



Dr.WEB

Antivirus pour Windows

Manuel utilisateur



© **Doctor Web, 2021. Tous droits réservés**

Le présent document est un document d'information et de référence concernant le logiciel de la famille Dr.Web y spécifié. Ce document ne justifie pas les conclusions exhaustives sur la présence ou l'absence de tout paramètre fonctionnel et/ou technique dans le logiciel de la famille Dr.Web et ne peut pas être utilisé pour déterminer la conformité du logiciel de la famille Dr.Web aux exigences, tâches techniques et/ou paramètres quelconques ainsi qu'aux autres documents de tierces personnes.

Ce document est la propriété de Doctor Web et peut être utilisé uniquement à des fins personnelles de l'acheteur du produit. Aucune partie de ce document ne peut être reproduite, publiée ou transmise sous quelque forme que ce soit, par quelque moyen que ce soit et dans quelque but que ce soit sinon pour une utilisation personnelle de l'acheteur sans attribution propre.

Marques déposées

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk, KATANA et le logo Dr.WEB sont des marques déposées et des marques commerciales de Doctor Web en Russie et/ou dans d'autres pays. D'autres marques déposées, marques commerciales et noms de société utilisés dans ce document sont la propriété de leurs titulaires respectifs.

Limitation de responsabilité

En aucun cas Doctor Web et ses revendeurs ne sont tenus responsables des erreurs/lacunes éventuelles pouvant se trouver dans cette documentation, ni des dommages directs ou indirects causés à l'acheteur du produit, y compris la perte de profit.

Antivirus Dr.Web pour Windows

Version 11.5

Manuel utilisateur

31/08/2021

Doctor Web, Siège social en Russie

Adresse : 2-12A, 3e rue Yamskogo polya, 125124 Moscou, Russie

Site web : <https://www.drweb.com/>

Téléphone : +7 (495) 789-45-87

Vous pouvez trouver les informations sur les bureaux régionaux sur le site officiel de la société.

Doctor Web

Doctor Web — éditeur russe de solutions de sécurité informatique.

Doctor Web propose des solutions antivirus et antispam efficaces pour les institutions publiques, les entreprises, ainsi que pour les particuliers.

Les solutions antivirus Dr.Web sont connues depuis 1992 pour leur excellence en matière de détection des programmes malveillants et leur conformité aux standards internationaux de sécurité.

Les certificats et les prix attribués, 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 !



Contenu

1. Introduction	6
1.1. Contenu de ce Manuel	7
1.2. Conventions et abréviations	7
1.3. Méthode de détection des menaces	8
2. Pré-requis système	13
3. Installation, modification et suppression du programme	16
3.1. Installation du programme	16
3.2. Modification des composants du programme	20
3.3. Suppression du logiciel	22
4. Licence	25
4.1. Comment activer la licence	26
4.2. Renouveler la licence	33
4.3. Fichier clé	34
5. Mise en route	36
5.1. Tester l'antivirus	37
6. Outils	39
6.1. Gestionnaire de licences	39
6.2. Réseau antivirus	40
6.3. Gestionnaire de quarantaine	41
6.4. Support	42
6.4.1. Créer un rapport	43
7. Mise à jour des bases et des modules de programme	47
8. Scanner Dr.Web	49
8.1. Lancement et modes d'analyse	49
8.2. Actions en cas de détection de menaces	51
8.3. Lancement du Scanner avec les paramètres de la ligne de commande	53
8.4. Scanner en ligne de commande	53
8.5. Lancement de l'analyse selon la planification	54
9. Configuration	55
10. Paramètres généraux	56
10.1. Notifications	56
10.2. Mise à jour	60



10.3. Réseau	63
10.4. Autoprotection	65
10.5. Dr.Web Cloud	67
10.6. Réseau antivirus	69
10.7. Avancé	70
11. Exclusions	73
11.1. Dossiers et fichiers	73
11.2. Applications	75
12. Composants de protection	80
12.1. SplDer Guard	80
12.1.1. Configurer SplDer Guard	81
12.2. SplDer Mail	85
12.2.1. Configurer SplDer Mail	86
12.3. Scanner	90
12.4. Pare-feu	92
12.4.1. Apprentissage du Pare-feu	93
12.4.2. Configuration du Pare-feu	95
12.5. Dr.Web pour Outlook	106
12.5.1. Analyse antivirus	107
12.5.2. Journal des événements	109
12.5.3. Statistiques	110
12.6. Protection préventive	111
13. Statistiques	117
14. Support technique	119
15. Annexe A. Paramètres supplémentaires de ligne de commande	120
15.1. Paramètres du Scanner et du Scanner en ligne de commande	120
15.2. Paramètres du Module de mise à jour	127
15.3. Codes de retour	130
16. Annexe B. Menaces et méthodes de neutralisation	132
16.1. Classification de menaces	132
16.2. Actions appliquées aux menaces détectées	137
17. Annexe C. Principes de nomination des menaces	138



1. Introduction

Antivirus Dr.Web pour Windows est destiné à protéger la mémoire système, les disques durs et les supports amovibles tournant sous les OS de la famille Microsoft® Windows® contre menaces de tout types : virus, rootkits, trojans, spywares, adwares, hacktools et d'autres objets malveillants provenant de sources externes.

Du point de vue de l'architecture, Antivirus Dr.Web pour Windows est composé de plusieurs modules responsables des fonctions différentes. Le moteur antivirus et les bases virales sont communs pour tous les composants et les plateformes différentes.

Les composants du produit sont constamment mis à jour, les bases virales, les bases des catégories de ressources web et les bases des règles de filtrage antispam de messages e-mail sont régulièrement complétées par les signatures de virus. La mise à jour permanente assure un niveau actuel de la protection des appareil de l'utilisateur, ainsi que des applications et des données. Pour une protection supplémentaires contre des logiciels malveillants, on utilise les méthodes de l'analyse heuristiques réalisées dans le moteur antivirus.

Antivirus Dr.Web pour Windows peut détecter et supprimer les programmes indésirables (adwares, dialers, canulars, riskwares et hacktools) de votre ordinateur. Dr.Web utilise ses composants antivirus standard pour détecter des programmes indésirables et appliquer des actions aux fichiers qu'ils contiennent.

Chaque solution antivirus Dr.Web pour les systèmes d'exploitation Microsoft® Windows® inclut l'ensemble de composants suivants :

[Scanner Dr.Web](#) : scanner antivirus avec interface graphique, lancé sur demande de l'utilisateur ou selon la planification. Il analyse votre ordinateur à la recherche de virus et autres logiciels malveillants.

[Scanner en ligne de commande Dr.Web](#) : version du Scanner Dr.Web avec l'interface de la ligne de commande.

[SplDer Guard](#) : moniteur antivirus qui réside toujours en mémoire vive et analyse les processus lancés et les fichiers créés et détecte toute activité malveillante.

[SplDer Mail](#) : moniteur antivirus de messagerie pour les postes de travail qui intercepte toutes les requêtes de clients de messagerie fonctionnant sur l'ordinateur aux serveurs de messagerie via les protocoles POP3/SMTP/IMAP4/NNTP (sous IMAP4 on comprend le protocole IMAPv4rev1). Il détecte et neutralise les menaces avant que les messages soient reçus du serveur (ou envoyés sur le serveur de messagerie) par le client de messagerie.

[Dr.Web pour Outlook](#) : plug-in qui analyse les boîtes mail Microsoft Outlook pour la présence de menaces.

[Pare-feu Dr.Web](#) : pare-feu personnel qui protège votre ordinateur d'un accès non autorisé et prévient la perte de données vitales via le réseau.



Module de mise à jour : il permet aux utilisateurs enregistrés de recevoir et d'installer automatiquement les mises à jour des bases virales et des modules Dr.Web.

Agent Dr.Web : module qui vous aide à configurer et à gérer les composants du produit antivirus.

Protection préventive : composant contrôlant l'accès aux objets importants du système et assurant l'intégrité des applications lancées et des fichiers de l'utilisateur ainsi que la protection contre les exploits.

1.1. Contenu de ce Manuel

Ce Manuel Utilisateur décrit l'installation et l'utilisation optimale de Dr.Web.

Vous pouvez trouver une description détaillée des éléments de la GUI dans le système d'aide accessible depuis n'importe quel composant.

Ce Manuel Utilisateur décrit l'installation du logiciel et contient des conseils sur son utilisation et sur la résolution des problèmes les plus courants causés par les menaces virales. Surtout, il décrit les modes de fonctionnement standard des composants de Dr.Web (avec les paramètres par défaut).

Les Annexes contiennent des informations détaillées sur la façon de paramétrer Dr.Web, pour les utilisateurs expérimentés.



Etant en développement constant, l'interface du logiciel peut afficher d'autres images que celles contenues dans le présent Manuel. Vous pouvez trouver les informations toujours à jour sur <https://download.drweb.com/doc>.

1.2. Conventions et abréviations

Les styles utilisés dans ce manuel :

Style	Commentaire
	Avertissement sur des situations potentielles d'erreurs et sur les éléments importants auxquels il faut faire attention.
<i>Réseau antivirus</i>	Un nouveau terme ou l'accent mis sur un terme dans les descriptions.
<IP-address>	Champs destinés à remplacer les noms fonctionnels par leurs valeurs.
Enregistrer	Noms des boutons de l'écran, des fenêtres, des éléments de menu et d'autres éléments de l'interface du logiciel.
CTRL	Touches du clavier.



Style	Commentaire
C:\Windows\	Noms de fichiers/dossiers ou fragments de programme.
Annexe A	Liens vers les autres chapitres du manuel ou liens vers des ressources externes.

1.3. Méthode de détection des menaces

Toutes les solutions antivirus créées par Doctor Web utilisent un ensemble de méthodes de détection, ce qui leur permet d'effectuer des analyses en profondeur des fichiers suspects.

Analyse de signature

Cette méthode de détection est appliquée en premier lieu. Elle est mise en oeuvre en examinant le contenu de l'objet à la recherche des signatures de menaces connues. Une Signature est une séquence continue et finie d'octets qui est nécessaire et suffisante pour identifier une menace. La comparaison du contenu de l'objet avec les signatures n'est pas effectuée directement, mais par leur somme de contrôle ce qui permet de réduire considérablement la taille des entrées dans les bases de données virales tout en préservant le caractère unique de la conformité et par conséquent, l'exactitude de la détection des menaces et du traitement des objets infectés. Les entrées dans les bases virales Dr.Web sont rédigées de sorte que la même entrée peut détecter des classes entières ou des familles de menaces.

Origins Tracing

Cette une technologie unique Dr.Web permettant de détecter les nouvelles menaces ou celles modifiées et utilisant des mécanismes de contamination ou un comportement malveillant qui sont déjà connus de la base de données virale. Cette technologie intervient à la fin de l'analyse par signature et assure une protection des utilisateurs utilisant des solutions antivirus Dr.Web contre des menaces telles que Trojan.Encoder.18 (également connu sous le nom « gpcodex »). En outre, l'utilisation de la technologie Origins Tracing peut réduire considérablement le nombre de faux positifs de l'analyseur heuristique. Les noms des menaces détectées à l'aide d'Origins Tracing sont complétés par `.Origin`.

Émulation de l'exécution

La méthode d'émulation d'exécution de code est utilisée pour détecter les virus polymorphes et cryptés si la recherche à l'aide des sommes de contrôle des signatures est inapplicable ou très compliquée en raison de l'impossibilité de construire des signatures fiables. La méthode consiste à simuler l'exécution du code en utilisant l'*émulateur* — un modèle du processeur et de l'environnement du programme. L'Émulateur fonctionne avec un espace mémoire protégé (*tampon d'émulation*). Dans ce cas, les instructions ne sont pas transmises au processeur central pour



exécution réelle. Si le code traité par l'émulateur est infecté, alors le résultat de son émulation est un rétablissement du code malveillant d'origine disponible pour une analyse de signature.

Analyse heuristique

Le fonctionnement de l'analyseur heuristique est fondé sur un ensemble d'*heuristiques* (hypothèses, dont la signification statistique est confirmée par l'expérience) des signes caractéristiques de code malveillant et, inversement, de code exécutable sécurisé. Chaque attribut ou caractéristique du code possède un score (le nombre indiquant l'importance et la validité de cette caractéristique). Le score peut être positif si le signe indique la présence d'un comportement de code malveillant, et négatif si le signe ne correspond pas à une menace informatique. En fonction du score total du contenu du fichier, l'analyseur heuristique calcule la probabilité de la présence d'un objet malveillant inconnu. Si cette probabilité dépasse une certaine valeur de seuil, l'objet analysé est considéré comme malveillant.

Ce mécanisme permet de construire des hypothèses heuristiques sur la présence d'objets malveillants dans les objets, de logiciels compressés par des outils de compression (emballeurs), non seulement par des outils connus des développeurs des produits Dr.Web, mais également par des outils de compression nouveaux et inexplorés. Lors de la vérification des objets emballés, une technologie d'analyse de leur entropie structurelle est également utilisée, cette technologie peut détecter les menaces sur les spécificités de la localisation des fragments de leur code. Cette technologie permet avec une seule entrée de la base de données de détecter un ensemble de différents types de menaces qui sont emballées du même packer polymorphe. L'analyseur heuristique utilise également la technologie FLY-CODE — un algorithme universel pour l'extraction des fichiers.

Comme tout système basé sur des hypothèses, l'analyseur heuristique peut commettre des erreurs de type I (omettre une menace inconnue) ou de type II (faire un faux positif). Par conséquent, les objets marqués par l'analyseur heuristique comme « malveillants » reçoivent le statut « suspects ».

Analyse de comportement

Les techniques de l'analyse de comportement permettent d'analyser la cohérence des actions de tous les processus du système. Si une application se comporte comme un programme malveillant, ses actions seront bloquées.

Dr.Web Process Heuristic

La technologie de l'analyse de comportement Dr.Web Process Heuristic protège contre les nouveaux programmes les plus dangereux qui sont capables d'éviter la détection par les moyens traditionnels : le mécanisme de signatures et le mécanisme heuristique.

Dr.Web Process Heuristic analyse le comportement de chaque programme lancé en consultant le service cloud Dr.Web qui est mis à jour constamment. Dr.Web Process Heuristic se base sur les



connaissances actuelles sur le comportement des programmes malveillants, il évalue le niveau de danger et prend les mesures nécessaires afin de neutraliser la menace.

Cette technologie permet de minimiser les pertes dues à l'action d'un virus inconnu — en cas de consommation minimum des ressources du système à protéger.

Dr.Web Process Heuristic contrôle toutes les tentatives de modifier le système :

- il identifie les processus de programmes malveillants qui modifient des fichiers utilisateur d'une manière indésirable (par exemple, les tentatives de chiffrement de la part des trojans-encodeurs), y compris les fichiers se trouvant dans des répertoires accessibles par le réseau ;
- il empêche les tentatives de programmes malveillants de s'infiltrer dans des processus d'autres applications ;
- il protège les zones critiques du système contre les modifications par les programmes malveillants ;
- il détecte et arrête des scripts et des processus malveillants, suspects et peu fiables ;
- il bloque la possibilité de modifier les zones d'amorçage du disque par les programmes malveillants afin d'éviter le lancement (par exemple, d'un bootkit) sur l'ordinateur ;
- il prévient la désactivation de la mode sécurisée Windows en bloquant les modifications du registre ;
- il n'autorise pas aux programmes malveillants de modifier les règles de lancement de programmes ;
- il bloque les téléchargements de nouveaux pilotes ou de pilotes inconnus qui sont lancés sans avertissement de l'utilisateur ;
- il bloque l'autodémarrage de programmes malveillants et des applications particulières, par exemple des anti-antivirus en les empêchant de s'enregistrer dans le registre pour le lancement ultérieur ;
- il bloque les branches du registre qui sont responsables des pilotes des dispositifs virtuels ce qui rend impossible l'installation du cheval de Troie sous forme d'un nouveau dispositif virtuel ;
- il ne permet pas au logiciel malveillant de perturber le fonctionnement normal des services système.

Dr.Web Process Dumper

L'analyseur complexe des menaces compressées Dr.Web Process Dumper augmente considérablement le niveau de détection des menaces supposées « nouvelles » (ce sont des menaces connues dans la base virale de Dr.Web, mais elle sont masquées sous de nouveaux packers) et exclut la nécessité d'ajouter dans les bases de nouvelles entrées portant sur les menaces. Vu que les bases virales Dr.Web gardent leur taille réduite, les pré-requis système n'augmentent pas et les mises à jour restent légères pendant que la détection et la désinfection de menaces est de haut niveau.



Dr.Web ShellGuard

La technologie Dr.Web ShellGuard protège l'ordinateur contre les *exploits* — les objets malveillants qui essaient d'exploiter les vulnérabilités afin d'obtenir le contrôle sur les applications attaquées et sur le système entier.

Dr.Web ShellGuard protège les applications les plus utilisées installées sur les ordinateurs tournant sous Windows :

- les navigateurs web (Internet Explorer, Mozilla Firefox, Yandex.Browser, Google Chrome, Vivaldi Browser, etc.) ;
- les applications MS Office, y compris MS Office 2016 ;
- les applications système ;
- les applications utilisant les technologies java, flash et pdf ;
- les lecteurs média.

En analysant des actions potentiellement dangereuses, le système de protection grâce à la technologie Dr.Web ShellGuard se base non seulement sur les règles établies qui sont sauvegardées sur l'ordinateur mais aussi sur les connaissances du service cloud Dr.Web dans lequel sont collectées :

- les données sur les algorithmes des programmes aux intentions malveillantes ;
- les informations sur les fichiers sains ;
- les informations sur les signatures numériques compromises des développeurs de logiciels célèbres ;
- les informations sur les signatures numériques des logiciels publicitaires ou potentiellement dangereux ;
- les algorithmes de protection de telles ou telles applications.

Méthode de l'apprentissage machine

Elle est utilisée pour rechercher et neutraliser les objets malveillant qui ne sont pas encore inclus dans les bases virales. L'avantage de cette méthode est que le code malveillant est détecté en fonction de ses caractéristiques, sans être exécuté.

La détection de menaces est basée sur la classification des objets malveillants par les caractéristiques particulières. La technologie de l'apprentissage machine est basée sur les machines à vecteurs de support et elle permet d'effectuer la classification et l'enregistrement des fragments du code de langages de script dans la base. Ensuite, les objets détectés sont analysés pour leur conformité aux caractéristiques du code malveillant. La technologie de l'apprentissage machine met à jour automatiquement la liste des caractéristiques et les bases virales. Grâce à la connexion au service cloud, de grands volumes de données sont traités plus vite et l'apprentissage constant du système assure la protection préventive contre les menaces les plus récentes. De plus, la technologie peut fonctionner sans la connexion permanente au cloud.



La méthode de l'apprentissage machine économise les ressources du système d'exploitation car elle ne nécessite pas l'exécution du code pour détecter des menaces et l'apprentissage machine dynamique peut s'effectuer sans la mise à jour permanente de bases virales comme c'est le cas de l'analyse de signatures.

Technologies cloud de détection de menaces

Les méthodes cloud de détection permettent d'analyser n'importe quel objet (fichier, application, extension pour le navigateur, etc.) par la somme de contrôle. La somme de contrôle est une séquence de lettres et chiffres de la longueur spécifiée. Lors de l'analyse par la somme de contrôle les objets sont vérifiés dans la base existante et puis, ils sont classés en catégories : sains, suspects, malveillants, etc.

Une telle technologie réduit le temps de l'analyse des fichiers et économise les ressources de l'appareil. Vu que c'est la somme de contrôle unique est analysée et non pas l'objet, la décision est prise tout de suite. S'il n'y a pas de connexion aux serveurs Dr.Web, les fichiers sont analysés de manière locale et l'analyse cloud est reprise après la restauration de la connexion.

Ainsi, le service cloud de Doctor Web collecte les informations sur de multiples utilisateurs et met rapidement à jour les données sur les menaces inconnues auparavant ce qui augmente l'efficacité de la protection des appareils.



2. Pré-requis système




Avant d'installer Dr.Web :

- supprimez tout autre antivirus installé sur votre machine afin d'éviter les incompatibilités de ses composants résidents avec les composants résidents de Dr.Web ;
- si Pare-feu Dr.Web est installé, vous devrez supprimer tout autre pare-feu installé sur votre ordinateur ;
- installez toutes les mises à jour critiques recommandées par Microsoft. Si l'OS n'est plus supporté, migrez vers une nouvelle version de l'OS.

Dr.Web est incompatible avec les produits de la protection proactive d'autres développeurs.

Dr.Web peut être installé et fonctionne sur un ordinateur possédant au minimum ces pré-requis :

Composant	Pré-requis
Processeur	Processeur pleinement compatible i686.
Système d'exploitation	<p>Pour les plateformes 32-bits :</p> <ul style="list-style-type: none">• Windows XP avec Service Pack 2 ou supérieur ;• Windows Vista avec Service Pack 2 ou supérieur ;• Windows 7 avec Service Pack 1 ou supérieur ;• Windows 8 ;• Windows 8.1 ;• Windows 10 21H1 ou une version antérieure. <p>Pour les plateformes 64-bits :</p> <ul style="list-style-type: none">• Windows Vista avec Service Pack 2 ou supérieur ;• Windows 7 avec Service Pack 1 ou supérieur ;• Windows 8 ;• Windows 8.1 ;• Windows 10 21H1 ou une version antérieure.



Vu que la société Microsoft ne supporte plus l'algorithme de hachage SHA-1, assurez-vous que votre système d'exploitation supporte l'algorithme de hachage SHA-256 avant d'installer Antivirus Dr.Web pour Windows sous Windows Vista/Windows 7. Pour ce faire, installez toutes les



Composant	Pré-requis
	<p>mises à jour recommandées depuis le Centre de mise à jour Windows. Pour en savoir plus sur les paquets de mises à jour nécessaires, visitez le site officiel de la société Doctor Web .</p>
RAM disponible	512 Mo et plus.
Résolution	Résolution d'écran recommandée est au minimum de 800x600.
Support d'environnements virtuels et cloud	Le programme fonctionne dans les environnements suivants : <ul style="list-style-type: none">• VMware ;• Hyper-V ;• Xen ;• KVM.
Autre	Le plug-in Dr.Web pour Outlook nécessite l'installation du client Microsoft Outlook intégré dans Microsoft Office : <ul style="list-style-type: none">• Outlook 2000 ;• Outlook 2002 ;• Outlook 2003 ;• Outlook 2007 ;• Outlook 2010 avec Service Pack 2 ;• Outlook 2013 ;• Outlook 2016.

Pour le fonctionnement correct de Dr.Web, les ports suivants doivent être ouverts :

Destination	Direction	Numéros de ports
Pour activer et renouveler une licence	sortant	443
Pour mettre à jour (si l'option de mise à jour via https est activée)	sortant	443
Pour mettre à jour	sortant	80
Pour envoyer les notifications		25 ou 465 (ou en fonction des paramètres des notifications par e-mail)



Destination	Direction	Numéros de ports
Pour se connecter au service Dr.Web Cloud	sortant	2075 (y compris les ports UDP)

Pour d'autres pré-requis, se référer au système d'exploitation correspondant.



3. Installation, modification et suppression du programme

Avant d'installer Antivirus Dr.Web pour Windows, consultez les [pré-requis système](#) et effectuez les actions suivantes :

- installer toutes les mises à jour critiques de Microsoft pour la version de l'OS utilisée sur votre ordinateur (elles sont disponibles sur le site de mises à jour de la société à la page : <https://windowsupdate.microsoft.com>) ;
- vérifier le système de fichiers en utilisant les outils système, et en cas d'erreurs détectées, résoudre le problème ;
- fermer toutes les applications en cours.



Avant de procéder à l'installation, il est nécessaire de supprimer tous les logiciels antivirus installés sur l'ordinateur et les pare-feu afin d'éviter une éventuelle incompatibilité de leurs composants résidents.

Il est nécessaire d'avoir les droits administrateur sur l'ordinateur pour installer Dr.Web.

L'installation de Dr.Web se fait dans l'un des modes suivants :

- en mode de la ligne de commande ;
- en mode de l'assistant d'installation.

3.1. Installation du programme



Il est nécessaire d'avoir les droits administrateur sur l'ordinateur pour installer Dr.Web.

Installation en mode de la ligne de commande

Pour installer Dr.Web en tâche de fond, entrez dans la ligne de commande le nom du fichier exécutable avec les paramètres nécessaires (ces paramètres affectent l'installation en tâche de fond, la langue d'installation et le redémarrage après l'installation, ainsi que l'installation du Pare-feu) :

Paramètre	Valeur
installFirewall	Le Pare-feu Dr.Web sera installé.
lang	Langue utilisée pour l'installation. La valeur de ce paramètre est la langue au format ISO 639-1.
reboot	Redémarre l'ordinateur automatiquement après l'installation complète.



Paramètre	Valeur
silent	Installation en tâche de fond.

Par exemple, pour lancer une installation de Dr.Web en tâche de fond avec un redémarrage après l'installation, exécutez la commande suivante :

```
drweb-11.5-av-win.exe /silent yes /reboot yes
```

Installation en mode de l'assistant d'installation

Pour lancer l'installation en mode standard, suivez l'une des instructions ci-dessous :

- si vous avez un fichier exécutable unique, lancez-le ;
- si vous possédez le package d'installation enregistré sur le disque Dr.Web, insérez le disque dans le lecteur. Si le démarrage automatique est activé pour ce lecteur, l'installation va démarrer automatiquement. Si le démarrage automatique n'est pas activé, lancez le fichier autorun.exe se trouvant sur le disque. Une fenêtre affichant le menu d'autorun sera ouverte. Cliquez sur le bouton **Installer**.

Suivez les instructions de l'assistant d'installation. A chaque étape avant la copie de fichier sur l'ordinateur, vous pouvez réaliser les fonctions suivantes :

- pour revenir vers l'étape précédente de l'installation, cliquez sur **Retour** ;
- pour passer à l'étape suivante, cliquez sur **Suivant** ;
- pour interrompre l'installation, cliquez sur **Annuler**.

Procédure d'installation

1. Si un autre antivirus est déjà installé sur votre ordinateur, l'Assistant d'installation va vous alerter sur l'incompatibilité de Dr.Web avec d'autres solutions antivirus, et il vous sera proposé de les supprimer.



Avant l'installation, le statut du fichier d'installation est vérifié. S'il existe une version plus récente du fichier d'installation, vous serez invité à la télécharger.

2. A cette étape, vous êtes invité à vous connecter aux [services cloud Dr.Web](#) qui permettent aux composants antivirus d'utiliser les données virales les plus récentes. Ces données sont stockées et mises à jour en temps réel sur les serveurs de Doctor Web. L'option est activée par défaut. Vous pouvez également indiquer si vous souhaitez d'installer Pare-feu Dr.Web.



Figure 1. Assistant d'installation

3. Pour sélectionner les composants que vous souhaitez installer, spécifiez le chemin d'installation de ces composants et d'autres paramètres puis cliquez sur **Paramètres d'installation**. Cette option est destinée aux utilisateurs expérimentés. Si vous voulez effectuer l'installation avec les paramètres par défaut, passez à l'étape 4.
 - Dans cette fenêtre, vous pouvez modifier l'ensemble de composants à installer.
 - Dans cette fenêtre, vous pouvez modifier le chemin d'installation.
 - Dans le troisième onglet de la fenêtre, vous pouvez cocher la case **Télécharger des mises à jour pendant l'installation** afin de télécharger les mises à jour des bases virales et des composants lors de l'installation. Cette fenêtre vous permet également de créer des raccourcis pour le lancement de Dr.Web.
 - Vous pouvez indiquer les paramètres du serveur proxy, si cela est nécessaire.Pour sauvegarder les modifications apportées, cliquez sur **OK**. Pour quitter sans enregistrer les modifications, cliquez sur **Annuler**.
4. Cliquez sur **Suivant**. Ainsi vous acceptez les termes du contrat de licence.
5. Dans la fenêtre **Assistant d'enregistrement**, il faut sélectionner l'une des options suivantes :
 - si vous possédez un [fichier clé](#) sur le disque dur ou sur un support amovible, sélectionnez **Spécifiez le chemin vers le fichier clé valide**. Pour sélectionner le fichier clé, cliquez sur **Parcourir** et sélectionnez le fichier nécessaire dans la fenêtre qui s'affiche. Pour en savoir plus, consultez le manuel [Activation de la licence avec le fichier clé](#) ;
 - si vous n'avez pas de fichier clé, mais vous voulez le recevoir durant l'installation, sélectionnez **Obtenir le fichier clé lors de l'installation**. Pour en savoir plus, consultez le manuel [Activation de la licence avec le numéro de série](#) ;



- pour continuer l'installation **sans licence**, sélectionnez **Obtenir le fichier clé plus tard**. La mise à jour n'est pas disponible tant que vous n'avez pas obtenu de fichier clé.

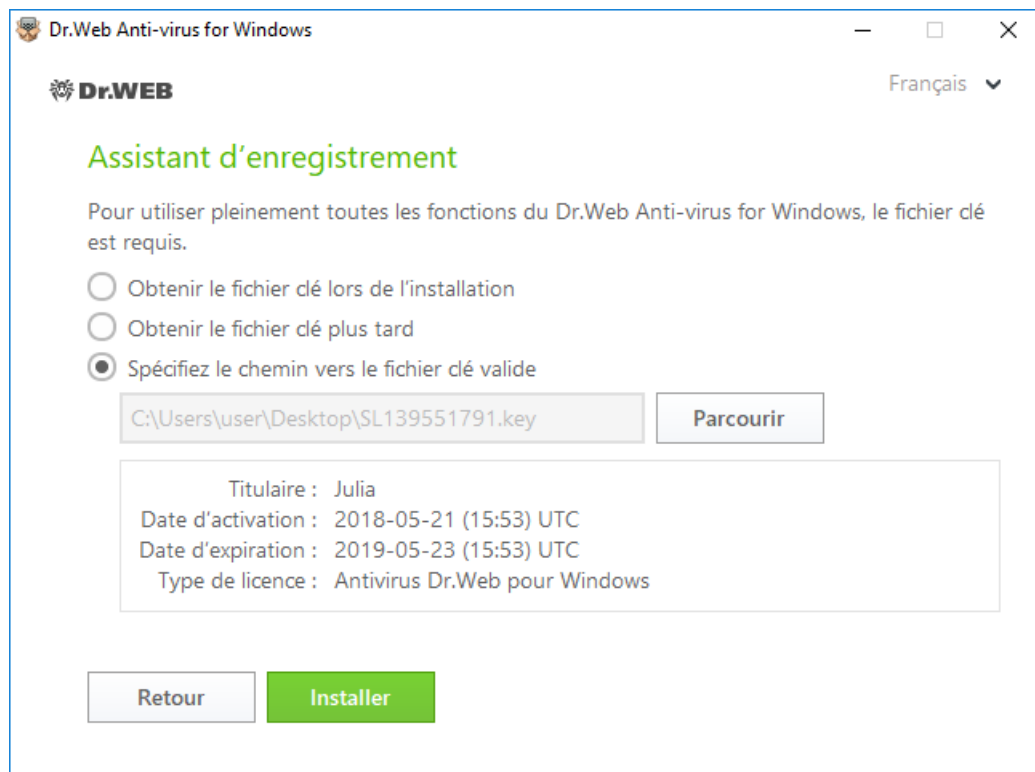


Figure 2. Assistant d'enregistrement

Cliquez sur **Installer**.

6. Si lors de l'installation vous avez spécifié ou reçu un fichier clé valide et que vous n'avez pas décoché la case **Télécharger des mises à jour pendant l'installation**, les bases virales et d'autres composants de Dr.Web seront mis à jour. La mise à jour démarre automatiquement et ne requiert aucune action supplémentaire.
7. Pour terminer l'installation, redémarrez l'ordinateur.

Erreur du service BFE lors de l'installation du logiciel Dr.Web

Pour le fonctionnement de certains composants de Dr.Web, il faut que le service du moteur de filtrage de base (BFE) soit lancé. Si ce service est manquant ou endommagé, l'installation de Dr.Web est impossible. L'endommagement ou l'absence du service BFE peut signaler la présence des menaces de sécurité sur votre ordinateur.

Si la tentative d'installer Dr.Web a échoué avec l'erreur du service BFE, faites le suivant :

1. Scannez le système avec l'utilitaire gratuit CureIt! de Doctor Web. Vous pouvez télécharger l'utilitaire sur le site : <https://free.drweb.com/download+cureit+free/>.
2. Restaurez le service BFE. Pour cela, vous pouvez utiliser l'utilitaire de résolution de problèmes du Pare-feu créé par Microsoft (pour les systèmes d'exploitation Windows 7 ou les versions



supérieures). Vous pouvez télécharger l'utilitaire sur le site : <https://support.microsoft.com/en-us/help/17613/automatically-diagnose-and-fix-problems-with-windows-firewall>.

3. Lancez l'Assistant d'installation Dr.Web et effectuez l'installation selon la procédure standard décrite ci-dessus.

Si le problème persiste, contactez le support technique de Doctor Web.

3.2. Modification des composants du programme

1. Pour supprimer ou modifier les composants de Dr.Web, sélectionnez (en fonction du système d'exploitation) :

Système d'exploitation	Suite des actions			
Windows XP	Menu Démarrer	Démarrer → Panneau de configuration → Ajout/suppression de programmes		
	Menu Démarrer classique	Démarrer → Paramètres → Panneau de configuration → Ajout/suppression de programmes		
Windows Vista	Menu Démarrer	Démarrer → Panneau de configuration	Affichage classique	Programmes et fonctionnalités
			Page d'accueil	Programmes → Programmes et fonctionnalités
	Menu Démarrer classique	Démarrer → Paramètres → Panneau de configuration → Programmes et fonctionnalités		
Windows 7	Démarrer → Panneau de configuration	Petites/grandes icônes : Programmes et fonctionnalités		



Système d'exploitation	Suite des actions			
		Catégorie : Programmes → Suppression de programmes		
Windows 8, Windows 8.1, Windows 10	Panneau de configuration	Petites/grandes icônes : Programmes et fonctionnalités		
		Catégorie : Programmes → Suppression de programmes		

2. Dans la liste des programmes installés, sélectionnez la ligne portant le nom du programme.
3. Cliquez sur **Modifier**. Dans ce cas, l'Assistant de suppression/modification des composants du programme va s'afficher.

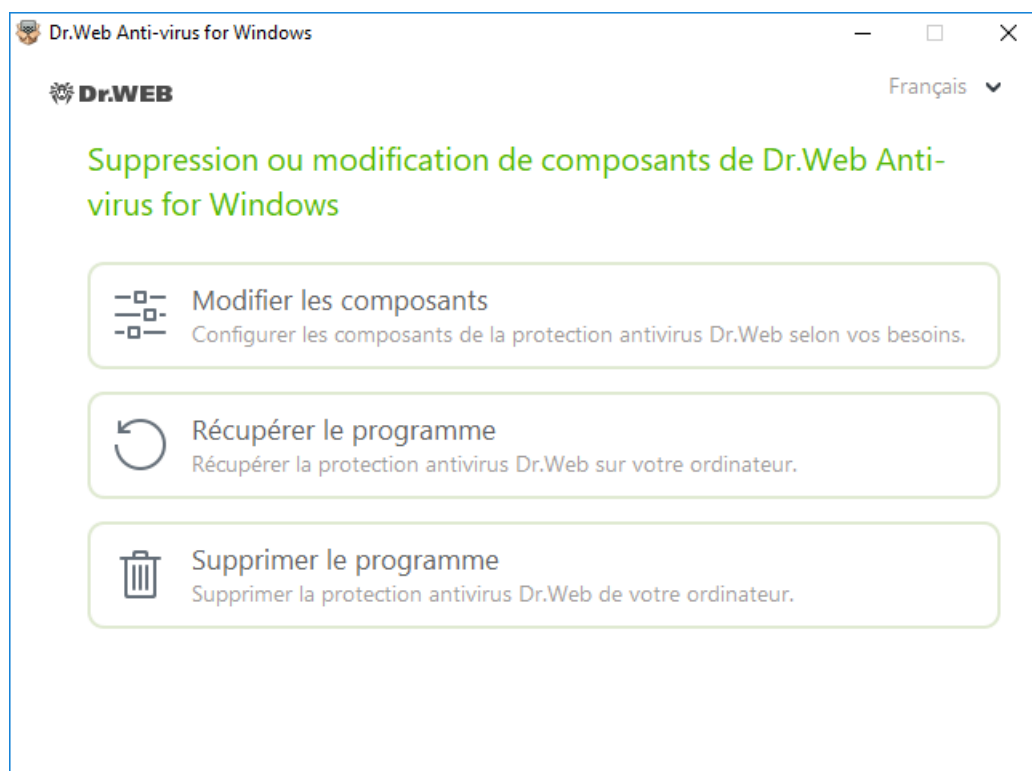


Figure 3. Assistant de suppression/modification des composants



4. Sélectionnez l'une des options :

- **Modifier les composants.** Dans la fenêtre qui apparaît, cochez les cases contre les composants à ajouter et décochez les cases contre les composants à désinstaller. Dès que la configuration est déterminée, cliquez sur **Appliquer**.
- **Récupérer le programme**, s'il faut restaurer la protection antivirus sur votre ordinateur. Cette fonction est appliquée au cas où certains composants de Dr.Web seraient endommagés.
- **Supprimer le programme**, pour [supprimer](#) tous les composants installés.

3.3. Suppression du logiciel



Après la suppression de Dr.Web, votre ordinateur ne sera plus protégé contre les virus et d'autres programmes malveillants.

