoute un préfixe aux sujet des messages classés comme spam. Ce préfixe est spécifié dans le champ se trouvant en bas. L'ajout de ce préfixe vous permet de créer des règles de filtrage des courriers classés commes spam si le client de messagerie ne permet pas de paramétrer les filtres selon les en-têtes des messages (par exemple MS Outlook Express).

Si la case **Allow Cyrillic text** (**Autoriser le texte cyrillique**) est cochée, le filtre antispam ne classe pas les messages en codage

cyrillique comme spam sans analyse préalable. En cas de case décochée, il est fort probable que de tels messages seront classés comme spam.

La case **Allow Chinese/Japanese/Korean text** (**Autoriser le texte chinois/japonais/coréen**) fonctionne de la même manière.

Les champs **White list** (**White liste**) et **Black list** (**Black liste**) contiennent les listes Black et White des adresses d'expéditeurs.

- Si l'adresse d'expéditeur est ajoutée dans la liste White, les messages provenant de cette adresse ne subissent pas l'analyse antispam. Cependant, si les noms de domaine expéditeur et destinataire sont identiques et que ce nom de domaine est inscrit dans la liste White avec le sympbole "*", ce message sera contrôlé.

  ▸ Méthodes de remplissage de la liste

  - afin d'ajouter un expéditeur dans la liste, saisissez son adresse email complète (par exepmle `mail@example.net`). Tous les messages provenant de cette adresse seront délivrés sans contrôle antispam ;
  - les adresses email différentes sont espacées par le symbole ";"
  - pour ajouter à la liste des expéditeurs un certain type d'adresse, entrez un masque déterminant ces adresses. Le masque définit un modèle déterminant un objet. Le masque peut comprendre des symboles utilisés dans les adresses email ainsi que le symbole * remplaçant toute séquence de n'importe quels symboles y compris une séquence vide.

    Par exemple les variantes ci-dessous sont possibles :

    - `mailbox@domain.com`
    - `*box@domain.com`
    - `mailbox@dom*`
    - `*box@dom*`

Le symbole * ne peut être mis qu'au début ou à la fin de l'adresse.

Le symbole @ est obligatoire.

- pour assurer la réception des messages provenant des adresses qui appartiennent à un domaine déterminé, utilisez le symbole * à la place du nom d'utilisateur. Par exemple pour recevoir tous les messages provenant des adresses depuis le domaine example.net, saisissez *@example.net.
- pour assurer la réception des messages provenant des adresses contenant un nom d'utilisateur déterminé, quel que soit le nom de domaine utilisez le symbole * à la place du nom de domaine. Par exemple pour recevoir tous les messages provenant des expéditeurs dont le nom de BAL est ivanov, saisissez ivanov@*.

- Si l'adresse de l'expéditeur est ajoutée dans la Black liste, les messages concernés seront classés comme spam sans analyse supplémentaire.

  ‣ Méthodes de remplissage de la liste

  - pour ajouter un expéditeur déterminé dans la liste, entrez son adresse email complète (par exemple spam@spam.ru). Tous les messages provenant de cette adresse seront automatiquement classés comme spam ;
  - les adresses email différentes sont espacés par le symbole ";"
  - pour ajouter des adresses déterminées dans la liste des expéditeurs, entrez un masque déterminant ces adresses. Le masque définit un modèle déterminant un objet. Le masque peut comprendre des symboles utilisés dans les adresses email ainsi que le symbole * remplaçant toute séquence de n'importe quels symboles y compris une séquence vide.

    Par exemple les variantes ci-dessous sont possibles :

    - mailbox@domain.com
    - *box@domain.com

- `mailbox@dom*`
- `*box@dom*`

Le symbole `*` ne peut être mis qu'au début ou à la fin de l'adresse.

Le symbole `@` est obligatoire.

- pour classer comme spam tous les messages provenant des adresses du domaine déterminé, utilisez le symbole `*` à la place du nom d'utilisateur. Par exemple pour que tous les messages provenant des expéditeurs du domaine `spam.ru` soient classés comme spam, saisissez `*@spam.ru` ;
- pour classer comme spam tous les messages provenant des adresses contenant un nom d'utilisateur déterminé, quel que soit le nom de domaine utilisez le symbole `*` à la place du nom de domaine. Par exepmle pour que tous les messages provenant des expéditeurs dont le nom de BAL est `ivanov` soient classés comme spam, saisissez `ivanov@*`.
- les adresses appartenant au domaine du destinataire ne sont pas traitées. Par exemple si la BAL du destinataire (votre BAL) se trouve dans le domaine `mail.ru`, les adresses des expéditeurs du domaine `mail.ru` ne seront pas traités par le filtre antispam.

Tous les messages vérifiés reçoivent les en-têtes suivants :

- **X-DrWeb-SpamState: Yes/No**. La valeur **Yes** correpont au statut spam associé au message, la valeur **No** signifie que selon **SpIDer Mail** le message est classé comme non spam.
- **X-DrWeb-SpamVersion: version**. **version** est la version de la bibliothèque du filtre antispam **Vade Retro**.

En cas d'erreur dans la détection du spam, merci de transférer les messages concernés aux adresses spécialisées. En cas de « fausse alerte » merci de le signaler à vrnonspam@drweb.com. En cas de pénétration du spam, veuillez vous adresser à vrspam@drweb.com. Merci d'envoyer tous les messages en pièce jointe (pas dans le corps du message).

10.2.1.2. Paramètres avancés de l'analyse

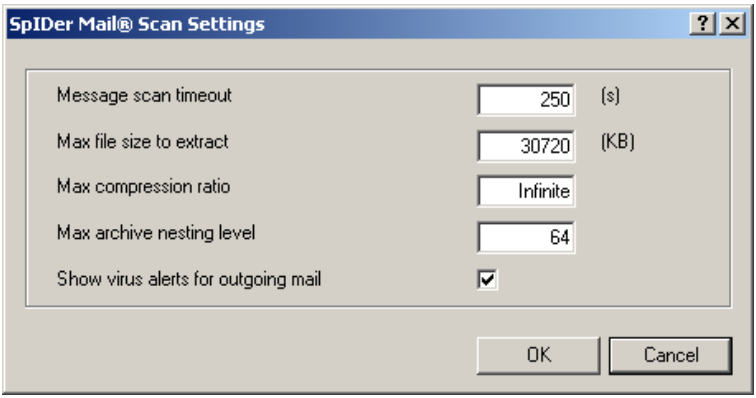


Figure 10-3. Fenêtre de Configuration de SpIDer Mail.

Cette fenêtre vous permet de configurer les paramètres supplémentaires de l'analyse du courrier électronique.

Le jeu de paramètres listés ci-dessous détermine les conditions selon lesquelles les messages composés seront classés comme non vérifiés compte tenu du fait que leur vérification mobilise trop de ressources :

- **Message scan timeout** (**Délai d'attente lors du scan de message**) – le délai maximum pendant lequel le message subit une analyse. Dès que la valeur spécifiée est dépassée, le traitement est arrêté ;
- **Max file size to extract** (**Taille max des fichiers à extraire)** – si le gardien de courrier estime qu'après l'extraction des fichiers, la taille de l'archive dépassera la valeur spécifiée, les

fichiers ne seront pas extraits et l'archive ne sera pas analysée ;

- **Max compression ratio** (**Ratio max de compression de l'archive**) – si le gardien de courrier estime que le ratio de compression de l'archive dépasse la valeur spécifiée, elle ne sera pas désarchivée, ni analysée ;
- **Max archive nesting level** (**Profondeur max d'emboîtement**) – si la profondeur d'emboîtement de l'archive dépasse la valeur spécifiée, l'archive sera analysée jusqu'à la limitation spécifiée.

La case **Show virus alerts for outgoing mail flag** (**Alertes virales sur le courrier sortant**) est cochée par défaut. Ceci active l'affichage de la fenêtre informant sur le refus de livraison du message infecté sur le serveur SMTP. En général, le client de messagerie crée aussi un message analogue, dans ce cas, vous pouvez décocher la case.

10.2.2. Onglet Actions

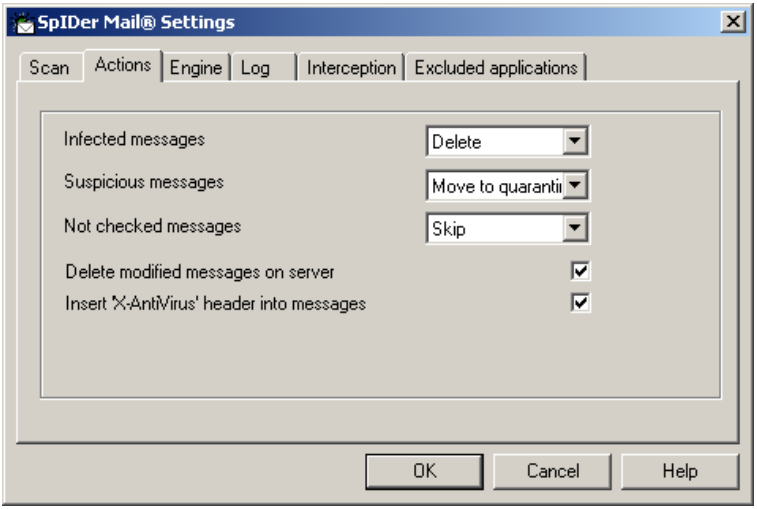


Figure 10-4. Fenêtre de Configuration de SpIDer Mail. Onglet Actions. Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet permet de configurer les réactions du gardien **SpIDer Mail** en cas de détection de fichiers infectés ou suspects contenus dans le courrier électronique.

Configuration des actions

Pour configurer les actions à appliquer aux objets malveillants détectés, utilisez les paramètres suivants :

- La liste déroulante **Infected messages** (**Messages infectés**) permet de configurer une réaction de **SpIDer Mail** en cas de détection d'un message contenant un objet malicieux.
- La liste déroulante **Suspicious messages** (**Messages suspects**) permet de configurer une réaction de **SpIDer Mail** en cas de détection d'un message contenant probablement un

virus (réaction du moteur heuristique).

- La liste déroulante **Not checked messages** (**Messages non vérifiés**) permet de configurer une réaction de **SpIDer Mail** en cas de détection des messages dont l'analyse n'a pas pu être achevée.

La case **Delete modified messages on server** (**Supprimer les messages modifiés sur le serveur**) est cochée par défaut. Dans ce cas, les messages entrants auquels une des réactions **Delete (Supprimer**) ou **Quarantine** (**Quarantaine**) a été appliquée sont supprimés depuis le serveur POP3/IMAP4 quels que soient les paramètres du client de messagerie.