1. Pour supprimer le logiciel Antivirus Dr.Web pour Windows, sélectionnez (en fonction du système d'exploitation) :

Système d'exploitation	Suite des actions			
Windows XP	Menu Démarrer	Démarrer → Panneau de configuration → Ajout/suppression de programmes		
	Menu Démarrer classique	Démarrer → Paramètres → Panneau de configuration → Ajout/suppression de programmes		
Windows Vista	Menu Démarrer	Démarrer → Panneau de configuration	Affichage classique	Programmes et fonctionnalités
			Page d'accueil	Programmes → Programmes et fonctionnalités



Système d'exploitation	Suite des actions			
	Menu Démarrer classique	Démarrer → Paramètres → Panneau de configuration → Programmes et fonctionnalités		
Windows 7	Démarrer → Panneau de configuration	Petites/grandes icônes : Programmes et fonctionnalités		
		Catégorie : Programmes → Suppression de programmes		
Windows 8, Windows 8.1, Windows 10	Panneau de configuration	Petites/grandes icônes : Programmes et fonctionnalités		
		Catégorie : Programmes → Suppression de programmes		

Dans la liste qui apparaît, sélectionnez la ligne affichant le nom du programme.

2. Cliquez sur **Supprimer**.



En cas de suppression des composants de Dr.Web, la fenêtre **Désactivation de l'Autoprotection** apparaît. Dans cette fenêtre, saisissez le code de confirmation, puis cliquez sur **Désactivation de l'Autoprotection**.

3. Dans la fenêtre **Paramètres sauvegardés**, cochez les cases contre les éléments à conserver après la suppression du logiciel. Les objets et les paramètres conservés peuvent être utilisés par le logiciel en cas de réinstallation. Par défaut, toutes les options sont activées : **Quarantaine**, **Configuration de Dr.Web Anti-virus for Windows** et **Copies de fichiers protégées**. Cliquez sur **Installer**.
4. Dans la fenêtre suivante, pour confirmer la désinstallation de Dr.Web saisissez le code affiché, puis cliquez sur **Supprimer le programme**.



5. Les modifications entrent en vigueur après le redémarrage de l'ordinateur. Vous pouvez reporter le redémarrage en cliquant sur **Ultérieurement**. Cliquez sur **Redémarrer maintenant** pour terminer la désinstallation et modifier l'ensemble des composants Dr.Web tout de suite.



4. Licence

Les droits de l'utilisateur d'utiliser Dr.Web sont régis par une licence achetée sur le site de Doctor Web ou chez les partenaires. La licence accorde le droit d'utiliser toutes les fonctionnalités du produit durant toute la durée de validité. La licence régit les droits d'utilisateur définis conformément au [Contrat de licence](#) que l'utilisateur accepte lors de l'installation du logiciel.

Chaque licence possède un *numéro de série* unique et un fichier spécifique est lié à la licence sur l'ordinateur de l'utilisateur. Ce fichier s'appelle le *fichier clé* de licence et il régule le fonctionnement de Dr.Web conformément aux paramètres de la licence. Pour plus d'infos sur le fichier clé de licence, voir la rubrique [Fichier clé](#).

Méthodes d'activation de la licence

Vous pouvez activer la licence commerciale par l'une des méthodes suivantes :

- lors de l'installation du produit à l'aide de l'Assistant d'enregistrement ;
- à n'importe quel moment à l'aide de l'Assistant d'enregistrement inclus dans le Gestionnaire de licences ;
- sur le site officiel de Doctor Web à l'adresse <https://products.drweb.com/register/>.

L'activation de la licence dans l'Assistant d'enregistrement se fait avec le numéro de série ou le fichier clé. Les utilisateurs de Windows XP peuvent activer la licence uniquement avec le fichier clé.

Pour plus d'infos sur l'activation de la licence, voir la rubrique [Comment activer la licence](#).

Si vous avez des questions sur la licence, consultez la [liste des questions les plus fréquentes](#) sur le site de Doctor Web.

Questions possibles

Comment puis-je transférer la licence sur un autre ordinateur ?

Vous pouvez transférer votre licence commerciale sur un autre ordinateur à l'aide du fichier clé ou le numéro de série. Si vous voulez transférer la licence sur un ordinateur tournant sous Windows XP, vous pouvez le faire en utilisant le fichier clé seulement.

Pour transférer la licence sur un autre ordinateur

- avec le numéro de série :
 1. Supprimez Dr.Web de l'ordinateur duquel vous voulez transférer la licence ou activez une autre licence sur cet ordinateur.
 2. Activez la licence actuelle sur l'ordinateur sur lequel vous voulez transférer la licence. Pour ce faire, utilisez l'Assistant d'enregistrement lors de l'enregistrement du produit ou après



l'installation lors du fonctionnement du produit (voir [Activation avec le numéro de série](#)).

- avec le fichier clé :
 1. Copiez le fichier clé de l'ordinateur duquel vous voulez transférer la licence. Par défaut, le [fichier clé](#) se trouve dans le dossier d'installation de Dr.Web et il a l'extension .key.
 2. Supprimez Dr.Web de l'ordinateur duquel vous voulez transférer la licence ou activez une autre licence sur cet ordinateur.
 3. Activez la licence actuelle sur l'ordinateur sur lequel vous voulez transférer la licence. Pour ce faire, utilisez l'Assistant d'enregistrement lors de l'installation du produit ou après l'installation lors du fonctionnement du produit (voir [Activation avec le fichier clé](#)).

J'ai oublié l'e-mail d'enregistrement. Comment puis-je le restaurer ?

Si vous avez oublié l'adresse e-mail que vous aviez indiquée lors de l'enregistrement, vous devez contacter le support technique de Doctor Web à l'adresse <https://support.drweb.com>.

Si vous envoyez une demande depuis une adresse différente de celle que vous avez indiquée lors de l'enregistrement, le spécialiste du support technique peut vous demander de fournir une photo ou un scan du certificat de licence, le ticket de paiement de la licence, la lettre de la boutique en ligne et d'autres justificatifs.

Comment puis-je changer l'e-mail d'enregistrement ?

Si vous voulez changer l'adresse e-mail que vous avez indiquée lors de l'enregistrement, utilisez le service spécial de changement d'e-mail se trouvant à l'adresse https://products.drweb.com/register/change_email.

4.1. Comment activer la licence

Pour utiliser toutes les fonctionnalités et les composants du logiciel, il faut activer la licence. L'activation de la licence se fait avec un fichier clé ou un numéro de série. Les utilisateurs de Windows XP peuvent [activer la licence](#) uniquement avec le fichier clé



Si vous êtes déjà un utilisateur de Dr.Web, vous pouvez bénéficier d'une extension de votre licence de 150 jours. Pour activer le bonus, entrez votre numéro de série ou indiquez le chemin vers l'ancienne licence dans la fenêtre qui s'ouvre avant l'entrée des données d'enregistrement.

Activation de la licence avec le numéro de série

Si vous avez un numéro de série, vous pouvez

- activer la licence lors de l'installation du produit à l'aide de l'Assistant d'enregistrement :
 1. Lancez l'installation du produit. A l'étape 5 de l'installation, sélectionnez l'élément **Obtenir le fichier clé lors de l'installation**. Cliquez sur **Installer**.

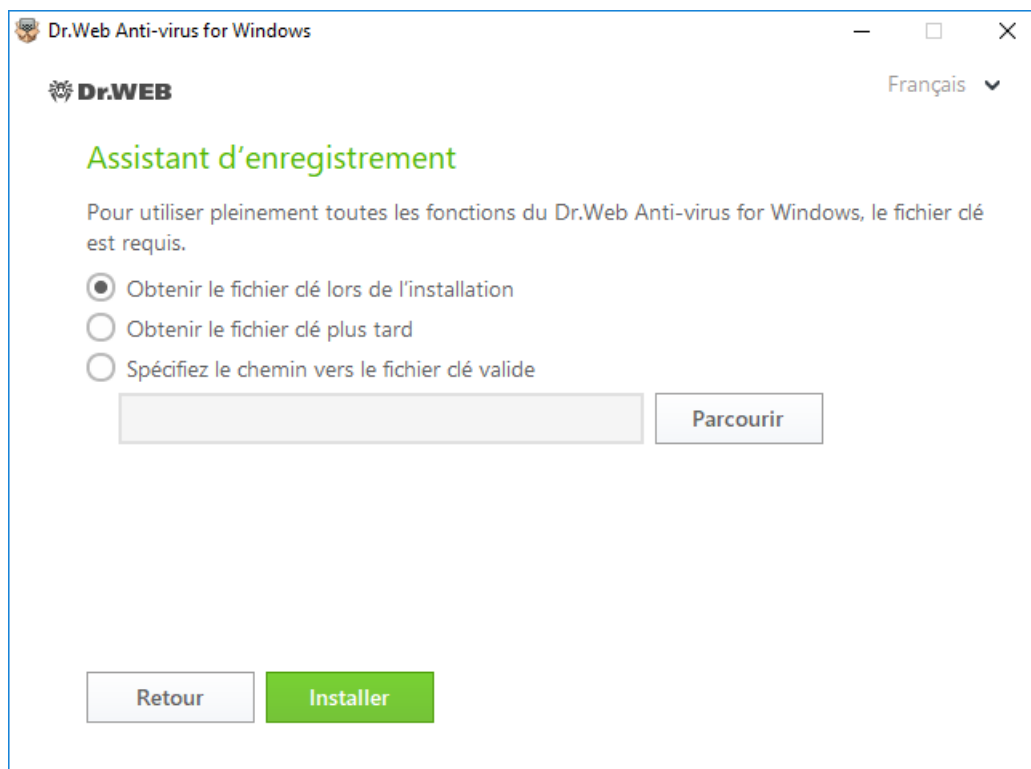


Figure 4. Installation. Assistant d'enregistrement


2. L'installation du produit commencera. A la fin de l'étape Obtention de licence, la fenêtre de l'Assistant d'enregistrement s'ouvrira. Entrez le numéro de série et cliquez sur **Activer**. Si le numéro de série n'a pas été enregistré, une fenêtre s'ouvrira dans laquelle vous devrez indiquer les données d'enregistrement.



Figure 5. Assistant d'enregistrement. Activation de la licence

3. Continuez l'installation du produit en suivant les instructions de l'Assistant d'installation.

Si l'activation de la licence a échoué, un message d'erreur s'affiche. Vérifiez la connexion Internet ou cliquez sur **Réessayer** pour corriger les données erronées.

- activer la licence à n'importe quel moment à l'aide de l'Assistant d'enregistrement inclus dans le Gestionnaire de licences :
1. Ouvrez le [menu de Dr.Web](#)  et sélectionnez l'élément **Licence**. La fenêtre du Gestionnaire de licences va s'afficher. Cliquez sur **Acheter ou activer une nouvelle licence**.

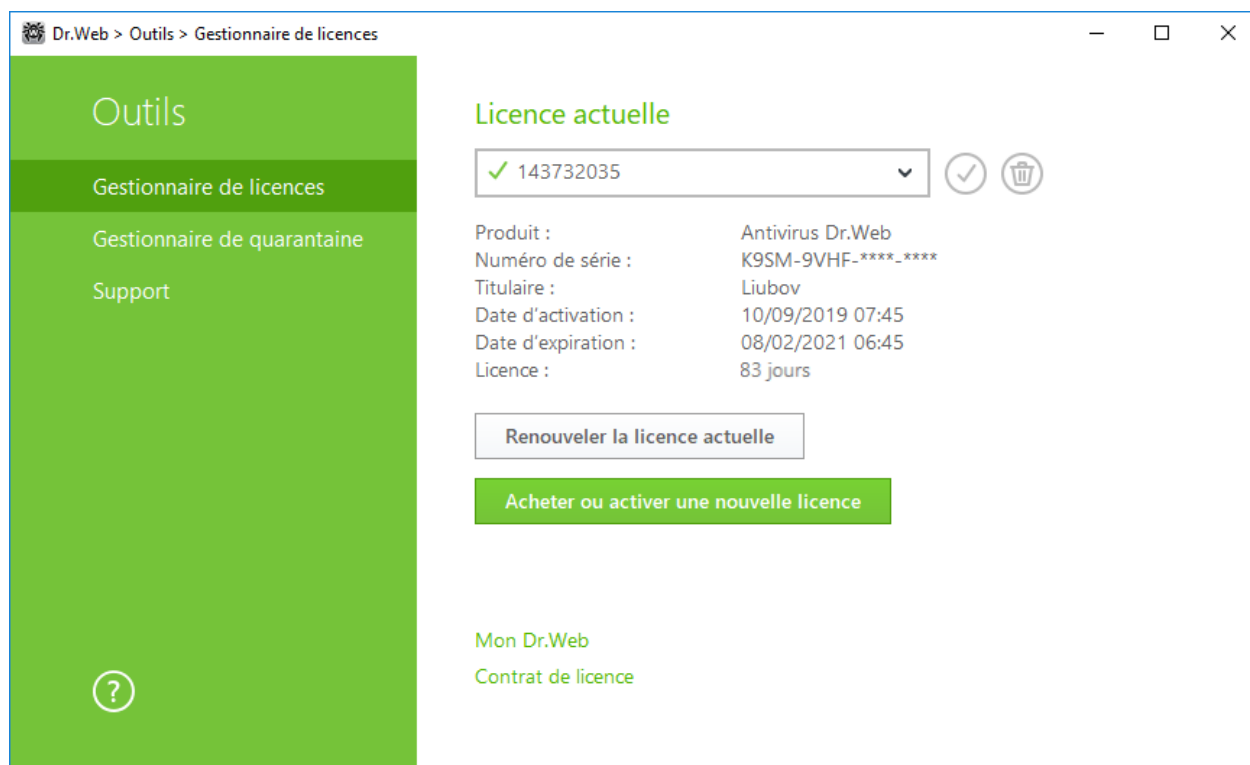


Figure 6. Gestionnaire de licences

2. La fenêtre de l'Assistant d'enregistrement s'ouvrira. Entrez le numéro de série et cliquez sur **Activer**. Si le numéro de série n'a pas été enregistré, une fenêtre s'ouvrira dans laquelle vous devrez indiquer les données d'enregistrement.



Figure 7. Assistant d'enregistrement. Activation de la licence

Si l'activation de la licence a échoué, un message d'erreur s'affiche. Vérifiez la connexion Internet ou cliquez sur **Réessayer** pour corriger les données erronées.

- enregistrer le numéro de série sur le [site](#) Doctor Web et obtenir le fichier clé à l'aide duquel vous pouvez activer la licence.

Activation de la licence avec le fichier clé

Si vous avez un fichier clé, vous pouvez activer la licence :

- lors de l'installation du produit à l'aide de l'Assistant d'enregistrement :
 1. Lancez l'installation du produit. A l'étape 5 de l'installation, sélectionnez l'élément **Spécifiez le chemin vers le fichier clé valide**. Cliquez sur **Installer**.

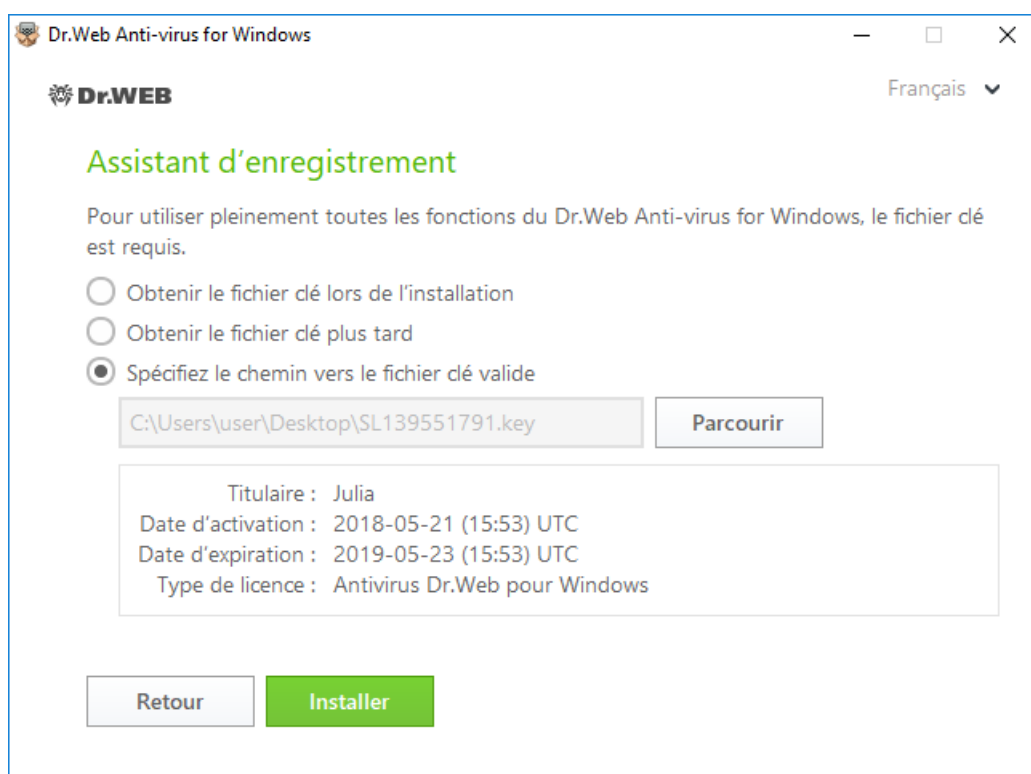



Figure 8. Installation. Assistant d'enregistrement

2. Continuez l'installation du produit en suivant les instructions de l'Assistant d'installation.
- à n'importe quel moment à l'aide de l'Assistant d'enregistrement inclus dans le Gestionnaire de licences :
 1. Ouvrez le [menu de](#) Dr.Web  et sélectionnez l'élément **Licence**. La fenêtre du Gestionnaire de licences va s'afficher. Cliquez sur **Acheter ou activer une nouvelle licence**.

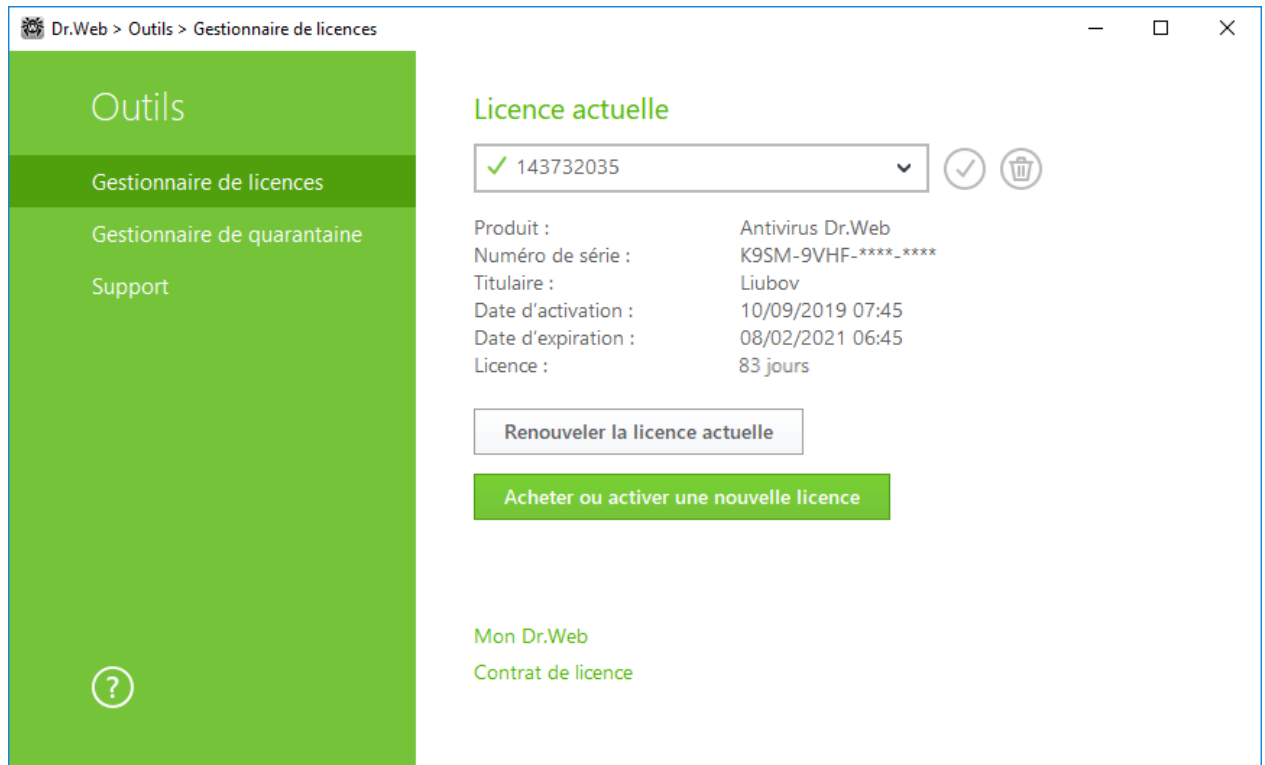


Figure 9. Gestionnaire de licences

2. La fenêtre de l'Assistant d'enregistrement s'ouvrira. Cliquez sur le lien **ou spécifiez un fichier clé**. Dans la fenêtre qui s'ouvre, spécifiez le chemin vers le nouveau fichier clé.

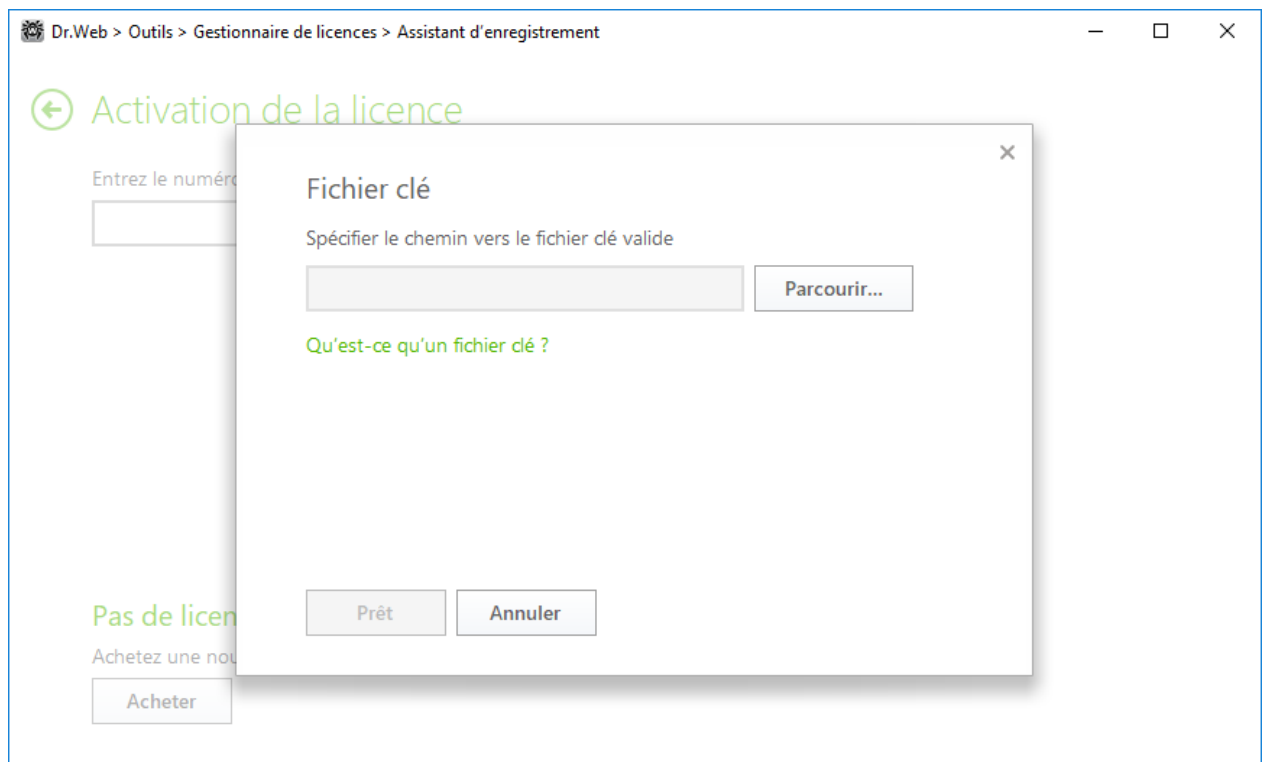


Figure 10. Assistant d'enregistrement. Activation de la licence



Activations de la licence sous Windows XP

Les utilisateurs de Windows XP peuvent activer la licence uniquement avec le fichier clé. Si vous n'avez pas de fichier clé, mais vous possédez un numéro de série, il faudra l'enregistrer sur le [site](#) de Doctor Web. Après l'enregistrement, vous recevrez un lien de téléchargement du fichier clé. Utilisez ce fichier clé pour [activer la licence](#).

Réactivation

Vous pourriez avoir à réactiver votre licence si vous perdez le fichier clé.



En cas de la réactivation de la licence, vous recevez le même fichier clé qui vous a été fourni précédemment à condition que la licence n'ait pas expiré.

Si vous réinstallez le produit ou l'installez sur plusieurs ordinateurs, la réactivation du numéro de série n'est pas requise. Vous pouvez utiliser le fichier clé obtenu lors du premier enregistrement.

Le nombre de demandes de fichiers clés est limité. Un numéro de série ne peut pas être enregistré plus de 25 fois. Si ce nombre est dépassé, aucun fichier clé ne vous sera pas envoyé. Dans ce cas, pour recevoir un fichier clé perdu, contactez le [Support technique](#) en décrivant votre problème en détails, en fournissant les données personnelles que vous avez indiquées lors de votre enregistrement, ainsi que le numéro de série. Le fichier clé vous sera envoyé par le service support technique à votre adresse e-mail.

Questions possibles

Comment puis-je transférer la licence sur un autre ordinateur ?

Vous pouvez transférer votre licence commerciale sur un autre ordinateur à l'aide du fichier clé ou le numéro de série. Si vous voulez transférer la licence sur un ordinateur tournant sous Windows XP, vous pouvez le faire en utilisant le fichier clé seulement.

Pour transférer la licence sur un autre ordinateur


- avec le numéro de série :
 1. Supprimez Dr.Web de l'ordinateur duquel vous voulez transférer la licence ou activez une autre licence sur cet ordinateur.
 2. Activez la licence actuelle sur l'ordinateur sur lequel vous voulez transférer la licence. Pour ce faire, utilisez l'Assistant d'enregistrement lors de l'enregistrement du produit ou après l'installation lors du fonctionnement du produit (voir [Activation avec le numéro de série](#)).



- avec le fichier clé :
 1. Copiez le fichier clé de l'ordinateur duquel vous voulez transférer la licence. Par défaut, le [fichier clé](#) se trouve dans le dossier d'installation de Dr.Web et il a l'extension .key.
 2. Supprimez Dr.Web de l'ordinateur duquel vous voulez transférer la licence ou activez une autre licence sur cet ordinateur.
 3. Activez la licence actuelle sur l'ordinateur sur lequel vous voulez transférer la licence. Pour ce faire, utilisez l'Assistant d'enregistrement lors de l'installation du produit ou après l'installation lors du fonctionnement du produit (voir [Activation avec le fichier clé](#)).


4.2. Renouveler la licence

Vous pouvez renouveler la licence actuelle à l'aide du Gestionnaire de licences.

1. Ouvrez le [menu de](#) Dr.Web  et sélectionnez l'élément **Licence**.
2. Dans la fenêtre du Gestionnaire de licences, cliquez sur **Renouveler la licence actuelle**. Une page du site de Doctor Web s'ouvrira et vous pourrez continuer votre achat sur cette page.

Dr.Web supporte la mise à jour à la volée. Dans ce cas, vous n'avez pas à réinstaller Dr.Web ou interrompre son fonctionnement. Pour renouveler la licence de Dr.Web, il vous faudra activer une nouvelle licence.

Activation de la licence

1. Ouvrez la fenêtre du Gestionnaire de licences en cliquant sur l'élément **Licence** dans le [menu de](#) Dr.Web . Cliquez sur **Acheter ou activer une nouvelle licence**.
2. Dans la fenêtre qui s'affiche entrez le numéro de série ou cliquez sur le lien **ou spécifiez un fichier clé** et indiquez le chemin vers le fichier clé. Les utilisateurs de Windows XP peuvent [activer la licence](#) uniquement avec le fichier clé.

Les instructions détaillées sur l'activation de la licence sont disponibles dans la rubrique [Comment activer la licence](#).

Si la licence que vous voulez renouveler a expiré, Dr.Web commencera à utiliser la nouvelle licence.

Si la licence que vous voulez renouveler n'a pas encore expiré, les jours restants seront automatiquement ajoutés à la nouvelle licence. Dans ce cas, l'ancienne licence sera bloquée et vous recevrez un avertissement correspondant sur l'e-mail que vous avez indiqué lors de l'enregistrement. Il est également recommandé de supprimer l'ancienne licence à l'aide du [Gestionnaire de licences](#).

Si vous avez des questions sur le renouvellement de la licence, consultez la [liste des questions les plus fréquentes](#) sur le site de Doctor Web.





Questions possibles

Après le renouvellement de la licence, j'ai reçu un message informant que mon fichier clé sera bloquée dans 30 jours.

Si la licence renouvelée n'a pas encore expiré, les jours restants s'ajoutent automatiquement à la nouvelle licence. Dans ce cas, la licence servant de base pour le renouvellement sera bloquée. Si vous utilisez une licence bloquée, les composants de Dr.Web ne marchent pas et la mise à jour ne se fait pas.

Il est recommandé de supprimer l'ancienne licence du produit. Pour ce faire, faites le suivant :

1. Ouvrez le [menu de Dr.Web](#)  en [mode administrateur](#) et sélectionnez l'élément **Licence**. La fenêtre du Gestionnaire de licences va s'afficher.
2. Dans le menu déroulant, sélectionnez la licence servant de base pour le renouvellement et cliquez sur le bouton .

4.3. Fichier clé

Les droits d'utilisation de Dr.Web sont spécifiés dans le fichier spécial dit le *fichier clé*. Les fichiers clés reçus lors de l'installation ou dans le kit de distribution du produit sont installés automatiquement et ne requièrent aucune action supplémentaire.

Le fichier clé possède l'extension .key et contient les informations suivantes :

- liste des composants antivirus fournis dans la licence ;
- durée de la licence pour le produit ;
- disponibilité du Support Technique pour l'utilisateur ;
- autres restrictions (notamment, le nombre d'ordinateurs sur lesquels vous êtes autorisé à utiliser l'antivirus).



Par défaut, le fichier clé est placé dans le dossier d'installation de Dr.Web. Dle logiciel vérifie le fichier régulièrement. Ne modifiez pas le fichier pour éviter de compromettre la licence.


Si aucun fichier clé valide n'est trouvé, les composants de Dr.Web sont bloqués.

Un fichier clé de Dr.Web valide satisfait aux critères suivants :

- la licence n'a pas expiré ;
- l'intégrité du fichier clé n'a pas été violée.

Si l'une des conditions n'est pas respectée, le fichier clé devient invalide et Dr.Web arrête de détecter et de neutraliser les programmes malveillants et laisse passer les messages sans les analyser.



Si durant l'installation de Dr.Web, vous n'avez pas reçu le fichier clé et que vous n'avez pas spécifié le chemin d'accès à ce fichier, un fichier clé temporaire est utilisé. Ce fichier clé fournit les fonctionnalités complètes de Dr.Web. Cependant, dans le [menu](#) de Dr.Web , l'élément **Mise à jour** n'est pas présent. Les mises à jour ne seront pas téléchargées jusqu'à ce que vous activiez une licence ou une version d'essai ou jusqu'à ce que vous indiquiez le chemin d'accès au fichier clé valide via le **Gestionnaire de licences**.

Il est recommandé de conserver le fichier clé durant toute la durée de validité de la licence ou de la version d'essai.






5. Mise en route


Lorsque Dr.Web est installé, l'icône  s'affiche dans la zone de notification Windows.




Si le programme n'est pas lancé, ouvrez le groupe **Dr.Web** et sélectionnez **SpIDer Agent** dans le menu **Démarrer**.

L'icône Dr.Web indique l'état actuel du logiciel :

-  : tous les composants nécessaires sont activés et fonctionnent correctement ;
-  : l'Autoprotection Dr.Web ou un des composants est désactivé, ce qui compromet la sécurité de l'antivirus et de votre ordinateur. Activez l'autoprotection ou le composant désactivé ;
-  : le lancement des composants est attendu après le démarrage du système d'exploitation, attendez le lancement des composants ; ou une erreur est survenue lors du démarrage d'un composant important de Dr.Web, votre ordinateur risque d'être infecté. Veuillez vérifier la présence d'un fichier clé valide, et si nécessaire, [installez](#) le fichier clé.

Conformément aux [paramètres](#), au-dessus de l'icône  des notifications ou des bulles d'information peuvent également être affichées.

Pour accéder au menu de Dr.Web, cliquez sur l'icône  dans la zone de notification Windows.



Pour accéder aux composants et aux paramètres de protection et pour désactiver les composants, vous devez avoir les privilèges administrateur.

Le menu Dr.Web  vous offre les outils principaux de gestion et de configuration du logiciel.

Mon Dr.Web. Ouvre votre espace personnel sur le site officiel de Doctor Web. Cette page vous fournit des informations sur votre licence y compris sa durée et son numéro de série, vous permet de renouveler votre licence, de contacter le support technique et plus encore.

Licence. Ouvre [Gestionnaire de licences](#).

Outils. Ouvre un menu donnant accès aux sections suivantes :


- [Gestionnaire de quarantaine](#) ;
- [Support](#).


Composants de protection. Accès rapide à la liste des composants de protection où vous pouvez activer ou désactiver chacun des composants.

Mise à jour. Informations sur le statut des mises à jour des composants et des bases virales. Lance une mise à jour.

Scanner. Accès rapide au lancement de trois modes différents.



Mode de fonctionnement . Permet de passer du mode utilisateur au mode administrateur. Par défaut, Dr.Web démarre en mode utilisateur restreint, qui ne donne pas accès à [Configuration](#) ni aux paramètres des [composants de protection](#). Pour passer à un autre mode, cliquez sur le cadenas. Si l'UAC est activé, le système d'exploitation demandera un accès aux privilèges administrateur. De plus, vous devez également entrer le mot de passe si vous avez activé l'option **Protéger les paramètres de Dr.Web par mot de passe** dans la fenêtre [Configuration](#). Veuillez noter que vous serez de nouveau en mode utilisateur 15 minutes après être passé en mode administrateur. Si vous êtes toujours en train de configurer les paramètres lorsque ce délai expire, vous reviendrez en mode utilisateur après la fermeture de la fenêtre de configuration.

Statistiques . Ouvre les statistiques sur les composants durant la session ouverte incluant le nombre d'objets scannés, infectés et suspects, les actions qui leur ont été appliquées, etc.

Configuration . Ouvre la fenêtre des paramètres généraux, des paramètres des composants de protection et des exclusions.



Pour accéder aux paramètres des composants et ouvrir votre espace personnel **Mon Dr.Web**, vous devez également entrer le mot de passe si vous avez activé l'option **Protéger les paramètres de Dr.Web par mot de passe** dans la fenêtre [Configuration](#).

Si vous avez oublié votre mot de passe pour accéder aux paramètres de produit, veuillez contacter le [support technique](#).

Aide . Ouvre le manuel.

5.1. Tester l'antivirus

Test avec le fichier EICAR

Le fichier de test EICAR (European Institute for Computer Anti-Virus Research) permet de tester les performances des programmes antivirus utilisant la méthode de détection par signatures.

Dans ce but, la plupart des éditeurs d'antivirus utilisent généralement un programme test.com standard. Ce programme a été spécialement conçu pour que les utilisateurs puissent tester les capacités de détection des outils antivirus nouvellement installés sans compromettre la sécurité de leur ordinateur. Bien que le programme test.com ne soit pas un virus, il est traité par la plupart des antivirus comme tel. Sur la détection de ce « virus », la solution antivirus Dr.Web établit le rapport suivant : `EICAR Test File (Not a Virus!)`. D'autres outils antivirus alertent les utilisateurs de la même façon.

Le programme test.com est un fichier-COM 68-bits qui imprime la ligne suivante sur la console lorsqu'il s'est exécuté : `EICAR-STANDARD-ANTIVIRUS-TEST-FILE!`



Le fichier test.com contient la chaîne de caractères suivante seulement :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Pour créer votre propre fichier test avec le « virus », vous devez créer un nouveau fichier avec cette ligne et le sauvegarder comme test.com.



Lancé dans le [mode optimal](#), SplDer Guard n'interrompt pas le lancement du fichier de test EICAR et ne classe pas telle situation comme dangereuse puisque ce fichier ne représente aucun danger pour l'ordinateur. Cependant, lors de la copie ou de la création de ce fichier, SplDer Guard le traite automatiquement comme un programme malveillant et par défaut le déplace en Quarantaine.

Test avec le fichier CloudCar

Pour vérifier le fonctionnement du service [Dr.Web Cloud](#), utilisez le fichier de test CloudCar créé par l'organisation AMTSO (Anti-Malware Testing Standards Organization). Ce fichier est créé spécialement pour vérifier le fonctionnement de services antivirus cloud et il n'est pas malveillant.

Vérification du fonctionnement de Dr.Web Cloud

1. Assurez-vous que l'utilisation du service [Dr.Web Cloud](#) est activée.
2. Téléchargez le fichier de test. Pour ce faire, suivez le lien <https://www.amtso.org/feature-settings-check-cloud-lookups/> et cliquez sur **Download the CloudCar Testfile**.
3. Si le composant SplDer Guard est installé et activé, une fois sur l'ordinateur, le fichier sera automatiquement déplacé en quarantaine. Si le composant SplDer Guard n'est pas installé ou qu'il est désactivé, scannez le fichier téléchargé. Pour ce faire, sélectionnez l'élément **Analyser par Dr.Web** dans le menu contextuel de l'icône du fichier.
4. Assurez-vous que le fichier de test est traité par Dr.Web comme `CLOUD:AMTSO.Test.Virus`. Le préfixe `CLOUD` dans le nom de la menace signifie le fonctionnement correct de Dr.Web Cloud.



6. Outils

Ouvrez le menu de Dr.Web  et lancez les **Outils**. Pour rendre toutes les options accessibles passez en [mode administrateur](#).

Pour obtenir des informations sur votre licence ou pour obtenir une nouvelle licence, sélectionnez [Gestionnaire de licences](#).

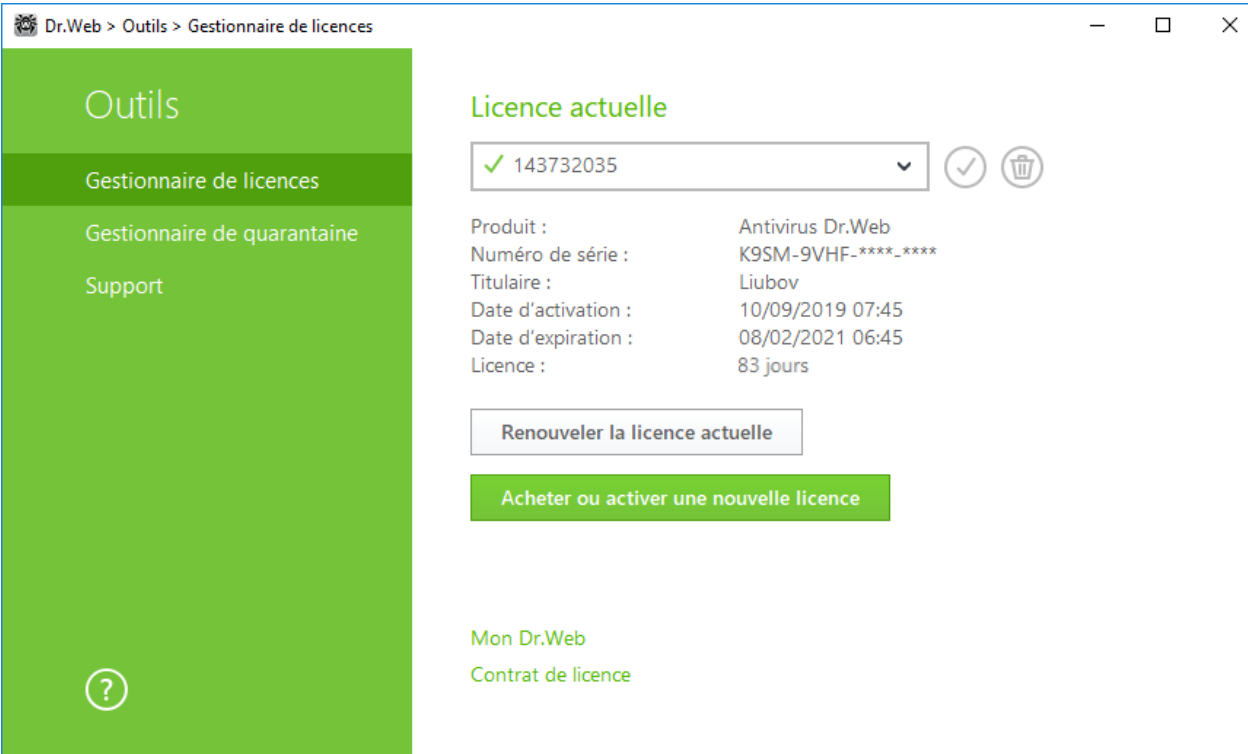
Pour accéder aux produits de Dr.Web installés sur les autres ordinateurs au sein de votre réseau local, sélectionnez la section [Réseau antivirus](#).

Pour voir la liste des fichiers isolés et restaurer les fichiers de la quarantaine, sélectionnez [Gestionnaire de quarantaine](#).

Si vous rencontrez un problème ou que vous avez une question sur l'utilisation de Dr.Web, sélectionnez la section [Support](#).

6.1. Gestionnaire de licences



Dans cette fenêtre, vous pouvez consulter les informations sur toutes les [licences](#) de Dr.Web sauvegardées sur votre ordinateur ainsi que modifier la licence actuelle, la renouveler ou acheter une nouvelle licence et l'activer.



Produit :	Antivirus Dr.Web
Numéro de série :	K9SM-9VHF-****-****
Titulaire :	Liubov
Date d'activation :	10/09/2019 07:45
Date d'expiration :	08/02/2021 06:45
Licence :	83 jours

Figure 11. Informations sur la licence actuelle



Pour voir les informations sur la licence qui n'est pas actuelle, sélectionnez la licence nécessaire dans la liste déroulante. En mode administrateur, le bouton  permet de supprimer la licence consultée, tandis que le bouton  permet de la désigner comme actuelle. Notez qu'il est impossible de supprimer la dernière licence valide.

Si vous cliquez sur **Acheter ou activer une nouvelle licence**, le programme ouvre la fenêtre dans laquelle vous pouvez acheter ou [activer la nouvelle licence](#).

Si vous cliquez sur **Renouveler la licence actuelle**, le programme va ouvrir la page sur le site Doctor Web sur laquelle seront affichés tous les paramètres de la licence utilisée.

Avancé

Le lien [Mon Dr.Web](#) ouvre votre espace personnel sur le site officiel de Doctor Web avec le navigateur utilisé par défaut sur votre ordinateur. Cette page vous fournit des informations sur votre licence y compris sa durée et son numéro de série, et permet de renouveler la licence, contacter le support technique et plus encore.

Le lien [Contrat de licence](#) ouvre le texte du contrat de licence sur le site de Doctor Web.

6.2. Réseau antivirus

Le composant **Réseau antivirus** n'est pas inclus dans l'ensemble du produit Antivirus Dr.Web. Cependant vous pouvez autoriser l'accès à Antivirus Dr.Web sur votre ordinateur. Pour ce faire cochez la case **Autoriser la gestion à distance** dans la section [Réseau antivirus de paramètres du module de gestion SpIDer Agent](#) et saisissez le mot de passe qui sera requis pour la gestion à distance.



Si vous utilisez la clé pour Dr.Web Security Space vous pouvez télécharger la documentation correspondante sur le site <https://download.drweb.com/doc> et prendre connaissance du composant Réseau antivirus.

L'utilisateur ayant le droit de gestion à distance de l'Antivirus Dr.Web sur votre ordinateur aura l'accès aux onglets suivants :

- A propos de
- [Licence](#)
- Mon Dr.Web
- Aide
- [Outils](#)
- [Mise à jour](#)
- [Configuration](#)



Vous pouvez consulter des statistiques, activer ou désactiver des modules et éditer leurs paramètres. Les éléments Quarantaine et Scanner sont indisponibles. Les paramètres et les statistiques du Pare-feu Dr.Web ne sont pas disponibles non plus, cependant vous pouvez activer ou désactiver ce composant.

6.3. Gestionnaire de quarantaine

La fenêtre contient des informations sur la Quarantaine de Dr.Web qui permet d'isoler les fichiers suspectés d'être malveillants. La Quarantaine stocke également les copies de sauvegarde des fichiers traités par Dr.Web.

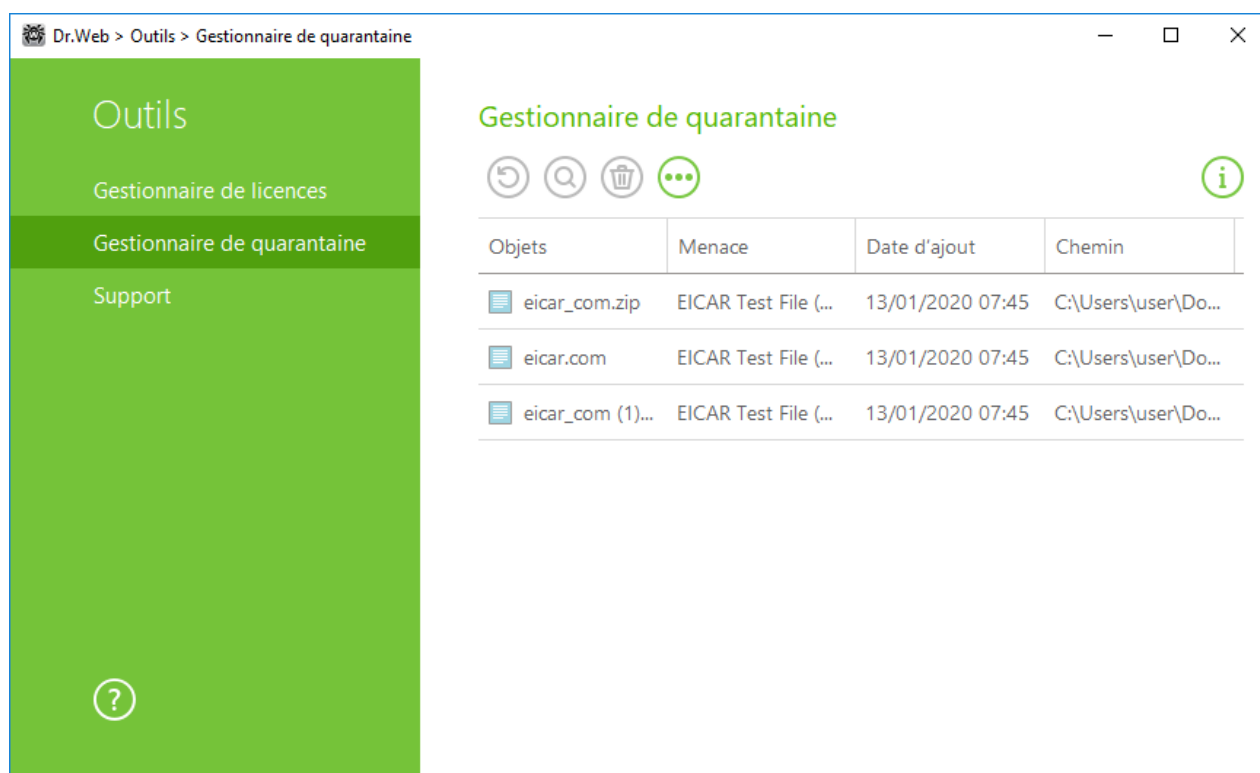


Figure 12. Objets en quarantaine

Utilisez les [paramètres du Gestionnaire de quarantaine](#) pour choisir le mode d'isolation des objets infectés sur les supports amovibles. Lorsque cette option est activée, les menaces détectées sont déplacées dans le dossier sur le support amovible sans être chiffrées. Le dossier de Quarantaine est créé sur les supports amovibles uniquement lorsqu'ils sont accessibles en écriture. L'utilisation de dossiers séparés et le non chiffrement sur les supports amovibles prévient la perte de données.

Le tableau central liste les informations suivantes sur les objets placés en quarantaine auxquels vous avez accès :


- **Objets** : nom de l'objet placé en quarantaine ;
- **Menace** : type de logiciel malveillant déterminé par Dr.Web lorsque l'objet est placé en quarantaine ;
- **Date d'ajout** : date à laquelle l'objet a été déplacé en quarantaine ;



- **Chemin** : chemin complet du fichier avant qu'il ne soit placé en quarantaine.



Dans la fenêtre de Gestionnaire de quarantaine les fichiers sont visibles uniquement pour les utilisateurs qui ont l'accès à ces fichiers. Pour afficher les objets cachés, il faut posséder les droits d'administrateur.

Les copies de sauvegarde déplacées en quarantaine sont affichées dans le tableau par défaut. Pour les voir dans la liste des objets, cliquez sur  et dans la liste déroulante, sélectionnez l'élément **Montrer les copies de réserve**.

Gestion des objets en quarantaine

En [mode administrateur](#), les boutons suivants sont disponibles pour chaque objet :


- **Restaurer** : déplacer un ou plusieurs objets sélectionnés sous les noms spécifiés vers le dossier nécessaire ;



Utilisez cette option uniquement si vous êtes sûr que les objets sélectionnés ne sont pas nocifs.

- **Rescanner** : scanner l'objet déplacé en quarantaine encore une fois.
- **Supprimer** : supprimer un ou plusieurs objets sélectionnés de la quarantaine et du système.

Ces actions sont également disponibles dans le menu contextuel qui s'ouvre si vous cliquez droit sur un ou plusieurs objets.

Pour supprimer tous les objets de la quarantaine en même temps, cliquez sur le bouton  et sélectionnez **Tout supprimer** dans la liste déroulante.

6.4. Support

Cette rubrique contient des informations sur la version du produit, sur les composants, la date de la dernière mise à jour et des liens utiles pour vous aider à résoudre des problèmes pouvant survenir durant l'utilisation de Dr.Web.

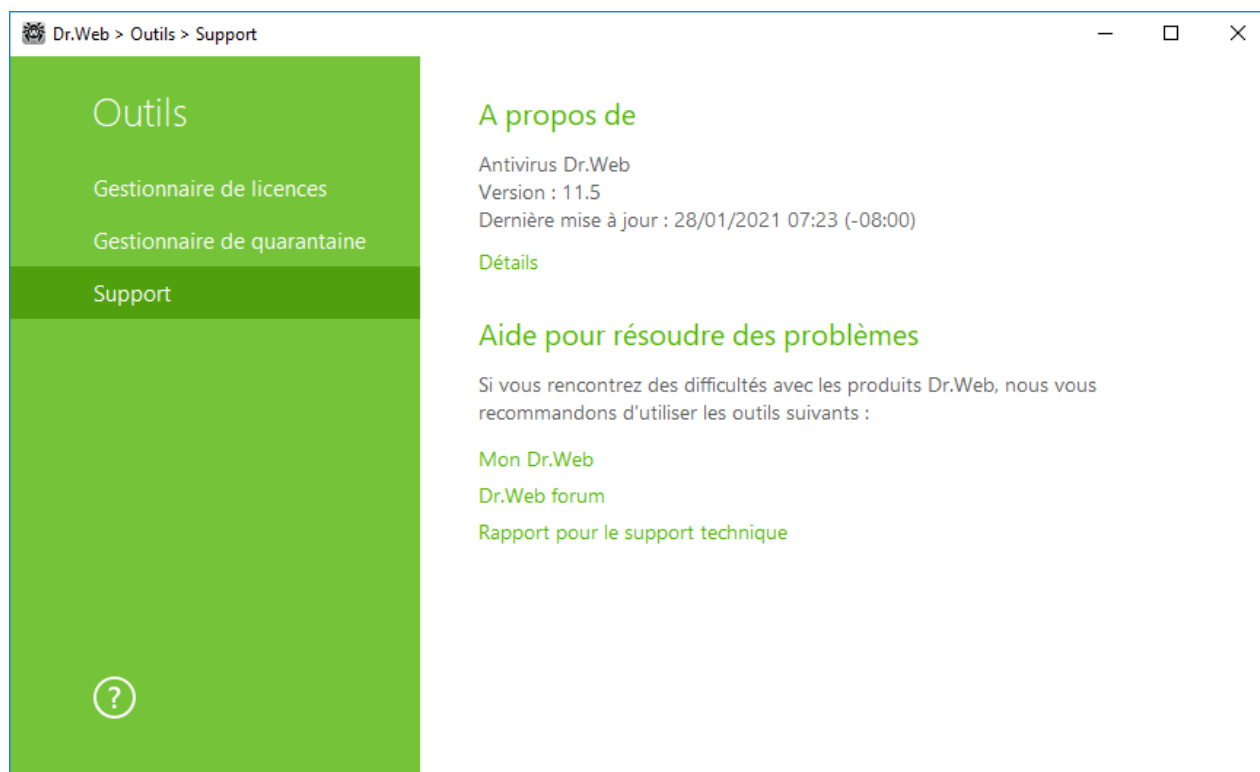


Figure 13. Informations sur la version du produit et support

Si vous avez des questions, utilisez les outils suivants.

Mon Dr.Web. Ouvre votre espace personnel sur le site officiel de Doctor Web. Cette page vous fournit des informations sur votre licence y compris sa durée et son numéro de série, vous permet de renouveler votre licence, de contacter le support technique et plus encore.

Dr.Web forum. Ce lien ouvre le forum Dr.Web à la page <https://forum.drweb.com>.

Rapport pour le support technique. Ce lien lance l'assistant qui vous aidera à [créer un rapport](#) contenant les informations importantes concernant la configuration de votre système et le fonctionnement de votre ordinateur.

Si vous n'avez pas trouvé la solution de votre problème, vous pouvez demander une assistance directe du support technique de Doctor Web en remplissant le formulaire dans la section du support à la page <https://support.drweb.com>. Vous pouvez joindre le rapport pour le service technique, des captures d'écran et d'autres informations nécessaires.


Pour trouver le bureau Doctor Web le plus proche de chez vous et tous les contacts nécessaires, visitez la page <https://company.drweb.com/contacts/offices>.

6.4.1. Créer un rapport

Pour contacter le support technique de Doctor Web, vous pouvez générer un rapport sur votre système d'exploitation et le fonctionnement de Dr.Web.



Pour créer un rapport

1. Ouvrez le menu .
2. Passez sur la page **Outils**.
3. Sélectionnez **Support**.

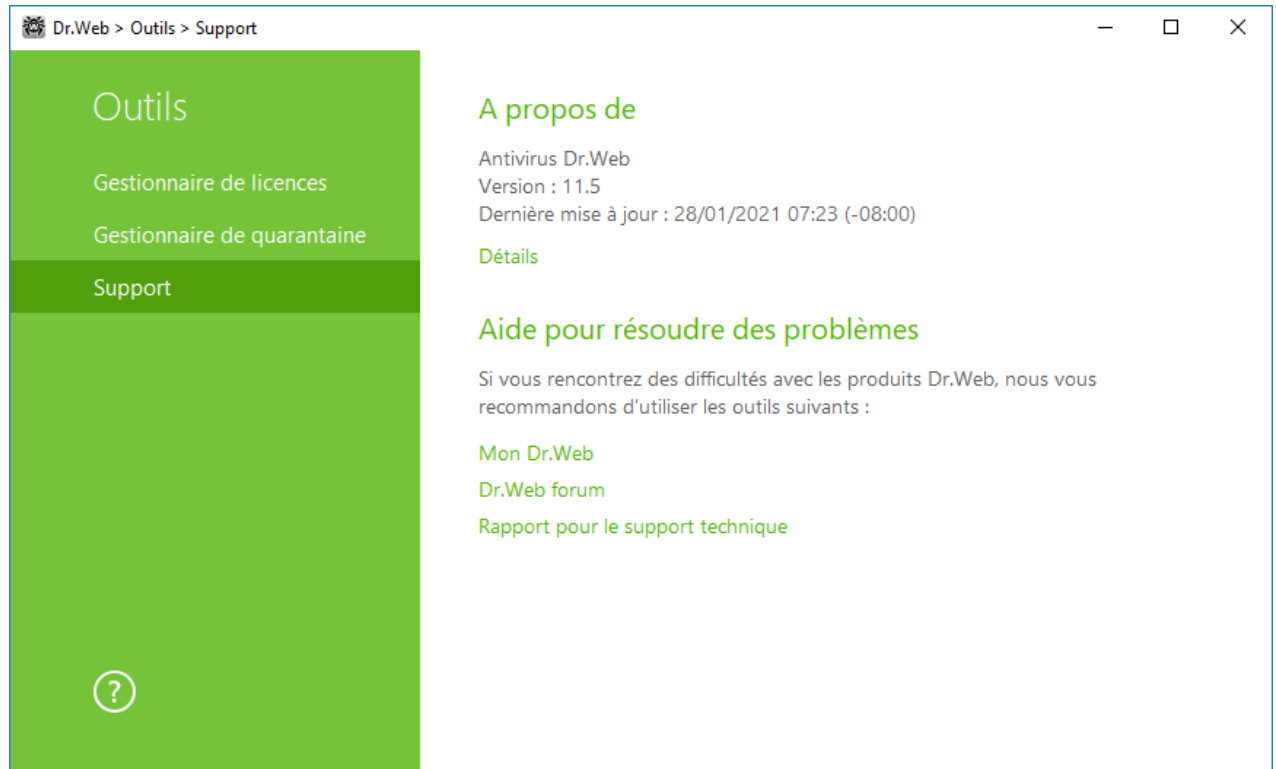


Figure 14. Support

4. Cliquez sur le lien **Rapport pour le support technique**.
5. Dans la fenêtre qui s'affiche, cliquez sur le bouton **Créer un rapport**.

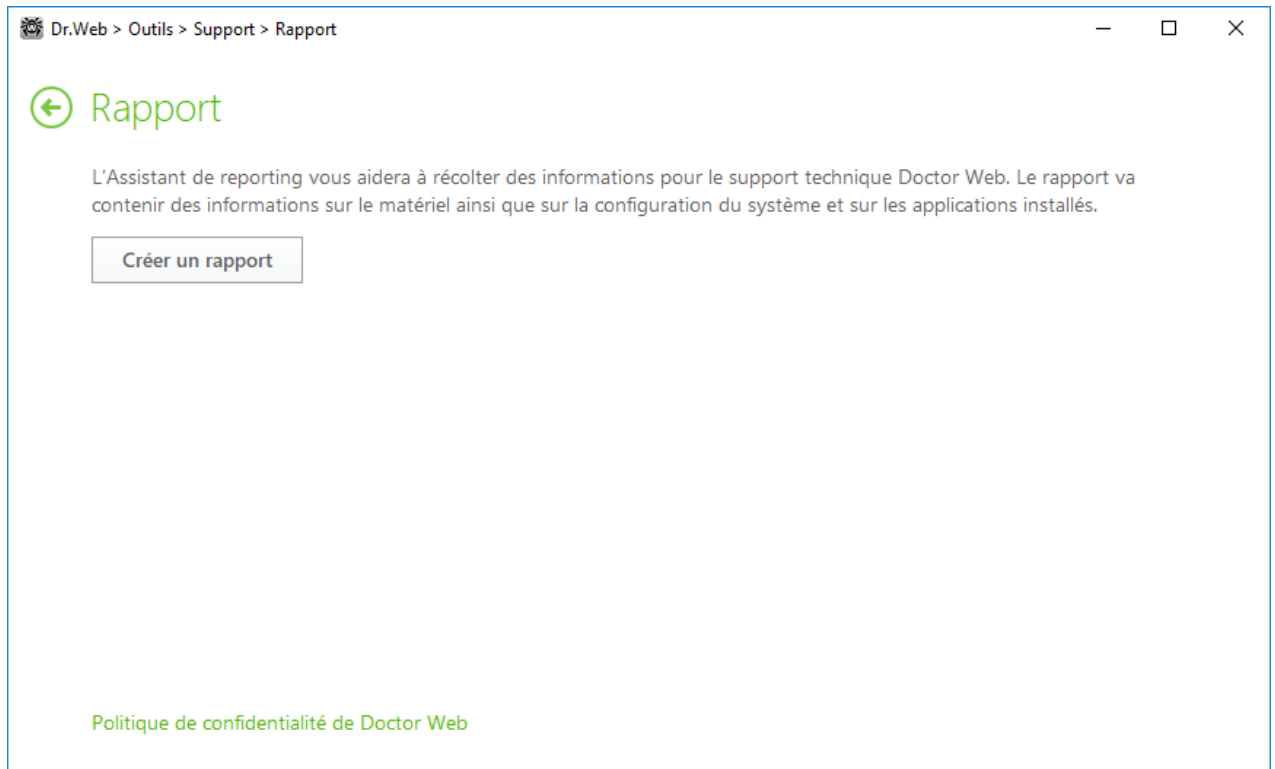


Figure 15. Création d'un rapport

Le rapport sera créé automatiquement et enregistré sous forme d'archive dans le dossier Doctor Web se trouvant dans le dossier du profil utilisateur %USERPROFILE%.

Pour créer un rapport, cliquez sur le bouton correspondant. Le rapport va inclure :

1. Informations techniques sur le système d'exploitation :

- généralités sur l'ordinateur ;
- sur les processus en cours d'exécution ;
- sur les tâches programmées ;
- sur les services et pilotes ;
- sur le navigateur par défaut ;
- applications installées ;
- sur la politique de restrictions ;
- sur le fichier HOSTS ;
- sur les serveurs DNS ;
- journal des événements système ;
- liste des répertoires système ;
- branches de la base de registre ;
- fournisseurs Winsock ;
- connexions réseau ;
- rapports du débogueur Dr.Watson ;



- indice de performances.
2. Informations sur les solutions antivirus Dr.Web.
 3. Informations sur les plug-ins Dr.Web :
 - Dr.Web pour IBM Lotus Domino ;
 - Dr.Web pour Kerio MailServer ;
 - Dr.Web pour Kerio WinRoute.

Des informations sur les solutions antivirus Dr.Web se trouvent dans l'Observateur d'Événements (Event Viewer) dans les **Journaux des applications et services** → **Doctor Web**.

Création du rapport depuis la ligne de commande

Pour générer le rapport, utilisez la commande suivante :

```
/auto
```

Par exemple : dwsysinfo.exe /auto

Le rapport sera enregistré sous forme d'archive dans le dossier Doctor Web se trouvant dans le dossier du profil utilisateur %USERPROFILE%.

Vous pouvez également utiliser la commande :

```
/auto /report:[<chemin complet vers l'archive>]
```

où :

- <chemin complet vers l'archive> : chemin d'accès au fichier de rapport.

Par exemple : dwsysinfo.exe /auto /report:C:\report.zip




7. Mise à jour des bases et des modules de programme

Les produits Dr.Web utilisent les bases virales pour détecter les objets malveillants. Ces bases contiennent les informations sur tous les programmes malveillants connus. Les mises à jour régulières permettent de détecter de nouveaux virus, de bloquer leur diffusion et, parfois, de désinfecter les fichiers infectés qui n'étaient pas curables auparavant. Outre les bases virales, les modules de programme Dr.Web et l'aide du produit sont mis à jour.

Pour la mise à jour de Dr.Web, une connexion à Internet ou au miroir de mise à jour (dossier local ou réseau), ou au Réseau antivirus avec le miroir de mises à jour configuré sur au moins un des ordinateurs est requise. La source de mises à jour et les autres paramètres sont configurés dans la section de paramètres **Général** → **Mise à jour**. Pour plus d'infos sur la configuration des paramètres de la mise à jour du programme Dr.Web, consultez la section [Mise à jour](#).

Vérification du statut des mises à jour

Pour vérifier le statut des bases virales et des composants, ouvrez le [menu](#) Dr.Web . S'ils sont à jour, l'inscription **Aucune mise à jour n'est requise** sera affichée dans le menu.

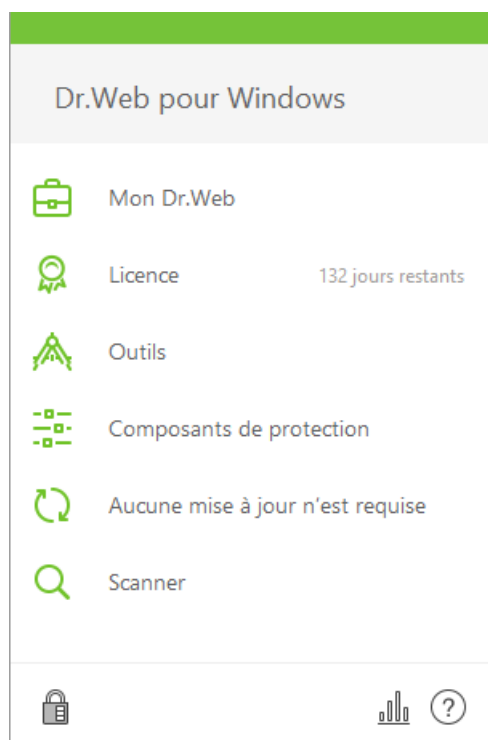


Figure 16. Menu Dr.Web


Lancement d'une mise à jour

Lors d'une mise à jour Dr.Web télécharge et installe automatiquement tous les fichiers mis à jour en fonction de votre version de Dr.Web, ainsi qu'une nouvelle version de Dr.Web si elle est disponible.



Après une mise à jour des fichiers exécutables ou des bibliothèques, un redémarrage de la machine peut être requis. Dans ce cas, une alerte sera affichée.



Lancement d'une mise à jour depuis le menu de Dr.Web

1. Ouvrez le [menu](#) de Dr.Web  et sélectionnez l'élément **Licence**. En fonction du statut des bases et des composants, le nom de cet élément peut varier.
2. Une fenêtre apparaît et affiche les informations sur les bases virales et les composants ainsi que la date de la dernière mise à jour. Pour lancer une mise à jour cliquez sur **Mettre à jour**.

Lancement d'une mise à jour depuis la ligne de commande

Ouvrez le dossier d'installation de Dr.Web (%PROGRAMFILES%\Common Files\Doctor Web\Updater) et lancez `drwupsrv.exe`. La liste des paramètres se trouve dans l'[Annexe A](#).

Rapports

Vous pouvez consulter les rapport de la mise à jour dans la section **Statistiques**. Pour ce faire, ouvrez le [menu de](#) Dr.Web  et passez dans la section **Statistiques** .

Les rapports de la mise à jour sont également enregistrés dans le fichier `dwupdater.log` situé dans le dossier `%allusersprofile%\Doctor Web\Logs\`.



8. Scanner Dr.Web

Scanner Dr.Web pour Windows vous permet de lancer le scan antivirus des secteurs d'amorçage, de la mémoire vive, des fichiers particuliers et des objets contenus dans des structures complexes telles que les archives, les conteneurs et les e-mails avec des pièces jointes. Toutes les [méthodes de détection](#) de menaces sont utilisées pour l'analyse.

Lorsqu'un objet malveillant est détecté, Scanner Dr.Web informe seulement sur la menace détectée. Le rapport sur les résultats de l'analyse s'affiche dans un tableau où vous pouvez choisir une action nécessaire pour traiter l'objet malveillant ou suspect. Vous pouvez appliquer les actions définies par défaut à toutes les menaces détectées ou sélectionner une méthode appropriée pour traiter des objets particuliers.


Les actions par défaut sont optimales pour la plupart des cas, mais si besoin est, vous pouvez les modifier dans la [fenêtre de configuration](#) de Scanner Dr.Web. Les actions à porter sur un objet particulier peuvent être choisies après la fin de l'analyse, tandis que les paramètres généraux relatifs à la neutralisation des types différents de menaces doivent être spécifiés avant de procéder à l'analyse.

8.1. Lancement et modes d'analyse



Si vous utilisez Windows Vista ou un système d'exploitation ultérieur, il est recommandé de lancer Scanner Dr.Web avec les droits d'administrateur. Sinon, les fichiers et les dossiers auxquels l'utilisateur sans droits n'a pas accès (y compris les dossiers système) ne seront pas analysés.

Lancer le Scanner Dr.Web

1. Dans le [menu](#)  sélectionnez l'élément **Scanner**. Le menu d'accès rapide aux différents modes d'analyse va s'ouvrir.

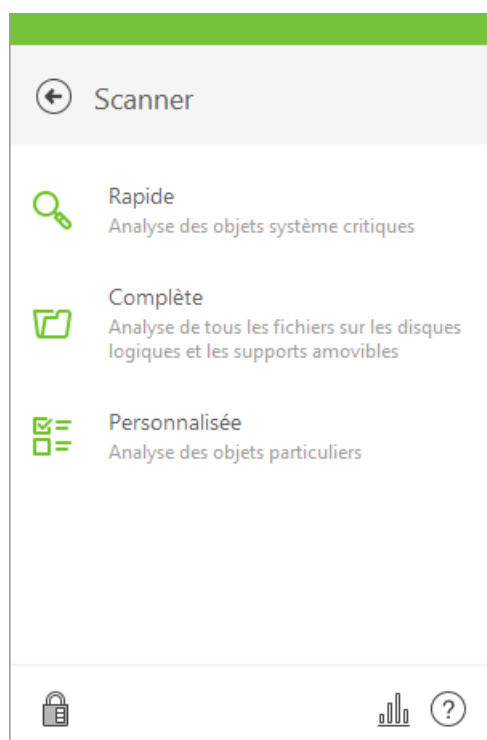


Figure 17. Sélection du mode de l'analyse effectuée par le scanner

2. Sélectionnez le mode d'analyse nécessaire :

- l'élément **Personnalisée** pour scanner uniquement les objets que vous avez désignés. La fenêtre de sélection de fichiers pour l'analyse par le Scanner Dr.Web va s'ouvrir ;
- l'élément **Rapide** pour analyser uniquement les zones critiques de Windows ;
- l'élément **Complète**, pour analyser tous les fichiers.

Vous pouvez également lancer Scanner avec la configuration par défaut pour analyser un fichier ou un dossier immédiatement, sélectionnez **Scan Dr.Web** dans le menu du fichier ou du dossier (sur le Bureau ou dans l'explorateur Windows).

Configurer le Scanner Dr.Web

Vous pouvez configurer les paramètres de fonctionnement et les réactions du Scanner Dr.Web envers les menaces détectées dans la rubrique **Configuration** → **Composants de protection** → **Scanner**.

Description des modes d'analyse

Analyse rapide

Dans ce mode sont analysés :

- secteurs d'amorçage de tous les disques ;
- mémoire vive ;



- dossier racine du disque de démarrage ;
- dossier système Windows ;
- dossier des Documents de l'utilisateur (« Mes documents ») ;
- fichiers temporaires ;
- points de restauration du système ;
- présence de rootkits (si le scan a été lancé en mode administrateur).




Dans ce mode les archives et les fichiers e-mail ne sont pas scannés.

Analyse complète

Dans ce mode, la mémoire vive et tous les disques durs (y compris les secteurs d'amorçage) sont scannés. La recherche des rootkit est également effectuée.

Analyse personnalisée

Lorsque vous sélectionnez l'analyse personnalisée, dans la fenêtre du Scanner Dr.Web vous pouvez spécifier les objets à vérifier : tout fichier ou dossier, ainsi que la mémoire vive, les secteurs d'amorçage etc. Pour commencer l'analyse cliquez sur **Lancer l'analyse** Pour ajouter des objets dans la liste, cliquez sur .

Processus de l'analyse

Dès que l'analyse commence, les bouton **Pause** et **Stop** dans la partie droite de la fenêtre deviennent disponibles. A chaque étape de l'analyse, vous pouvez faire le suivant :

- Pour suspendre l'analyse, cliquez sur **Pause**. Pour reprendre l'analyse après la pause, cliquez sur **Reprendre**.
- Pour arrêter l'analyse définitivement, cliquez sur **Stop**.

De cette fenêtre vous pouvez retourner dans la fenêtre de sélection de mode de scan.



Le bouton **Pause** est indisponible lors de l'analyse de la mémoire vive et des processus.

8.2. Actions en cas de détection de menaces

Après la fin d'analyse, Scanner Dr.Web informe seulement sur les menaces détectées et propose des actions optimales pour leur neutralisation. Vous pouvez neutraliser toutes les menaces détectées en une seule fois. Pour cela, après la fin de l'analyse, sélectionnez toutes les menaces et



cliquez sur le bouton **Neutraliser**, et Scanner Dr.Web appliquera des actions définies par défaut qui sont optimales pour toutes les menaces détectées.



En cliquant sur **Neutraliser**, vous appliquez les actions aux objets sélectionnés dans le tableau. Il faut sélectionner manuellement certains objets ou groupes d'objets auxquels il faut appliquer l'action en cliquant sur **Neutraliser**. Pour ce faire, utilisez les cases contre les noms des objets ou le menu déroulant dans l'en-tête du tableau.

Sélection d'une action

1. Dans le champ **Action** de la liste déroulante, sélectionnez une action pour chaque objet (par défaut, Scanner Dr.Web suggère une action optimale).
2. Cliquez sur **Neutraliser**. Scanner Dr.Web va neutraliser toutes les menaces sélectionnées en une seule fois.

Restrictions existantes :

- il est impossible de désinfecter les objets suspects ;
- il est impossible de déplacer ou supprimer les objets qui ne sont pas des fichiers (par exemple, les secteurs d'amorçage) ;
- il est impossible d'effectuer aucune action pour des fichiers particuliers au sein des archives, des packages d'installation ou dans des e-mails. Dans ce cas, l'action sera appliquée à l'objet entier.

Le journal détaillé sur le fonctionnement du programme est enregistré sous forme du fichier journal `dwscanner.log` se trouvant dans le répertoire `%USERPROFILE%\Doctor Web`.

Nom de colonne	Description
Objet	Cette colonne comporte le nom de l'objet suspect ou contaminé (nom du fichier : en cas de contamination d'un fichier, Boot sector si un secteur d'amorçage est contaminé, Master Boot Record si le MBR du disque dur est infecté).
Menace	Ici vous trouverez le nom du virus ou d'une modification virale selon la classification interne de Doctor Web (la modification d'un virus connu est un code du virus modifié de telle manière que le scanner peut le détecter mais que les algorithmes de neutralisation appropriés au virus d'origine n'y peuvent pas être appliqués). Pour les objets suspects détectés, il est indiqué que l'objet est « probablement infecté » et le type du virus supposé selon la classification de l'analyseur heuristique est également affiché.
Action	Cette colonne contient l'action recommandée pour la menace détectée. Cliquez sur la flèche sur ce bouton pour définir l'action pour la menace sélectionnée. Vous pouvez appliquer l'action indiquée sur le bouton séparément, sans neutraliser les menaces restantes. Pour ce faire, cliquez sur ce bouton.



Nom de colonne	Description
Chemin	Ce colonne affiche le chemin complet vers le fichier correspondant.



Si dans les [paramètres](#) du Scanner Dr.Web, vous avez coché la case **Neutraliser les menaces détectées** pour le paramètre **Après la fin de l'analyse**, les menaces seront neutralisées automatiquement.

8.3. Lancement du Scanner avec les paramètres de la ligne de commande

Vous pouvez lancer Scanner Dr.Web en mode ligne de commande. Ce mode vous permet de configurer les paramètres nécessaires pour la session courante de scan ainsi qu'une liste d'objets spécifiques à scanner 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.