Si la case **Insert 'X-AntiVirus' header into messages** (**Inserer l'en-tête 'X-AntiVirus' dans les messages**) est cochée, dans tous les messages vérifiés les en-têtes suivants seront ajoutés :

- **X-DrWeb-SpamState: Yes/No**. La valeur **Yes** correspond au statut spam associé au message, la valeur **No** signifie que selon **SpIDer Mail** le message est classé comme non spam.
- **X-DrWeb-SpamVersion: version**. **Version** est la version de la bibliothèque du filtre antispam Vade Retro.

Réactions disponibles

Les actions suivantes peuvent être appliquées aux objets détectés :

- **Delete** (**Supprimer**) – dans ce cas, le gardien de courrier ne transmet pas le message au client de messagerie. A la place du message supprimé, un message sur la procédure réalisée sera envoyé au client de messagerie.
- **Quarantine** (**Quarantaine**) – le message ne sera pas transmis au client de messagerie mais sera déplacé vers le dossier de Quarantaine. A la place du message déplacé, le client de messagerie recevra un message sur la procédure réalisée.
- **Skip** (**Laisser passer**) **–** transmettre les messages au client de messagerie de manière standard.

Toute option appliquée aux messages sortants, sauf l'action **Laisser passer** enraîne un refus de transmission du message vers le serveur SMTP.

Tableau 7. Réactions de SpIDer Mail lors de l'analyse du courrier électronique

Objet	Réaction		
	Supprimer	Quarantaine	Laisser passer
Messages infectés	+	+/*	
Messages suspects	+	+/*	+
Messages non vérifiés	+	+	+/*

Légende

+	l'action est autorisée pour ce type d'objet
+/*	l'action est spécifiée en tant que réaction par défaut pour ce type d'objet

10.2.3. Onglet Engine (Moteur)

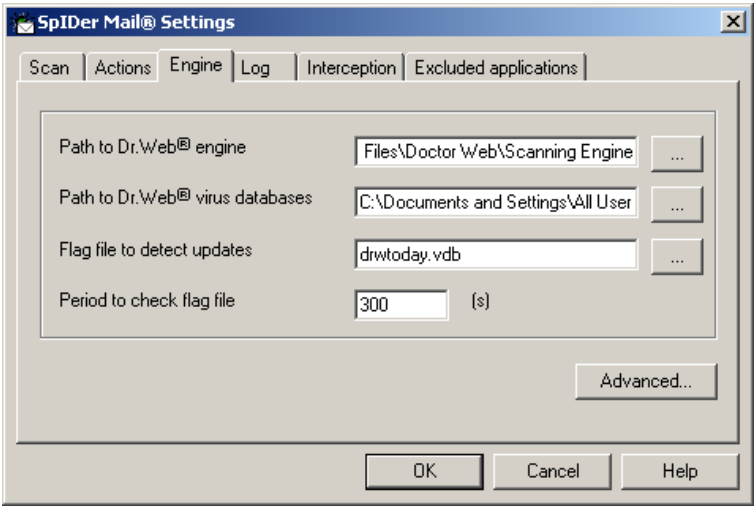


Figure 10-5. Fenêtre de Configuration de SpIDer Mail. Onglet Engine (Moteur).

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet permet de configurer le fonctionnement du moteur antivirus.

Si nécessaire, vous pouvez spécifier l'emplacement spécifique du moteur antivirus (noyau) et des bases virales.

Si durant l'exécution du gardien une nouvelle mise à jour des bases virales est rendue disponible par le **Module de mises à jour**, le gardien télécharge immédiatement les bases renouvelées. Si les bases virales sont mises à jour par un autre moyen (par exemple copiées directement vers le répertoire d'installation), le gardien peut également télécharger les bases renouvelées sans redémarrer le programme. Ceci est assuré par un mécanisme de vérification du fichier "flag" (qui contient par défaut les informations sur les toutes dernières mises à jour de la base). La modification du fichier "flag" signifie la nécessité de mettre à jour les bases virales. Vous pouvez configurer le nom,

l'emplacement du fichier 'flag" ainsi qu'un espacement de temps entre les contrôles (la valeur par défaut est 300 secondes).

Cliquez sur le bouton **Advanced** (**Avancé**) pour configurer les paramètres avancés du moteur antivirus.

10.2.3.1. Paramètres avancès des moteurs de recherche

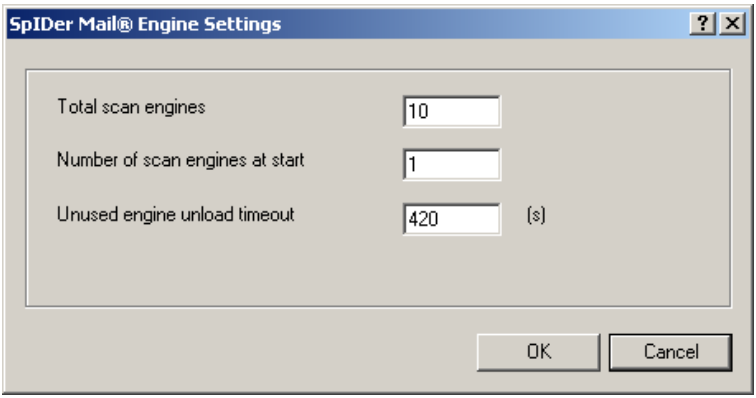


Figure 10-6. Fenêtre de Configuration de SpIDer Mail.

L'onglet vous permet de configurer les paramètres avancés des moteurs de recherche :

- Le champ **Total scan engines** (**Total de moteurs de recherche**) pemet de spécifier un nombre total de moteurs chargés simultanément.
- Le champ **Numbers of scan engines at start** (**Nombre de moteurs au démarrage**) spécifie un nombre de moteurs à charger au démarrage de **SpIDer Mail**.
- Le champ **Unused engines unload timeout** (**Délai de décharge des moteurs non utilisés**) spécifié une durée à l'écheance duquel le module non utilisé sera déchargé.

10.2.4. Onglet Log (Journal)

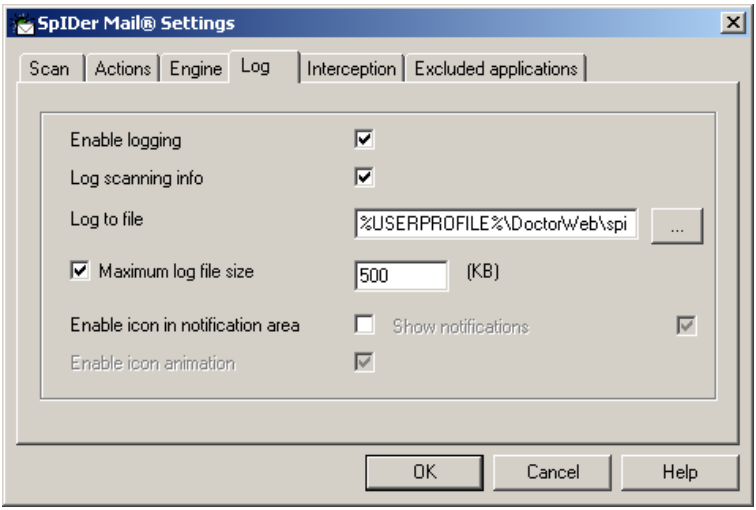


Figure 10-7. Fenêtre de Configuration de SpIDer Mail. Onglet Log (Journal).

Pour plus d'information sur les paramètres spécifiés par cette boîte de dialogue, cliquez sur l'élément respectif de la fenêtre sur l'illustration

L'onglet permet de configurer les paramètres d'écriture dans le fichier de log de **SpIDer Mail**.

La case cochée **Enable logging** (**Ecrire un fichier de log**) active l'écriture dans le fichier de log par **SpIDer Mail**. La case est cochée par défaut.

Vous pouvez configurer les paramètres suivants du fichier de log :

- Cochez la case **Log scanning info** (**Log des objets contrôlés)** pour activer l'écriture des informations sur tous les objets vérifiés y compris les objets sains.
- Dans le champ **Log to file** (**Ecrire un fichier de log**) vous pouvez spécifier le chemin et le nom du fichier de log. Cliquez sur le bouton ... pour sélectionner un objet dans

l'explorateur système.

- Cochez la case **Maximum log file size** (**Taille max du fichier de log**) pour limiter la taille maximale du fichier de log et spécifier une taille maximale en Ko.

Vous pouvez également configurer les paramètres supplémentaires :

- Cochez la case **Enable icon in the notification area (Afficher l'icône**) pour activer l'affichage de l'icône de **SpIDer Mail** dans la zone de notification de la barre des tâches.
- Cochez la case **Enable icon animation** (**Icône animée**) pour activer l'animation de l'icône de **SpIDer Mail** dans la zone de notification de la barre des tâches.
- Cochez la case **Show notifications** (**Afficher les notifications**) pour activer l'affichage des info-bulles au-dessus de l'icône de **SpIDer Mail** vous informant sur la version du programme, le nombre total de définitions virales etc. L'info-bulle s'affiche après le démarrage du programme.

10.2.5. Onglet Interception

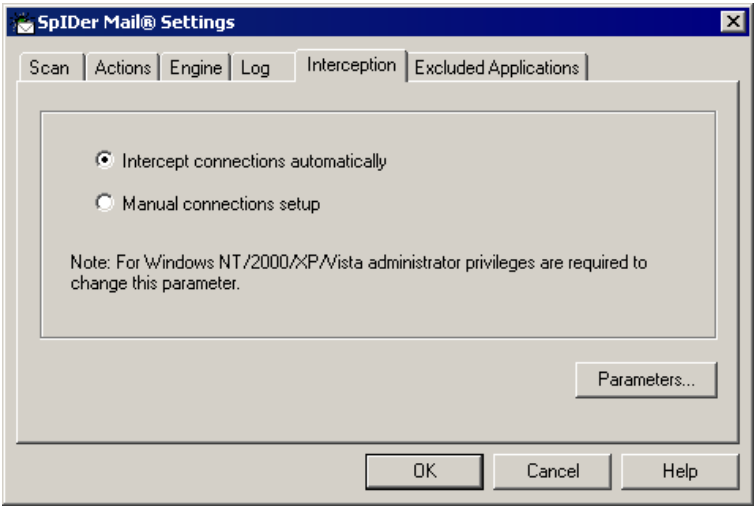


Figure 10-8. Fenêtre de Configuration de SpIDer Mail. Onglet Interception.