Syntaxe de la commande de lancement :

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

La liste des objets à scanner peut être vide ou contenir plusieurs éléments séparés par des blancs. Si le chemin vers les objets à analyser n'est pas spécifié, la recherche sera effectuée dans le dossier d'installation Dr.Web.

Les objets les plus souvent vérifiés sont les suivants :

- /FAST : commande d'effectuer une [analyse rapide](#) du système.
- /FULL : commande d'effectuer une [analyse complète](#) de tous les disques durs et de tous les supports amovibles (y compris les secteurs d'amorçage).
- /LITE : commande d'effectuer un scan du système en analysant la mémoire vive, les secteurs d'amorçage de tous les disques, une recherche des rootkit sera également réalisée.

Paramètres : les clés de la ligne de commande déterminant la configuration du logiciel. 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). Les clés commencent par le symbole slash (/) et sont séparées par des espaces comme les autres paramètres de ligne de commande.

8.4. Scanner en ligne de commande

Le jeu de composants Dr.Web inclut également le Scanner en ligne de commande qui permet de réaliser l'analyse en mode ligne de commande et offre à l'utilisateur des possibilités avancées de configuration.



Le Scanner en ligne de commande place les fichiers suspects pouvant contenir des objets malveillants en Quarantaine.

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

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

La clé commence par le symbole « / », plusieurs 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, consulter l'[Annexe A](#).

Codes de retour :

0 : l'analyse est achevée avec succès, aucun objet infecté n'est trouvé

1 : l'analyse est achevée avec succès, des objets infectés ont été détectés

10 : les clés non valides sont spécifiées

11 : le fichier clé est introuvable ou ne supporte pas le Scanner en ligne de commande

12 : Scanning Engine n'est pas lancé

255 : l'analyse est interrompue par l'utilisateur

8.5. Lancement de l'analyse selon la planification

Lors de l'installation de Dr.Web, une tâche d'analyse antivirus est automatiquement créée dans le Planificateur de tâche Windows (par défaut, la tâche est désactivée).

Pour consulter les paramètres de tâche, ouvrez le **Panneau de configuration** (affichage détaillé) → **Outils d'administration** → **Planificateur de tâches**.

Dans la liste de tâches, sélectionnez la tâche d'analyse antivirus. Vous pouvez activer la tâche ainsi que configurer l'heure du démarrage et spécifier des paramètres nécessaires.

Sur l'onglet **Général** en bas de la fenêtre, des informations générales sur la tâche et les options de sécurité sont affichées. Sur les onglets **Déclencheurs** et **Conditions** vous pouvez spécifier les conditions qui déclenchent l'exécution de la tâche. Pour consulter l'historique des événements, allez sur l'onglet **Journal**.



Vous pouvez également créer vos propres tâches d'analyse antivirus. Pour en savoir plus, consultez la rubrique d'aide et la documentation de l'OS Windows.



Si Pare-feu est installé, il bloquera le planificateur de tâches après l'installation de Dr.Web et le premier redémarrage du système. Les **tâches planifiées** seront effectuées uniquement après le second redémarrage si une nouvelle règle a déjà été créée.



9. Configuration

Pour configurer les paramètres, ouvrez le menu de Dr.Web , et lancez **Configuration**  en [mode administrateur](#).

Protection par mot de passe

Pour restreindre l'accès aux paramètres de Dr.Web sur votre ordinateur, activez l'option **Protéger les paramètres de Dr.Web par mot de passe**. Dans la fenêtre qui s'affiche, indiquez le mot de passe qui sera requis pour configurer Dr.Web, confirmez-le et cliquez sur **OK**.



Si vous avez oublié le mot de passe, contactez le [Support technique](#).

Gérer les paramètres

Pour restaurer les paramètres par défaut, choisissez **Réinitialiser les paramètres** dans la liste déroulante.

Si vous souhaitez utiliser les paramètres de Dr.Web que vous avez déjà configurés sur un autre ordinateur, sélectionnez **Importer** dans la liste déroulante.

Si vous souhaitez utiliser vos paramètres sur d'autres ordinateurs, sélectionnez **Exporter** dans la liste déroulante. Ensuite, utilisez le même onglet sur un autre ordinateur.



10. Paramètres généraux

Le centre unique de gestion des paramètres vous permet de configurer les paramètres principaux de tout l'ensemble antivirus.

Pour accéder aux paramètres principaux de Dr.Web, ouvrez le menu , lancez **Configuration**  en [mode administrateur](#) et sélectionnez la section **Général**.



Pour accéder aux paramètres généraux de Dr.Web, vous êtes invité à entrer le mot de passe si vous avez coché la case **Protéger les paramètres de Dr.Web par mot de passe** dans la section [Configuration](#).

Pour configurer l'affichage de notifications sur l'écran et la réception de notifications par e-mail, sélectionnez la section [Notifications](#).

Pour modifier la source ou la fréquence des mise à jour ou créer un miroir de mise à jour, sélectionnez [Mise à jour](#).

Pour configurer l'utilisation du serveur proxy ou l'analyse des données transmises via des protocoles sécurisés, sélectionnez [Réseau](#).

Pour configurer les paramètres de sécurité avancés, sélectionnez la section [Autoprotection](#).

Pour configurer l'accès au service cloud de Doctor Web, sélectionnez [Dr.Web Cloud](#).


Si vous voulez autoriser l'accès au produit Dr.Web installé sur votre ordinateur depuis d'autres ordinateurs, sélectionnez [Réseau antivirus](#).

Pour modifier la langue d'interface ou les paramètres du journal ou de la quarantaine, sélectionnez [Avancé](#).

10.1. Notifications

Dans cette section, vous pouvez configurer les paramètres de réception de notifications de fonctionnement de Antivirus Dr.Web pour Windows.

Notifications pop-up

Activez l'option correspondante pour avoir des notifications pop-up sur l'icône de Dr.Web  dans la zone de notification Windows.

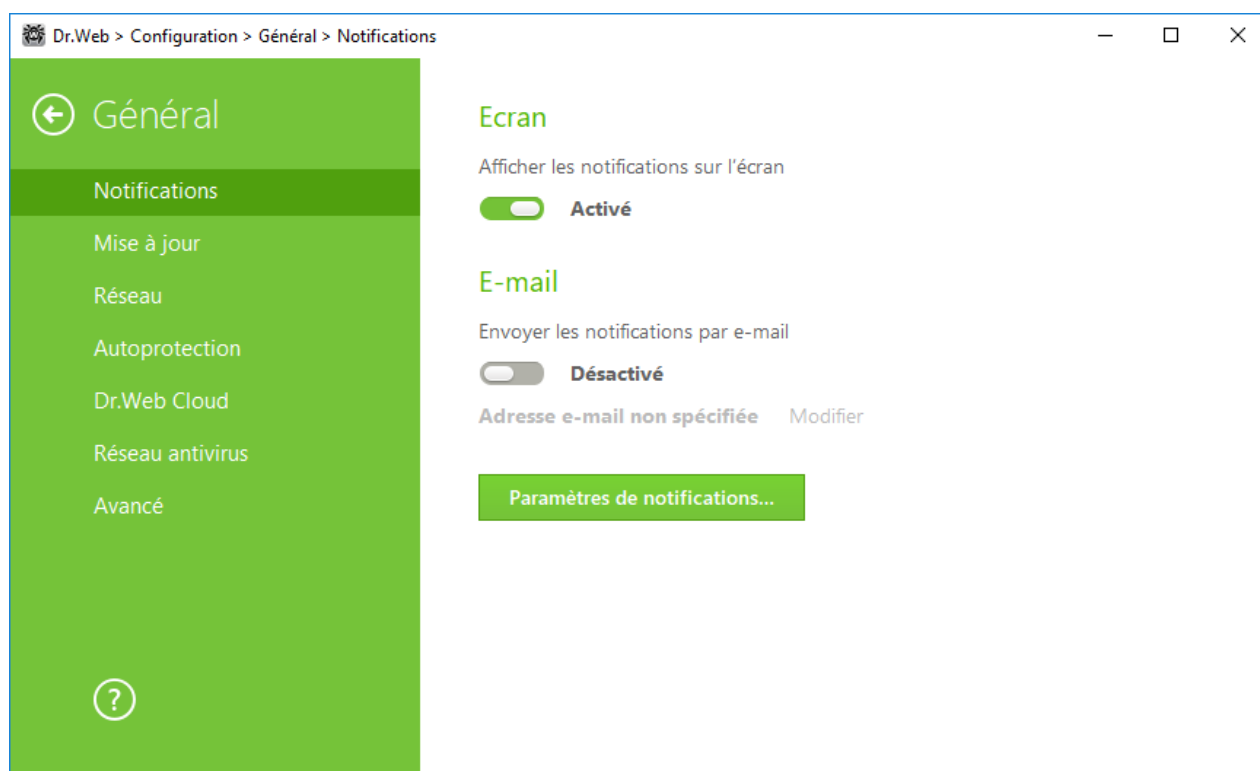


Figure 18. Paramètres de notifications

Notifications e-mail

Pour recevoir des notifications sur les événements par e-mail, exécutez les actions suivantes :

1. Activez l'option **Envoyer les notifications par e-mail**.
2. Dans la fenêtre qui s'affiche, spécifiez l'adresse e-mail que vous souhaitez utiliser pour recevoir les notifications. Il est nécessaire de confirmer l'utilisation de cette adresse à l'étape 7.
3. Cliquez sur **Suivant**.
4. Indiquez les données du compte depuis lequel les notifications seront envoyées.
 - Si la liste des serveurs de messagerie contient le serveur nécessaire, sélectionnez-le et indiquez le login et le mot de passe de votre compte.
 - Si la liste des serveurs de messagerie ne contient pas le serveur nécessaire, cliquez sur **Spécifiez manuellement** et remplissez les champs nécessaires dans la fenêtre qui s'affiche.

Paramètre	Description
Serveur SMTP	Entrez l'adresse du serveur de messagerie qui sera utilisé par Dr.Web pour envoyer les notifications e-mail.
Port	Entrez le port du serveur de messagerie auquel Dr.Web va se connecter pour envoyer des notifications e-mail.
Login	Entrez le login pour se connecter au serveur de messagerie.



Paramètre	Description
Mot de passe	Entrez le mot de passe à utiliser pour se connecter au serveur de messagerie.
Utiliser SSL/TLS	Cochez cette case si vous voulez utiliser le chiffrement SSL/TLS lors de la transmission des messages.
Authentification NTLM	Cochez cette case si vous voulez effectuer l'authentification via le protocole NTLM.

5. Cliquez sur **Envoyer un message de test** si vous voulez vérifier si le compte est indiqué correctement. Le message sera envoyé à l'adresse de laquelle les notifications doivent être envoyées (configurée à l'étape 4).
6. Cliquez sur **Suivant**.
7. Entrez le code de confirmation qui sera envoyée à l'adresse e-mail que vous avez indiquée à l'étape 2 pour recevoir les notifications. Si vous n'avez pas reçu le code pendant 10 minutes, cliquez sur **Envoyer le code encore une fois**. Si vous n'entrez pas le code de confirmation, les notifications ne seront pas envoyées à cette adresse.
8. Pour modifier l'adresse e-mail et les autres paramètres, cliquez sur **Modifier** et répétez toutes les actions à commencer par l'étape 2.
9. Cliquez sur le bouton **Paramètres des notifications** et spécifiez les types de notifications nécessaires. Par défaut tous les types des notifications envoyées par e-mail, sont désactivés.

Paramètres des notifications

1. Cliquez sur **Paramètres des notifications**.
2. Choisissez les notifications que vous souhaitez recevoir. Pour afficher les pop-ups, cochez les cases dans la colonne **Ecran**. Pour recevoir les notifications par e-mail, cochez la case dans la colonne **E-mail**. Si vous ne voulez pas recevoir les notifications des événements, décochez les cases.

Type de notification	Description
Menace détectée	Notifications des menaces détectées par les composants SplDer Guard. Ces notifications sont activées par défaut.
Notifications critiques	Notifications critiques des événements suivants : <ul style="list-style-type: none">• des connexions en attente de réponse du Pare-feu ont été détectées. Ces notifications sont activées par défaut.
Notifications majeures	Notifications importantes des événements suivants :



Type de notification	Description
Notifications mineurs	Notifications mineures des événements suivants : <ul style="list-style-type: none">• mise à jour réussie ;• erreur de mise à jour ; Les notifications sont désactivées par défaut.
Licence	Notifications des événements suivants : <ul style="list-style-type: none">• la licence va expirer ;• la licence actuelle n'est pas trouvée ;• la licence actuelle est bloquée.

3. Si nécessaire, configurez des paramètres avancés de l'affichage des notifications :

Option	Description
Ne pas afficher les notifications en mode plein écran	Notifications s'affichant lorsque vous travaillez avec des applications en mode plein écran (affichage des films, graphiques etc.). Décochez la case pour recevoir toujours de telles notifications.
Afficher les notifications du Pare-feu dans une fenêtre séparée en mode plein écran	Affichage des notifications du Pare-feu sur un bureau séparée lorsque des applications tournent en mode plein écran (jeux, vidéo). Décochez la case pour afficher les notifications sur le même bureau que celui où une application est lancée en mode plein écran.

4. Si vous avez choisi une ou plusieurs notifications par e-mail, configurez l'[envoi d'e-mails](#) depuis votre ordinateur.



Les notifications sur certains événements ne sont pas incluses dans les groupes listés et s'affichent toujours à l'utilisateur :

- installation des mises à jour prioritaires exigeant un redémarrage ;
- redémarrage pour achever la neutralisation des menaces ;
- redémarrage pour activer/désactiver l'hyperviseur ;
- demande de l'autorisation de modification de l'objet par le processus.

10.2. Mise à jour

Dans cette section du logiciel, vous pouvez configurer les paramètres suivants de la mise à jour de Dr.Web :

- [périodicité des mises à jour](#) ;
- [source de mises à jour](#) ;
- [composants à mettre à jour](#) ;
- [miroir de mise à jour](#).

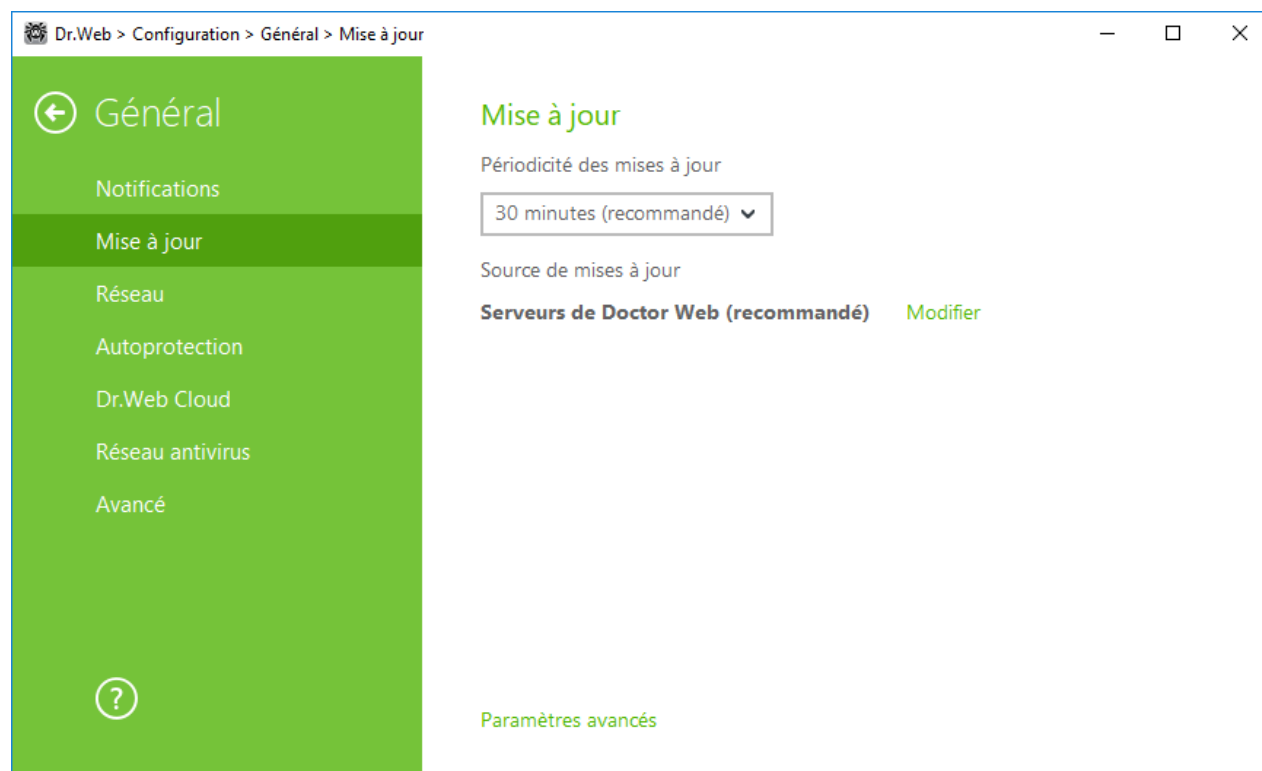



Figure 19. Paramètres de la mise à jour

Périodicité des mises à jour

La valeur par défaut (30 minutes) est optimale pour maintenir les informations sur les menaces à jour. Pour spécifier la périodicité de mises à jour, sélectionnez la valeur nécessaire dans le menu déroulant.

La mise à jour se fait en tâche de fond. Vous pouvez également sélectionner la valeur **Manuellement**. Dans ce cas, il vous faudra lancer la mise à jour du produit manuellement depuis le [menu de](#) Dr.Web . Vous pouvez trouver les instructions détaillées concernant le lancement de la mise à jour dans la rubrique [Mise à jour](#).



Configuration de la source de mises à jour

La valeur **Serveurs de Doctor Web (recommandé)** est spécifiée pour défaut en tant que source de mises à jour. Pour configurer la source de mises à jour qui vous convient le mieux, faites le suivant :

1. Dans la section des paramètres **Général** → **Mise à jour**, dans l'élément **Source de mises à jour**, cliquez sur le lien **Modifier**. La fenêtre de configuration de la source de mises à jour va s'ouvrir.

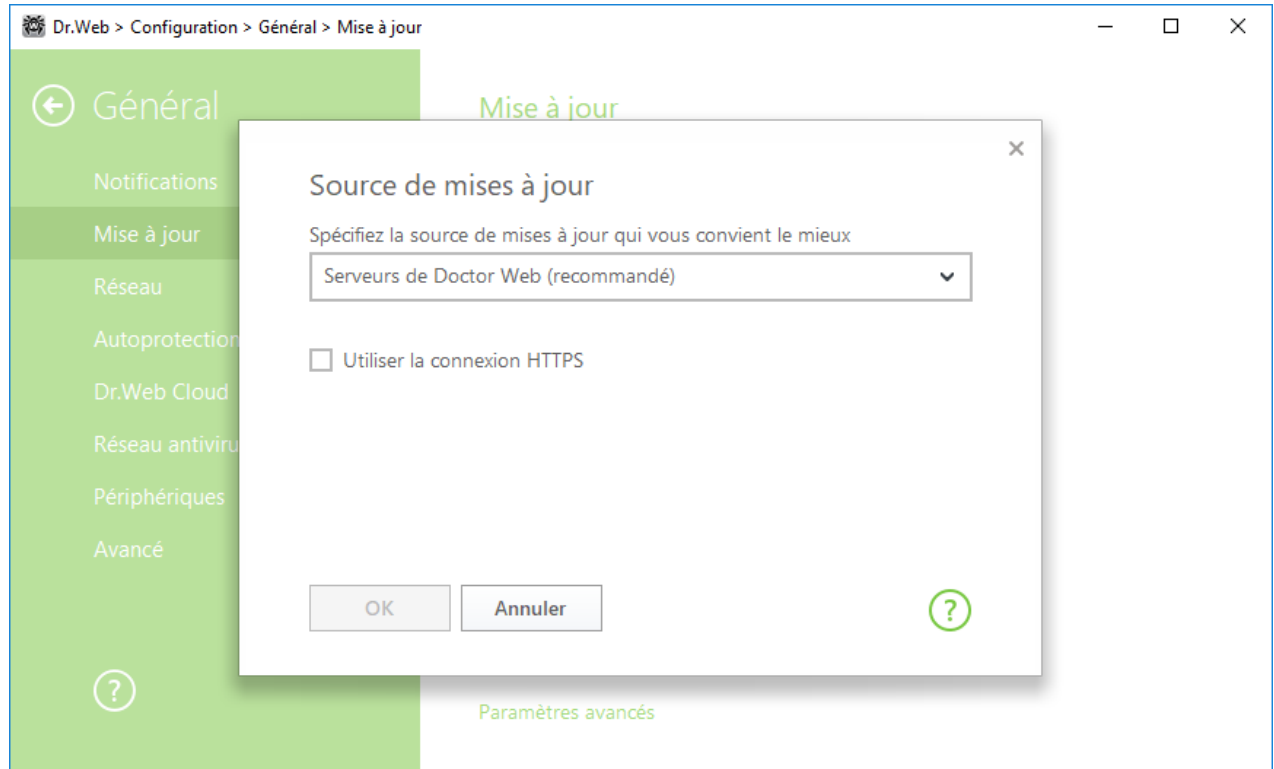


Figure 20. Source de mises à jour

2. Dans le menu déroulant, spécifiez la source de mises à jour qui vous convient le mieux.
 - **Serveurs de Doctor Web (recommandé)**. La mise à jour s'effectue depuis les serveurs de Doctor Web via Internet. Si vous voulez télécharger les mises à jour via le protocole sécurisé, activez l'option **Utiliser la connexion HTTPS**.
 - **Dossier local ou réseau**. La mise à jour s'effectue depuis un dossier local ou un dossier réseau dans lequel sont copiées les mises à jour. Spécifiez le chemin vers ce dossier, ainsi que le nom de l'utilisateur et le mot de passe si nécessaire.
 - **Réseau antivirus**. La mise à jour sera effectuée via le réseau local depuis l'ordinateur sur lequel est installé le produit Dr.Web et où un miroir de mise à jour a été créé. Sélectionnez l'ordinateur qui sera utilisé en tant que source de mises à jour.
3. Cliquez sur **OK** pour enregistrer les modifications.



Paramètres avancés

Configuration des composants mis à jour

Vous pouvez choisir l'un des moyens suivants pour télécharger les mises à jour des composants de Dr.Web :

- **Tout (recommandé)**. Les mises à jour des bases virales Dr.Web ainsi que les mises à jour du moteur antivirus et d'autres composants de Dr.Web sont téléchargées ;
- **Uniquement les bases**. Seules les mises à jour des bases virales Dr.Web et du moteur antivirus sont téléchargées ; les autres composants de Dr.Web ne sont pas mis à jour.

Création d'un miroir de mise à jour

Le miroir de mise à jour est un ordinateur configuré en tant que source de mises à jour pour les autres ordinateurs du réseau local. Le miroir de mise à jour peut être utilisé pour mettre à jour Dr.Web sur les ordinateurs qui ne sont pas connectés à Internet.

Pour configurer votre ordinateur en tant que miroir de mise à jour, faites le suivant :

1. Dans la section de paramètres **Général** → **Mise à jour**, ouvrez **Paramètres avancés** et activez l'utilisation du miroir de mise à jour à l'aide de l'interrupteur . La fenêtre de configuration du miroir de mise à jour va s'ouvrir.

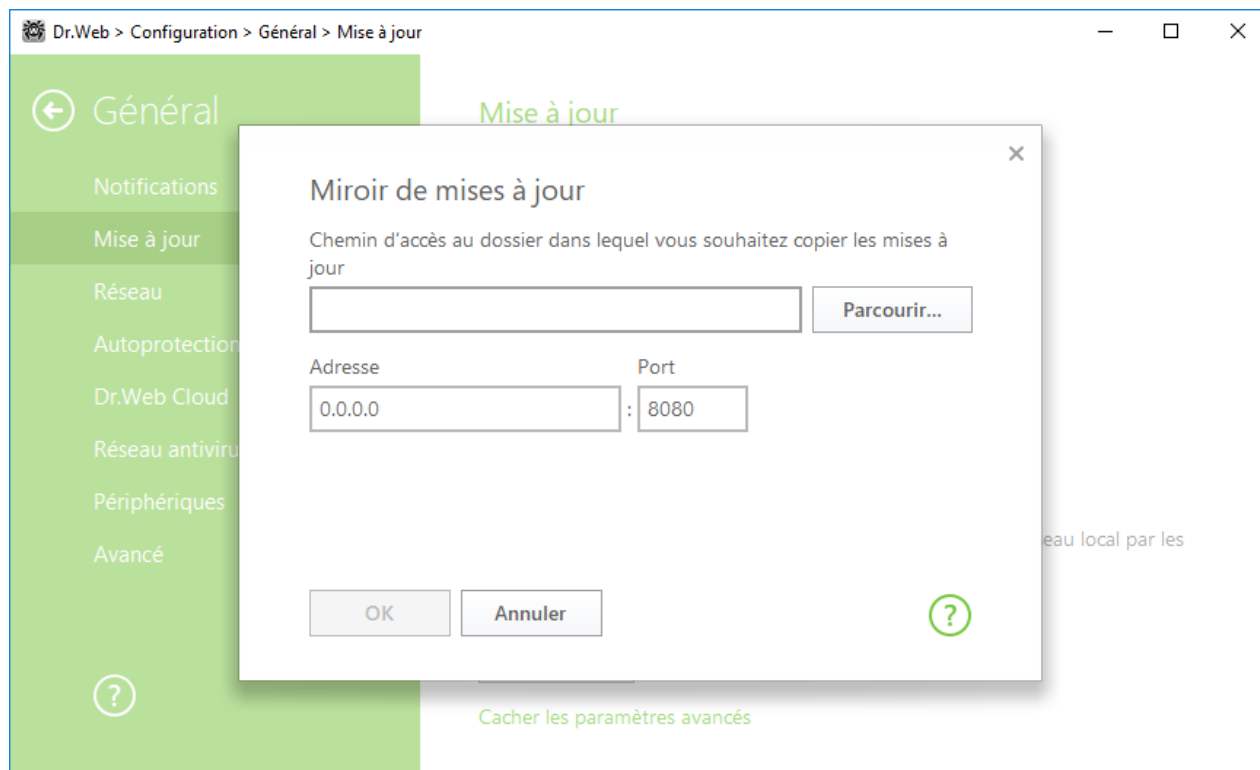


Figure 21. Miroir de mise à jour

2. Spécifiez le chemin d'accès au dossier dans lequel les mises à jour seront copiées.



3. Si votre ordinateur comprend plusieurs sous-réseaux, vous pouvez indiquer l'adresse qui sera disponible pour un réseau seulement. Vous pouvez également indiquer le port sur lequel le serveur HTTP recevra des requêtes de connexion.
4. Cliquez sur **OK** pour enregistrer les modifications.

La périodicité de téléchargement des mises à jour sur le miroir correspondra à la valeur spécifiée dans l'élément **Périodicité des mises à jour**, dans la section des paramètres **Général** → **Mise à jour**.

10.3. Réseau

Utiliser le serveur proxy

Si nécessaire, vous pouvez activer l'utilisation d'un serveur proxy et configurer ses paramètres. Cliquez sur **Modifier** pour paramétrer le serveur proxy :

Paramètre	Description
Adresse	Spécifiez l'adresse du serveur proxy.
Port	Spécifiez le port du serveur proxy.
Login	Spécifiez le nom du compte pour se connecter au serveur proxy.
Mot de passe	Spécifiez le mot de passe du compte utilisé pour se connecter au serveur proxy.
Type d'authentification	Sélectionnez un type d'authentification nécessaire pour se connecter au serveur proxy.

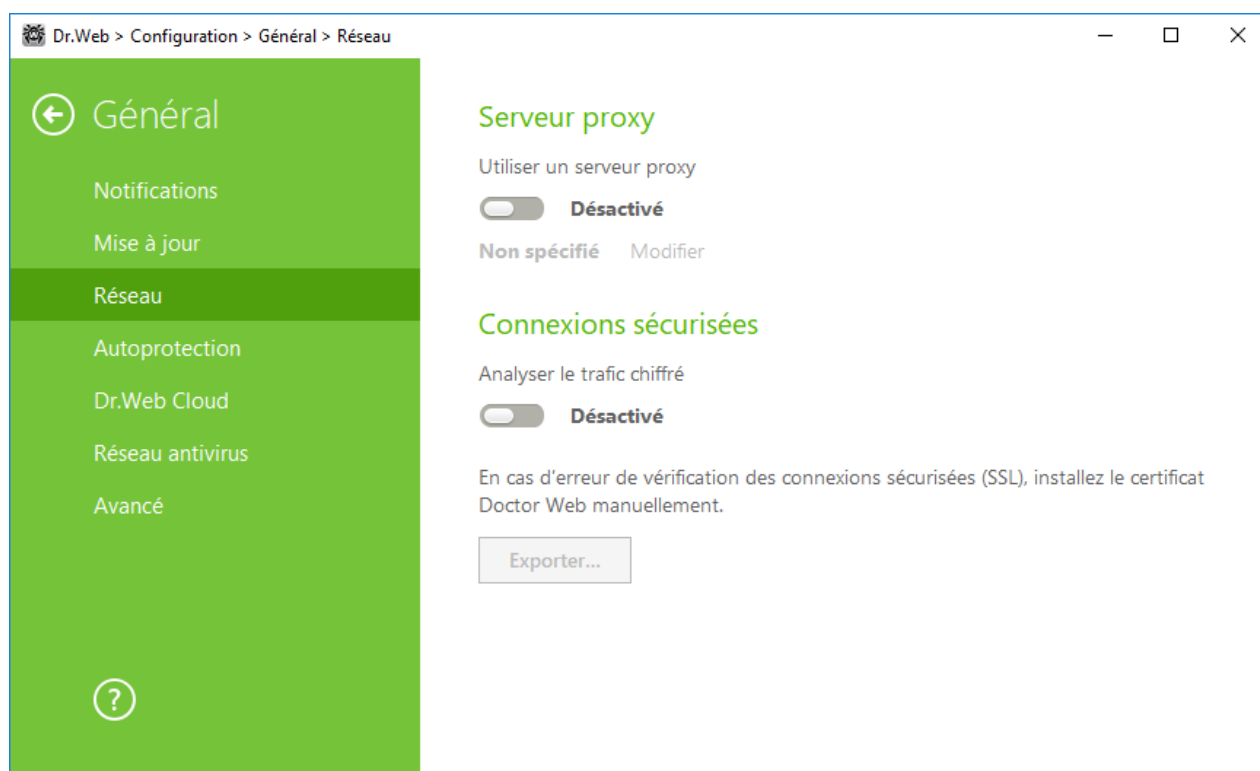


Figure 22. Connexion au serveur proxy et analyse du trafic chiffré

Connexions sécurisées

Pour que Dr.Web analyse les données transmises via les protocoles cryptographiques SSL, TLS ou STARTTLS, activez l'option **Analyser le trafic chiffré**. SpIDer Mail va analyser les données transmises via les protocoles POP3S, SMTPS, IMAPS

Si l'application utilisant les connexions chiffrées ne se connecte pas au stockage de certificats système Windows, il faut exporter le certificat de sécurité de Doctor Web et l'importer manuellement dans chaque application.



Durée de validité du certificat de sécurité — 1 an. Si cela est nécessaire, importez le certificat de nouveau chaque année.

Qu'est-ce qu'un certificat de sécurité

Le certificat de sécurité est un document électronique confirmant que le programme certifié a été vérifié dans une autorité de certification. Les certificats de sécurité s'appellent également les certificats SSL car le protocole SSL (Secure Socket Layer — couches de sockets sécurisés) est utilisé pour leur fonctionnement. Il assure l'interaction protégé par le chiffrement entre les hôtes du réseau Internet, par exemple entre l'utilisateur et le serveur web.

L'installation (l'importation) du certificat de sécurité d'un hôte web dans le programme utilisant



Internet garantit que la communication sera effectuée en mode sécurisé avec la vérification de l'authenticité. Dans ce cas, les cybercriminels auront du mal à intercepter les données.

L'importation du certificat de Doctor Web peut être requis pour les logiciels suivants :

- navigateur Opera ;
- navigateur Firefox ;
- client de messagerie Mozilla Thunderbird ;
- client de messagerie The Bat!, etc.

Comment exporter et importer le certificat de Doctor Web ?

1. Cliquez sur le bouton **Exporter**.
2. Sélectionnez le dossier dans lequel vous voulez sauvegarder le certificat. Cliquez sur **OK**.
3. Importez le certificat dans l'application nécessaire dans les paramètres de l'application. Pour plus d'infos sur l'importation du certificat dans l'application, voir les documents de référence de l'application nécessaire.



Si l'option **Analyser le trafic chiffré** est activée, pour le fonctionnement correct de certains clients de stockages cloud (tels que Google Drive, Dropbox, Yandex.Disk, etc.), il faut [exclure ces applications de l'analyse effectuée par le composant SplDer Gate](#).

10.4. Autoprotection

Dans cette section, vous pouvez configurer les paramètres de l'autoprotection de Dr.Web contre l'influence non autorisée des programmes attaquant les antivirus ou contre les dommages accidentels.

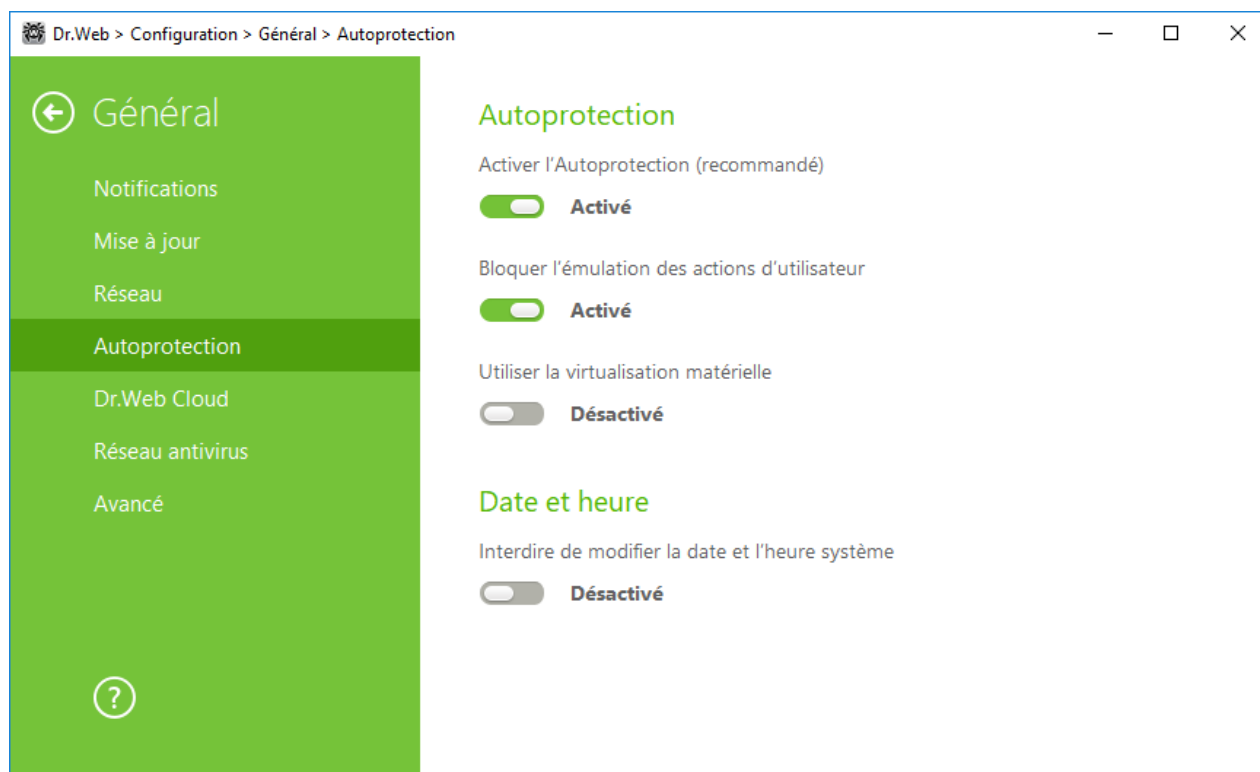


Figure 23. Paramètres de la protection Dr.Web

Autoprotection

L'option **Activer l'Autoprotection (recommandé)** permet de protéger les fichiers et les processus de Dr.Web contre l'accès non autorisé. Il n'est pas recommandé de désactiver l'Autoprotection.



En cas de problèmes survenus lors de l'utilisation d'outils de défragmentation, il est recommandé de désactiver temporairement l'Autoprotection.

Pour réaliser un rollback vers le point de restauration du système, il est nécessaire de désactiver le module d'Autoprotection.

L'option **Bloquer l'émulation des actions d'utilisateur** permet de prévenir les modifications automatiques dans les paramètres de Dr.Web, y compris l'exécution de scripts qui imitent l'interaction de l'utilisateur avec Dr.Web et qui sont lancés par l'utilisateur (par exemple, des scripts de modification des paramètres de Dr.Web, de suppression de la licence et d'autres actions visant la modification du fonctionnement de Dr.Web).

Le paramètre **Utiliser la virtualisation matérielle** permet d'utiliser plus de fonctionnalités de l'ordinateur pour détecter et neutraliser les menaces et pour rendre l'autoprotection Dr.Web plus fiable. Pour activer cette option, le redémarrage de l'ordinateur est requis.



La virtualisation matérielle fonctionne si les particularités matérielles de votre ordinateur et le système d'exploitation supportent la virtualisation matérielle.

L'activation de cette option peut provoquer un conflit de compatibilité avec des logiciels tiers.

En cas de problèmes, désactivez cette option.

Pour les plateformes 32-bits la virtualisation matérielle n'est pas supportée.