Pour plus d'information sur les paramètres spécifiés par cette boîte de dialogue, cliquez sur l'élément respectif de la fenêtre sur l'illustration

L'onglet vous permet de configurer les paramètres de l'interception des connexions aux serveurs POP3/SMTP/IMAP4/NNTP.

Sélectionnez le mode d'interception :

- automatique est le mode le plus simple ;
- manuelle est le mode à utiliser dans les cas où l'interception automatique est indisponible pour certaines adresses ou pour toutes les adresses des serveurs (le même mode sera appliqué pour toutes les adresses).

Après avoir sélectionné un mode, cliquez sur le bouton **Parameters (Paramètres)**. La fenêtre de configuration de l'interception selon le mode sélectionné sera ouverte.

10.2.5.1. Interception automatique

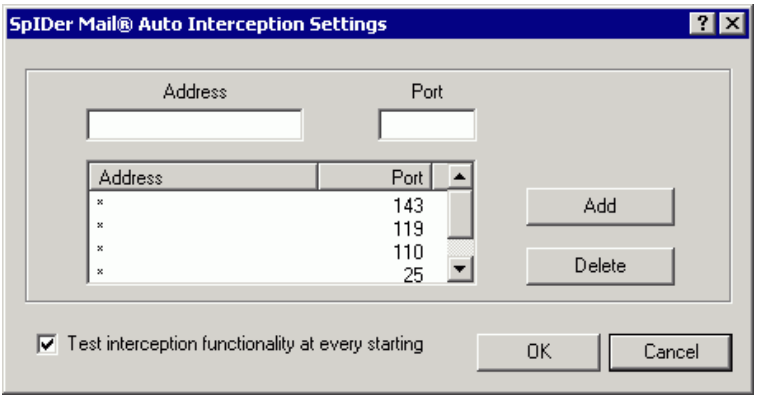


Figure 10-9. Fenêtre de Configuration de l'interception automatique de SpIDer Mail.

L'onglet permet de configurer l'interception en mode automatique.

La liste des adresses des serveurs de messagerie comprend par défaut quatre éléments listés ci-dessous :

- toute adresse avec le port 143 – serveurs standard IMAP4,
- toute adresse avec le port 119 – serveurs standard NNTP,
- toute adresse avec le port 110 – serveurs standard POP3,
- toute adresse avec le port 25 – serveurs standard SMTP.

Vous pouvez éditer la liste ci-dessus :

1. Pour ajouter un élément dans la liste, entrez les informations correspondantes dans les champs **Address** (**Adresse**) et **Port** (**Port**), cliquez ensuite sur le bouton **Add** (**Ajouter**).
2. Afin d'enlever un élément de la liste, sélectionnez-le et cliquez ensuite sur le bouton **Delete** (**Supprimer**).

Si la case **Test interception functionality at every starting** (**Tester les interceptions au démarrage**) est cochée, le testing de l'interception automatique sera activé. Si lors du testing il s'avère que l'interception en mode automatique n'est pas opérationnelle pour une

connexion, passez au mode manuel d'interception.

10.2.5.2. Interception manuelle

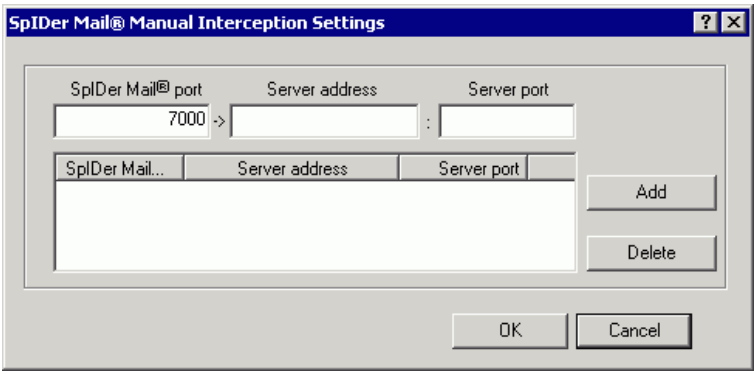


Figure 10-10. Fenêtre de Configuration de l'interception manuelle de SpIDer Mail.

L'onglet permet de configurer le mode manuel d'interception des connexions aux serveurs de messagerie. Activé dans ce mode, le gardien **SpIDer Mail** fonctionne en tant que serveur proxy entre les clients de messagerie et les serveurs de messagerie, seules les connexions spécifiées dans les paramètres de manière explicite seront surveillées par le gardien. Ce type d'interception nécessite une modification de la configuration de la connexion des clients de messagerie.

La liste des adresses à intercepter est rédigée de sorte que chaque entrée établit une correspondance entre la configuration du gardien **SpIDer Mail** et celle du serveur de messagerie.

Par défaut, la liste est vide. Vous pouvez y ajouter des entrées.

Configuration de l'interception des connexions en mode manuel

1. Rédigez une liste des serveurs de messagerie pour lesquels les requêtes adressées doivent être interceptées, spécifiez également les numéros de port pour les serveurs respectifs en ordre croissant sans espace. Il est recommandé de commencer par le nombre 7000. Les numéros seront nommés ci-après les *ports SpIDer Mail*.

Le gardien de courrier **SpIDer Mail** supporte les serveurs de messagerie opérant selon les protocoles POP3, SMTP, IMAP4 ou NNTP.

2. Dans la configuration du gardien de courrier **SpIDer Mail**, sélectionnez l'élément **Interception**.
3. Puis choisissez l'interception manuelle et cliquez sur le bouton **Connection Settings** (**Configuration**).
4. Dans la fenêtre de dialogue qui apparaît, entrez les informations suivantes :
   - dans le champ **SpIDer Mail port** (**Port SpIDer Mail**) – *le port SpIDer Mail* sélectionné pour le serveur de messagerie ;
   - dans le champ **Server address** (**Adresse du serveur**) – le nom de domaine ou l'adresse IP du serveur de messagerie ;
   - dans le champ **Server port** (**Port du serveur**) – le numéro du port utilisé par le serveur de messagerie.
5. Cliquez sur **Add** (**Ajouter**).
6. Si nécessaire, reprenez les étapes 4 et 5 pour d'autres serveurs. Pour arrêter l'interception des connexions au serveur, sélectionnez l'élément respectif dans la liste et cliquez sur le bouton **Delete** (**Supprimer**).
7. A la fin de l'édition de la configuration, cliquez sur **OK** pour sauvegarder les modifications apportées ou sur le bouton **Annuler** pour refuser les modifications.

8. Configurez le client de messagerie pour le fonctionnement avec le gardien de courrier **SpIDer Mail** en mode d'interception manuelle.

Configuration du client de messagerie

Si **SpIDer Mail** fonctionne selon une configuraiton utilisateur d'interception, modifiez la configuration de votre client de messagerie de manière suivante :

- spécifiez `localhost` en tant qu'adresse du serveur pour les courriers entrants et sortants ;
- spécifiez *port SpIDer Mail* sélectionné pour le serveur de messagerie associé en tant que port du serveur de messagerie.

En général, il est nécessaire de mettre dans les paramètres de l'adresse du serveur de messagerie les informations ci-dessous :

`localhost`:**<***port_SpIDer_Mail***>**

où <*port_SpIDer_Mail*> est un port que vous avez sélectionné pour le serveur de messagerie correspondant.

‣ Exemple.

Si le serveur de messagerie ayant l'adresse `pop.mail.ru` et le port `110` est associé au *port SpIDer Mail* `7000`, dans la configuration du client de messagerie, il faut spécifier `localhost` en tant que serveur du courrier entrant et `7000` en tant que port.

10.2.6. Onglet Excluded Applications (Applications à exclure)

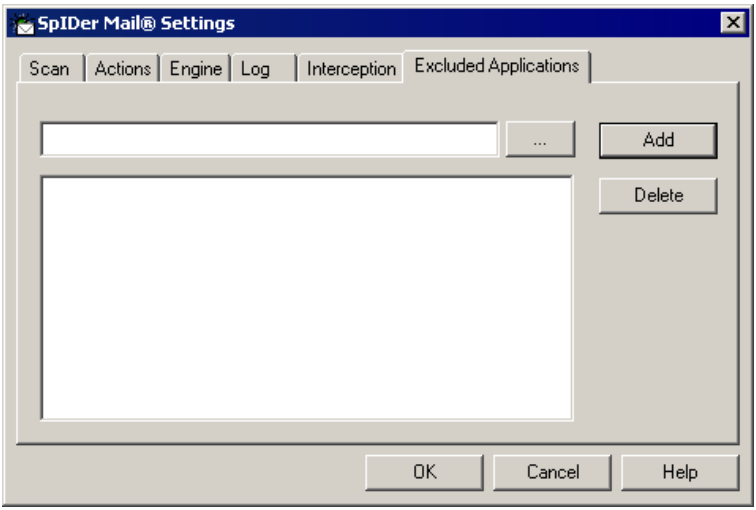


Figure 10-11. Fenêtre de Configuration de SpIDer Mail. Onglet Excluded Applications (Application à exclure).

Pour la rubrique d'aide sur les paramètres se trouvant sur un autre onglet, cliquez sur cet onglet dans l'illustration

L'onglet permet de spécifier une liste des applications dont la bande passante ne sera pas interceptée et par suite ne sera pas analysée par le gardien de courrier.

La marche à suivre pour configurer une liste des applications :

1. Entrez le chemin vers le fichier exécutable de l'application. Vous pouvez aussi utiliser le bouton ... et sélectionner un objet avec l'explorateur système.
2. Cliquez sur le bouton **Add** (**Ajouter**). L'application sera ajoutée dans la liste se trouvant en bas.

3. Pour enlever une application de la liste, sélectionnez l'exécutable associé à l'application dans la liste et cliquez ensuite sur le bouton **Delete** (**Supprimer**).

Chapitre 11. Dr.Web pour Outlook

Les fonctions clé du composant

Le module ajoutable **Dr.Web pour Outlook** réalise les fonctions suivantes :

- analyse antivirus des fichiers contenus dans les pièces jointe des courriers ;
- analyse du courrier entrant via la connexion sécurisée SSL ;
- analyse antispam du courrier ;
- détection et neutralisation des malwares ;
- utilisation du moteur heuristique renforçant la protection contre les virus inconnus.

Activation/Désactivation

L'activation et désactivation du module **Dr.Web pour Outlook** se fait depuis le menu contextuel de l'**Agent**.

Configuration du module Dr.Web pour Outlook

Dans le client de messagerie Microsoft Outlook, pour accéder à la configuration et aux statistiques de l'application, consultez la rubrique **Outils** → **Options** → onglet **Dr.Web Antivirus**.

L'onglet **Dr.Web Antivirus** dans les paramètres de Microsoft Outlook n'est disponible qu'à condition que l'utilisateur dispose des droits permettant de modifier les paramètres. Les droits sont spécifiés sur le **Serveur** par l'administrateur du réseau antivirus.

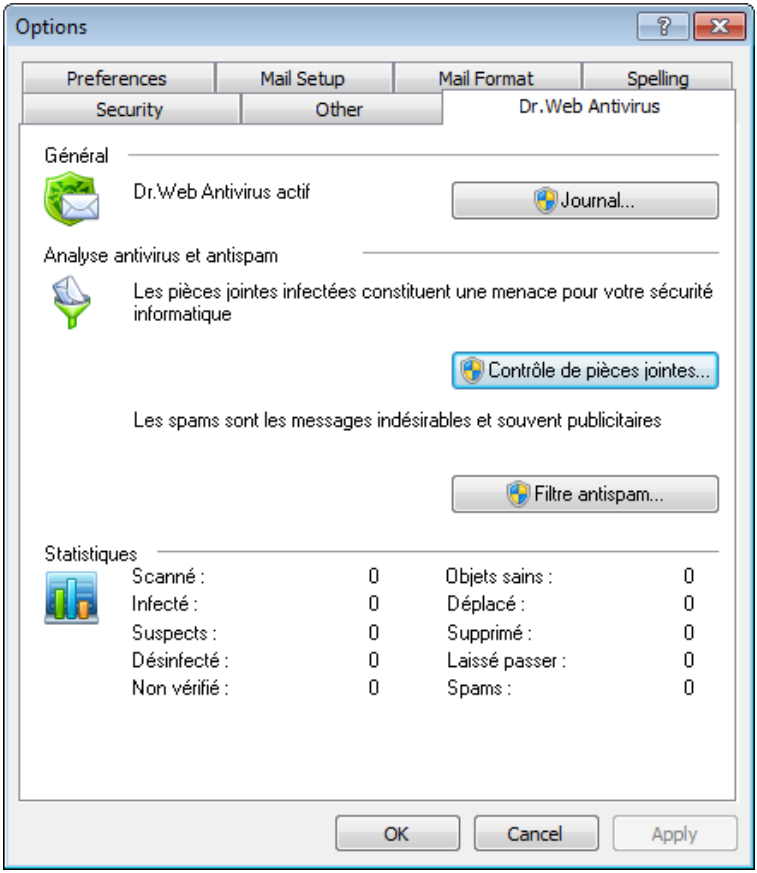


Figure 11-1. Fenêtre de Configuration de Microsoft Outlook. Onglet Antivirus Dr.Web.

L'onglet **Dr.Web Antivirus** affiche le statut actuel de la protection (active/inactive) et permet d'accéder aux fonctions suivantes de l'application :

- Journal - permet de configurer l'écriture des événements dans le fichier de log ;
- Contrôle des pièces jointes - permet de configurer le contrôle du courrier électronique et de spécifier des réactions en cas de

détection d'objets malveillants ;

- Filtre antispam - permet de spécifier les réactions de l'application en cas de détection de messages spam ainsi que de créer des Black et White listes ;
- Statistiques - affiche des informations sur les objets analysés et traités par l'application.

11.1. Analyse antivirus

Diverses méthodes de détection des virus sont utilisées par **Dr.Web pour Outlook**. Les réactions spécifiées par l'utilisateur seront appliquées aux objets malveillants détectés : l'application peut réparer des objets infectés, ainsi qu'en supprimer ou en déplacer vers la Quarantaine afin de les isoler et de préserver la sécurité.

11.1.1. Objets malveillants

L'application **Dr.Web pour Outlook** détecte les objets malveillants suivants :

- archives infectées ;
- bombes de décompression ;
- adwares ;
- hacktools ;
- dialers payants ;
- canulars ;
- riskwares.

11.1.2. Réactions

Dr.Web pour Outlook permet de configurer une réaction de l'application en cas de détection de fichiers infectés ou suspects ainsi que de programmes malveillants lors de l'analyse des pièces jointes du courrier électronique.

Afin de configurer l'analyse des pièces jointes et de définir les réactions face à des objets malveillants détectés, dans le client de messagerie Microsoft Outlook, allez à la rubrique **Outils** → **Options** → onglet **Dr.Web Antivirus** et cliquez sur le bouton **Contrôle de pièces jointes**.

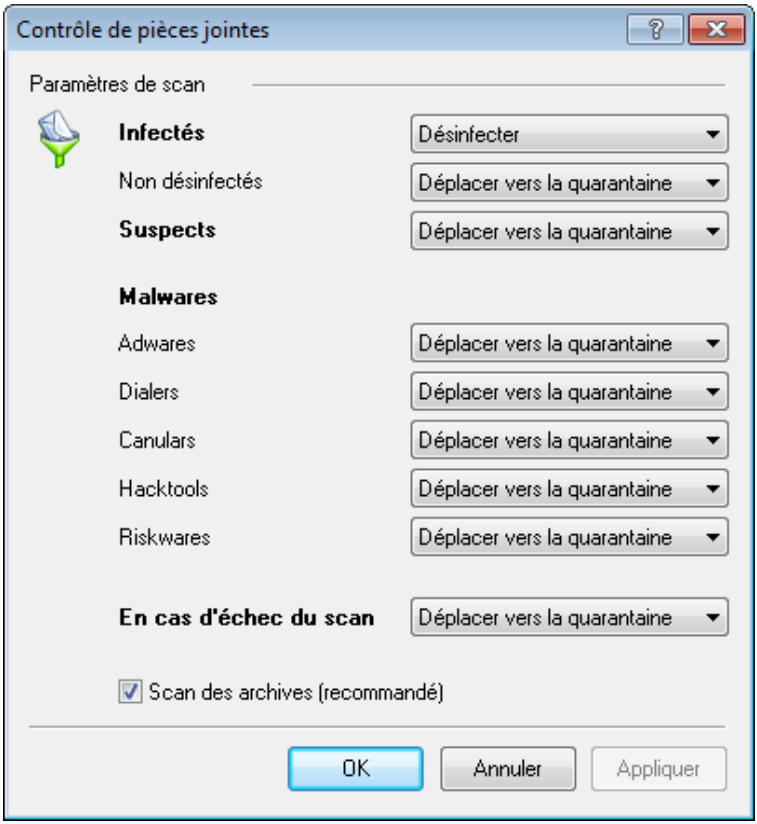


Figure 11-2. Fenêtre de Configuration de Contrôle de pièces jointes.

La fenêtre **Contrôle de pièces jointes** est disponible à condition que l'utilisateur dispose des droits administrateur.

Sous Windows Vista ou supérieur, si vous cliquez sur le bouton **Contrôle de pièces jointes** :

- Lorsque UAC est activé : l'administrateur sera invité à confirmer l'action de l'application, l'utilisateur qui ne dispose pas de droits d'administrateur sera invité à saisir les informations d'authentification de l'administrateur système.
- Lorsque UAC est désactivé : l'administrateur peut modifier les paramètres de l'application, l'utilisateur ne pourra pas accéder à la modification des paramètres.

La fenêtre **Contrôle de pièces jointes** vous permet de configurer les réactions de l'application sur diverses catégories d'objets vérifiés ainsi qu'en cas d'erreurs survenues lors de l'analyse. Il existe également une possibilité de configurer l'analyse des archives.

Utilisez les paramètres listés ci-dessous pour configurer les réactions sur les objets malveillants détectés :

- La liste déroulante **Infectés** définit la réaction en cas de détection d'objets contaminés par des virus connus et probablement réparables.
- La liste déroulante **Non désinfectés** définit la réaction en cas de détection d'objets infectés par un virus connu mais irréparable ainsi qu'en cas d'échec de la désinfection.
- La liste déroulante **Suspects** définit la réaction lors de la détection d'objets probablement infectés par un virus (réaction du moteur heuristique).
- La rubrique **Malwares** définit la réaction en cas de détection des malwares suivants :
  - Adwares ;
  - Dialers ;
  - Canulars ;
  - Hacktools ;
  - Riskwares.
- La liste déroulante **En cas d'échec du scan** permet de configurer les réactions dans le cas où l'analyse de la pièce jointe est impossible, par exemple en cas de pièce jointe

contenant un fichier endommagé ou protégé par un mot de passe.

- La case **Scan des archives (recommandé)** permet d'activer ou de désactiver l'analyse des archives contenues dans les pièces jointes. Pour activer l'analyse, cochez la case et décochez-la pour désactiver l'analyse.

Le jeu de réactions applicables est fonction de l'événement viral.

Les réactions ci-dessous sont applicables aux objets détectés :

- **Désinfecter** - l'application va tenter de réparer le fichier infecté ;
- **Comme incurables** - la réaction sélectionnée pour les objets incurables sera appliquée à l'objet infecté ;
- **Supprimer** - supprimer l'objet depuis le système ;
- **Déplacer vers la quarantaine** - isoler l'objet dans le dossier de Quarantaine ;
- **Laisser passer** - laisser l'objet passer sans modifications.

Tableau 8. Réactions applicables aux objets malveillants détectés

Objet	Action				
	Désin-fecter	Comme pour les incurables	Supprimer	Déplacer vers la quarantaine	Laisser passer
Infectés	+/*	+			
Incurables			+	+/*	
Suspects			+	+/*	+
Adwares			+	+/*	+
Dialers payants			+	+/*	+
Canulars			+	+/*	+
Hacktools			+	+/*	+
Riskwares			+	+/*	+
En cas d'erreur d'analyse			+	+/*	+

Légende

+	L'action est autorisée pour ce type d'objet
+/*	L'action est déterminée en tant que réaction par défaut pour ce type d'objet

11.2. Analyse antispam

Dr.Web pour Outlook effectue une analyse antispam de tous les courriers avec le filtre antispam **Vade Retro** et filtre les messages selon les paramètres spécifiés par l'utilisateur.

Pour configurer l'analyse antispam des messages dans le client de messagerie Microsoft Outlook, allez dans l'onglet **Outils** → **Options** → onglet **Dr.Web Antivirus**, cliquez ensuite sur le bouton **Filtre antispam**. La fenêtre de Configuration du Filtre antispam va s'ouvrir.

La rubrique **Filtre antispam** n'est disponible qu'à condition que **Dr.Web Agent** fonctionne sous licence Antivirus + Antispam.

Si l'utilisation du filtre antispam n'est pas autorisée par la licence, les paramètres de l'analyse antispam ne seront pas disponibles et l'analyse antispam ne sera pas effectuée.

La fenêtre **Filtre antispam** est disponible à condition que l'utilisateur dispose des droits de l'administrateur système.