Date et heure

Certains programmes malveillants modifient la date et l'heure système. Dans ce cas, les mises à jour des bases virales ne se font pas selon la planification, la licence peut être considérée comme obsolète et les composants de la protection peuvent être désactivés.

L'option **Interdire de modifier la date et l'heure système** permet d'empêcher les modifications manuelles ou automatiques de l'heure et de la date système ainsi que du fuseau horaire. Cette restriction s'applique à tous les utilisateurs. Vous pouvez configurer les [notifications](#) afin d'être informé d'une tentative de modification de l'heure système.

10.5. Dr.Web Cloud

Dans cette rubrique, vous pouvez vous connecter aux services cloud de Doctor Web et participer au programme d'amélioration de la qualité des produits Dr.Web.



Figure 24. Connexion à Dr.Web Cloud

Service Cloud

Dr.Web Cloud permet à la protection antivirus d'utiliser des informations actuelles sur les menaces, ces informations sont mises à jour sur les serveurs de Doctor Web en temps réel.

En fonction des [paramètres de mises à jour](#), les informations sur les menaces utilisées par les composants de la protection antivirus peuvent être obsolètes. Les services Cloud peuvent, de façon fiable, restreindre l'accès des utilisateurs de votre ordinateur aux sites de contenu non désirable ainsi que restreindre l'accès aux fichiers infectés.

Programme d'amélioration de la qualité du logiciel

Si vous participez au programme d'amélioration de la qualité du logiciel, des données non personnelles sur le fonctionnement de Dr.Web sur votre ordinateur seront périodiquement envoyées sur les serveurs de la société. Les données reçues ne sont pas utilisées pour vous identifier ni vous contacter.

Cliquez sur le lien **Politique de confidentialité de Doctor Web** pour consulter cette politique sur le [site](#) officiel de Doctor Web.

10.6. Réseau antivirus

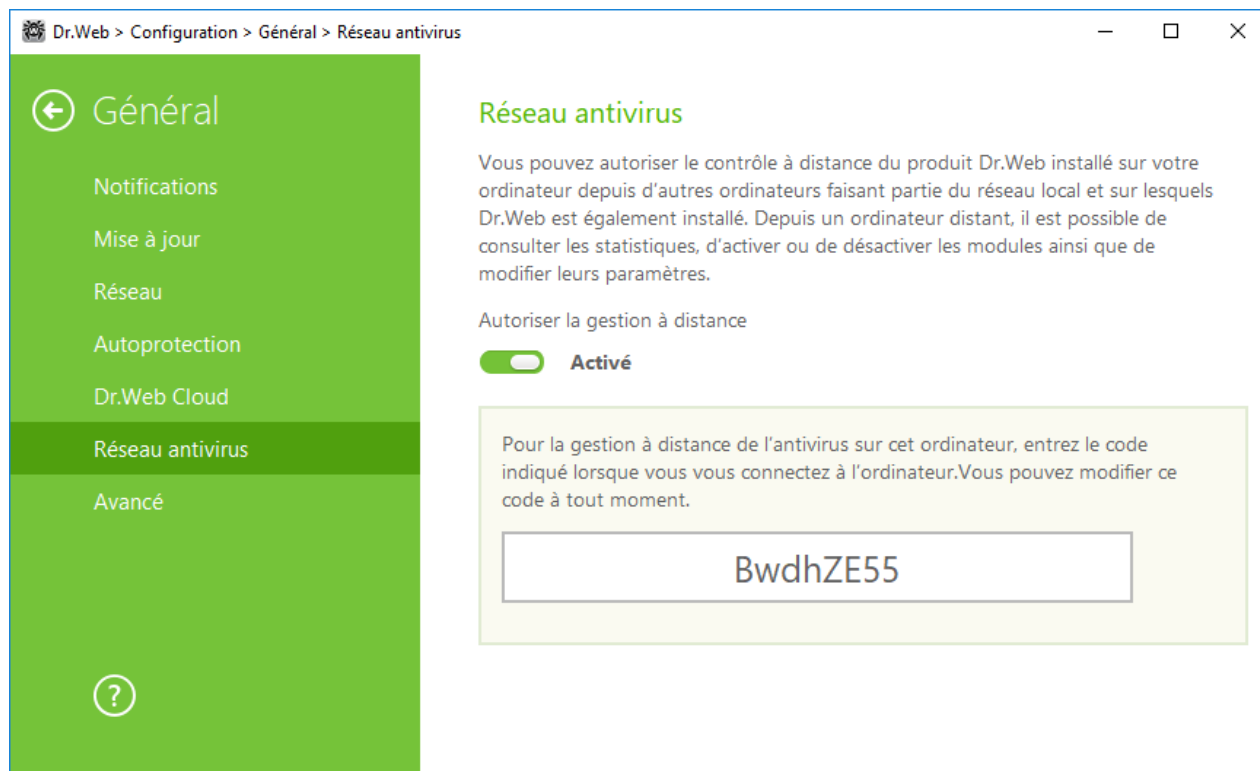


Figure 25. Activation de la gestion distante de l'antivirus

Vous pouvez autoriser l'accès à l'Antivirus Dr.Web sur votre ordinateur. Pour ce faire, activez l'option **Autoriser la gestion à distance** et spécifiez le mot de passe qu'il faudra saisir pour la gestion de votre antivirus à distance.



Si vous utilisez la clé pour Dr.Web Security Space vous pouvez télécharger la documentation correspondante sur le site <https://download.drweb.com/doc> et prendre connaissance du composant Réseau antivirus.

L'utilisateur ayant le droit de gestion à distance de l'Antivirus Dr.Web sur votre ordinateur aura l'accès aux onglets suivants :

- A propos de
- [Licence](#)
- Mon Dr.Web
- Aide
- [Outils](#)
- [Mise à jour](#)
- [Configuration](#)



Vous pouvez consulter des statistiques, activer ou désactiver des modules et éditer leurs paramètres. Les éléments Quarantaine et Scanner sont indisponibles. Les paramètres et les statistiques du Pare-feu Dr.Web ne sont pas disponibles non plus, cependant vous pouvez activer ou désactiver ce composant.

10.7. Avancé

Dans cette section, vous pouvez spécifier la langue du logiciel, les paramètres du journal et de la Quarantaine.

Dans la liste déroulante, vous pouvez choisir une langue du logiciel. La liste de langues se complète automatiquement et à l'heure actuelle, elle contient toutes les localisations disponibles de l'interface graphique de Dr.Web pour le moment donné.

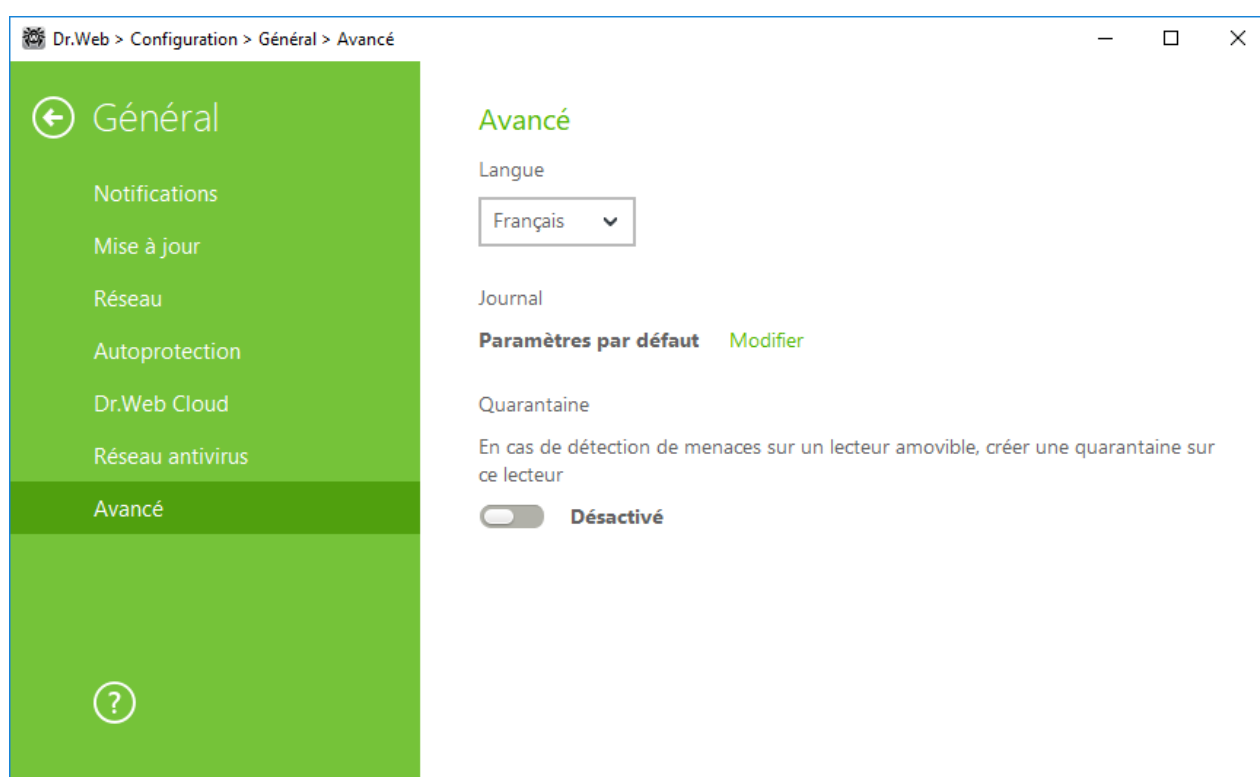


Figure 26. Paramètres avancés

Paramètres du Journal

Pour configurer les paramètres de journal, cliquez sur le bouton correspondant **Modifier**.



Par défaut, la taille des fichiers de journal est limitée à 10 Mo (pour le composant SpIDer Guard — 100 Mo). Si la taille du fichier de journal excède la limite, le contenu du fichier est réduit à :

- la taille spécifiée si le fichier de journal obtenu après le scan de la session en cours n'excède pas cette limite ;



- la taille du fichier de journal obtenu après le scan de la session en cours, si le fichier de journal global excède la limite.

Par défaut pour tous les composants de Dr.Web le journal est conservé en mode standard et les informations suivantes sont enregistrées :

Composant	Information
SplDer Guard	<p>Les heures des mises à jour et des démarrages/arrêts de SplDer Guard, les événements viraux, les noms des fichiers scannés, les noms des packers et le contenu des objets complexes analysés (archives, pièces jointes d'e-mail, conteneurs de fichiers).</p> <p>Il est recommandé d'utiliser ce mode pour déterminer les objets les plus fréquemment scannés par SplDer Guard. Si nécessaire, vous pouvez ajouter ces objets dans la liste des exclusions afin d'augmenter les performances de l'ordinateur.</p>
SplDer Mail	<p>Les heures des mises à jour et des démarrages/arrêts de SplDer Mail, les événements viraux, les paramètres d'interception des connexions, les informations sur les fichiers scannés, les noms des packers et le contenu des archives scannées.</p> <p>Il est recommandé d'utiliser ce mode lors du test des paramètres d'interception des connexions avec les serveurs de messagerie.</p>
Scanner	<p>Dans ce mode, les événements qui sont journalisés ce sont les mises à jour, les démarrages et les arrêts du Scanner Dr.Web, les menaces détectées, ainsi que les informations sur les noms des packers et sur le contenu des archives scannées.</p>
Pare-feu	<p>Pare-feu n'écrit pas le journal en mode standard. Si vous activez les journaux détaillés, le Pare-feu collecte des données sur les paquets réseau (pcap logs).</p>
Mise à jour Dr.Web	<p>Liste des fichiers Dr.Web mis à jour et état de leur téléchargement, détails sur l'exécution de scripts auxiliaires, date et heure des mises à jour, détails sur le redémarrage des composants Dr.Web après la mise à jour.</p>
Service Dr.Web	<p>Informations sur les composants Dr.Web, modification de paramètres des composants, activation ou désactivation des composants, événements relatifs à la protection préventive, connexion au réseau antivirus.</p>

Créer des dumps de mémoire

L'option **Créer des dumps de mémoire en cas d'erreurs de l'analyse** permet de sauvegarder les informations utiles sur le fonctionnement de plusieurs composants de Dr.Web. Cette option aide les spécialistes du support technique de Doctor Web à analyser un problème en détails et à trouver une solution. Il est recommandé d'activer cette option à la demande du support technique de Doctor Web ou lorsque des erreurs de scan ou de neutralisation surviennent. Le dump de mémoire



est sauvegardé dans un fichier .dmp situé dans le dossier %PROGRAMFILES%\Common Files\Doctor Web\Scanning Engine\ folder.

Pour activer les journaux détaillés



Lors de la journalisation détaillée le maximum d'informations sur le fonctionnement des composants Dr.Web est fixé. Cela va désactiver la restriction de taille de fichiers de journal et augmenter la charge de Dr.Web et du système d'exploitation. Il est recommandé d'utiliser ce mode uniquement lorsque des erreurs de composants surviennent ou sur requête du Support Technique Doctor Web.

1. Pour activer les journaux détaillés pour un composant Dr.Web, cochez la case correspondante.
2. Par défaut, le mode de journal détaillé est utilisé avant le premier redémarrage de l'OS. S'il est nécessaire d'enregistrer les le comportement d'un composant avant et après le redémarrage, cochez la case **Continuer à écrire le journal détaillé après le redémarrage (Utiliser seulement sur demande du support technique de Doctor Web)**.
3. Sauvegardez les modifications.



Paramètres de quarantaine

Vous pouvez choisir le mode d'isolation pour les objets infectés, détectés sur les supports amovibles. Lorsque cette option est activée, les menaces détectées sont déplacées dans le dossier sur le support amovible sans être chiffrées. Le dossier de quarantaine est créé uniquement lorsque le support amovible est accessible en écriture. L'utilisation de dossiers séparés et du non chiffrement sur les supports amovibles permet de prévenir la perte de données. Si l'option est désactivée, la menace détectée est mise en quarantaine sur le disque local.



11. Exclusions

Dans cette section, vous pouvez configurer les exclusions des analyses par les composants SpIDer Guard, SpIDer Mail et Scanner et ajouter des adresses d'expéditeurs dans la liste noire ou blanche pour que les messages qu'ils envoient ne soient pas analysés pour la présence de spam.

Pour configurer les exclusions, ouvrez le menu , lancez **Configuration**  en [mode administrateur](#) et sélectionnez la section **Exclusions**.

Pour exclure certains fichiers ou dossiers du scan, sélectionnez la rubrique [Dossiers et fichiers](#).

Pour exclure certains processus du scan de composants de Dr.Web sélectionnez la rubrique [Applications](#).

11.1. Dossiers et fichiers

Dans cette section, vous pouvez spécifier la liste des fichiers et dossiers qui sont exclus du scan de SpIDer Guard et de Scanner. Vous pouvez exclure les dossiers de quarantaine, les dossiers de travail de certains programmes, les fichiers temporaires (fichiers swap), etc.

La liste est vide par défaut. Ajoutez des fichiers et dossiers aux exclusions ou utilisez des masques pour désactiver le scan de certains groupes de fichiers. Tout objet ajouté peut être exclu du scan des deux composants ou du scan de chaque composant séparément.

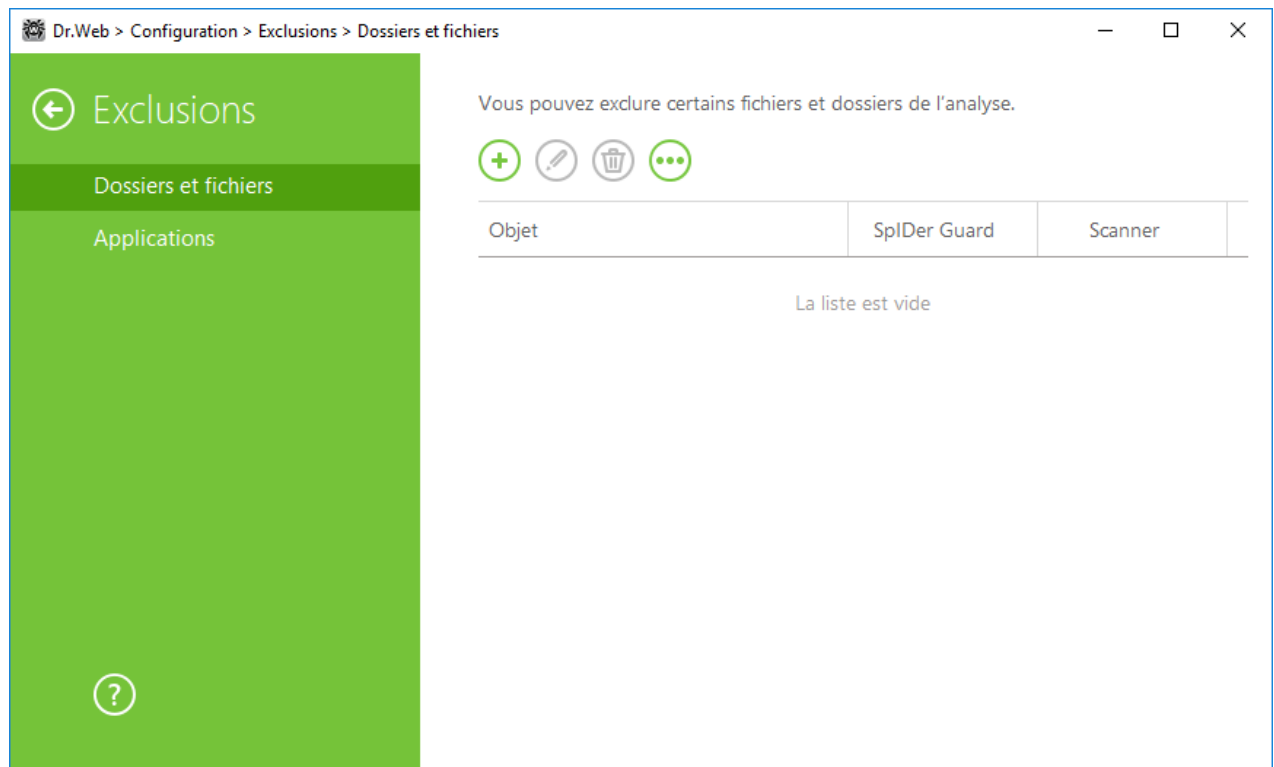



Figure 27. Exclusion des fichiers et des dossiers de l'analyse



Pour configurer la liste des exclusions

1. Faites une des actions suivantes pour ajouter un dossier ou un fichier à la liste :

- pour ajouter un fichier ou dossier existant, cliquez sur . Dans la fenêtre qui s'ouvre, cliquez sur **Parcourir** et choisissez le fichier ou le dossier dans la fenêtre standard d'ouverture de fichier. Vous pouvez entrer manuellement le chemin complet vers le fichier ou le dossier, ou modifier le chemin dans le champ réservé à cet effet avant de l'ajouter à la liste . Par exemple :
 - `C:\folder\file.txt` : exclut de l'analyse le fichier file.txt se trouvant dans le dossier C:\folder.
 - `C:\folder` : exclut de l'analyse tous les sous-dossiers et les fichiers se trouvant dans le dossier C:\folder.
- pour exclure de l'analyse un fichier avec un nom particulier, entrez dans le champ de saisie le nom du fichier y compris l'extension. Il n'est pas nécessaire de spécifier le chemin d'accès au fichier . Par exemple :
 - `file.txt` : exclut de l'analyse tous les fichiers avec le nom file et l'extension .txt dans tous les dossiers.
 - `file` : exclut de l'analyse tous les fichiers avec le nom file sans extension dans tous les dossiers.
- pour exclure du scan des fichiers ou des dossiers du type particulier, entrez le masque qui les détermine dans le champ de saisie.



Un masque désigne les éléments communs aux noms des objets, ainsi :

- le caractère « * » remplace toute séquence (potentiellement vide) de caractères ;
- le caractère « ? » remplace n'importe quel caractère (un seul caractère) ;

Exemples :

- `rapport*.doc` : un masque qui désigne tous les documents Microsoft Word dont les noms commencent par le mot « rapport », par exemple, les fichiers rapport-fevrier.doc, rapport121209.doc etc. ;
- `*.exe` : un masque qui désigne tous les fichiers exécutable ayant l'extension EXE, par exemple, setup.exe, iTunes.exe etc. ;
- `photo????09.jpg` : un masque qui désigne tous les fichiers des images au format JPG dont le nom commence par « photo » et se termine par « 09 », dans ce cas entre ces deux fragments, dans le nom de fichier, il y a quatre n'importe quels symboles, par exemple photo121209.jpg, photopapa09.jpg ou photo----09.jpg.
- `file*` : exclut de l'analyse tous les fichiers, dont les noms commencent pas file, avec n'importe quelle extension dans tous les dossiers.
- `file.*` : exclut de l'analyse tous les fichiers avec le nom file et n'importe quelle extension dans tous les dossiers.
- `C:\folder**` : exclut de l'analyse tous les sous-dossiers et les fichiers se trouvant dans le dossier C:\folder. Cependant les fichiers dans les sous-dossiers seront scannés.



- C:\folder* : exclut de l'analyse tous les fichiers se trouvant dans le dossier C:\folder ainsi que dans tous les sous-dossiers à tout niveau d'emboîtement.
 - C:\folder*.txt : exclut de l'analyse les fichiers de type *.txt se trouvant dans le dossier C:\folder. Les fichiers *.txt se trouvant dans les sous-dossiers seront scannés.
 - C:\folder**.txt : exclut de l'analyse les fichiers de type *.txt uniquement dans les sous-dossiers du premier niveau d'emboîtement dans le répertoire C:\folder.
 - C:\folder***.txt : exclut de l'analyse les fichiers de type *.txt dans les sous-dossiers de tout niveau d'emboîtement dans le dossier C:\folder. Les fichiers *.txt se trouvant dans le dossier C:\folder seront scannés.
2. Dans la fenêtre de configuration, indiquez les composants qui ne doivent pas scanner ce fichier.
 3. Cliquez sur **OK**. Le fichier ou dossier apparaît dans la liste.
 4. Pour modifier une exclusion, sélectionnez l'élément nécessaire dans la liste et cliquez sur .
 5. Pour ajouter de nouveaux fichiers ou dossiers à la liste, répétez les étapes 1 et 2. Pour retirer un fichier ou un dossier de la liste, sélectionnez-le dans la liste et cliquez sur .

Gestion des objets dans la liste

Si vous cliquez sur , les actions suivantes seront disponibles :

- **Exporter** : cette option permet de sauvegarder la liste créée des exclusions pour l'utiliser sur un autre ordinateur sur lequel est installé Dr.Web.
- **Importer** : cette option permet d'utiliser la liste des exclusions créée sur un autre ordinateur.
- **Désélectionner tout** : cette option permet de supprimer tous les objets de la liste des exclusions.

11.2. Applications

Dans cette section, vous pouvez spécifier la liste des programmes et des processus à exclure du scan de SpIDer Guard et SpIDer Mail.

Par défaut, la liste est vide.

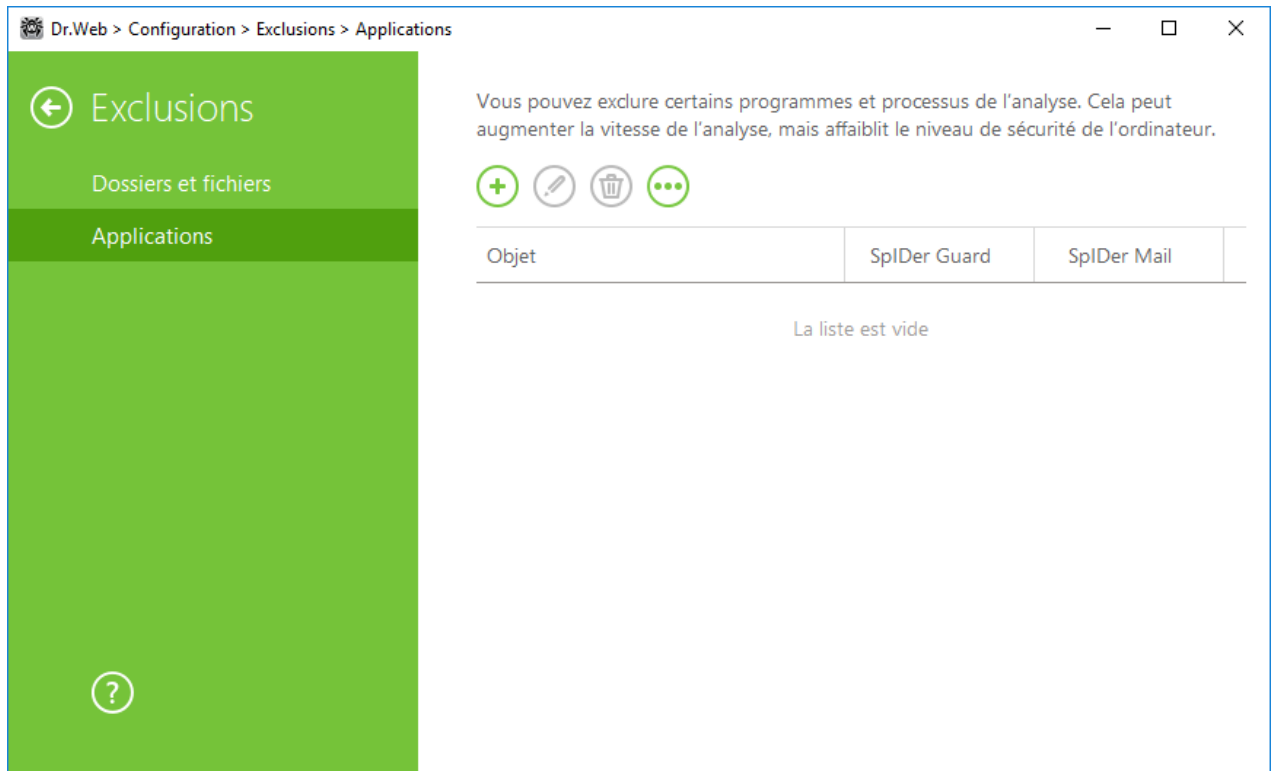


Figure 28. Liste des applications à exclure

Pour configurer la liste des exclusions

1. Pour ajouter un programme ou un processus à la liste des exclusions, cliquez sur . Exécutez une des actions suivantes :
 - dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir** et sélectionnez l'application dans la fenêtre standard d'ouverture de fichier. Vous pouvez entrer manuellement le chemin complet vers l'application dans le champ de saisie . Par exemple :
`C:\Program Files\folder\example.exe`
 - pour exclure une application de l'analyse, entrez son nom dans le champ de saisie. Dans ce cas, il n'est pas nécessaire de spécifier le chemin complet vers l'application . Par exemple :
`example.exe`
 - pour exclure de l'analyse des applications du type particulier, entrez le masque qui les détermine dans le champ de saisie

Un masque désigne les éléments communs aux noms des objets, ainsi :

- le caractère « * » remplace toute séquence (potentiellement vide) de caractères ;
- le caractère « ? » remplace n'importe quel caractère (un seul caractère) ;

Exemples de configuration des exclusions :

- `C:\Program Files\folder*.exe` : exclut de l'analyse les applications dans le dossier `C:\Program Files\folder`. Dans les sous-dossiers, les applications seront analysées.



- `C:\Program Files**.exe` : exclut de l'analyse uniquement les applications dans les sous-dossiers du premier niveau d'emboîtement du dossier `C:\Program Files`.
- `C:\Program Files***.exe` : exclut de l'analyse les applications dans les sous-dossiers de tout niveau d'emboîtement du dossier `C:\Program Files`. Dans le dossier `C:\Program Files`, les applications seront analysées.
- `C:\Program Files\folder\exam*.exe` : exclut de l'analyse toutes les applications dans le dossier `C:\Program Files\folder` dont les noms commencent par « exam ». Dans les sous-dossiers, ces applications seront analysées.
- `example.exe` : exclut de l'analyse toutes les applications avec le nom `example` et l'extension `.exe` dans tous les dossiers.
- `example*` : exclut de l'analyse dans tous les dossiers les applications de tout type dont les noms commencent par `example`.
- `example.*` : exclut de l'analyse toutes les applications avec le nom `example` et n'importe quelle extension dans tous les dossiers.
- vous pouvez exclure une application de l'analyse par le nom de variable, si dans les paramètres des variables système, le nom et la valeur de cette variable sont spécifiées. Par exemple :
 - `%EXAMPLE_PATH%\example.exe` : exclut de l'analyse l'application selon le nom de la variable système. Vous pouvez spécifier le nom et la valeur de la variable système dans les paramètres du système d'exploitation.

Sous Windows 7 et supérieur : **Panneau de configuration** → **Système** → **Paramètres système avancés** → **Avancé** → **Variable d'environnement** → **Variables système**.

Nom de la variable dans l'exemple : `EXAMPLE_PATH`.

Valeur de la variable dans l'exemple : `C:\Program Files\folder`.

2. Dans la fenêtre de configuration, indiquez les composants qui ne doivent pas analyser l'application sélectionnée. Pour les objets exclus de l'analyse par le composant SpIDer Mail, indiquez les conditions supplémentaires.

Paramètre	Description
Indépendamment de la présence de la signature numérique d'application	Sélectionnez ce paramètre si l'application doit être exclue du scan indépendamment de la présence de la signature numérique.
En cas de présence de la signature numérique d'application	Sélectionnez ce paramètre si l'application doit être exclue du scan uniquement en cas de présence de la signature numérique d'application. Sinon l'application sera scannée par les composants.



Paramètre	Description
Tout trafic	Sélectionnez ce paramètre pour exclure du scan le trafic chiffré et non chiffré de l'application.
Trafic chiffré	Sélectionnez ce paramètre pour exclure du scan seulement le trafic chiffré de l'application.
Via toutes les adresses IP et tous les ports	Sélectionnez ce paramètre pour exclure du scan le trafic acheminé vers toutes les adresses IP et tous les ports.
Via les adresses IP et les ports indiqués	Sélectionnez ce paramètre pour indiquer les adresses IP et les ports dont le trafic sera exclu du scan. Le trafic acheminé des autres adresses IP et des ports sera scanné (s'il n'est pas exclu par un autre paramètre).
Spécifier des adresses et des ports	<p>Pour configurer les exclusions de manière précise, utilisez les recommandations suivantes :</p> <ul style="list-style-type: none">• pour exclure de l'analyse un domaine particulier par un port particulier, indiquez, par exemple, <code>site.com:80</code> ;• pour exclure de l'analyse le trafic par un port non standard (par exemple, 1111) il faut indiquer : <code>*:1111</code> ;• pour exclure de l'analyse le trafic du domaine par n'importe quel port, indiquez : <code>site:*</code>

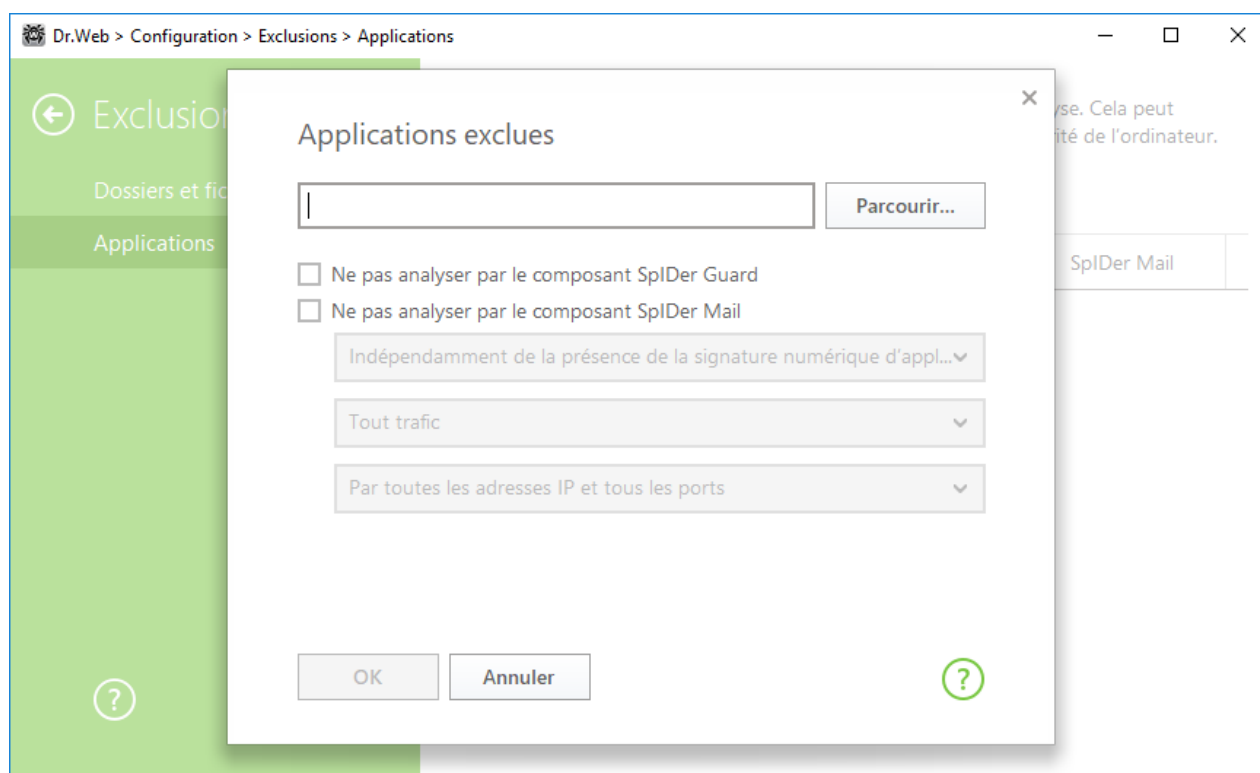






Figure 29. Exclusion d'applications

3. Cliquez sur **OK**. L'application sélectionnée va apparaître dans la liste.
4. Si nécessaire, reproduisez la marche à suivre pour y ajouter d'autres programmes.

Gestion des objets dans la liste

Pour éditer une exclusion, sélectionnez l'élément nécessaire dans la liste et cliquez sur . Pour supprimer une application de la liste des exclusions, sélectionnez l'élément nécessaire dans la liste et cliquez sur .



Si vous cliquez sur , les actions suivantes seront disponibles :

- **Exporter** : cette option permet de sauvegarder la liste créée des exclusions pour l'utiliser sur un autre ordinateur sur lequel est installé Dr.Web.
- **Importer** : cette option permet d'utiliser la liste des exclusions créée sur un autre ordinateur.
- **Désélectionner tout** : cette option permet de supprimer tous les objets de la liste des exclusions.



12. Composants de protection

Les composants de protection assure le scan du système, l'analyse des messages pour la présence de menaces et du spam, le contrôle des connexions réseau et du trafic HTTP.

Pour configurer les composants de protection, ouvrez le menu , lancez **Configuration**  en [mode administrateur](#) et sélectionnez la section **Composants de protection**.



La configuration des composants est possible uniquement avec [les privilèges d'administrateurs](#).

Pour configurer le scan des fichiers ou des processus en cours, allez à l'onglet [SpIDer Guard](#).

Pour configurer l'analyse du courrier, sélectionnez [SpIDer Mail](#).

Pour contrôler les connexions et le transfert de données via Internet et pour bloquer les connexions suspectes au niveau des paquets et des applications, allez à l'onglet [Pare-feu](#).

Pour configurer les paramètres généraux de scan de fichiers et d'objets différents et les réactions à la détection des fichiers infectés, suspects ou des programmes malveillants, sélectionnez [Scanner](#).

Pour contrôler les applications tierces, sélectionnez la section [Protection préventive](#).

12.1. SpIDer Guard

SpIDer Guard est un composant antivirus résidant en mémoire vive qui scanne les fichiers et la mémoire « à la volée » et détecte instantanément toute activité malveillante.

Avec les paramètres par défaut, SpIDer Guard analyse à la volée des fichiers créés ou modifiés sur le disque dur ainsi que tous les fichiers ouverts depuis un support amovible. De même, SpIDer Guard suit constamment les processus lancés pour détecter les comportements suspects et, s'il en détecte un, bloque les processus malveillants. En cas de détection des objets infectés, SpIDer Guard applique les actions définies par les paramètres configurés.

Les fichiers en archives et les boîtes aux lettres ne sont pas scannés. Si un fichier en archive ou en pièce jointe d'un e-mail est infecté, l'objet malveillant sera détecté et immédiatement neutralisé par SpIDer Guard au moment de l'extraction du fichier avant que l'ordinateur soit infecté. Pour prévenir la pénétration des objets malveillants diffusés via le courrier électronique sur votre ordinateur, [utilisez](#) SpIDer Mail.

Lors de la détection d'un objet infecté, SpIDer Guard applique les actions d'après les [paramètres indiqués](#). Vous pouvez modifier ces paramètres pour configurer des réactions automatiques à appliquer aux différents événements viraux.



Par défaut SpIDer Guard se lance automatiquement à chaque démarrage de Windows et ne peut être déchargé durant la session Windows en cours.

12.1.1. Configurer SpIDer Guard



Pour accéder aux paramètres de SpIDer Guard, vous êtes invité à entrer le mot de passe si vous avez activé l'option **Protéger les paramètres de Dr.Web par mot de passe** dans la section [Configuration](#).

Les paramètres par défaut permettent une utilisation optimale du produit. Ne les modifiez pas si ce n'est pas nécessaire.