Sous Windows Vista ou supérieur, si vous cliquez sur le bouton **Filtre antispam** :

- Lorsque UAC est activé : l'administrateur sera invité à confirmer l'action de l'application, l'utilisateur qui ne dispose pas de droits d'administrateur sera invité à saisir les informations d'authentification de l'administrateur système.
- Lorsque UAC est désactivé : l'administrateur peut modifier les paramètres de l'application, l'utilisateur ne pourra pas accéder à la modification des paramètres.

11.2.1. Configuration du filtre antispam

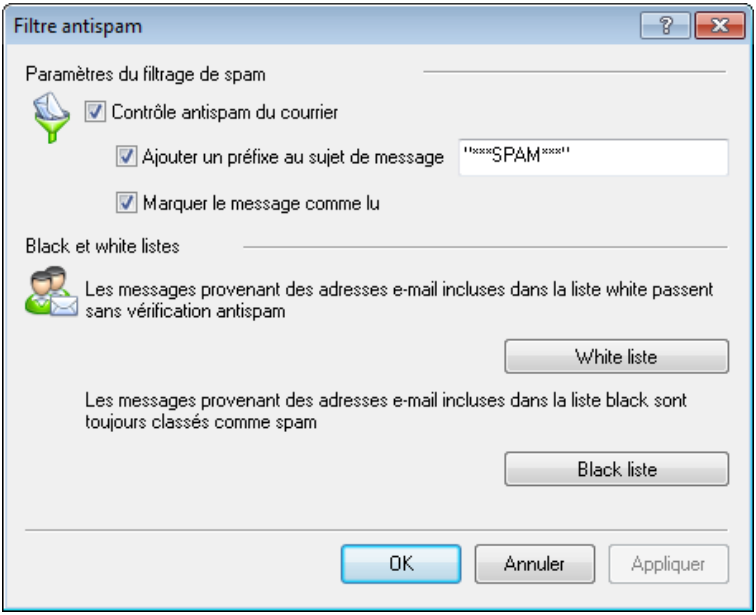


Figure 11-3. Fenêtre de Configuration du filtre antispam.

La marche à suivre pour configurer le filtre antispam :

- Cochez la case **Contrôle antispam du courrier** pour activer le filtre antispam.
- Si vous souhaitez ajouter un texte dans les en-têtes des messages classés comme spam, cochez la case **Ajouter un préfixe au sujet des messages**. Le texte à ajouter peut être mis dans le champ de texte se trouvant à droite de la case à cocher. Le préfixe inséré par défaut est ******SPAM******.
- Les messages vérifiés peuvent être marqués comme lus dans les propriétés de message. Pour cela, cochez la case **Marquer le message comme lu**. La case **Marque le message comme lu** est cochée par défaut.

- Vous pouvez aussi configurer les listes White et Black pour filtrer le courrier.

En cas d'erreur dans la détection du spam, merci de transférer les messages concernés aux adresses spécialisées pour contribuer à l'amélioraton du filtrage.

▸ Plus d'info

- En cas de « fausse alerte » merci de le signaler à vrnonspam@drweb.com.
- En cas de pénétration du spam, veuillez vous adresser à vrspam@drweb.com.

Merci d'envoyer tous les messages en pièce jointe (et non dans le corps du message).

11.2.2. Listes Black et White

Les listes Black et White servent à filtrer les messages.

Pour afficher ou modifier la liste Black ou White, depuis l'élément configuration du filtre antispam cliquez sur le bouton **Black liste** ou **White liste**.

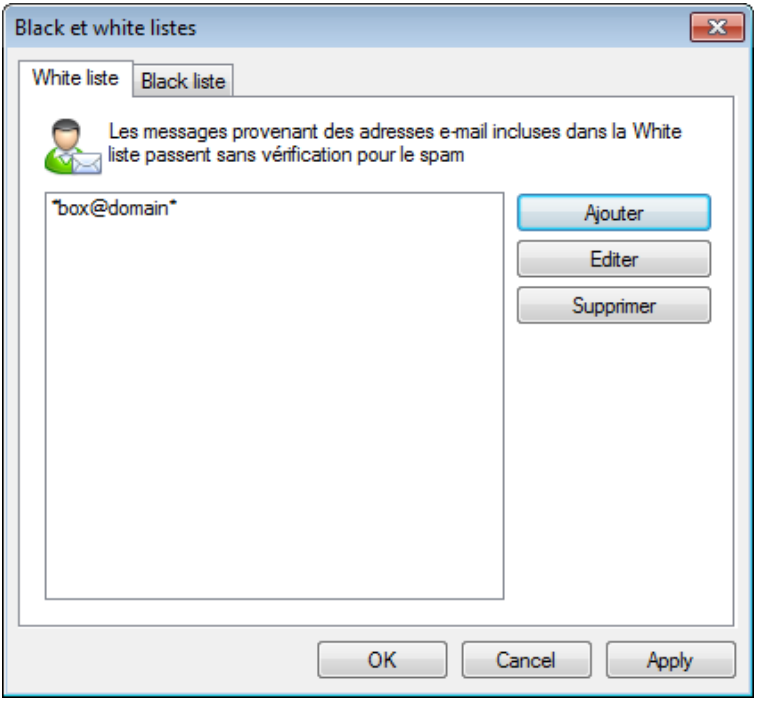


Figure 11-4. Fenêtre de configuration de la liste White du filtre antispam.

Pour ajouter une adresse dans la liste Black ou White :

1. Cliquez sur le bouton **Ajouter**.
2. Entrez l'adresse électronique dans le champ approprié (voir les méthodes de remplissage des listes white et black).
3. Cliquez sur **OK** dans la fenêtre **Editer la liste**.

Pour modifier des adresses dans la liste :

1. Sélectionnez une adresse à modifier, puis cliquez sur **Editer**.
2. Apportez les modifications nécessaires.
3. Dans la fenêtre **Editer la liste**, cliquez sur **OK**.

Pour supprimer une adresse de la liste :

1. Sélectionnez l'adresse dans la liste.
2. Cliquez sur **Supprimer**.

Dans la fenêtre **Listes Black et White** cliquez sur **OK** pour sauvegarder les modifications apportées.

Liste White

Si l'adresse de l'expéditeur est dans la liste White, les messages provenant de cette adresse ne subissent pas l'analyse antispam. Cependant, si les noms de domaine destinataire et expéditeur sont identiques et que ce nom de domaine est inscrit dans la liste White avec le symbole "*", ce message sera contrôlé.

▸ Méthodes de remplissage de la liste

- afin d'ajouter un expéditeur dans la liste, saisissez son adresse email complète (par exepmle `mail@example.net`). Tous les messages provenant de cette adresse seront délivrés sans contrôle antispam ;
- chaque élément de la liste peut comprendre une seule adresse email ou un seul masque d'adresses ;
- pour ajouter à la liste des expéditeurs un certain type d'adresse, entrez un masque déterminant les adresses nécessaires. Le masque définit un modèle déterminant un objet. Le masque peut comprendre des symboles utilisés dans les adresses email ainsi que le symbole * remplaçant toute séquence de n'importe quels symboles y compris une séquence vide.

  Par exemple les variantes ci-dessous sont possibles :

  - `mailbox@domain.com`
  - `*box@domain.com`
  - `mailbox@dom*`
  - `*box@dom*`

Le symbole * ne peut être mis qu'au début ou à la fin de l'adresse.

Le symbole @ est obligatoire.

- pour assurer la réception des messages provenant des adresses qui appartiennent à un domaine déterminé, utilisez le symbole * à la place du nom d'utilisateur. Par exemple pour recevoir tous les messages provenant des adresses depuis le domaine example.net, saisissez *@example.net.
- pour assurer la réception des messages provenant des adresses contenant un nom d'utilisateur déterminé, quel que soit le nom de domaine utilisez le symbole * à la place du nom de domaine. Par exemple pour recevoir tous les messages provenant des expéditeurs dont le nom de BAL est ivanov, saisissez ivanov@*.

Liste Black

Si l'adresse de l'expéditeur est dans la liste Black, les messages provenant de cette adresse seront classés comme spam sans analyse supplémentaire.

▸ Méthodes de remplissage de la liste

- pour ajouter un expéditeur déterminé dans la liste, entrez son adresse email complète (par exemple spam@spam.ru). Tous les messages provenant de cette adresse seront automatiquement classés comme spam ;
- chaque élément de la liste peut comprendre une seule adresse email ou un seul masque d'adresses ;
- pour ajouter des adresses déterminées dans la liste des expéditeurs, entrez un masque déterminant les adresses nécessaires. Le masque définit un modèle déterminant un objet. Le masque peut comprendre des symboles utilisés dans les adresses email ainsi que le symbole * remplaçant toute séquence de n'importe quels symboles y compris une séquence vide.

  Par exemple les variantes ci-dessous sont possibles:

- `mailbox@domain.com`
- `*box@domain.com`
- `mailbox@dom*`
- `*box@dom*`

Le symbole `*` ne peut être mis qu'au début ou à la fin de l'adresse.

Le symbole `@` est obligatoire.

- pour classer comme spam tous les messages provenant des adresses du domaine déterminé, utilisez le symbole `*` à la place du nom d'utilisateur. Par exemple pour que tous les messages provenant des expéditeurs du domaine `spam.ru` soient classés comme spam, saisissez `*@spam.ru` ;
- pour classer comme spam tous les messages provenant des adresses contenant un nom d'utilisateur déterminé, quel que soit le nom de domaine utilisez le symbole `*` à la place du nom de domaine. Par exepmle pour que tous les messages provenant des expéditeurs dont le nom de BAL est `ivanov` soient classés comme spam, saisissez `ivanov@*` ;
- les adresses appartenant au domaine du destinataire ne sont pas traitées. Par exemple si la BAL du destinataire (votre BAL) se trouve dans le domaine `mail.ru`, les adresses des expéditeurs du domaine `mail.ru` ne seront pas traités par le filtre antispam.

11.3. Journalisation des événements

Dr.Web pour Outlook écrit les erreurs survenues et les événements dans les journaux suivants :

- journal d'événements système (Event Log) ;
- journal texte de débogage.