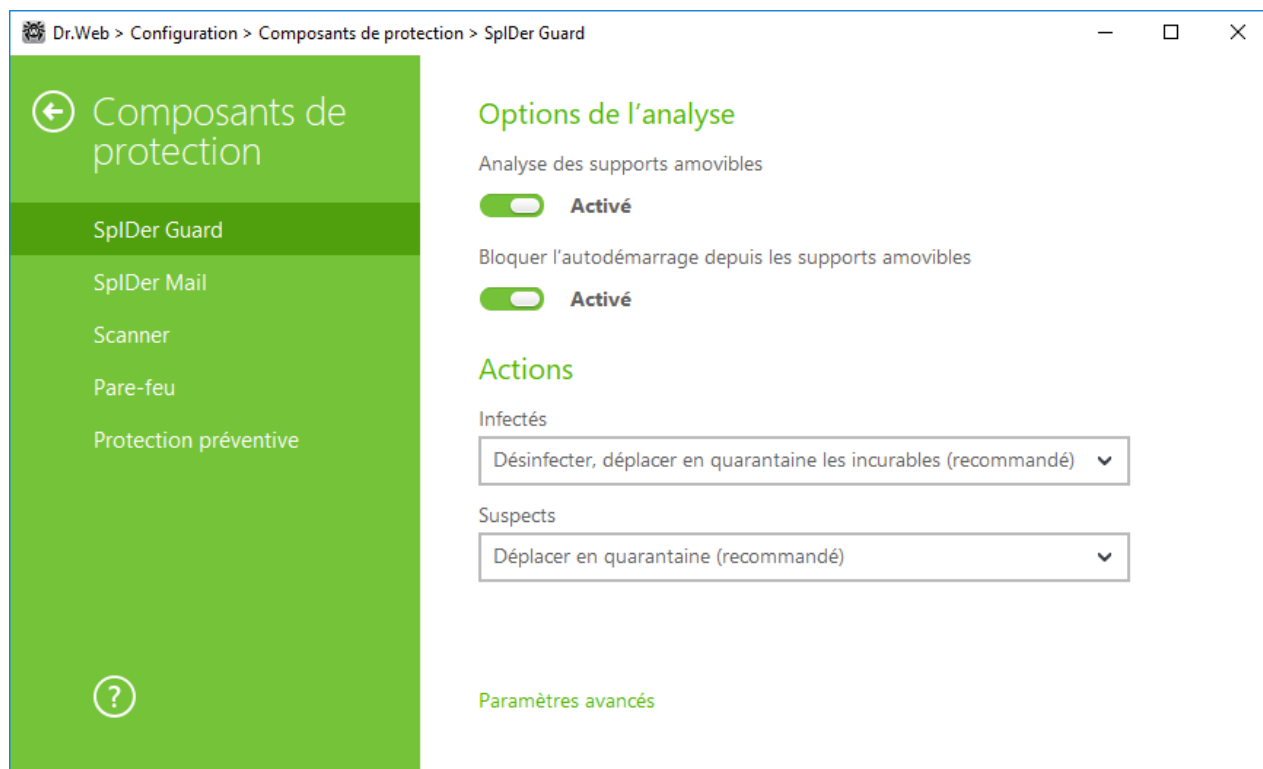


Figure 30. Configuration de SpIDer Guard

Options de l'analyse

SpIDer Guard analyse par défaut les fichiers ouverts, modifiés et lancés sur les supports amovibles (disques CD/DVD, clés USB, etc) et bloque le lancement automatique de leur contenu actif. L'utilisation de ces paramètres permet de prévenir l'infection de votre ordinateur via les supports amovibles. Si ces options sont désactivées, les objets sur les supports amovibles ne seront pas analysés.



En cas de problèmes lors de l'installation des programmes utilisant le fichier autorun.inf, il est recommandé de désactiver temporairement l'option **Bloquer l'autodémarrage depuis les supports amovibles**.

Actions

Dans cette rubrique, vous pouvez configurer les réactions de SpIDer Guard à la détection des fichiers infectés, suspects ou des programmes malveillants.

La réaction est spécifiée séparément pour chaque catégorie des objets :

- **Infectés** : objets infectés par un virus connu et (supposé) curable ;
- **Suspects** : objets suspectés d'être infectés par des virus ou de contenir un objet malveillant ;
- objets potentiellement dangereux. Pour afficher toute la liste, cliquez sur le lien **Paramètres avancés**.

Vous pouvez modifier séparément la réaction de SpIDer Guard vis-à-vis de chaque type d'objets. Les actions disponibles dépendent du type de menace.

Par défaut, SpIDer Guard essaie de désinfecter les fichiers qui sont infectés par un virus connu et considéré comme curable, tandis que les autres objets qui sont considérés comme les plus dangereux sont placés en [Quarantaine](#). Les canulars, les hacktools et les riskwares sont ignorées par défaut. Les réaction de SpIDer Guard sont similaires aux réactions correspondantes du Scanner Dr.Web.

Les actions suivantes sont disponibles pour appliquer aux objets détectés :

Action	Description
Désinfecter, déplacer en quarantaine les incurables	Indique de restaurer l'objet dans son état original avant infection. Si l'objet est incurable, ou que la tentative de désinfection a échoué, cet objet est déplacé en quarantaine. Cette action est possible uniquement pour les virus connus, sauf les Trojans et les fichiers infectés au sein des objets complexes (les archives, les fichiers de messagerie ou les conteneurs de fichiers).
Désinfecter, supprimer les incurables	Indique de restaurer l'objet dans son état original avant infection. Si l'objet est incurable, ou que la tentative de désinfection a échoué, l'action appliquée aux virus incurables est appliquée. Cette action est possible uniquement pour les virus connus, sauf les Trojans et les fichiers infectés au sein des objets complexes (les archives, les fichiers de messagerie ou les conteneurs de fichiers).
Supprimer	Supprimer l'objet.



Action	Description
	Aucune action n'est appliquée aux secteurs d'amorçage.
Déplacer en quarantaine	Déplacer l'objet dans le dossier spécial de Quarantaine . Aucune action n'est appliquée aux secteurs d'amorçage.
Ignorer	Ignorer l'objet sans lui appliquer aucune action ni afficher d'alerte. Cette action est disponible uniquement pour les programmes malveillants dont adwares, dialers, canulars, hacktools et riskwares.



SpIDer Guard n'analyse pas les objets complexes comme les archives, les boîtes e-mails ou les conteneurs de fichiers. Aucune action ne leur est appliquée.

Des copies de sauvegarde de tous les objets traités sont stockées dans la [Quarantaine](#).

Mode d'analyse

Dans cette partie, vous pouvez déterminer quels objets requièrent une analyse « à la volée » par SpIDer Guard.

Paramètre	Description
Optimal (recommandé)	Ce mode de scan est utilisé par défaut. Dans ce mode, SpIDer Guard analyse les objets dans les cas suivants : <ul style="list-style-type: none">• pour les objets sur les disques durs, lorsqu'il y a une tentative d'exécuter un fichier, de créer un nouveau fichier ou d'écrire sur un fichier existant ou sur le secteur d'amorçage ;• pour les objets sur les supports amovibles : à chaque tentative d'accéder à un fichier ou à un secteur d'amorçage (écrire, lire, exécuter).
Paranoïde	Dans ce mode, SpIDer Guard analyse les fichiers et les secteurs d'amorçage sur les disques durs ou réseau et sur les supports amovibles en cas de tentative d'y accéder (créer, écrire, lire, exécuter).



Lancé dans le mode optimal, SpIDer Guard n'interrompt pas le lancement du [fichier de test EICAR](#) et ne classe pas telle situation comme dangereuse puisque ce fichier ne représente aucun danger pour l'ordinateur. Cependant, lors de la copie ou de la création de ce fichier, SpIDer Guard le traite automatiquement comme un programme malveillant et par défaut le déplace en Quarantaine.



Détails et recommandations

Le mode **Optimal** est recommandé après une [analyse](#) de tous les disques durs effectuée par le Scanner Dr.Web. Lorsque ce mode est activé, SpIDer Guard prévient la pénétration de nouveaux virus et d'autres programmes malveillants dans votre ordinateur via les supports amovibles sans analyser de nouveaux les objets déjà scannés.

Le mode **Paranoïde** assure une protection maximum mais réduit les performances de la machine.

Dans tous les modes, SpIDer Guard analyse les objets en réseau et les supports amovibles uniquement si les options correspondantes sont activées dans le groupe de paramètres **Options de l'analyse**.



Le système d'exploitation peut reconnaître certains supports amovibles comme des disques durs (notamment les disques durs externes à l'interface USB). Veuillez utiliser ces dispositifs avec beaucoup de précautions et analysez-les avec le Scanner Dr.Web lorsqu'ils sont connectés à l'ordinateur.

SpIDer Guard ne contrôle pas les archives ni les courriers électroniques par défaut. Ceci n'affecte pas la sécurité de votre ordinateur lorsqu'il est protégé en permanence par SpIDer Guard. Si un fichier contenu dans une archive ou une pièce jointe d'e-mail est infecté, l'objet malveillant sera détecté et immédiatement neutralisé par SpIDer Guard lorsque vous tenterez d'extraire le fichier archivé ou de télécharger la pièce jointe.

Paramètres avancés

Ce groupe de paramètres vous permet de configurer les options du scan à la volée qui seront appliquées dans tous les modes de fonctionnement de SpIDer Guard. Vous pouvez activer :

- l'utilisation de l'analyseur heuristique ;
- l'analyse des programmes et modules en cours de démarrage ;
- l'analyse des fichiers d'installation ;
- l'analyse des fichiers en réseau local (non recommandé) ;
- l'analyse de l'ordinateur pour la présence des rootkits (recommandé) ;
- l'analyse des scripts exécutés par Windows Script Host et PowerShell (pour Windows 10).

Analyse heuristique

Par défaut, SpIDer Guard effectue l'analyse en utilisant l'[analyseur heuristique](#). Si l'option est désactivée, il effectue l'analyse uniquement par signatures de virus connus.



Scan Anti-rootkit en tâche de fond

Le composant Anti-rootkit intégré à Dr.Web offre des fonctions de scan en tâche de fond du système d'exploitation à la recherche de menaces complexes ainsi que des fonctionnalités de traitement des infections actives lorsque c'est nécessaire.

Si cette option est activée, Antiroutkit Dr.Web réside de manière permanente en mémoire. A la différence du scan à la volée des fichiers effectué par SpIDer Guard, le scan des rootkits (programmes malveillants utilisés pour dissimuler les modifications apportés dans l'OS telles que le fonctionnement de certains processus, la modification des clés de la base de registre, des dossiers et fichiers) inclut la vérification des objets autorun, des processus et des modules en cours, de la mémoire vive (RAM), des disques MBR/VBR, du BIOS de l'ordinateur et d'autres objets système.

Une des fonctionnalités principales de Anti-rootkit Dr.Web est sa faible consommation des ressources système ainsi que sa prise en considération des capacités hardware.

Lorsque Antiroutkit Dr.Web détecte une menace, il notifie l'utilisateur et neutralise l'activité malveillante.



Durant l'analyse en tâche de fond pour la présence de rootkits, les fichiers et dossiers indiqués dans l'[onglet correspondant](#) sont exclus du scan.

Le scan Anti-rootkit en tâche de fond est activé par défaut.



La désactivation de SpIDer Guard n'a pas d'impact sur l'analyse en tâche de fond. Si le paramètre est activé, l'analyse en tâche de fond est effectuée indépendamment du statut de SpIDer Guard.

12.2. SpIDer Mail

SpIDer Mail est un moniteur de courrier qui s'installe par défaut avec les autres composants et reste en permanence en mémoire. Il se lance au démarrage du système de manière automatique.

SpIDer Mail supporte l'analyse du trafic chiffré de messagerie.

Traitement des e-mails

Tous les messages entrants sont interceptés par SpIDer Mail avant d'être réceptionnés par les clients messagerie. Les messages sont analysés à la recherche de virus avec le niveau de détail le plus élevé possible. S'ils ne comportent aucun virus ou objet suspect, les messages sont acheminés dans la boîte de réception en mode « transparent », comme s'ils venaient immédiatement du serveur. La même procédure est appliquée aux messages sortants avant leur envoi au serveur.



Par défaut, SpIDer Mail [réagit](#) aux messages infectés aussi bien qu'aux messages qui n'ont pas été analysés (à cause de leur structure compliquée par exemple) de cette façon :

- les codes malicieux sont supprimés des messages infectés puis les messages sont délivrés. Cette action est appelée *désinfection* du message ;
- les messages comportant des objets suspects sont déplacés en [Quarantaine](#) dans des fichiers à part ; le client de messagerie reçoit alors une alerte. Cette action est appelée *déplacement* du message. Les messages supprimés ou déplacés sont également supprimés du serveur POP3 ou IMAP4 ;
- les messages qui n'ont pas été analysés et les messages sains sont transmis sans modifications (*sautés*).

Les messages sortants infectés ou suspects ne sont pas envoyés au serveur, l'utilisateur est alerté que le message ne sera pas envoyé (généralement, le client messagerie sauvegarde les messages).

Les paramètres par défaut de SpIDer Mail sont optimaux pour les utilisateurs novices, fournissant une protection maximum tout en sollicitant au minimum l'intervention de l'utilisateur. Cependant, SpIDer Mail peut bloquer par défaut certaines options des outils de messagerie (par exemple, l'envoi d'un message à plusieurs destinataires peut être considéré comme un envoi massif, ou bien les messages entrants ne sont pas analysés à la recherche de spam), de l'information utile contenue dans une partie saine d'un message infecté peut devenir inaccessible dans les cas de suppression automatique. Les utilisateurs avancés peuvent [configurer](#) l'analyse des e-mails et les réactions de SpIDer Mail aux différents événements.

Analyse des e-mails par d'autres composants

Scanner Dr.Web peut également détecter des virus dans les messageries de différents formats, mais SpIDer Mail comporte plusieurs avantages :

- tous les formats de messageries ne sont pas supportés par le Scanner Dr.Web. En utilisant SpIDer Mail, les messages infectés ne sont même pas délivrés dans la boîte de réception ;
- Scanner Dr.Web n'analyse pas les boîtes de réception au moment de la réception des e-mails, mais à la demande de l'utilisateur ou selon la planification. De plus, cette action consomme des ressources et prend beaucoup de temps.

Ainsi, parmi tous les composants de Dr.Web avec leurs paramètres par défaut, SpIDer Mail détecte les virus et les objets suspects contenus dans les e-mails en premier et les empêche de pénétrer dans votre ordinateur. L'action de SpIDer Mail est plutôt économe en ressources système ; l'analyse des e-mails peut être effectuée sans les autres composants.

12.2.1. Configurer SpIDer Mail

Pour que SpIDer Mail analyse les données transmises via les protocoles cryptographiques, activez l'option **Analyser le trafic chiffré** dans la rubrique [Réseau](#).



Pour accéder aux paramètres du pare-feu, SpIDer Mail demande le mot de passe si vous avez activé l'option **Protéger les paramètres de Dr.Web par mot de passe** dans la section [Configuration](#).

Les paramètres par défaut permettent une utilisation optimale du produit. Ne les modifiez pas si ce n'est pas nécessaire.

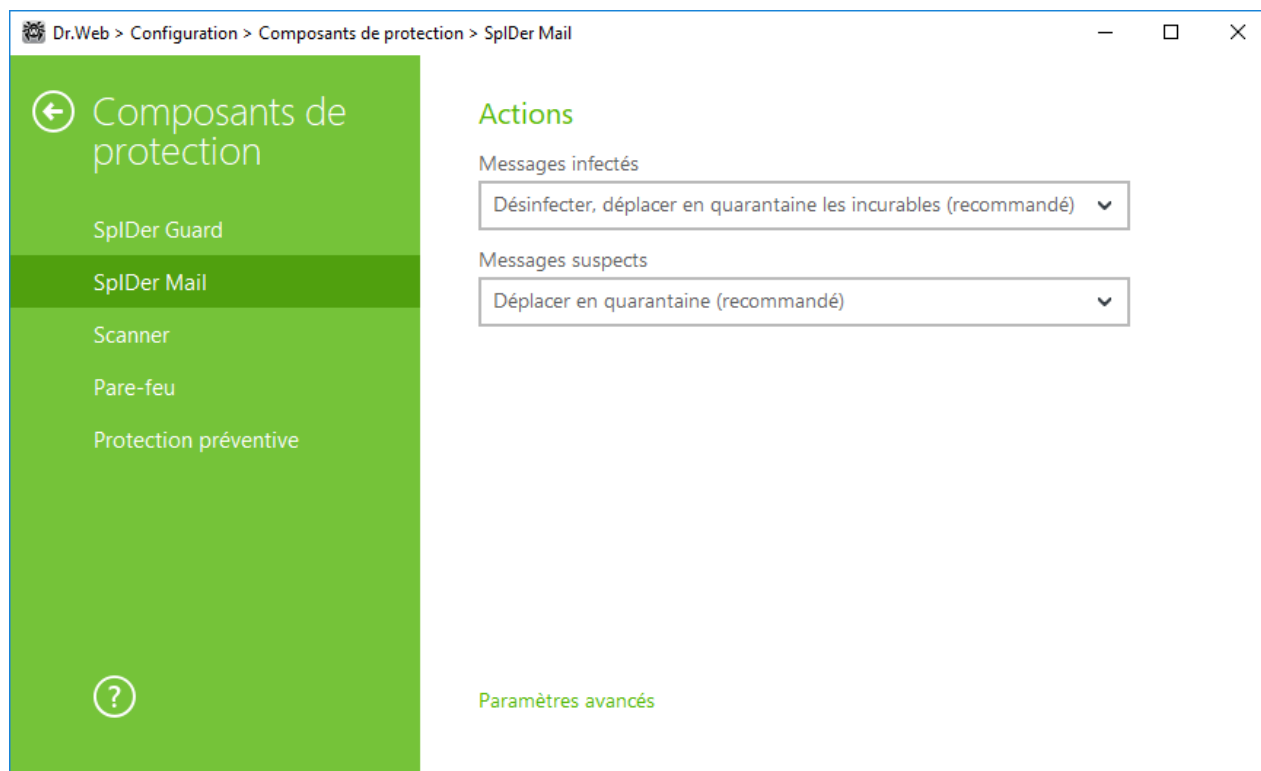


Figure 31. Configuration de SpIDer Mail

Actions

Par défaut, SpIDer Mail tente de désinfecter les messages infectés par un virus connu et (supposé) curable et déplace les messages incurables et suspects, comme les dialers et les adwares, en [Quarantaine](#) tout en ignorant les menaces mineures. D'autres messages sont délivrés par le Moniteur de courrier *sans traitement*.

Les réactions de SpIDer Mail sont similaires à celles du Scanner Dr.Web.

Vous pouvez spécifier pour SpIDer Mail une des réactions suivantes :

Action	Description
Désinfecter, déplacer en	Restaurer le message dans son état initial avant infection. Si le message est incurable, ou que la tentative de désinfection a échoué, le message est placé en quarantaine.



Action	Description
quarantaine les incurables	Disponible pour les messages infectés par des virus connus et « curables » seulement, exceptés les trojans éliminés dès leur détection. Cette action n'est pas applicable aux messages contenus dans les archives, quel que soit le type de virus.
Désinfecter, supprimer les incurables	Restaurer le message dans son état initial avant infection. Si le virus est incurable, ou que la tentative de désinfection a échoué, le message est supprimé.
Supprimer	Supprimer le message. Dans ce cas, le message n'est pas envoyé au destinataire, le client de messagerie reçoit une notification de l'opération effectuée.
Déplacer en quarantaine	Déplacer le message dans la Quarantaine . Dans ce cas, le message n'est pas envoyé au destinataire, le client de messagerie reçoit une notification sur l'opération effectuée.
Ignorer	Commande d'adresser le message à la boîte de réception comme d'habitude, c'est-à-dire sans entreprendre aucune action.

Si un e-mail contient un objet malveillant, chaque réaction, exceptée **Ignorer** a pour résultat un échec de l'envoi de l'e-mail au serveur de messagerie ou à la boîte de réception.

Pour accroître la sécurité de la protection antivirus par rapport au niveau par défaut, sélectionnez l'élément **Déplacer en quarantaine** dans la liste **Non vérifiés**. Il est recommandé d'analyser les fichiers déplacés plus tard avec le Scanner Dr.Web.



Si vous souhaitez désactiver la protection contre les e-mails suspects, assurez-vous que SpIDer Guard contrôle constamment votre ordinateur.

Actions sur les messages

Dans ce groupe, vous pouvez configurer des actions additionnelles à appliquer lorsque SpIDer Mail contrôle les messages.

Paramètre	Description
Ajouter l'en-tête 'X-Antivirus' dans les messages	Activée par défaut. Commande à SpIDer Mail d'ajouter les résultats du scan et des informations sur la version de Dr.Web à l'en-tête des messages après le scan. Vous ne pouvez pas éditer le format de l'en-tête ajouté.



Paramètre	Description
Supprimer les messages modifiés sur le serveur	Commande à SpIDer Mail de supprimer depuis le serveur de messagerie les messages supprimés ou déplacés en Quarantaine par SpIDer Mail quels que soient les paramètres de votre client messagerie.

Optimisation de l'analyse

Vous pouvez configurer SpIDer Mail pour qu'il reconnaisse les messages trop compliqués et dont le scan est trop consommateur de temps, comme non vérifiés. Pour cela, activez l'option **Délai d'attente lors de l'analyse de message** et indiquez la durée maximum de scan d'un message. Après l'expiration de ce délai, SpIDer Mail arrête de vérifier le message. La valeur 250 secondes est utilisée par défaut.

Scan des archives

Activez l'option **Analyse des archives** si vous souhaitez que SpIDer Mail analyse les fichiers archivés transférés par e-mail. Les paramètres suivants seront disponibles :

- **Taille maximum des fichiers à décompresser.** Si la taille des fichiers extraits excède cette limite, SpIDer Mail ne les décompresse ni ne les analyse. La valeur 30720 Ko est utilisée par défaut ;
- **Ratio maximum de compression de l'archive.** Si la compression dépasse la limite, SpIDer Mail ne décompresse ni n'analyse l'archive. La valeur 0 est utilisée par défaut ;
- **Niveau maximum d'imbrication de l'archive.** Si le nombre de fichiers archivés dépasse la limite, SpIDer Mail analyse les archives jusqu'à ce que cette limite soit atteinte. La valeur 64 est utilisée par défaut.

Pour activer des paramètres d'optimisation, cochez les cases correspondantes.



Il n'existe pas de restrictions pour un paramètre si la valeur est égale à 0.

Paramètres avancés

Dans ce groupe, vous pouvez spécifier les options supplémentaires d'analyse des e-mails :

- utilisation de l'analyse heuristique – dans ce mode, des [mécanismes spécialisés](#) sont utilisés de sorte qu'ils permettent de détecter, dans le courrier électronique, des objets suspects, avec une forte probabilité, contaminés par des virus inconnus. Pour désactiver l'analyse heuristique, décochez la case **Utiliser l'analyse heuristique (recommandé)** ;
- analyse de packages d'installation. Cette option est désactivée par défaut.



12.3. Scanner



Pour accéder aux paramètres du Scanner, vous êtes invité à entrer le mot de passe si vous avez activé l'option **Protéger les paramètres de Dr.Web par mot de passe** dans la fenêtre [Configuration](#).

Les paramètres par défaut permettent une utilisation optimale du produit. Ne les modifiez pas si ce n'est pas nécessaire.

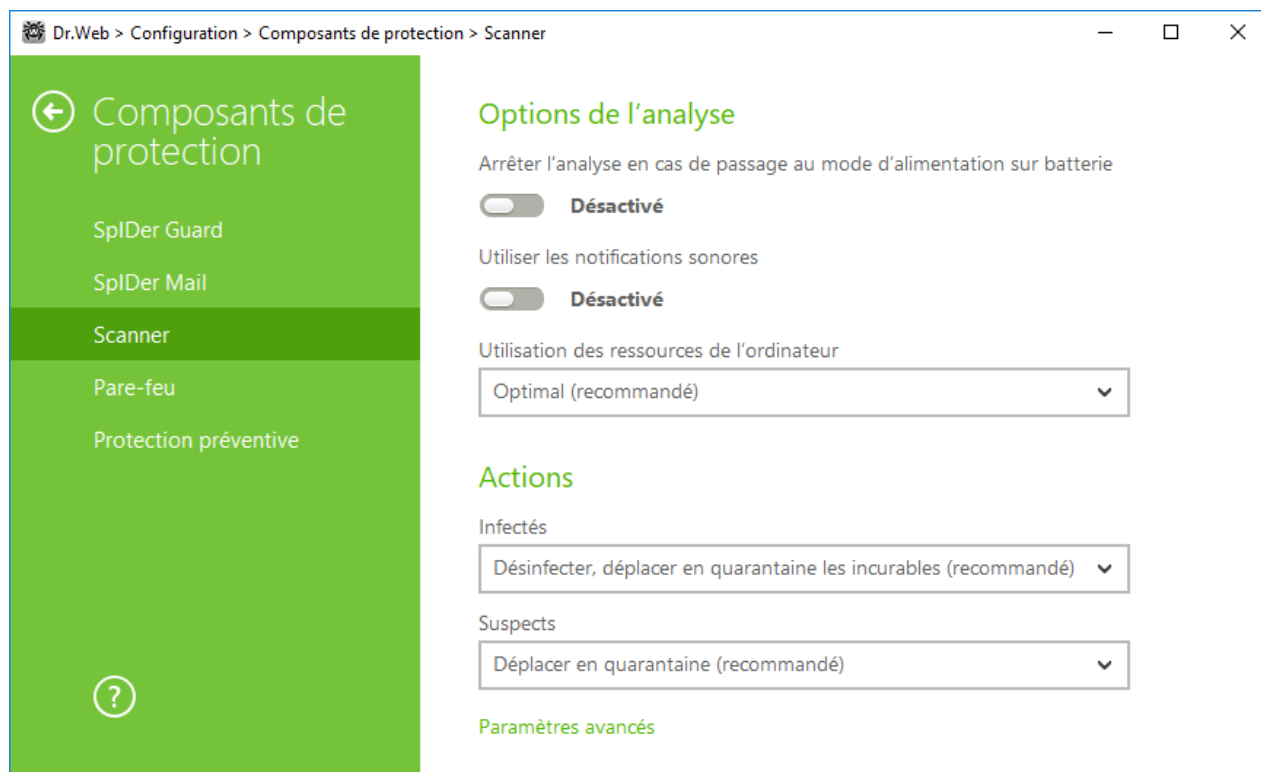


Figure 32. Configuration du Scanner

Options de l'analyse

Dans cette rubrique, vous pouvez configurer les paramètres généraux du Scanner Dr.Web :

- **Arrêter l'analyse en cas de passage au mode d'alimentation sur batterie.** Activez cette option pour arrêter l'analyse en cas de passage en mode d'alimentation sur la batterie. Cette option est désactivée par défaut.
- **Utiliser les notifications sonores.** Activez cette option pour commander au Scanner Dr.Web d'accompagner chaque événement d'un signal sonore. Cette option est désactivée par défaut.
- **Utilisation des ressources de l'ordinateur.** Cette option limite l'utilisation des ressources de l'ordinateur par le Scanner Dr.Web. La valeur optimale est utilisée par défaut.



Actions

Dans cette rubrique, vous pouvez configurer la réaction du Scanner lors de la détection d'objets infectés ou suspects et de programmes malveillants.

La réaction est spécifiée séparément pour chaque catégorie des objets :

- **Infectés** : objets infectés par un virus connu et (supposé) curable ;
- **Suspects** : objets suspectés d'être infectés par des virus ou de contenir un objet malveillant ;
- objets potentiellement dangereux.

Vous pouvez modifier séparément la réaction du Scanner vis-à-vis de chaque type d'objets. Les actions disponibles dépendent du type de menace.

Par défaut, le Scanner essaie de désinfecter les fichiers qui sont infectés par un virus connu et qui sont considérés comme curables, tandis que les autres objets qui sont considérés comme les plus dangereux sont placés en [Quarantaine](#).

Les actions suivantes sont disponibles pour appliquer aux objets détectés :

Action	Description
Désinfecter, déplacer en quarantaine les incurables	Indique de restaurer l'objet dans son état original avant infection. Si l'objet est incurable, ou que la tentative de désinfection a échoué, cet objet est déplacé en quarantaine. Cette action est possible uniquement pour les virus connus, sauf les Trojans et les fichiers infectés au sein des objets complexes (les archives, les fichiers de messagerie ou les conteneurs de fichiers).
Désinfecter, supprimer les incurables	Indique de restaurer l'objet dans son état original avant infection. Si l'objet est incurable, ou que la tentative de désinfection a échoué, l'action appliquée aux virus incurables est appliquée. Cette action est possible uniquement pour les virus connus, sauf les Trojans et les fichiers infectés au sein des objets complexes (les archives, les fichiers de messagerie ou les conteneurs de fichiers).
Supprimer	Supprimer l'objet. Aucune action n'est appliquée aux secteurs d'amorçage.
Déplacer en quarantaine	Déplacer l'objet dans le dossier spécial de Quarantaine . Aucune action n'est appliquée aux secteurs d'amorçage.
Ignorer	Ignorer l'objet sans lui appliquer aucune action ni afficher d'alerte.



Action	Description
	Cette action est disponible uniquement pour les programmes malveillants dont adwares, dialers, canulars, hacktools et riskwares.



Si un virus ou un code suspect est détecté au sein des objets complexes comme les archives, les boîtes e-mails ou les conteneurs de fichiers, les actions sur les menaces contenues dans tels objets sont appliquées à l'objet entier et non seulement à sa partie infectée.

Paramètres avancés

Vous pouvez désactiver le scan des packages d'installation, des archives et des fichiers de messagerie. Le scan de ces objets est activé par défaut.

Vous pouvez configurer le comportement du Scanner après le scan :

1. **N'appliquer aucune action.** Scanner va afficher le tableau contenant la liste des menaces détectées.
2. **Neutraliser les menaces détectées.** Scanner va appliquer automatiquement les actions aux menaces détectées.
3. **Neutraliser les menaces détectées et arrêter l'ordinateur.** Scanner va appliquer automatiquement les actions aux menaces détectées et après, l'ordinateur sera arrêté.

12.4. Pare-feu

Pare-feu Dr.Web protège votre ordinateur des accès non autorisés et prévient les fuites de données vitales via les réseaux. Il gère les tentatives de connexion et les transferts de données et vous aide à bloquer les connexions non désirées ou suspectes au niveau des applications et du réseau.

Pare-feu fournit les fonctionnalités suivantes :

- contrôle et filtrage de tout le trafic entrant et sortant ;
- contrôle d'accès au niveau des applications ;
- filtrage des paquets au niveau du réseau ;
- sélection rapide des règles ;
- journal des événements.



12.4.1. Apprentissage du Pare-feu

Après l'installation du Pare-feu, il faudra un certain temps pour apprendre le logiciel lors de votre travail sur l'ordinateur. Le mode d'apprentissage concerne les modes suivants du Pare-feu (pour en savoir plus sur les modes du Pare-feu, consultez la rubrique [Configuration du pare-feu](#)) :

- **Créer automatiquement des règles pour les applications connues** (spécifié par défaut) ;
- **Mode interactif.**

En mode **Créer automatiquement des règles pour les applications connues**, si le système ou les application tentent de se connecter au réseau, le Pare-feu vérifie si ces applications sont de confiance et si les règles de filtrage sont spécifiés. S'il n'y a pas de règles, Dr.Web affiche une alerte où vous pouvez spécifier la règle. Les règles ne sont pas spécifiées pour les application de confiance. La connexion au réseau est autorisée à ces applications.

Les applications de confiance comprennent les applications système, les applications ayant le certificat Microsoft et les applications figurant dans la liste des applications de confiance de Dr.Web.

En mode **Mode interactif**, si le système ou les applications tentent de se connecter au réseau, le Pare-feu vérifie si les règles de filtrage sont spécifiées pour ces programmes. S'il n'y en a pas, une alerte s'affiche et vous invite à créer une règle qui sera appliquée chaque fois lors du traitement des connexions pareilles.



Lors du fonctionnement sous un compte limité (Invité), Pare-feu Dr.Web n'affiche pas d'alertes à l'utilisateur sur les tentatives d'accéder au réseau. Les alertes de ce type seront affichées en mode administrateur seulement si cette session est active en même temps que la session de l'invité.

Règles pour les applications

1. En cas de détection d'une tentative de se connecter au réseau, pour prendre une décision, prenez connaissance des informations qui s'affichent lors d'une alerte :

Champ	Description
Application	Le nom de l'application concernée. Assurez-vous que le chemin vers le fichier exécutable spécifié dans le champ Chemin vers l'application correspond à sa localisation habituelle.
Chemin vers l'application	Le chemin complet vers le fichier exécutable de l'application et son nom.
Signature numérique	Signature numérique de l'application.
Adresse	Protocole et adresse de l'hôte auquel on tente de se connecter.



Champ	Description
Port	Le port utilisé lors de la tentative de connexion.
Direction	Direction de connexion.

- Après avoir pris une décision, sélectionnez l'action appropriée en bas de la fenêtre :
 - pour bloquer la connexion une fois, sélectionnez l'action **Bloquer pour une fois** ;
 - pour autoriser l'application à se connecter une seule fois, sélectionnez **Autoriser pour une fois** ;
 - pour ouvrir une fenêtre où vous pouvez créer une nouvelle règle de filtrage, sélectionnez **Créer une règle**. Dans la fenêtre ouverte, vous pouvez soit choisir une des règles prédéfinies, soit [créer une règle pour cette application](#).
- Cliquez sur **OK**. Pare-feu exécute l'action sélectionnée et ferme la fenêtre de notification.



Dans certains cas, le système d'exploitation Windows ne permet pas l'identification explicite d'un service qui est lancé comme un processus système. Lorsqu'une tentative de connexion d'un service système est détectée, notez le port utilisé pour la connexion. Si vous utilisez l'application qui peut s'adresser à ce port, autorisez la connexion.

Lorsque la connexion a été initiée par une application connue par le Pare-feu (possédant déjà des règles) mais que cette application a été lancée par un processus parent inconnu, une notification sera affichée par le Pare-feu.

Pour définir les règles de processus parents

- En cas de détection d'une tentative de se connecter au réseau depuis une application lancée par un programme inconnu pour le Pare-feu, prenez connaissance des informations sur le fichier exécutable du programme parent.
- Dès que vous avez pris une décision concernant l'opération à réaliser, sélectionnez l'une des actions suivantes :
 - pour bloquer la connexion de l'application au réseau une fois, cliquez sur **Bloquer** ;
 - pour autoriser l'application à se connecter au réseau une fois, cliquez sur **Autoriser** ;
 - pour créer une nouvelle règle de filtrage d'application, sélectionnez **Créer une règle**. Dans la fenêtre ouverte, configurez les [paramètres du processus parent](#).
- Cliquez sur **OK**. Pare-feu exécute l'action sélectionnée et ferme la fenêtre de notification.

Lorsqu'une application inconnue a été lancée par une autre application inconnue, une notification s'affiche avec les détails. Si vous cliquez sur **Créer une règle**, une nouvelle fenêtre s'ouvrira, vous permettant de créer de nouvelles règles pour cette application et ses processus parents.

12.4.2. Configuration du Pare-feu

Dans cette section, vous pouvez configurer les paramètres suivants du Pare-feu :

- sélectionnez le mode opératoire ;
- [configurer la liste](#) des applications autorisées ;
- configurer les paramètres des réseaux connus.



Pour accéder aux paramètres du pare-feu, vous êtes invité à entrer le mot de passe si vous avez activé l'option **Protéger les paramètres de Dr.Web par mot de passe** dans la section [Configuration](#).

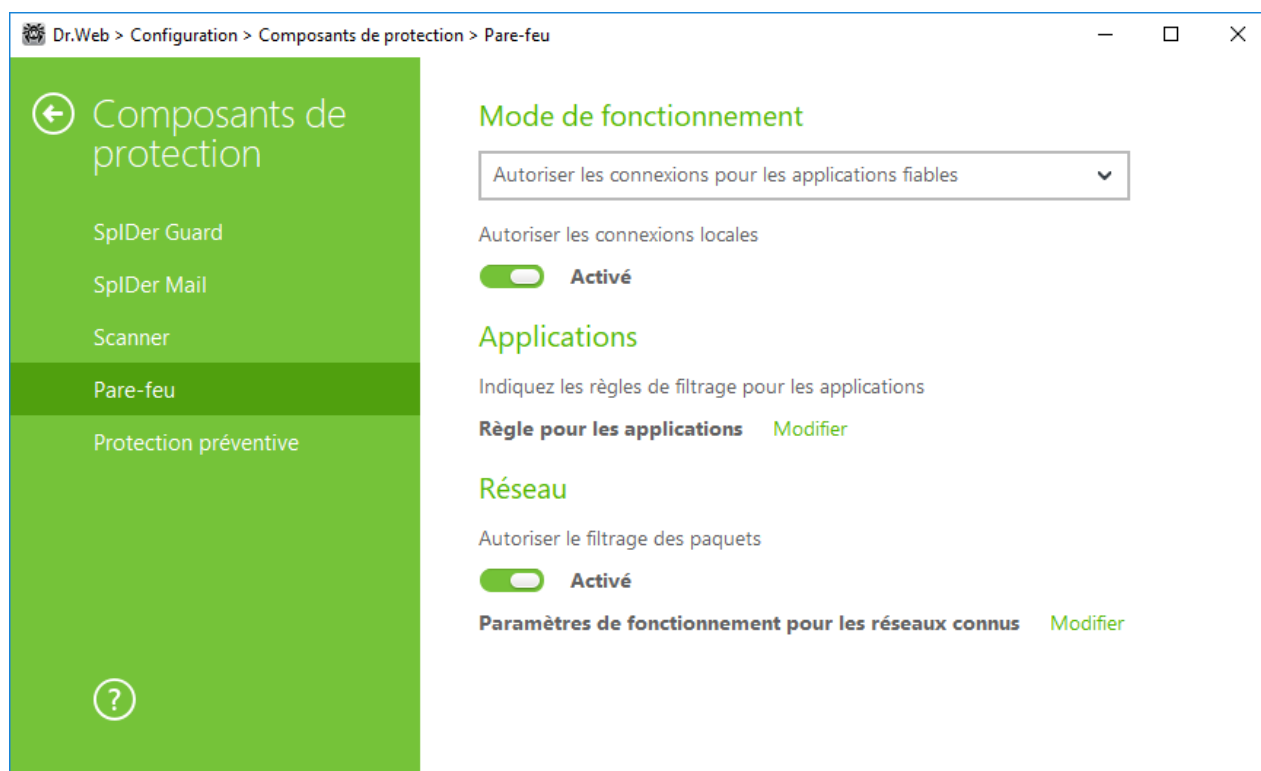


Figure 33. Paramètres principaux du Pare-feu

Par défaut, Pare-feu ne crée pas de règles pour les applications connues. Quel que soit le mode opératoire, les événements sont journalisés.