11.3.1. Journal d'événements système

Le journal d'événement système (Event Log) collecte les informations suivantes :

- messages sur l'arrêt ou le démarrage de l'application ;
- paramètres du fichier clé de licence : validité ou non validité de la licence, la durée de validité de la licence (ces informations sont écrites au démarrage, lors du fonctionnement ou lors du remplacement du fichier clé de licence) ;
- paramètres des modules de programme : scanner, moteur, bases virales (ces informations sont écrites au démarrage ou lors de la mise à jour des modules) ;
- message sur la non validité de la licence : fichier clé absent, autorisation manquante sur l'utilisation des modules de programme dans le fichier clé, licence bloquée, violation d'intégrité du fichier clé (ces informations sont écrites au démarrage et lors du fonctionnement de l'application) ;
- messages sur la détection des virus ;
- notification sur l'expiration de la licence (ces informations sont écrites 30, 15, 7, 3, 2 ou 1 jour(s) avant la date d'expiration).

Pour afficher le journal d'événements système :

1. Allez au **Panneau de configuration** système.
2. Sélectionnez la rubrique **Outils d'administration** → **Observateur d'événements**.
3. Dans la partie gauche de la fenêtre **Observateur d'événements**, sélectionnez l'élément **Application**. La liste des événement enregistrés dans le journal par des applications utilisateur sera ouverte dans la partie droite de la fenêtre. La source des messages pour **Dr.Web pour Outlook** est l'application **Dr.Web pour Outlook**.

11.3.2. Journal texte de débogage

Le journal texte de débogage collecte les informations listées ci-dessous :

- messages sur le validité ou non validité de la licence ;
- messages sur la détection des virus ;
- messages sur des erreurs survenues lors de l'écriture dans des fichiers ou lors de la lecture depuis des fichiers ainsi que sur des erreurs d'analyse des archives ou des fichiers protégés par mot de passe ;
- paramètres des modules de programme : scanner, moteur, bases virales ;
- messages sur les arrêts urgents du moteur de l'application ;
- notifications sur l'expiration de la licence (ces informations sont écrites 30, 15, 7, 3, 2 et 1 jour(s) avant la date d'expiration).

L'activation de l'écriture dans le journal texte ralentit le fonctionnement du système. Il n'est recommandé d'activer cette option qu'en cas d'erreurs lors du fonctionnement de l'application **Dr.Web pour Outlook**.

Configuration de la journalisation des événements

1. Dans l'onglet **Antivirus Dr.Web**, cliquez sur le bouton **Journal**. La fenêtre de Configuration du Journal apparaît.
2. Sélectionnez un niveau de détail (entre 0 et 5) pour l'écriture des événements :
   - niveau **0** correspond à la journalisation désactivée dans le journal texte de débogage,
   - niveau **5** correspond au niveau de détail maximum des événements enregistrés.

   Par défaut, l'écriture dans le journal est désactivée.
3. Spécifiez une taille maximum du fichier de log (en Ko).
4. Cliquez sur **OK** pour sauvegarder les modifications apportées.

La fenêtre **Journal** est disponible à condition que l'utilisateur dispose des droits administrateur.

Sous Windows Vista ou supérieur, si vous cliquez sur le bouton **Journal** :

- Lorsque UAC est activé : l'administrateur sera invité à confirmer l'action de l'application, l'utilisateur qui ne dispose pas des droits d'administrateur sera invité à saisir les informations d'authentification de l'administrateur système.
- Lorsque UAC est désactivé : l'administrateur peut modifier les paramètres de l'application, l'utilisateur ne pourra pas accéder à la modification des paramètres.

L'affichage du journal des événements liés à l'application

Pour afficher le journal texte des événements liés à l'application, cliquez sur le bouton **Afficher dans le dossier**. Le dossier contenant le journal sera ouvert.

Par défaut, le journal est sauvegardé dans le fichier `DrWebOutlook.log` se trouvant dans le profil utilisateur, dans le répertoire `DoctorWeb`.

L'écriture dans le fichier de log `DrWebOutlook.log` est effectuée séparément pour chaque utilisateur du système.

11.4. Statistiques

L'onglet **Outils** → **Options** → onglet **Dr.Web Antivirus** de Microsoft Outlook offre des informations statistiques sur le total des objets analysés et traités par l'application.

Les objets sont divisés en catégories suivantes :

- **Analysés** - le total des messages analysés.
- **Infectés** - le total des messages contenant des virus.

- **Suspects** - le total des messages probablement infectés par des virus (réaction du moteur heuristique).
- **Désinfectés** - le total des objets réparés par l'application.
- **Non vérifiés** - le total des objets dont l'analyse est impossible ou entraîne des erreurs d'analyse.
- **Sains** - le total des messages qui ne contiennent aucun objet malveillants.

Les informations suivantes seront également affichées:

- **Déplacés** - le total des objets déplacés vers la Quarantaine.
- **Supprimés** - le total des objets supprimés depuis le système.
- **Laissés passer** - le total des objets laissés passés sans modifications.
- **Messages spam** - le total des messages classés comme spam.

Par défaut, les statistiques sont sauvegardées dans le fichier `drwebforoutlook.stat` se trouvant dans le profil utilisateur dans le répertoire `DoctorWeb`. Pour effacer les statistiques, il faut supprimer ce fichier.

Le fichier de statistiques `drwebforoutlook.stat` est écrit séparément pour chaque utilisateur système.

Les statistiques de l'application **Dr.Web pour Outlook** sont transférées à l'**Agent** pour qu'il les envoie au **Serveur** avec les statistiques relatives aux autres composants de **Dr.Web Enterprise Security Suite**.

Annexe A. Clés de la ligne de commande pour le Dr.Web Scanner NT4

Cette rubrique décrit les clés de ligne de commande pour **Dr.Web Scanner NT4**.

Les clés pour **Dr.Web Scanner** sont décrites dans la Rubrique le Manuel **Dr.Web pour Windows**, dans la sous-rubrique **Annexe A** : **Paramètres du Scanner et du Scanner en ligne de commande**.

Lors de l'exécution de l'analyse, le **Scanner Dr.Web** démarre. En option, vous pouvez spécifier des paramètres supplémentaires d'analyse. Dans le champ de saisie **Arguments** vous pouvez entrer les clés listées ci-dessous (séparées par un espace) :

- **/@**<*nom_fichier*> ou **/@+**<*nom_fichier*> – pour vérifier les objets mentionnés dans le fichier spécifié. Chaque objet est paramétré par une ligne séparée du fichier-liste. Il est possible d'entrer le chemin complet avec le nom de fichier ou une ligne `?boot`, pour vérifier les secteurs de démarrage. La version GUI du scanner permet de paramétrer les noms de fichiers selon un masque ou les noms de répertoires. Le fichier-liste peut être rédigé à l'aide de tout éditeur de texte manuellement ou automatiquement à l'aide des applications utilisant le scanner pour l'analyse des fichiers spécifiés. Après l''analyse, si la clé ne contient pas le symbole +, le fichier-liste sera supprimé par le scanner.
- **/AL** – pour analyser tous les fichiers sur le support spécifié ou dans le répertoire spécifié, indépendamment de l'extension ou du format.
- **/AR** – pour analyser les fichiers archivés. Actuellement, on assure l'analyse (sans désinfection) des archives créées par les outils d'archivage suivants : ARJ, ZIP, PKZIP, ALZIP, RAR, AL RAR, LHA, GZIP, TAR, BZIP2, 7-ZIP, ACE etc., ainsi que des archives MS CAB – Windows Cabinet Files et des images ISO des

disques optiques (CD et DVD). Cette orthographe (**/AR**) de clé assure la prévention de l'utilisateur en cas de détection d'une archive contenant des fichiers suspects ou infectés. Les modificateurs ajoutés à la clé : **D**, **M** ou **R** activent les autres actions :

- **/ARD** – supprimer ;
- **/ARM** – déplacer (par défaut, vers le dossier de Quarantaine) ;
- **/ARR** – renommer (par défaut, le premier symbole de l'extension est remplacé par #). Si la clé se termine par le modificateur N, le nom de logiciel d'archivage ne sera pas imprimé après le nom de fichier archivé.

◆ **/CU** – les actions sur les fichiers infectés et sur les secteurs de démarrage de disques. Sans paramètres complémentaires **D**, **M** ou **R**, la désinfection des objets curables et la suppression des objets incurables seront effectuées (si une autre action n'est pas spécifiée par le paramètre **/IC**). D'autres actions ne peuvent être appliquées qu'aux fichiers infectés :

- **/CUD** – supprimer ;
- **/CUM** – déplacer (par défaut, vers le dossier de Quarantaine) ;
- **/CUR** – renommer (par défaut, le premier caractère de l'extension est remplacé par le symbole **#**).

◆ **/SPR**, **/SPD** ou **/SPM** – les actions sur les fichiers suspects :

- **/SPR** – renommer,
- **/SPD** – supprimer,
- **/SPM** – déplacer.

◆ **/ICR**, **/ICD** ou **/ICM** – les actions sur les fichiers incurables :

- **/ICR** – renommer,
- **/ICD** – supprimer,
- **/ICM** – déplacer.

◆ **/MW** – les actions sur tout type de programme malveillant. Cette orthographe de la clé (**/MW**) active la notification à l'utilisateur. Si la clé est complétée par un modificateur **D**, **M**, **R** ou **I**, les actions suivantes seront effectuées :

- **/MWD** – supprimer ;

- **/MWM** – déplacer (par défaut, vers le dossier de Quarantaine) ;
- **/MWR** – renommer (par défaut, le premier caractère de l'extension est remplacé par le symbole #) ;
- **/MWI** – ignorer. Les actions sur certains types de programmes malveillants peuvent être déterminées avec les clés suivantes : **/ADW**, **/DLS**, **/JOK**, **/RSK**, **/HCK**.

- **/DA** – analyser le PC une seule fois par jour. La date du processus d'analyse s'écrit dans le fichier de configuration, celui-ci doit être accessible pour la création ou une réécriture postérieure.
- **/EX** – analyser les fichiers ayant les extensions spécifiées dans le fichier de configuration. Par défaut ou en cas d'inaccessibilité de ce dernier, ce sont les extensions suivantes : EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, MSG, CHM, XML, PRC, ASP, LSP, MSO, OBD, THE*, EML, NWS, SWF, MPP, TBB.

Dans le cas où un élément de la liste des objets à vérifier contient une extension spécifiée explicitement, même avec les symboles spécifiques * et ?, tous les fichiers de la liste spécifiés par cet élément seront analysés et pas seulement les fichiers correspondants à la liste des extensions.

- **/FN** – télécharger les caractères cyrilliques dans l'adapteur vidéo (seulement pour **Dr.Web** pour **DOS**).
- **/GO** – mode de fonctionnement par lots. Toutes les questions qui requièrent une réponse utilisateur sont ignorées ; les décisions nécessitant une sélection sont prises automatiquement. Ce mode est utile pour l'analyse automatique des fichiers, par ex. lors d'une analyse de vingt-quatre heures des courriers électroniques sur le serveur.
- **/SCP:**<*n*> – détermine une priorité du scan. <*n*> peut varier entre 1 et 50 (inclus).
- **/SHELL** – pour la version GUI du scanner. Cette clé désactive l'affichage de mots de bienvenue, l'analyse en mémoire et

l'analyse des fichiers d'autodémarrage. Les listes sauvegardées des chemins vers les fichiers et les dossiers analysés par défaut ne sont pas chargées. Ce mode permet d'utiliser la version GUI du scanner au lieu de la version en ligne de commande seulement pour les objets mentionnés dans les paramètres de la ligne de commande.

- **/ST** – la clé active le mode discret de la version GUI du scanner. Le logiciel fonctionne sans ouvrir de fenêtres et s'arrête automatiquement. Mais en cas de détection d'objets infectés, la fenêtre du scanner s'ouvrira dès l'analyse terminée. Ce mode prévoit que la liste des objets à scanner est paramétrée en ligne de commande.
- **/HA** – pour l'analyse heuristique des fichiers et la détection des virus pouvant se trouver dans de tels fichiers.
- **/INI:**<*chemin*> – utiliser un fichier de configuration alternatif avec le nom ou le chemin spécifié.
- **/NI** – ne pas utiliser les paramètres écrits dans le fichier de configuration `drweb32.ini`.
- **/LNG:**<*nom_fichier*> ou **/LNG** – utiliser le fichier alternatif de ressources linguistiques (`.dwl`) avec le nom ou le chemin spécifié. Si le chemin n'est pas spécifié, les ressources linguistiques par défaut (anglais, built-in) seront utilisées.
- **/ML** – analyser les fichiers sous format de mail (UUENCODE, XXENCODE, BINHEX et MIME). Cette ortographe de clé (/ML) active la notification utilisateur en cas de détection d'un objet suspect ou infecté dans une archive de mail. Les modificateurs ajoutés D, M, ou R, activent les actions suivantes :
  - **/MLD** – supprimer ;
  - **/MLM** – déplacer (par défaut, vers le dossier de Quarantaine) ;
  - **/MLR** – renommer (par défaut, le premier caractère de l'extension est remplacé par le symbole `#`) .
  - En outre, la clé peut se terminer par le modificateur supplémentaire `N` (d'autres modificateurs peuvent être également spécifiés). Dans ce cas, les informations sur les fichiers de mail ne seront pas imprimées.
- **/NS** – désactiver la possibilité d'interrompre l'analyse du PC. Si ce paramètre est spécifié, l'utilisateur ne peut pas interrompre le

fonctionnement du programme avec la touche ESC (ECHAP).

- **/OK** – afficher la liste complète des objets en cours d'analyse, en ajoutant aux objets sains la note OK.
- **/PF** – demander une confirmation pour l'analyse de la disquette suivante.
- **/PR** – afficher une requête de confirmation avant de procéder à l'action.
- **/QU** – le scanner va analyser les objets spécifiés dans la ligne de commande (les fichiers, disques, dossiers), à la fin de l'analyse le scanner s'arrête de façon automatique (seulement pour la version GUI du scanner).
- **/RP**<*nom_fichier*> ou **/RP+**<*nom_fichier*> – écrire le rapport sur le fonctionnement du programme dans le fichier dont le nom est spécifié dans la clé. Si le nom de fichier n'est pas spécifié, écrire le rapport dans le fichier déterminé par défaut. Le symbole + fait ajouter de nouvelles entrées, sinon le fichier sera écrasé.
- **/NR** – ne pas créer de fichier de log.
- **/SD** – vérifier les sous-dossiers.
- **/SO** – activer les sons.
- **/SS** – à la fin du fonctionnement, sauvegarder les modes spécifiés lors du dernier démarrage dans le fichier de configuration.
- **/TB** – vérifier les secteurs de démarrage et les secteurs de Master Boot Record (MBR) du disque dur.
- **/TM** – effectuer une analyse antivirus dans la mémoire vive (y compris la partie système Windows - seulement pour les scanners pour OS Windows).
- **/TS** – effectuer une analyse antivirus des fichiers d'autodémarrage (dans le dossier `Autodémarrage`, les fichiers de système `.ini`, la base de registre Windows). La clé est utilisée uniquement pour les **Scanners pour Windows**.
- **/UP** ou **/UPN** – vérifier les exécutables traités par les outils de compression suivants : ASPACK, COMPACK, DIET, EXEPACK, LZEXE etc. ; les fichiers modifiés par des applications BJFNT, COM2EXE, CONVERT, CRYPTCOM etc., ainsi que les fichiers immunisés par les vaccins CPAV, F-XLOCK, PGPROT, VACCINE etc. Pour désactiver l'affichage du nom de l'utilitaire utilisé pour

la compression, modification ou vaccination du fichier analysé, la clé **/UPN** peut être appliquée.

- **/WA** – ne pas quitter le programme sans avoir pressé n'importe quelle touche en cas de détection de virus ou d'objets suspects (seulement pour les scanners en ligne de commande).
- **/?** – afficher une rubrique d'aide abrégée sur le fonctionnement du programme.

Certains paramètres permettent d'ajouter le symbole "-" à la fin. Cette forme négative du paramètre désactive le mode correspondant. Cette fonction peut être utile au cas où le mode est activé par défaut ou selon les paramètres donnés dans le fichier de configuration. Voici la liste des paramètres de ligne de commande permettant d'ajouter cette option "négative" :

/ADW /AR /CU /DLS /FN /HCK /JOK /HA /IC /ML /MW /OK / PF /PR /RSK /SD /SO /SP /SS/TB /TM /TS /UP /WA

Pour les clés **/CU**, **/IC** è **/SP** l'option "négative" annule toute action mentionnée dans les paramètres respectifs. Cela signifie que le rapport va contenir des informations sur les objets infectés et suspects sans appliquer aucune action à ces objets.

Pour les clés /INI et /RP les formes "négatives" respectives sont les suivantes /NI et /NR.

Aucune forme négative n'est prévue pour les clés **/AL** et **/EX**, mais l'une annule l'autre.

Si la ligne de commande contient quelques clés contradictoires, seule la dernière clé est active.

Clés du Scanner en ligne de commande DWScancl

- **/AR** – scanner les archives. L'option est activée par défaut.
- **/AC** – scanner les conteneurs. L'option est activée par défaut.
- **/AFS** – utiliser un slash droit pour spécifier l'emboîtement dans l'archive. L'option est désactivée par défaut.

- **/ARC:**<*nombre*> – ratio maximum de compression. Si le **Scanner** détecte que le ratio dépasse le maximum spécifié, l'extraction depuis l'archive ne se fait pas et le scan de l'archive ne sera pas effectué. Par défaut – illimité.
- **/ARL:**<*nombre*> – niveau maximum d'emboîtement de l'archive scannée. Par défaut – illimité.
- **/ARS:**<*nombre*> – taille maximum de l'archive scannée, en Ko. Par défaut – illimité.
- **/ART:**<*nombre*> – seuil de vérification du ratio de compression (la taille minimum du fichier dans l'archive à partir de laquelle s'effectue la vérification du ratio de compression), en Ko. Par défaut – illimité.
- **/ARX:**<*nombre*> – taille maximum des objets archivés à scanner, en Ko. Par défaut – illimité.
- **/BI** – afficher des informations sur les bases virales. L'option est active par défaut.
- **/DR** – scanner les dossiers de manière récursive (vérifier les sous-dossiers). L'option est active par défaut.
- **/E:**<*nombre*> – utiliser un nombre spécifié de moteurs.
- **/FL:**<*nom_du_fichier*> – scanner les chemins spécifiés dans le fichier.
- **/FM:**<*masque*> – scanner les fichiers par masque. Par défaut, tous les fichiers sont scannés.
- **/FR:**<*expr_régulière*> – scanner les fichiers selon une expression régulière. Par défaut, tous les fichiers sont scannés.
- **/H** ou **/?** – afficher la rubrique d'aide sur le fonctionnement du programme.
- **/HA** – réaliser une analyse heuristique des fichiers afin d'y rechercher des virus inconnus. L'option est active par défaut.
- **/KEY:**<*fichier_clé*> – spécifier le chemin vers le fichier clé. Le paramètre est nécessaire si le fichier clé se trouve dans un dossier autre que le dossier dans lequel se trouve le **Scanner en ligne de commande**. Par défaut, le fichier clé depuis le dossier d'installation de l'**Antivirus** sera utilisée.
- **/LN** – scanner les fichiers par raccourcis associés. L'option est désactivée par défaut.
- **/LS** – scanner sous le compte LocalSystem. L'option est

désactivée par défaut.

- **/MA** – scanner les fichiers d'email. L'option est active par défaut.
- **/MC:**<*nombre*> – spécifier un nombre maximum de tentatives de désinfecter le fichier. Par défaut – illimité.
- **/NB** – ne pas créer les copies de sauvegardes des fichiers désinfectés/supprimés. L'option est désactivée par défaut.
- **/NI[:X]** – niveau de l'utilisation des ressources système, en pourcentage. Ce paramètre détermine le volume de mémoire utilisé pour le processus de scan et la priorité système de la tâche de scan. Par défaut – illimité.
- **/NT** – scanner les flux NTFS. L'option est active par défaut.
- **/OK** – afficher la liste complète des objets scannés et accompagner les objets sains par une note **Ok**. L'option est désactivée par défaut.
- **/P:**<*priorité*> – priorité de la tâche de scan en cours dans la file des tâches de scan :
  - *0* – inférieure.
  - *L* – basse.
  - *N* – normale. Priorité par défaut.
  - *H* – supérieur.
  - *M* – maximum.
- **/PAL**:<*nombre*> – niveau d'emboîtement des outils de compression. Par défaut – 1000.
- **/RA**:<*nom_du_fichier*> – ajouter le journal de fonctionnement du logiciel dans le fichier spécifié. Par défaut – ne pas créer un journal.
- **/RP**:<*nom_du_fichier*> – écrire le journal de fonctionnement du logiciel dans le fichier spécifié. Par défaut – ne pas créer un journal.
- **/RPC:**<*nombre*> – délai de connexion à **Scanning Engine**, en secondes. Par défaut – 30 s.
- **/RPCD** – utiliser l'identificateur dynamique RPC.
- **/RPCE** – utiliser l'adresse cible dynamique RPC.
- **/RPCE:**<*adresse cible*> – utiliser l'adresse cible RPC spécifiée.
- **/RPCH:**<*nom_hôté*> – utiliser le nom d'hôte spécifié pour les

appels RPC.