Les paramètres par défaut permettent une utilisation optimale du produit. Ne les modifiez pas si ce n'est pas nécessaire.

Le paramètre **Autoriser les connexions locales** permet à toutes les applications d'établir des connexions locales sur votre ordinateur (depuis l'interface ou à l'interface 127.0.0.1 (localhost)). Cette option s'applique après la vérification de conformité des connexions aux règles spécifiées. Désactivez cette option pour appliquer des règles de filtrage indépendamment du fait que la connexion se fait via le réseau ou au sein de votre ordinateur.



Sélection du mode opératoire

Sélectionnez un des modes suivants :

- **Créer automatiquement des règles pour les applications connues** : mode dans lequel toutes les applications de confiance sont autorisées à accéder aux ressources réseau (utilisé par défaut). Pour les autres applications, un avertissement s'affiche où vous pouvez spécifier une règle (voir la rubrique [Apprentissage du Pare-feu](#)) ;
- **Autoriser les connexions inconnues** : mode d'accès libre, lorsque toutes les applications inconnues sont autorisées à accéder au réseau ;
- **Mode interactif** : [mode d'apprentissage](#) dans lequel l'utilisateur possède un contrôle total sur les réactions du Pare-feu ;
- **Bloquer les connexions inconnues** : mode d'accès restreint, lorsque toutes les connexions inconnues sont bloquées. Pour les connexions connues, le Pare-feu applique les règles appropriées.

Autoriser les connexions pour les applications de confiances

Ce mode est utilisé par défaut.

Dans ce mode, toutes les applications de confiance sont autorisées à accéder aux ressources réseau, y compris Internet. Les applications de confiance comprennent les applications système, les applications ayant le certificat Microsoft et les applications figurant dans la liste des applications de confiance de Dr.Web. Les règles pour ces applications ne sont pas affichées dans la liste de règles. Pour d'autres applications, Pare-feu offre une possibilité de bloquer ou d'autoriser une connexion inconnue ainsi que de créer une règle pour cette connexion.

Lorsqu'une application lancée par l'utilisateur ou que le système d'exploitation tentent de se connecter au réseau, Pare-feu vérifie s'il existe un ensemble de règles de filtrage pour l'application. S'il n'y en a pas, un avertissement est affiché et vous invite à choisir une solution temporaire ou à créer une règle qui sera appliquée à chaque fois lors du traitement des connexions pareilles.

Autoriser les connexions inconnues

Dans ce mode, l'accès aux ressources réseau, y compris Internet, est fourni à toutes les applications inconnues pour lesquelles les règles de filtrage ne sont pas spécifiées. Aucune notification sur les tentatives d'accès ne sont affichées par Pare-feu.

Mode interactif

Dans ce mode, vous avez un contrôle total sur les réactions du Pare-feu lors de la détection de connexions inconnues, ce qui forme le programme pendant que vous travaillez sur votre ordinateur.

Lorsqu'une application lancée par l'utilisateur ou que le système d'exploitation tentent de se connecter au réseau, Pare-feu vérifie s'il existe un ensemble de règles de filtrage pour l'application.



S'il n'y en a pas, un avertissement est affiché et vous invite à choisir une solution temporaire ou à créer une règle qui sera appliquée à chaque fois lors du traitement des connexions pareilles.

Bloquer les connexions inconnues

Dans ce mode, toutes les connexions inconnues aux ressources réseau y compris la connexion à Internet sont bloquées de manière automatique.

Lorsqu'une application lancée par l'utilisateur ou le système d'exploitation tente de se connecter au réseau, Pare-feu vérifie s'il existe des règles de filtrage pour ces programmes. S'il n'y en a pas, Pare-feu bloque automatiquement l'accès au réseau sans afficher aucune notification. S'il y a des règles de filtrage spécifiées pour la connexion en question, les actions déterminées seront effectuées.

Page Applications



Vous ne pouvez pas créer plus d'un ensemble de règles par application.

Le filtrage au niveau des applications vous aide à contrôler l'accès de diverses applications et processus aux ressources réseaux, et vous permet d'interdire ou d'autoriser aux applications de lancer d'autres processus. Vous pouvez créer des règles pour les applications système et utilisateur.

Dans cette rubrique, vous pouvez établir des [ensembles de règles de filtrage](#). Pour cela, vous pouvez créer de nouvelles règles, éditer les règles existantes ou supprimer les règles dont vous n'avez plus besoin. Chaque application est explicitement identifiée par le chemin vers son fichier exécutable. Le Pare-feu utilise le nom `SYSTEM` pour indiquer le noyau du système d'exploitation (le processus system pour lequel il n'y a pas de fichier exécutable correspondant).





Si vous avez créé une règle bloquant pour un processus ou que vous avez installé le mode Bloquer les connexions inconnues, et après, vous avez désactivé la règle bloquant ou modifié le mode de fonctionnement, le blocage reste activé jusqu'à la deuxième tentative d'établir une connexion après le redémarrage du processus.

Les règles pour les applications supprimées de votre ordinateur ne sont pas supprimées automatiquement. Pour supprimer de telles règles, sélectionnez l'élément **Suppression de règles non utilisées** dans le menu contextuel de la liste.

Règles pour les applications

Dans la fenêtre **Création d'un nouvel ensemble de règles pour l'application** (ou **Edition de l'ensemble de règles pour**), vous pouvez configurer l'accès de l'application aux ressources réseau ainsi qu'interdire ou autoriser le lancement d'autres applications.



Pour accéder à cette fenêtre, cliquez sur le bouton **Modifier** de l'élément **Règles pour les applications** dans les [paramètres](#) du Pare-feu, ensuite cliquez sur  dans la fenêtre qui s'affiche ou sélectionnez une application et cliquez sur .

Lors de fonctionnement du Pare-feu en [mode d'apprentissage](#), vous pouvez créer une règle depuis la fenêtre de notification de tentative de connexion non autorisée.

Lancer d'autres applications

Pour interdire ou autoriser à une application de lancer d'autres application, dans la liste déroulante **Lancement des application réseau**, sélectionnez :

- **Autoriser**, pour autoriser l'application à lancer des processus ;
- **Bloquer**, pour interdire à l'application de lancer des processus ;
- **Non spécifié**. Dans ce cas, l'application va fonctionner avec les paramètres spécifiés correspondant au [mode de fonctionnement](#) du Pare-feu.

Accès aux ressources réseau

1. Spécifiez le type d'accès aux ressources réseau :

- **Autoriser tout** : toutes les connexions seront autorisées ;
- **Bloquer tout** : toutes les connexions seront bloquées ;
- **Non spécifié**. Dans ce cas, l'application va fonctionner avec les paramètres spécifiés correspondant au [mode de fonctionnement](#) du Pare-feu.
- **Défini par l'utilisateur** : dans ce mode, vous pouvez créer un ensemble de règles qui autorisera ou bloquera différentes connexions.

2. Si vous avez sélectionné le mode **Défini par l'utilisateur** de l'accès aux ressources réseau, un tableau contenant les informations sur l'ensemble de règles pour l'application correspondante sera affiché ci-dessous.

Paramètre	Description
Activé	État de l'exécution de la règle.
Action	L'action que le Pare-feu doit accomplir lorsque une tentative de connexion à Internet est détectée : <ul style="list-style-type: none">• Bloquer les paquets : bloquer la tentative de connexion ;• Autoriser les paquets : autoriser la connexion.
Nom de règle	Nom de la règle.
Type de connexion	Direction de la connexion :



Paramètre	Description
	<ul style="list-style-type: none">• Entrant : la règle s'applique lorsque quelqu'un tente de se connecter à l'application sur votre machine, depuis le réseau ;• Sortant : la règle s'applique lorsqu'une application sur votre machine tente de se connecter au réseau ;• Toute : la règle s'applique sans tenir compte de la direction de la connexion.
Description	Description de la règle.

3. Si nécessaire, éditez l'ensemble de règle pré-installé ou créez un nouvel ensemble de règles pour l'application.
4. Si vous avez choisi de créer ou d'éditer une règle, [configurez les paramètres de la règle](#) dans la fenêtre ouverte.
5. Après avoir édité l'ensemble de règles, cliquez sur **OK** pour enregistrer les modifications apportées ou sur **Annuler** pour annuler les modifications. Les modifications apportées dans l'ensemble de règles sont conservées en cas de passage en autre mode.

Cochez la case **Demander confirmation en cas de changement d'objet (recommandé)** si vous voulez que l'application demande l'accès aux ressources réseau en cas de modification ou mise à jour des applications.

Configuration des paramètres de règles

Les règles de filtrage des applications contrôlent l'interaction entre une application en particulier et un certain hôte réseau.

Création et édition de la règle

Pour ajouter une nouvelle règle, cliquez sur le bouton dans la fenêtre **Edition de l'ensemble de règles pour**. Pour éditer une règle existante, sélectionnez la règle nécessaire et cliquez sur . Dans ce cas, le mode **Défini par l'utilisateur** doit être sélectionné dans l'élément **Accès aux ressources réseau**.

Configurez les paramètres suivants :

Paramètre	Description
Général	
Nom de règle	Le nom de la règle en cours de création/édition.
Description	La description abrégée de la règle.



Paramètre	Description
Action	L'action que le Pare-feu doit accomplir lorsque une tentative de connexion à Internet est détectée : <ul style="list-style-type: none">• Bloquer les paquets : bloquer la tentative de connexion ;• Autoriser les paquets : autoriser la connexion.
Statut	État de la règle : <ul style="list-style-type: none">• Activé : la règle est appliquée ;• Désactivé : la règle n'est pas appliquée temporairement.
Type de connexion	Direction de la connexion : <ul style="list-style-type: none">• Entrant : la règle s'applique lorsque quelqu'un tente de se connecter à l'application sur votre machine, depuis le réseau ;• Sortant : la règle s'applique lorsqu'une application sur votre machine tente de se connecter au réseau ;• Toute : la règle s'applique sans tenir compte de la direction de la connexion.
Journalisation	Mode de journalisation : <ul style="list-style-type: none">• Activé : enregistrer les événements ;• Désactivé : aucune information sur la règle n'est enregistrée.
Configuration de la règle	
Protocole	Les protocoles réseaux et transport utilisés lors de la tentative de connexion. Les protocoles réseaux suivants sont supportés : <ul style="list-style-type: none">• IPv4 ;• IPv6 ;• IP all : toute version de protocole IP. Les protocoles de transport suivants sont supportés : <ul style="list-style-type: none">• TCP ;• UDP ;• TCP & UDP – protocole TCP et UDP ;• RAW.



Paramètre	Description
Adresse locale/Adresse distante	<p>L'adresse IP du hôte distant pour la connexion. Vous pouvez spécifier soit une adresse spécifique (Égal), soit plusieurs adresses IP en utilisant une plage (Dans la plage), vous pouvez également utiliser le masque du sous-réseau (Masque) ou les masques de tous les sous-réseaux dans lesquels votre ordinateur à l'adresse réseau (MY_NETWORK).</p> <p>Pour appliquer la règle à tous les hôtes distants, sélectionnez Toute.</p>
Port local/Port distant	<p>Le port utilisé pour la connexion. Vous pouvez spécifier soit un port spécifique (Égal) ou une plage de port (Dans la plage).</p> <p>Pour appliquer la règle à tous les ports, cliquez sur Toute.</p>

Paramètres des réseaux

Le filtrage des paquets vous permet de contrôler l'accès au réseau quel que soit le programme qui initie la connexion. Pare-feu applique ces règles aux paquets réseaux d'un certain type transmis via les interfaces réseaux de votre ordinateur.

Ce type de filtrage vous fournit des mécanismes généraux de contrôle à la différence du [filtrage au niveau des applications](#).

Filtre de paquets

Dans la fenêtre Réseau, vous pouvez configurer un ensemble de règles de filtrage des paquets transmis via une interface particulière.


Pour accéder à cette fenêtre, cliquez sur **Modifier** dans l'élément **Paramètres de fonctionnement pour les réseaux connus** de la fenêtre de paramètres du Pare-feu. Sélectionnez dans la liste l'interface de votre choix et l'ensemble de règles correspondant. Si l'ensemble de règles nécessaire n'est pas présent dans la liste, vous pouvez le créer.


Le Pare-feu est fourni avec les ensembles de règles suivants :

- **Default Rule** : cet ensemble inclut des règles décrivant les configurations systèmes les plus fréquentes et prévenant contre les attaques réseaux communes. Cet ensemble de règles est utilisé par défaut pour les nouvelles [interfaces réseaux](#) ;
- **Allow All** : laisser passer tous les paquets ;
- **Block All** : bloquer tous les paquets.

Pour passer rapidement d'un mode de filtrage à un autre, vous pouvez [créer des ensembles de règles de filtrage](#).



Pour afficher toutes les interfaces disponibles ou ajouter une nouvelle interface dans le tableau, cliquez sur le bouton . Dans la fenêtre qui apparaît, vous pouvez spécifier les interfaces à afficher dans le tableau. Les interfaces actives seront affichées automatiquement dans le tableau.

Vous pouvez supprimer les interfaces réseau inactives du tableau affiché en cliquant sur .

Configuration du filtre de paquets





Pour gérer les ensembles de règles existants et ajouter de nouveaux ensembles, ouvrez la fenêtre **Configuration du filtre de paquets** en cliquant sur **Ensembles de règles**.

Sur cette page, vous pouvez :

- [configurer](#) des ensembles de règles de filtrage en ajoutant de nouvelles règles, en modifiant ou en supprimant des règles existantes ;
- [configurer](#) les paramètres avancés du filtrage.

Création d'un ensemble de règles

Pour créer un ensemble de règles, effectuez l'une des actions suivantes :

- pour créer un ensemble de règles d'une interface réseau, cliquez sur  ;
- pour éditer un ensemble de règles, sélectionnez-le dans la liste et cliquez sur  ;
- pour ajouter une copie de l'ensemble de règles existant, cliquez sur . La copie sera ajoutée au-dessous de l'ensemble sélectionné ;
- pour supprimer un ensemble de règles, sélectionnez-le et cliquez sur .

Paramètres avancés

Pour spécifier les paramètres avancés du filtrage de paquets, dans la fenêtre **Configuration du filtre de paquets**, activez les cases suivantes :

Option	Description
Activer le filtrage dynamique des paquets	<p>Cochez cette case pour filtrer les paquets selon l'état des connexions TCP existantes. Le Pare-feu bloquera les paquets qui ne correspondent pas aux connexions actives selon les spécifications des protocoles TCP. Cette option protège votre ordinateur contre les attaques DoS (par déni de service), scan des ressources, vol de données et autres opérations malveillantes.</p> <p>Il est également recommandé d'activer le filtrage dynamique des paquets si vous utilisez des protocoles de transfert de données complexes tels que FTP, SIP, etc.</p>






Option	Description
	Décochez cette case pour filtrer les paquets sans tenir compte des sessions TCP.
Traitement des paquets IP fragmentés	Cochez cette case pour garantir le traitement correct de larges volumes de données. La taille de MTU (Maximum Transmission Unit) peut varier en fonction des différents réseaux, ainsi les paquets IP importants peuvent arriver fragmentés. Lorsque cette option est activée, le Pare-feu applique la règle sélectionnée pour le premier fragment du paquet IP important à tous les autres fragments. Décochez cette case pour traiter tous les paquets indépendamment.

Cliquez sur **OK** pour sauvegarder les modifications apportées ou **Annuler** pour quitter sans enregistrer les modifications apportées.

La fenêtre **Pour configurer l'ensemble de règles** donne la liste des règles de filtrage de paquets pour l'ensemble sélectionné. Vous pouvez configurer la liste en ajoutant de nouvelles règles pour une application ou modifier les règles existantes et l'ordre de leur exécution. Les règles sont appliquées selon leur ordre dans la liste.





Pour chaque règle dans un ensemble, les informations suivantes s'affichent :

Paramètre	Description
Activé	État de l'exécution de la règle.
Action	L'action du Pare-feu lorsqu'un paquet est intercepté : <ul style="list-style-type: none">• Bloquer les paquets : bloquer le paquet ;• Autoriser les paquets : transmettre le paquet.
Nom de règle	Le nom de la règle.
Direction	Direction de la connexion : <ul style="list-style-type: none">•  : la règle s'applique lorsque le paquet provient du réseau ;•  : la règle s'applique lorsque le paquet est envoyé dans le réseau depuis votre machine ;•  : la règle s'applique sans tenir compte de la direction de la connexion.
Journalisation	Mode de journalisation des événements. Il spécifie des informations à enregistrer dans le journal : <ul style="list-style-type: none">• En-têtes seulement : enregistrer uniquement les en-têtes de paquets ;• Paquet entier : enregistrer les paquets entiers ;



Paramètre	Description
	<ul style="list-style-type: none">• Désactivé : aucune information n'est enregistrée.
Description	La description abrégée de la règle.



Édition ou création de l'ensemble de règles

1. Si nécessaire, spécifiez le nom ou changez le nom de l'ensemble de règles.
2. Utilisez les options suivantes pour créer des règles de filtrage :
 - pour ajouter une nouvelle règle, cliquez sur . La nouvelle règle est ajoutée au début de la liste ;
 - pour modifier la règle sélectionnée, cliquez sur  ;
 - pour ajouter une copie de la règle sélectionnée, cliquez sur . La copie est ajoutée devant la règle sélectionnée ;
 - pour supprimer la règle sélectionnée, cliquez sur .
3. Si vous avez choisi de créer une nouvelle règle ou d'éditer une règle existante, [configurez ses paramètres](#).
4. Utilisez la flèche près de la liste pour changer l'ordre des règles. Les règles sont appliquées en fonction de l'ordre dans lequel elles apparaissent dans l'ensemble.
5. A la fin de l'édition, cliquez sur le bouton **OK** pour sauvegarder les modifications apportées ou sur le bouton **Annuler** pour refuser les modifications.



Les paquets pour lesquels il n'y a pas de règles dans l'ensemble de règles sont automatiquement bloqués, sauf les paquets autorisés dans les règles du [Filtre d'applications](#).

Pour ajouter ou éditer une règle de filtrage

1. Dans la fenêtre de modification de l'ensemble de règles du filtre de paquets, cliquez sur  ou . Une fenêtre de création ou de modification de règle va s'ouvrir.
2. Configurez les paramètres suivants :

Paramètre	Description
Nom de règle	Le nom de la règle en cours de création/édition.
Description	La description abrégée de la règle.
Action	L'action du Pare-feu lorsqu'un paquet est intercepté : <ul style="list-style-type: none">• Bloquer les paquets : bloquer le paquet ;



Paramètre	Description
	<ul style="list-style-type: none">• Autoriser les paquets : transmettre le paquet.
Direction	Direction de la connexion : <ul style="list-style-type: none">• Entrant : la règle s'applique lorsque le paquet provient du réseau ;• Sortant : la règle s'applique lorsque le paquet est envoyé dans le réseau depuis votre machine ;• Toute : la règle s'applique sans tenir compte de la direction de la connexion.
Journalisation	Mode de journalisation des événements. Il spécifie des informations à enregistrer dans le journal : <ul style="list-style-type: none">• Paquet entier : enregistrer les paquets entiers ;• En-têtes seulement : enregistrer uniquement les en-têtes de paquets ;• Désactivé : aucune information n'est enregistrée.

3. Si nécessaire, ajoutez un critère de filtrage, par exemple le protocole de transport ou le protocole réseau en cliquant sur **Ajouter un critère**. La fenêtre Ajouter un critère de filtrage va s'ouvrir :

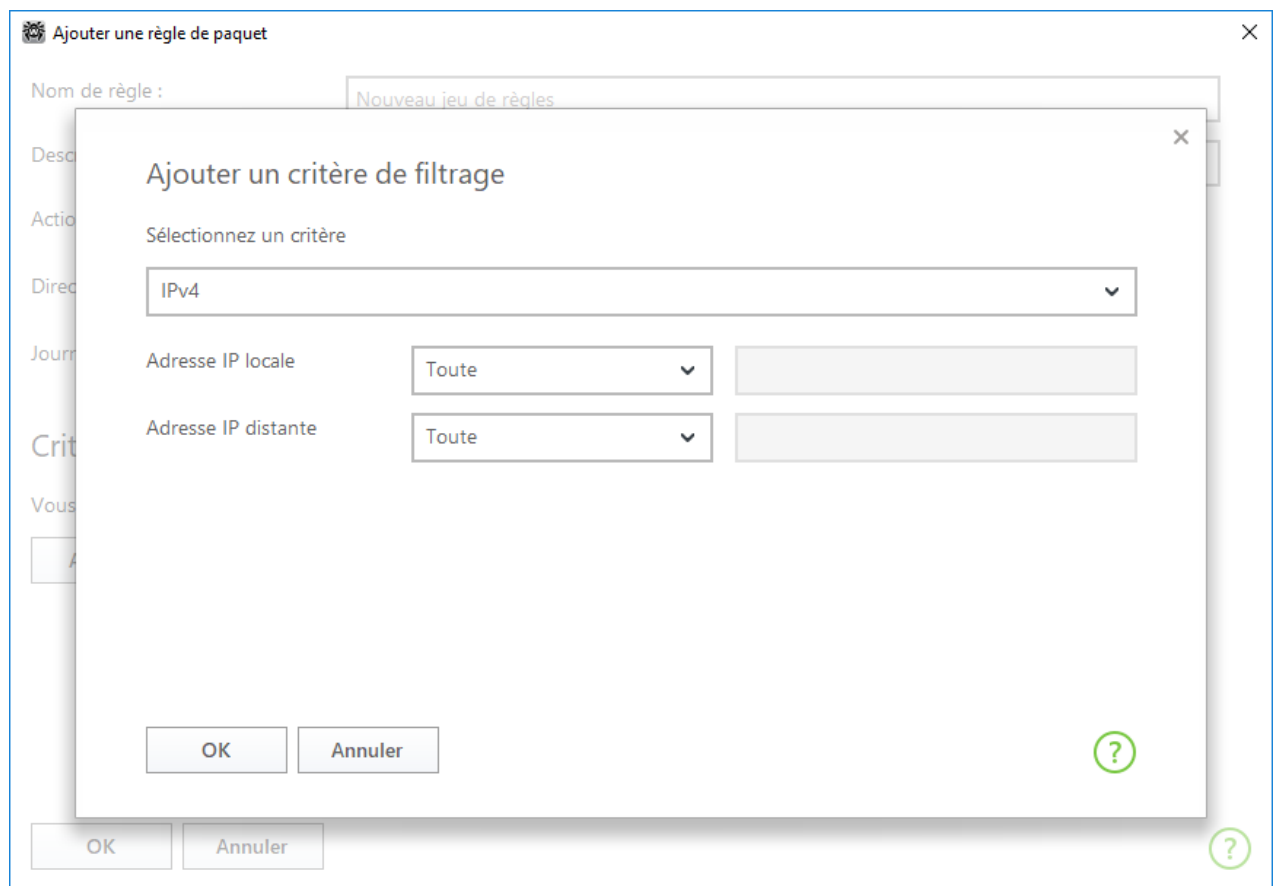


Figure 34. Ajout d'un critère de filtrage

Sélectionnez le critère nécessaire dans la liste déroulante. Dans cette fenêtre, vous pouvez configurer les paramètres pour le critère sélectionné. Vous pouvez ajouter autant de critères que



vous le souhaitez. Pour que l'action de la règle soit appliquée au paquet, il faut que le paquet réponde à tous les critères de la règle.

Des critères complémentaires sont disponibles pour certains en-têtes. Tous les critères ajoutés sont affichés dans la fenêtre d'édition de la règle de paquet et ils sont disponibles pour l'édition.

4. Cliquez ensuite sur **OK** pour enregistrer les modifications ou sur **Annuler** pour les annuler.



Si vous n'ajoutez aucun critère de filtrage, alors cette règle autorisera ou bloquera tous les paquets (en fonction du champ **Action**).

Si dans cette règle, dans l'en-tête IPv4, vous sélectionnez la valeur **Toute** pour les paramètres **Adresse IP locale** et **Adresse IP distante**, la règle sera appliquée à tout paquet contenant l'en-tête IPv4 et envoyé depuis l'adresse physique d'un ordinateur local.

12.5. Dr.Web pour Outlook

Les fonctions clés du composant

Le plug-in Dr.Web pour Outlook exécute les fonctions suivantes :

- analyse antivirus des fichiers contenus dans les pièces jointes des messages entrants ;
- analyse du courrier entrant via connexion sécurisée SSL ;
- détection et neutralisation des programmes malveillants ;
- utilisation du moteur heuristique afin de renforcer la protection contre les virus inconnus.

Configuration du module Dr.Web pour Outlook

Vous pouvez configurer les paramètres et consulter les statistiques du programme dans le client de messagerie Microsoft Outlook. Pour cela, allez dans la rubrique **Outils** → **Options** → onglet **Antivirus Dr.Web** (dans Microsoft Outlook 2010 — rubrique **Fichiers** → **Options** → **Compléments** puis sélectionnez le module Dr.Web pour Outlook et cliquez sur **Options du complément**).



L'onglet **Antivirus Dr.Web** dans les paramètres de Microsoft Outlook n'est disponible que si l'utilisateur dispose des droits permettant de modifier les paramètres.

L'onglet **Antivirus Dr.Web** affiche le statut actuel de la protection (active/inactive) et permet d'accéder aux fonctions suivantes :

- [Journal](#) permet de configurer l'écriture des événements dans le fichier de journal ;
- [Contrôle des pièces jointes](#) permet de configurer le contrôle du courrier électronique et de spécifier des réactions en cas de détection d'objets malveillants ;



- [Statistiques](#) affiche des informations sur les objets analysés et traités par l'application.

12.5.1. Analyse antivirus

Dr.Web pour Outlook utilise les diverses [méthodes de détection des virus](#). L'utilisateur peut spécifier les réactions à appliquer aux objets malveillants détectés : le programme peut réparer les objets infectés, ainsi que les supprimer ou les déplacer vers la [Quarantaine](#) pour les isoler et les conserver de manière sécurisée.

L'application Dr.Web pour Outlook détecte les objets malveillants suivants :

- objets infectés ;
- bombes de décompression ou bombes d'archive ;
- adwares ;
- hacktools ;
- dialers ;
- canulars ;
- riskwares ;
- spywares ;
- chevaux de Troie ;
- vers et virus.

Actions

Dr.Web pour Outlook peut être configuré pour réagir en cas de détection de fichiers infectés ou suspects et de programmes malveillants lors de l'analyse des pièces jointes du courrier électronique.

Pour configurer la vérification de la présence de virus dans les pièces jointes d'e-mail, dans l'application Microsoft Outlook, allez à **Outils** → **Options** → onglet **Antivirus Dr.Web** (dans Microsoft Outlook 2010, dans la section **Fichiers** → **Options** → **Compléments** choisissez Dr.Web pour Outlook et cliquez sur le bouton **Options du complément**) et cliquez sur **Analyse de pièces jointes**.



La fenêtre **Analyse de pièces jointes** est disponible à condition que l'utilisateur dispose des droits administrateur.

Sous l'OS Windows Vista ou supérieur, si vous cliquez sur le bouton **Analyse de pièces jointes** :

- Lorsque UAC est activé : l'administrateur sera invité à confirmer l'action de l'application, l'utilisateur qui ne dispose pas des droits 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 face à différentes 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 face aux objets malveillants détectés :

- la liste déroulante **Infectés** définit la réaction en cas de détection d'objets infectés par des virus connus et probablement curables ;
- la liste déroulante **Non désinfectés** définit la réaction en cas de détection d'objets infectés par un virus connu et incurable ainsi qu'en cas d'échec de la tentative de désinfection ;
- la liste déroulante **Suspects** définit la réaction face aux objets probablement infectés par un virus (réaction du moteur heuristique) ;
- la section **Programmes malveillants** définit la réaction en cas de détection des programmes malveillants suivants :
 - adwares ;
 - dialers ;
 - canulars ;
 - hacktools ;
 - riskware ;
- la liste déroulante **En cas d'échec de l'analyse** 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 **Analyse des archives** permet d'activer ou de désactiver l'analyse des fichiers archivés en pièce jointe. Cochez cette case pour activer l'analyse, décochez-la pour la désactiver.

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 (cette action est disponible uniquement pour les objets infectés) ;
- **Comme incurables** : la réaction sélectionnée pour les objets incurables sera appliquée à l'objet infecté (cette action est disponible uniquement pour les objets infectés) ;
- **Supprimer** : supprimer l'objet du système ;
- **Déplacer vers la quarantaine** : isoler l'objet dans le dossier de [Quarantaine](#) ;
- **Laisser passer** : laisser passer l'objet sans modifications.



12.5.2. Journal des événements

Dr.Web pour Outlook enregistre les erreurs survenues et les événements dans les journaux suivants :

- [journal d'événements système](#) (Event Log) ;
- [journal texte de débogage](#).

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 : 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) ;
- paramètres des modules : 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 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 ;
- notifications 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 du système d'exploitation**.
2. Sélectionnez la section **Outils d'administration** → **Observateur d'événements**.
3. Dans la partie gauche de la fenêtre **Observateur d'événements**, sélectionnez l'élément **Application**. La liste des événements enregistrés dans le journal par des applications utilisateur va s'afficher. La source des messages pour Dr.Web pour Outlook est l'application Dr.Web pour Outlook.

Journal texte de débogage

Le journal texte de débogage collecte les informations listées ci-dessous :

- messages sur la 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 : scanner, moteur, bases virales ;
- messages sur les arrêts urgents du moteur ;
- notifications sur l'expiration de la licence (ces informations sont écrites 30, 15, 7, 3, 2 ou 1 jour(s) avant la date d'expiration).

Configuration de la journalisation des événements

1. La fenêtre de paramètres du journal s'ouvre. Dans l'onglet **Antivirus Dr.Web**, cliquez sur le bouton **Journal**.
2. Pour obtenir le niveau maximum de détails du fichier de journal, cochez la case **Ecrire le journal détaillé**. Par défaut, la journalisation est paramétrée sur le mode régulier.



Obtenir le niveau maximum de détails des journaux influe sur les performances du serveur ; ainsi, il est recommandé d'activer le niveau maximum de détail uniquement en cas d'erreur de Dr.Web pour Outlook.

3. 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 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

Pour afficher le journal texte des événements, cliquez sur le bouton **Afficher dans le dossier**. Le dossier dans lequel est sauvegardé le journal sera ouvert.

12.5.3. Statistiques

Dans l'application Microsoft Outlook, la section **Outils** → **Options** → l'onglet **Antivirus Dr.Web** (en cas de Microsoft Outlook 2010, allez dans la section **Fichier** → **Options** → **Add-ins**, sélectionnez le module **Dr.Web pour Outlook** et cliquez sur **Options**) offre des informations statistiques sur le total d'objets analysés et traités par l'application.

Les objets sont divisés selon les 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 malveillant.

Les informations suivantes seront également affichées :

- **Déplacé** : le total des objets déplacés vers la Quarantaine ;
- **Supprimé** : le total des objets supprimés du système ;
- **Sautés** : le total des objets sautés 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 dossier %USERPROFILE%\Doctor Web.



Les informations statistiques sont accumulées au sein d'une session. Après le redémarrage de l'ordinateur ou lors du nouveau lancement de Antivirus Dr.Web pour Windows, les statistiques sont remises à zéro.

12.6. Protection préventive

Dans cette rubrique, vous pouvez configurer les réactions de Dr.Web à des actions d'autres applications qui pourraient compromettre la sécurité de votre ordinateur et choisir le niveau de la protection contre les exploits.

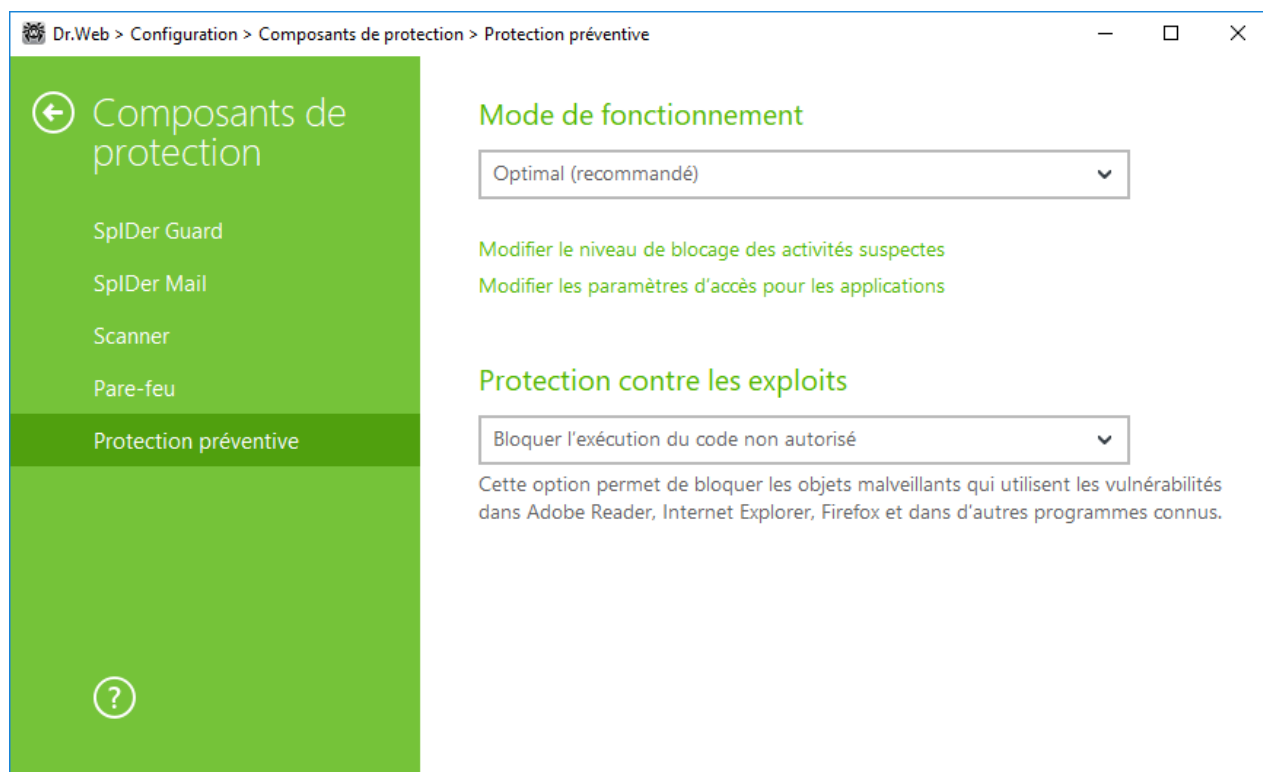



Figure 35. Configuration de la protection préventive

Dans ce cas, vous pouvez spécifier le mode de protection à part pour les applications concrètes et le mode général, dont les paramètres seront appliqués à tous les autres processus.


Pour spécifier le mode général de la protection préventive, sélectionnez-le dans la liste **Mode de fonctionnement** et cliquez sur l'option **Modifier le niveau de blocage des activités suspectes**. Dans le dernier cas, une fenêtre va s'afficher dans laquelle vous pouvez consulter les paramètres de chaque mode et les modifier. Toutes les modifications des paramètres sont enregistrées en mode Utilisateur. Dans cette fenêtre vous pouvez également créer un nouveau profil pour enregistrer les paramètres nécessaires.

Création d'un nouveau profil

1. Cliquez sur .
2. Dans la fenêtre qui s'affiche, indiquez le nom du nouveau profil.
3. Consultez les paramètres de protection spécifiés par défaut. Modifiez-les, si cela est nécessaire.

Pour configurer les paramètres de la protection préventive pour les applications concrètes, cliquez sur l'option **Modifier les paramètres d'accès pour les applications**. Dans la fenêtre qui s'affiche, vous pouvez ajouter une nouvelle règle pour l'application, modifier une règle déjà créée ou supprimer une règle inutile.

Ajouter une règle

1. Cliquez sur .



2. Dans la fenêtre qui s'affiche, cliquez sur **Parcourir** et spécifiez le chemin vers le fichier exécutable de l'application.
3. Consultez les paramètres de protection spécifiés par défaut. Modifiez-les, si cela est nécessaire.

Pour modifier une règle déjà créée, sélectionnez-la dans la liste et cliquez sur .

Pour supprimer une règle déjà créée, sélectionnez-la dans la liste et cliquez sur .

Pour en savoir plus sur chaque mode de fonctionnement, consultez la rubrique Niveau de la Protection préventive ci-dessous.

Niveau de la Protection préventive

Dans le mode **Optimal** spécifié par défaut, Dr.Web interdit la modification automatique des objets système, la modification qui indiquerait clairement une tentative malveillante d'endommager le système d'exploitation. L'accès bas niveau au disque est interdit, ainsi que toute modification du fichier HOSTS par les applications dont les actions sont considérées comme tentative d'endommager le système.



Seules les actions des applications qui ne sont pas de confiance sont bloquées.

Vous pouvez choisir le mode **Moyen**, s'il existe un risque élevé d'infection. Dans ce mode, l'accès aux objets critiques qui peuvent être potentiellement utilisés par des programmes malveillants est bloqué.