- **/RPCP:**<*protocole*> – utiliser le protocole spécifié RPC. Il est possible d'utiliser les protocoles : lpc, np, tcp.
- **/QL** – afficher la liste de tous les fichiers mis en **Quarantaine** sur tous les disques.
- **/QL:**<*nom du disque logique*> – afficher la liste des tous les fichiers mis en **Quarantaine** sur le disque logique spécifié.
- **/QR[:[d][:p]]** – supprimer les fichiers du disque spécifié <*d*> *(nom_du_disque_logique)*, se trouvant dans la **Quarantaine** depuis plus de <*p*> *(nombre)* jours. Si les valeurs <*d*> et <*p*> ne sont pas spécifiées, tous les fichiers se trouvant dans la **Quarantaine** seront supprimés depuis tous les disques logiques.
- **/QNA** – afficher les chemins entre guillemets doubles.
- **/REP** – scanner selon les liens symboliques. L'option est désactivée par défaut.
- **/SCC** – afficher le contenu des objets complexes. L'option est désactivée par défaut.
- **/SCN** – afficher le nom du conteneur. L'option est désactivée par défaut.
- **/SPN** – afficher le nom de l'outil de compression. L'option est désactivée par défaut.
- **/SLS** – afficher les logs sur l'écran. L'option est active par défaut.
- **/SPS** – afficher la progression du processus de scan. L'option est active par défaut.
- **/SST** – afficher la durée du scan. L'option est désactivée par défaut.
- **/TB** – scanner les secteurs de boot et les secteurs MBR du disque dur. L'option est désactivée par défaut.
- **/TM** – détecter les virus dans la mémoire vive (y compris la partie système Windows). L'option est désactivée par défaut.
- **/TS** – détecter les virus dans les fichiers d'autodémarrage (dossier Démarrage, fichiers système ini, base de registre Windows). L'option est désactivée par défaut.
- **/TR** – scanner les points de restauration système. L'option est désactivée par défaut.

- **/W**:<*secondes*> – durée maximum de scan, en secondes. Par défaut – illimité.
- **/WCL** – afficher dans la console compatible drwebwcl.
- **/X:S[:R]** – à la fin du scan, basculer la machine vers un mode de fonctionnement spécifié : arrêt/redémarrage/mode veille/ mode veille prolongé. Pour les modes arrêt/redémarrage, spécifier **R**.

Vous pouvez configurer les actions à appliquer aux différents types d'objets (**C** – désinfecter, **Q** – déplacer vers la quarantaine, **D** – supprimer, **I** – ignorer, **R** – informer. Par défaut, l'action Informer est spécifiée pour tous les types d'objet :

- **/AAD:**<*action*> – actions sur les adwares (actions possibles: DQIR).
- **/AAR:**<*action*> – actions sur les archives contaminées (actions possibles: DQIR).
- **/ACN:**<*action*> – actions sur les conteneurs contaminés (actions possibles: DQIR).
- **/ADL:**<*action*> – actions sur les dialers (actions possibles: DQIR).
- **/AHT:**<*action*> – actions sur les hacktools (actions possibles: DQIR).
- **/AIC:**<*action*> – actions sur les fichiers incurables (actions possibles: DQR).
- **/AIN:**<*action*> – actions sur les fichiers contaminés (actions possibles: CDQR).
- **/AJK:**<*action*> – actions sur les canulars (actions possibles: DQIR).
- **/AML:**<*action*> – actions sur les fichiers email contaminés (actions possibles: QIR).
- **/ARW:**<*action*> – actions sur les riskwares (actions possibles: DQIR).
- **/ASU:**<*action*> – actions sur les fichiers suspects (actions possibles: DQIR).

Certaines clés peuvent avoir des modificateurs activant ou désactivant le mode de fonctionnement de manière explicite. Par exemple :

/AC- le mode est explicitement désactivé,
/AC, **/AC+** le mode est explicitement activé.

Cette option peut être utile dans le cas où le mode est activé/désactivé par défaut ou selon le paramétrage du fichier de configuration. Les clés pouvant être utilisées avec des modificateurs sont les suivantes : **/AR**, **/AC**, **/AFS**, **/BI**, **/DR**, **/HA**, **/LN**, **/LS**, **/MA**, **/NB**, **/NT,** **/OK**, **/QNA**, **/REP**, **/SCC**, **/SCN**, **/SPN**, **/SLS**, **/SPS**, **/SST**, **/TB**, **/TM**, **/TS**, **/TR**, **/WCL**.

En cas de clé **/FL**, le modificateur "-" signifie : scanner les chemins listés dans le fichier spécifié et supprimer ce fichier.

En cas de clés **/ARC**, **/ARL**, **/ARS**, **/ART**, **/ARX**, **/NI[:X]**, **/PAL,** **/RPC**, **/W** dont la valeur est un chiffre, la valeur "0" enlève toute limitation.

Exemple d'utilisation des clés lors du démarrage du **Scanner en ligne de commande DWScancl**:

[*<chemin_vers_le_programme>*]`dwscancl /AR- /AIN:C /AIC:Q C:\`

scanner tous les fichiers se trouvant sur le disque `C`, excepté les archives ; désinfecter les fichiers infectés ; placer dans la **Quarantaine** les fichiers incurables.

Annexe B. Liste complète des OS supportés

OS de la famille UNIX :

Linux glibc 2.7 ou supérieur
FreeBSD 7.3 ou supérieur
Sun Solaris 10 (uniquement pour la plateforme Intel)

OS Windows :

- 32 bits :

Windows 98
Windows Millennium Edition
Windows NT4 (SP6a)
Windows 2000 Professional (SP4 avec Update Rollup 1)
Windows 2000 Server (SP4 avec Update Rollup 1)
Windows XP Professional (avec SP1 ou supérieur)
Windows XP Home (avec SP1 ou supérieur)
Windows Server 2003 (avec SP1 ou supérieur)
Windows Vista (avec SP1 ou supérieur)
Windows Server 2008 (avec SP1 ou supérieur)
Windows 7
Windows 8

- 64 bits :

Windows Server 2003 (avec SP1 ou supérieur)
Windows Vista (avec SP1 ou supérieur)
Windows Server 2008 (avec SP1 ou supérieur)
Windows Server 2008 R2
Windows 7

Windows Server 2012
Windows 8

SelfPROtect, SplDer Gate, Office Control, Firewall

- 32 bits :

Windows 2000 Professional (SP4 avec Update Rollup 1)
Windows 2000 Server (SP4 avec Update Rollup 1)
Windows XP Professional (avec SP1 ou supérieur)
Windows XP Home (avec SP1 ou supérieur)
Windows Server 2003 (avec SP1 ou supérieur)
Windows Vista (avec SP1 ou supérieur)
Windows Server 2008 (avec SP1 ou supérieur)
Windows 7
Windows 8

- 64 bits :

Windows Server 2003 (avec SP1 ou supérieur)
Windows Vista (avec SP1 ou supérieur)
Windows Server 2008 (avec SP1 ou supérieur)
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows 8

OS Windows Mobile

Windows Mobile 2003
Windows Mobile 2003 Second Edition
Windows Mobile 5.0
Windows Mobile 6.0
Windows Mobile 6.1
Windows Mobile 6.5

OS Novell NetWare

Novell NetWare 4.11 SP9
Novell NetWare 4.2
Novell NetWare 5.1
Novell NetWare 6.0
Novell NetWare 6.5

Mac OS X

Mac OS 10.6 (Snow Leopard)
Mac OS 10.6 Server (Snow Leopard Server)
Mac OS 10.7 (Lion)
Mac OS 10.7 Server (Lion Server)
Mac OS 10.8 (Mountain Lion)
Mac OS 10.8 (Mountain Lion Server)

OS Android

Android 1.6
Android 2.0
Android 2.1
Android 2.2
Android 2.3
Android 3.0
Android 3.1
Android 3.2
Android 4.0.

Les fonctions de **l'Agent** sous Windows Mobile et sous Novell NetWare sont décrites dans les manuels respectifs **Dr.Web Agent pour Windows Mobile** et **Dr.Web Agent pour Novell NetWare**.

Annexe C. Méthodes de détection des virus

Tous les composants antivirus **Dr.Web** utilisent en même temps plusieurs méthodes de détection des objets malveillants ce qui permet de vérifier de manière approfondie les fichiers suspects et de contrôler le comportement des programmes :

1. En premier lieu, l'analyse de *signature* est effectuée. Elle consiste à analyser le code des fichiers suspects afin de dépister des correspondances aux signatures des virus connus (la *signature* présente une séquence continue et finie de bytes qui est nécessaire et suffisante pour dépister un virus). La comparaison se fait selon le total de contrôle des signatures, ce qui permet de minimiser la taille des entrées dans les bases virales tout en gardant lune correspondance univoque et en assurant ainsi la validité de détection et l'efficacité de réparation des fichiers infectés. **Les bases virales Dr.Web** sont organisées de sorte qu'une seule entrée permette de détecter des classes entières de menaces.
2. A la fin de l'analyse de signature, la technologie unique **Origins Tracing™** est appliquée. Cette technologie permet de détecter de nouveaux virus et des virus modifiés utilisant des mécanismes connus de contamination des fichiers. Par exemple la technologie protège les utilisateurs des solutions antivirus **Dr.Web** contre des virus comme le Trojan.Encoder.18 (connu aussi sous le nom gpcode). De plus, la technologie **Origins Tracing** permet de minimiser considérablement le taux de fausses alertes du moteur heuristique.
3. Le fonctionnement du moteur heuristique est basé sur certaines connaissances (*heuristiques*) sur les critères caractéristiques du code viral et relatives au code sain. Chaque critère a un score (un nombre correspondant à la gravité et à la validité du critère). Compte tenu du score total calculé pour chaque fichier, le moteur heuristique détermine une probabilité de contamination du fichier par un virus inconnu. Comme tout système de validation des hypothèses, le moteur heuristique peut commettre des erreurs de premier ordre (non détection

des virus inconnus) et de deuxième ordre (fausse alerte).

Lors de tout type d'analyse, les compostants de l'antivirus **Dr.Web** utilisent les informations les plus récentes sur les programmes malveillants. Les signatures des virus, les informations sur leurs signes et modes de comportement sont mises à jour dès que les spécialistes du **Laboratoire antivirus Doctor Web** détectent de nouvelles menaces. La fréquence des mises à jour peut atteindre plusieurs fois par heure. Ainsi, la mise à jour automatisée et régulière des bases virales permet de détecter même des virus tout récents.

Référence

Référence

J

L

M

N

O

P

Q

Référence