L'utilisation de ce mode peut entraîner des problèmes de compatibilité avec des logiciels légitimes qui utilisent les branches du registre protégées.

Le niveau de protection **Paranoïde** est nécessaire pour avoir un contrôle total de l'accès aux objets Windows critiques. Dans ce mode, Dr.Web fournit également un contrôle interactif sur le chargement de pilotes et le démarrage automatique de programmes.

Dans le mode **Défini par l'utilisateur**, vous pouvez choisir vous-même le niveau de la protection pour chaque objet.

Objet protégé	Description
Intégrité des applications en cours d'exécution	Cette option permet la détection des processus qui injectent leur code dans les applications en cours d'exécution. Elle indique que le processus peut compromettre la sécurité de l'ordinateur. Les processus qui sont ajoutés à la Exclusions ne sont pas gérés.



Objet protégé	Description
Intégrité des fichiers des utilisateurs	Cette option permet la détection des processus qui modifient les fichiers utilisateur avec un algorithme connu qui indique que le processus peut compromettre la sécurité de l'ordinateur. Les processus qui sont ajoutés à Exclusions ne sont pas gérés.
Fichier HOSTS	Le système d'exploitation utilise le fichier HOSTS lors de sa connexion à Internet. Des modifications de ce fichier peuvent indiquer une infection virale.
Accès bas niveau au disque	Empêche les applications d'écrire sur les disques par secteurs évitant le système de fichiers.
Téléchargement de pilotes	Empêche les applications de charger des drivers nouveaux ou inconnus.
Objets critiques Windows	<p>D'autres options permettent la protection des branches de registre suivantes contre la modification (dans le profil système ainsi que dans les profils de tous les utilisateurs).</p> <p>Accès à Image File Execution Options :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options <p>Accès à User Drivers :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Drivers32• Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers <p>Paramètres de Winlogon :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL <p>Notificateurs Winlogon :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify <p>Autodémarrage de Windows :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Windows, Applnit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib <p>Associations de fichiers exécutables :</p> <ul style="list-style-type: none">• Software\Classes\exe, .pif, .com, .bat, .cmd, .scr, .lnk (clés)• Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (clés) <p>Politiques de restriction du démarrage des programmes (SRP) :</p> <ul style="list-style-type: none">• Software\Policies\Microsoft\Windows\Safer



Objet protégé	Description
	<p>Plugin Internet Explorer (objet application d'assistance du navigateur) :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects <p>Autodémarrage de programmes :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Run• Software\Microsoft\Windows\CurrentVersion\RunOnce• Software\Microsoft\Windows\CurrentVersion\RunOnceEx• Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup• Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup• Software\Microsoft\Windows\CurrentVersion\RunServices• Software\Microsoft\Windows\CurrentVersion\RunServicesOnce <p>Autodémarrage de politiques :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run <p>Configuration du mode sans échec :</p> <ul style="list-style-type: none">• SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal• SYSTEM\ControlSetXXX\Control\SafeBoot\Network <p>Paramètres de Session Manager :</p> <ul style="list-style-type: none">• System\ControlSetXXX\Control\Session Manager\SubSystems, Windows <p>Services système :</p> <ul style="list-style-type: none">• System\CurrentControlSetXXX\Services



Si un problème survient durant l'installation d'une mise à jour Microsoft importante ou durant l'installation et le fonctionnement de programmes (y compris des programmes de défragmentation), désactivez la protection préventive.

Vous pouvez [configurer](#) les notifications sur les actions de la protection préventive s'affichant sur le bureau et l'envoi de telles notifications par e-mail.

Protection contre les exploits

Cette option permet de bloquer les objets malveillants qui utilisent les vulnérabilités des applications connues. Sélectionnez le niveau nécessaire de la protection contre les exploits dans la liste déroulante.





Niveau de protection	Description
Bloquer l'exécution du code non autorisé	Une tentative d'un objet malveillant d'utiliser les vulnérabilités du logiciel pour obtenir l'accès aux zones critiques du système d'exploitation sera bloquée automatiquement.
Mode interactif	En cas de tentative d'un objet malveillant d'utiliser les vulnérabilités du logiciel pour obtenir l'accès aux zones critiques du système d'exploitation, Dr.Web affichera le message correspondant. Lisez les informations et sélectionnez une action nécessaire.
Autoriser l'exécution du code non autorisé	Une tentative d'un objet malveillant d'utiliser les vulnérabilités du logiciel pour obtenir l'accès aux zones critiques du système d'exploitation sera autorisée automatiquement.



13. Statistiques

Cette fenêtre contient les statistiques sur les événements importants de fonctionnement des composants de protection.

Pour consulter les informations sur le fonctionnement des composants, ouvrez le menu  et passez à la rubrique **Statistiques** . Sur la page **Statistiques**, les rapports pour les groupes suivants sont disponibles :

- Menaces
- Mise à jour

Le rapport détaillé est disponible pour les entrées des groupes **Menaces** et **Mise à jour**. Vous pouvez appliquer les filtres pour les entrées du rapport.

Activité réseau

Si Pare-feu Dr.Web est installé, le rapport de l'activité réseau est disponible.

Vous pouvez voir les informations sur les applications en cours, le journal des applications et le journal du filtre de paquet. Pour ce faire, sélectionnez l'objet nécessaire dans la liste déroulante.

Dans le rapport, les informations suivantes sont affichées pour chaque application en cours :

- direction de transmission de données ;
- protocole de fonctionnement ;
- adresse locale ;
- adresse distante ;
- taille du paquet de données envoyé ;
- taille du paquet de données reçu.

Dans le journal des applications, vous verrez :

- heure de début du fonctionnement de l'application ;
- nom de l'application ;
- nom de la règle du traitement de l'application ;
- direction de transmission de données ;
- action ;
- adresse cible.

Dans le journal du filtre de paquets, les informations suivantes sont affichées :


- heure de début du traitement du paquet de données ;
- direction de la transmission du paquet de données ;




- nom de la règle de traitement ;
- interface ;
- contenu du paquet.

Avec le bouton , vous pouvez exporter les entrées des journaux ou effacer les entrées des journaux.

Rapport détaillé


Pour consulter le rapport détaillé sur les événements du fonctionnement de Dr.Web, sélectionnez l'événement nécessaire et cliquez sur . Si vous cliquez sur ce bouton encore une fois, les données détaillées seront masquées.

Avec le bouton , vous pouvez supprimer, copier ou exporter les événements particuliers ou le rapport entier et vider le rapport.

Vous pouvez utiliser les filtres pour sélectionner des événements.

Filtres

Pour voir dans la liste uniquement les événements qui correspondent aux paramètres déterminés, utilisez les filtres. Pour tous les rapports il existe des filtres préinstallés qui sont disponibles dans la liste déroulante en haut de la page de chaque groupe.

Vous pouvez créer vos propres filtres d'événements. Pour créer un nouveau filtre, cliquez sur  et sélectionnez l'élément **Créer** dans la liste déroulante. Dans la fenêtre qui s'affiche, spécifiez les critères nécessaires de filtrage. Notez que vous pouvez spécifier plusieurs composants en même temps dans le champ **Composant**.

Vous pouvez trier les événements par codes. Pour ce faire, indiquez-les dans le champ **Code (par exemple : 100-103, -102, 403)** en respectant les règles suivants :

- séparez les codes par une virgule ;
- vous pouvez indiquer une plage de codes (par exemple, 100-103) ;
- le symbole « - » devant le code l'exclut de la plage.

Ainsi, une ligne du type suivant « 100-103, -102, 403 » signifie qu'il faut afficher tous les événements de « 100 » à « 103 », exclure du filtre le code « -102 » et afficher l'événement « 403 ».

Les filtres créés par l'utilisateur peuvent être modifiés ou supprimés.



14. Support technique

En cas de problèmes liés à l'installation ou au fonctionnement des produits de la société, avant de contacter le support technique, essayez de trouver la solution par un des moyens suivants :

- consultez les dernières versions des descriptions et des manuels à l'adresse <https://download.drweb.com/doc/> ;
- lisez la rubrique de questions fréquentes à l'adresse https://support.drweb.com/show_faq/ ;
- visitez des forums de Doctor Web à l'adresse <https://forum.drweb.com/>.

Si après avoir tout essayé, vous n'avez pas résolu le problème, utilisez un des moyens suivants pour contacter le support technique de Doctor Web :

- remplissez le formulaire de question dans la section correspondante de la rubrique <https://support.drweb.com/> ;
- appelez au numéro : 0 825 300 230.

Vous pouvez trouver les informations sur les bureaux régionaux de Doctor Web sur le site officiel à l'adresse <https://company.drweb.com/contacts/offices/>.



15. Annexe A. Paramètres supplémentaires de ligne de commande

Des paramètres de ligne de commande supplémentaires (clés) sont utilisés pour définir les paramètres des programmes lancés via l'ouverture d'un fichier exécutable. Ceci est relatif au Scanner Dr.Web Scanner en ligne de commande et au Module de mise à jour Dr.Web. Les clés peuvent définir des paramètres qui ne sont pas présents dans le fichier de configuration ou possèdent une priorité supérieure à ceux indiqués dans le fichier.

Les clés commencent par le signe « / » et sont séparées par des espaces comme les autres paramètres en ligne de commande.

15.1. Paramètres du Scanner et du Scanner en ligne de commande

Clé	Description
/AA	Appliquer automatiquement les actions aux menaces détectées (uniquement pour le Scanner).
/AC	Scanner les packages d'installation. L'option est activée par défaut.
/AFS	Utiliser un slash droit pour spécifier l'imbrication dans l'archive. L'option est désactivée par défaut.
/AR	Scanner les archives. L'option est activée par défaut.
/ARC : <taux_de_compression>	Taux maximum de compression. Si le scanner détecte que le taux dépasse le maximum spécifié, l'extraction depuis l'archive ne se fait pas et le scan d'une telle archive ne sera pas effectué. Par défaut — illimité.
/ARL : <niveau_d'imbrication>	Niveau maximum d'imbrication de l'archive scannée. Par défaut — illimité.
/ARS : <taille>	taille maximum de l'archive scannée, en Ko. Par défaut — illimité.
/ART : <taille>	Seuil de vérification du taux de compression (la taille minimum du fichier dans l'archive à partir de laquelle s'effectue la vérification du taux de compression), en Ko. Par défaut — illimité.



Clé	Description
/ARX: <taille>	Taille maximum des objets archivés à scanner, en Ko. Par défaut — illimité.
/BI	Afficher les informations sur les bases de données virales. L'option est activée par défaut.
/CUSTOM	Lancer le Scanner sur la page de l'analyse personnalisée. Si dans ce cas, les paramètres avancés sont spécifiés (par exemple, les objets à analyser ou les paramètres /TM, /TB), l'analyse personnalisée des objets spécifiés sera lancée. (Uniquement pour le Scanner).
/CL	Utiliser le service cloud Dr.Web. L'option est activée par défaut. (Uniquement pour le Scanner en ligne de commande).
/DCT	Ne pas afficher la durée calculée d'analyse. (Uniquement pour le Scanner en ligne de commande).
/DR	Scanner les dossiers de manière récursive (analyser les sous-dossiers). L'option est activée par défaut.
/E: <nombre_de_flux>	Effectuer une analyse à un nombre spécifié de flux.
/FAST	Lancer le analyse rapide du système. Si dans ce cas, les paramètres avancés sont spécifiés (par exemple, les objets à analyser ou les paramètres /TM, /TB), les objets spécifiés seront également analysés. (Uniquement pour le Scanner).
/FL: <nom_du_fichier>	Analyser les chemins spécifiés dans le fichier.
/FM: <masque>	Analyser les fichiers selon un masque. Par défaut, tous les fichiers seront analysés.
/FR: <expression_régulière>	Analyser les fichiers selon une expression régulière. Par défaut, tous les fichiers sont scannés.
/FULL	Lancer l'analyse complète de tous les disques durs et de tous les supports amovibles (y compris les secteurs d'amorçage). Si dans ce cas, les paramètres avancés sont spécifiés (par exemple, les objets pour l'analyse ou les paramètres /TM, /TB), l'analyse rapide et l'analyse des objets spécifiés seront lancées. (Uniquement pour le Scanner).
/FX: <masque>	Exclure de l'analyse les fichiers qui correspondent au masque. (Uniquement pour le Scanner en ligne de commande).



Clé	Description
/GO	Mode de fonctionnement du Scanner lors duquel les questions impliquant des réponses d'utilisateur sont ignorées ; les décisions impliquant un choix sont prises automatiquement. Il est utile d'utiliser ce mode pour l'analyse automatique des fichiers, par exemple, lors de l'analyse quotidien ou hebdomadaire du disque dur. Dans la ligne de commande, il est nécessaire de spécifier l'objet à analyser. Vous pouvez utiliser les paramètres /LITE, /FAST, /FULL avec le paramètre /GO. Dans ce mode, l'analyse s'arrête en cas de passage en fonctionnement sur batterie.
/H ou /?	Afficher la rubrique d'aide sur le fonctionnement du programme. (Uniquement pour le Scanner en ligne de commande).
/HA	Effectuer une analyse heuristique des fichiers afin d'y rechercher des menaces inconnues. L'option est activée 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. Par défaut, drweb32.key ou une autre clé appropriée depuis le dossier C:\Program Files\DrWeb\ sera utilisée.
/LITE	Effectuer une analyse du système y compris la mémoire vive, les secteurs d'amorçage de tous les disques, effectuer une recherche des rootkits. (Uniquement pour le Scanner).
/LN	Analyser les fichiers par raccourcis associés. L'option est désactivée par défaut.
/LS	Analyser sous le compte LocalSystem. L'option est désactivée par défaut.
/MA	Analyser les fichiers de messagerie. L'option est activée par défaut.
/MC : <nombre_de_tentatives >	Spécifier le 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 la



Clé	Description
	mémoire utilisée pour le processus de scan et la priorité système de la tâche de scan. Par défaut — illimité.
/NOREBOOT	Annule le redémarrage et l'arrêt du système après la fin de l'analyse. (Uniquement pour le Scanner).
/NT	Analyser les flux NTFS. L'option est activée par défaut.
/OK	Afficher la liste complète des objets scannés et accompagner les objets sains de la remarque 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 : supérieure. M : maximum.
/PAL : <niveau_d'imbrication>	Niveau d'imbrication maximum des outils de compression d'un fichier exécutable. Si le niveau d'imbrication dépasse la valeur spécifiée, l'analyse va uniquement jusqu'au niveau d'imbrication spécifié. Par défaut — 1000.
/QL	Afficher la liste de tous les fichiers mis en quarantaine sur tous les disques. (Uniquement pour le Scanner en ligne de commande).
/QL : <nom_du_disque_logique>	Afficher la liste de tous les fichiers mis en quarantaine sur le disque logique spécifié. (Uniquement pour le Scanner en ligne de commande).
/QNA	afficher les chemins entre guillemets doubles.
/QR [: [d] [:p]]	Supprimer du disque spécifié <d> (nom_du_disque_logique) les fichiers se trouvant dans la quarantaine pendant plus de <p> jours. Si les valeurs <d> et <p> ne sont pas spécifiées, tous les fichiers se trouvant dans la quarantaine seront supprimés de tous les disques logiques (uniquement pour le Scanner en ligne de commande).
/QUIT	Fermer le Scanner après l'analyse (indépendamment de l'application/non application des actions aux menaces détectées). (Uniquement pour le Scanner).



Clé	Description
/RA: <nom_du_fichier>	Ajouter le rapport du fonctionnement du programme dans le fichier spécifié. Par défaut, le rapport n'est pas enregistré dans le journal.
/REP	Analyser selon les liens symboliques. L'option est désactivée par défaut.
/RK	Analyse pour la présence de rootkits. L'option est désactivée par défaut.
/RE: <nom_du_fichier>	Enregistrer le rapport du fonctionnement du programme dans le fichier spécifié. Par défaut, le rapport n'est pas enregistré dans le journal.
/RPC: <s>	Délai de connexion à Scanning Engine, en secondes. Par défaut — 30 s. (Uniquement pour le Scanner en ligne de commande).
/RPCD	Utiliser l'identificateur dynamique RPC. (Uniquement pour le Scanner en ligne de commande).
/RPCE	Utiliser l'adresse cible dynamique RPC. (Uniquement pour le Scanner en ligne de commande).
/RPCE: <adresse_cible>	Utiliser l'adresse cible RPC spécifiée. (Uniquement pour le Scanner en ligne de commande).
/RPCH: <nom_d'hôte>	Utiliser le nom d'hôte spécifié pour les appels RPC. (Uniquement pour le Scanner en ligne de commande).
/RPCP: <protocole>	Utiliser le protocole spécifié RPC. Il est possible d'utiliser les protocoles : lpc, np, tcp. (Uniquement pour le Scanner en ligne de commande).
/SCC	Afficher le contenu des objets complexes. L'option est désactivée par défaut.
/SCN	Afficher le nom du package d'installation. L'option est désactivée par défaut.
/SLS	Afficher les logs sur l'écran. L'option est activée par défaut. (Uniquement pour le Scanner en ligne de commande).
/SPN	Afficher le nom de l'outil de compression. L'option est désactivée par défaut.
/SPS	Afficher la progression du processus de scan. L'option est activée par défaut (uniquement pour le Scanner en ligne de



Clé	Description
	commande).
/SST	Afficher la durée du scan. L'option est désactivée par défaut.
/ST	Lancement du Scanner en tâche de fond. Si le paramètre /GO n'est pas spécifié, le mode graphique s'affiche uniquement en cas de détection d'une menace. Dans ce mode, l'analyse s'arrête en cas de passage en fonctionnement sur batterie.
/TB	Analyser les secteurs de boot et les secteurs MBR du disque dur.
/TM	Détecter les menaces dans la mémoire vive (y compris la partie système de Windows).
/TR	Vérifier les points de restauration système.
/W:<S>	Durée maximum de scan, en secondes. Par défaut — illimité.
/WCL	Afficher dans la console drwebwcl. (Uniquement pour le Scanner en ligne de commande).
/X:S[:R]	A la fin du scan, basculer la machine vers un mode de fonctionnement spécifié : arrêt/redémarrage/mode veille/mode veille prolongée.

Vous pouvez configurer les actions à appliquer aux les objets divers (C — désinfecter, Q — déplacer vers la quarantaine, D — supprimer, I — ignorer, R — informer. L'action R est applicable uniquement au Scanner en ligne de commande. Par défaut, pour tous les objets — notifier (uniquement pour le Scanner en ligne de commande)) :

Action	Description
/AAD:<action>	actions appliquées aux adwares (actions possibles : DQIR)
/AAR:<action>	actions appliquées aux archives infectées (actions possibles : DQIR)
/ACN:<action>	actions appliquées aux packages d'installation infectés (actions possibles : DQIR)
/ADL:<action>	actions appliquées aux dialers (actions possibles : DQIR)
/AHT:<action>	actions appliquées aux hacktools (actions possibles : DQIR)
/AIC:<action>	actions appliquées aux fichiers incurables (actions possibles : DQR)



Action	Description
/AIN:<action>	actions appliquées aux fichiers infectés (actions possibles : CDQR)
/AJK:<action>	actions appliquées aux canulars (actions possibles : DQIR)
/AML:<action>	actions appliquées aux fichiers de messagerie infectés (actions possibles : QIR)
/ARW:<action>	actions appliquées aux riskwares (actions possibles : DQIR)
/ASU:<action>	actions appliquées aux 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 :

/AC, /AFS, /AR, /BI, /DR, /HA, /LN, /LS, /MA, /NB, /NT, /OK, /QNA, /REP, /SCC, /SCN, /SLS, /SPN, /SPS, /SST, /TB, /TM, /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, la valeur du paramètre « 0 » signifie que le paramètre est utilisé sans restrictions.

Exemple d'utilisation des clés lors du démarrage du Scanner en ligne de commande :

```
[<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. Pour lancer le Scanner pour Windows de manière analogique, à la place de dwscancl, saisissez la commande dwscanner.



15.2. Paramètres du Module de mise à jour

Paramètres généraux :

Paramètre	Description
-h [--help]	Afficher à l'écran la rubrique d'aide abrégée sur le programme.
-v [--verbosity] arg	Niveau de détail du journal : error (standard), info (élevé), debug (débogage).
-d [--data-dir] arg	Répertoire dans lequel sont conservés le référentiel et les paramètres.
--log-dir arg	Répertoire dans lequel le fichier de journal sera sauvegardé.
--log-file arg (=dwupdater.log)	Nom du fichier de journal.
-r [--repo-dir] arg	Répertoire du référentiel, (par défaut <data_dir>/repo).
-t [--trace]	Activer le traçage.
-c [--command] arg (=update)	Commande à exécuter : getversions — obtenir les versions, getcomponents — obtenir les composants, init — initialisation, update — mise à jour, uninstall — supprimer, exec — exécuter, keyupdate — mettre à jour la clé, download — télécharger.
-z [--zone] arg	Liste des zones à utiliser à la place des zones spécifiées dans le fichier de configuration.

Paramètres de la commande d'initialisation (init) :

Paramètre	Description
-s [--version] arg	Numéro de version.
-p [--product] arg	Nom du produit.
-a [--path] arg	Chemin d'installation du produit. Ce répertoire sera utilisé par défaut comme répertoire pour tous les composants inclus dans le produit. Le Module de mise à jour va vérifier la présence du fichier clé dans ce répertoire.
-n [--component] arg	Nom du composant et le répertoire d'installation au format <nom>, <chemin d'installation>.
-u [--user] arg	Nom de l'utilisateur du serveur proxy.



Paramètre	Description
-k [--password] arg	Mot de passe de l'utilisateur du serveur proxy.
-g [--proxy] arg	Serveur proxy pour la mise à jour au format <i><adresse>: <port></i> .
-e [--exclude] arg	Nom du composant à enlever du produit lors de l'installation.

Paramètres de la commande de mise à jour (update) :

Paramètre	Description
-p [--product] arg	Le nom du produit. Si un nom est spécifié, seul le produit correspondant sera mis à jour. Si aucun produit n'est spécifié, ni aucun composant, alors tous les produits seront mis à jour. S'il y a des composants spécifiés, ces composants seront mis à jour.
-n [--component] arg	Liste des composant à mettre à niveau vers une révision spécifiée. Syntaxe : <i><name></i> , <i><target revision></i> .
.-x [--selfrestart] arg (=yes)	Redémarrage après la mise à jour du Module de mise à jour. La valeur par défaut – <i>yes</i> . En cas de valeur <i>no</i> , une notification sur la nécessité de redémarrer sera affichée.
--geo-update	Obtenir une liste des adresses IP d'update.drweb.com avant la mise à jour.
--type arg (=normal)	Peut prendre l'une des valeurs suivantes : <ul style="list-style-type: none">• <i>reset-all</i> : forcer la mise à jour de tous les composants ;• <i>reset-failed</i> : annuler toutes les modifications pour les composants corrompus ;• <i>normal-failed</i> : essayer de mettre à niveau les composants y compris ceux qui sont corrompus, vers la dernière version ou vers une version spécifiée ;• <i>update-revision</i> : mettre à jour les composant au sein de la révision courante ;• <i>normal</i> : mettre à jour tous les composants.
-g [--proxy] arg	Serveur proxy pour la mise à jour au format <i><adresse>: <port></i> .
-u [--user] arg	Nom de l'utilisateur du serveur proxy.
-k [--password] arg	Mot de passe de l'utilisateur du serveur proxy.
--param arg	Transmettre les paramètres supplémentaires vers le script. Syntaxe : <i><nom>: <valeur></i> .



Paramètre	Description
-l [--progress-to-console]	Afficher sur la console des informations sur le chargement et l'exécution du script.

Paramètres de la commande d'obtention des composants (getcomponents) :

Paramètre	Description
-s [--version] arg	Numéro de version.
-p [--product] arg	Spécifiez le nom du produit pour consulter les composants inclus. Si aucun produit n'est spécifié, tous les composants correspondant à la version courante seront affichés.

Paramètres de la commande d'obtention des révisions (getrevisions) :

Paramètre	Description
-s [--version] arg	Numéro de version.
-n [--component] arg	Nom du composant.

Paramètres de la commande de suppression (uninstall) :

Paramètre	Description
-n [--component] arg	Nom du composant à supprimer.
-l [--progress-to-console]	Afficher sur la console des informations sur l'exécution de la commande.
--param arg	Transmettre les paramètres supplémentaires vers le script. Syntaxe : <nom>: <valeur>.
-e [--add-to-exclude]	Composants qui seront supprimés, leur mise à jour ne sera pas réalisée.

Paramètres de la commande de mise à jour automatique de la clé (keyupdate) :

Paramètre	Description
-m [--md5] arg	Somme de contrôle md5 de l'ancien fichier clé.



Paramètre	Description
-o [--output] arg	Nom du fichier.
-b [--backup]	Copie de sauvegarde de l'ancien fichier clé s'il existe.
-g [--proxy] arg	Serveur proxy pour la mise à jour au format <i><adresse>: <port></i> .
-u [--user] arg	Nom de l'utilisateur du serveur proxy.
-k [--password] arg	Mot de passe de l'utilisateur du serveur proxy.
-l [--progress-to-console]	Afficher sur la console des informations sur le téléchargement du fichier clé.

Paramètres de la commande de téléchargement (download) :

Paramètre	Description
--zones arg	Fichier contenant une liste des zones.
--key-dir arg	Répertoire dans lequel se trouve le fichier clé.
-l [--progress-to-console]	Afficher sur la console des informations sur l'exécution de la commande.
-g [--proxy] arg	Serveur proxy pour la mise à jour au format <i><adresse>: <port></i> .
-u [--user] arg	Nom de l'utilisateur du serveur proxy.
-k [--password] arg	Mot de passe de l'utilisateur du serveur proxy.
-s [--version] arg	Nom de la version.
-p [--product] arg	Nom du produit à télécharger.

15.3. Codes de retour

Les valeurs possibles du code de retour et les événements y correspondant sont les suivants :

Code de retour	Événement
0	Aucun virus ou soupçon de virus n'est détecté.
1	Les virus connus sont détectés.



Code de retour	Événement
2	Les modifications de virus connus sont détectées.
4	Les objets suspects sont détectés.
8	Les virus connus sont détectés dans une archive, un conteneur ou dans une boîte e-mail.
16	Les modifications de virus connus sont détectées dans une archive, un conteneur ou dans une boîte e-mail.
32	Les objets suspects sont détectés dans une archive, un conteneur ou dans une boîte e-mail.
64	Au moins un objet infecté a été désinfecté avec succès.
128	La désinfection/la renomination/le déplacement d'au moins un fichier infecté est effectué.

Le code de retour final, formé à la fin du scan, est égal à la somme des codes des événements survenus lors du scan (les termes peuvent être reconstitués d'après le code final).

Par exemple, le code de retour $9 = 1 + 8$ signifie que des virus connus (un virus) ont été détectés lors du scan, y compris dans les archives ; la désinfection n'a pas été effectuée ; il n'y avait plus aucun événement « viral ».



16. Annexe B. Menaces et méthodes de neutralisation

Avec le développement des technologies IT et des solutions réseau, les programmes malveillants de différents types, conçus pour attaquer les utilisateurs, deviennent de plus en plus répandus. Leur développement est apparu en même temps que la science des ordinateurs et les outils de protection contre eux ont progressé en même temps. Néanmoins, il n'existe toujours pas de classification commune pour toutes les menaces potentielles en raison du caractère imprévisible de leur développement et de leur constante amélioration.

Les programmes malveillants peuvent être diffusés via Internet, les réseaux locaux, les e-mails et les supports amovibles. Certains d'entre eux comptent sur l'imprudence des utilisateurs et leur manque d'expérience et peuvent fonctionner en mode complètement automatique. D'autres sont des outils contrôlés par un ordinateur qui peuvent endommager même le système le plus sécurisé.

Ce chapitre décrit les types de programmes malveillants les plus connus et les plus répandus, contre lesquels luttent les produits de Doctor Web.

16.1. Classification de menaces

Sous le terme « menace », ce classement comprend tout logiciel pouvant endommager directement ou indirectement l'ordinateur, le réseau, l'information ou porter atteinte aux droits de l'utilisateur (programmes malicieux ou indésirables). Dans le sens plus large du terme, « menace » peut signifier un danger potentiel pour l'ordinateur ou pour le réseau (une vulnérabilité pouvant être utilisée pour des attaques de pirates).

Tous les types de logiciels décrits ci-dessous peuvent présenter un danger pour les données de l'utilisateur et pour son droit à la confidentialité. Les logiciels qui ne dissimulent pas leur présence dans le système (par exemple, certains logiciels pour diffusion du spam ou analyseurs du trafic), normalement ne sont pas classés comme menaces, mais sous certaines conditions, ils peuvent causer des dommages à l'utilisateur.

Dans les produits et la documentation de Doctor Web, les menaces sont divisées en deux types, selon le niveau de danger qu'elles représentent :

- **menaces graves** : ce sont des menaces classiques qui sont capables de mener des actions destructives et illégales au sein du système (suppression et vol des informations défaillance du réseau etc.). Ce type de menace regroupe les logiciels appelés malveillants (virus, vers, programmes de Troie) ;
- **menaces insignifiantes** : ce sont des menaces considérées comme moins dangereuses que des menaces graves, mais qui sont à éviter elles aussi, car de tierces personnes peuvent s'en servir pour effectuer des actions nocives. De plus, toute présence de menaces, même insignifiantes, dans le système, témoigne de sa vulnérabilité. Les spécialistes de la protection informatique qualifient ce type de menaces de programmes « gris » ou « programmes potentiellement indésirables ». Les menaces insignifiantes sont représentées par des adwares, des dialers, des canulars, des riskwares et des hacktools.



Menaces graves

Virus informatiques

Ce type de menaces informatiques est capable d'introduire son code dans le code d'exécution d'autres logiciels. Cette pénétration porte le nom d'*infection*. Dans la plupart des cas, le fichier infecté devient lui-même porteur de virus et le code introduit n'est plus conforme à l'original. La majeure partie des virus est conçue pour endommager ou exterminer les données.

En fonction du type d'objet infecté, Doctor Web classe les virus selon les types suivants :

- **virus de fichier** infectent les fichiers de système d'exploitation (fichiers exécutables, fichiers dll). Ces virus sont activés lors de l'accès au fichier infecté ;
- **macrovirus** infectent les fichiers de documents utilisés par les applications Microsoft® Office et d'autres programmes utilisant des commandes macros généralement écrits en Visual Basic. Les macros, ce sont des programmes internes, écrits en langage de programmation totalement fonctionnel, qui sont automatiquement lancés sous des conditions déterminées (par exemple, dans Microsoft® Word, quand vous ouvrez, fermez, sauvegardez ou créez un document) ;
- **virus Script** sont écrits en langages des scénarios (langages de script). Ils infectent dans la plupart des cas d'autres fichiers script (par exemple, les fichiers du système d'exploitation). Ils peuvent infecter aussi d'autres types de fichiers qui supportent l'exécution des scénarios script, tout en se servant des scénarios vulnérables des applications Web ;
- **virus de téléchargement** infectent les secteurs boot des disques et des partitions aussi bien que les principaux secteurs boot des disques durs. Ils occupent peu de mémoire et restent prêts à remplir leurs fonctions jusqu'à ce qu'un déchargement, un redémarrage ou un arrêt du système ne soient effectués.

La plupart des virus possèdent des mécanismes spécifiques pour se dissimuler dans le système. Leurs méthodes de protection contre la détection s'améliorent sans cesse. Cependant, dans le même temps, de nouveaux moyens d'élimination de cette protection apparaissent. On peut également diviser les virus selon les principes de protection contre la détection :

- **les virus cryptés** chiffrent leur code à chaque infection pour éviter leur détection dans un fichier, un secteur boot ou un secteur de mémoire. Toutes les copies de tels virus contiennent seulement un petit fragment de code commun (procédure de décryptage), qui peut être utilisé comme une signature de virus ;
- **les virus polymorphes** cryptent également leur code, mais ils génèrent en plus une procédure de décryptage spéciale différente dans chaque copie de virus. Ceci signifie que de tels virus n'ont pas de signatures.

Les virus peuvent également être classifiés selon le langage de programmation dans lequel ils sont écrits (dans la plupart des cas c'est en assembleur, des langages de programmation de haut niveau, des langages script, etc.) ou selon les systèmes d'exploitation qu'ils ciblent.



Vers d'ordinateurs

Les vers sont récemment devenus beaucoup plus répandus que les virus et les autres programmes malveillants. Comme les virus, ils sont capables de créer leurs copies. Un ver infiltre un ordinateur via le réseau (généralement sous forme d'une pièce jointe dans les messages e-mail) et distribue ses copies fonctionnelles à d'autres ordinateurs. Pour se propager, les vers peuvent profiter des actions de l'utilisateur ou choisir le poste à attaquer de manière automatique.

Les vers ne consistent pas forcément en un seul fichier (le corps du ver). La plupart d'entre eux comportent une partie infectieuse (le shellcode) qui se charge dans la mémoire vive de l'ordinateur, puis télécharge le corps du ver via le réseau sous forme d'un fichier exécutable. Tant que le système n'est pas encore infecté par le corps du ver, vous pouvez régler le problème en redémarrant l'ordinateur (et la mémoire vive est déchargée et remise à zéro). Mais aussitôt que le corps du ver entre dans le système, seul l'antivirus peut le désinfecter.

A cause de leur propagation intense, les vers peuvent mettre hors service des réseaux entiers, même s'ils n'endommagent pas directement le système.

Doctor Web divise les vers d'après leur mode de propagation :

- **vers de réseau** se propagent à l'aide de différents protocoles réseau ou protocoles d'échanges de fichiers ;
- **vers de courrier** se propagent via les protocoles de courrier (POP3, SMTP, etc.).

Chevaux de Troie

Ce type de programmes malveillants ne peuvent se reproduire. Un Trojan effectue des actions malveillantes (endommage ou supprime des données, envoie des informations confidentielles, etc.) ou rend l'accès de l'ordinateur possible à un tiers, sans autorisation, afin de nuire à l'utilisateur.

Le masquage de Trojan et les fonctions malveillantes sont similaires à ceux d'un virus et peuvent même être un composant de virus. Cependant, la plupart des Trojans sont diffusés comme des fichiers exécutables séparés (via des serveurs d'échanges de fichiers, des supports amovibles ou des pièces jointes), qui sont lancés par l'utilisateur ou par une tâche système.

Vous trouverez ci-dessous la liste de certains types de trojans qui sont classés par les spécialistes de Doctor Web :

- **backdoors** : ce sont des programmes de Troie qui offrent un accès privilégié au système, contournant le mécanisme existant d'accès et de protection. Les backdoors n'infectent pas les fichiers, mais ils s'inscrivent dans le registre, modifiant les clés ;
- **droppers** : ce sont les fichiers qui contiennent dans leur corps les programmes malveillants. Une fois le dropper lancé, il copie sur le disque de l'utilisateur les fichiers malveillants sans avertir l'utilisateur et puis, il les lance ;



- **enregistreurs de frappe (keyloggers)** – ils sont utilisés pour collecter les données que l'utilisateur entre avec son clavier. Le but de ces actions est le vol de toute information personnelle (mots de passe, logins, numéros de cartes bancaires etc.) ;
- **clickers** – ils redirigent les liens quand on clique dessus. D'ordinaire, l'utilisateur est redirigé vers des sites déterminés (probablement malveillants) avec le but d'augmenter le trafic publicitaire des sites web ou pour organiser des attaques par déni de service (attaques DoS) ;
- **trojans proxy** – ils offrent au malfaiteur l'accès anonyme à Internet via l'ordinateur de la victime ;
- **rootkits** – ils sont destinés à intercepter les fonctions du système d'exploitation pour dissimuler leur présence dans le système. En outre, le rootkit peut masquer les processus des autres logiciels, les clés de registre, des fichiers et des dossiers. Le rootkit se propage comme un logiciel indépendant ou comme un composant supplémentaire d'un autre logiciel malicieux. Selon le principe de leur fonctionnement, les rootkits sont divisés en deux groupes : les rootkits qui fonctionnent dans le mode utilisateur (interception des fonctions des bibliothèques du mode utilisateur) (User Mode Rootkits (UMR)), et les rootkits qui fonctionnent dans le mode noyau (interception des fonctions au niveau du noyau système, ce qui rend toute détection et toute désinfection très difficile) (Kernel Mode Rootkits (KMR)).

Outre les actions listées ci-dessus, les programmes de Troie peuvent exécuter d'autres actions malveillantes, par exemple, changer la page d'accueil dans le navigateur web ou bien supprimer certains fichiers. Mais ces actions peuvent être aussi exécutées par les menaces d'autres types (par exemple, virus et vers).

Menaces insignifiantes

Hacktools

Les hacktools sont créés pour aider les hackers. Les logiciels de ce type les plus répandus sont des scanners de ports qui permettent de détecter les vulnérabilités des pare-feux (firewalls) et des autres composants qui assurent la sécurité informatique de l'ordinateur. Ces instruments peuvent également être utilisés par les administrateurs pour vérifier la solidité de leurs réseaux. Parfois, les logiciels utilisant les méthodes de l'ingénierie sociale sont aussi considérés comme hacktools.

Adwares

Sous ce terme, on désigne le plus souvent un code intégré dans des logiciels gratuits qui impose l'affichage d'une publicité sur l'ordinateur de l'utilisateur. Mais parfois, ce code peut être diffusé par d'autres logiciels malicieux et afficher la publicité, par exemple, sur des navigateurs Internet. Très souvent, ces logiciels publicitaires fonctionnent en utilisant la base de données collectées par des logiciels espions.



Canulars

Comme les adwares, ce type de programme malveillant ne provoque pas de dommage direct au système. Habituellement, les canulars génèrent des alertes sur des erreurs qui n'ont jamais eu lieu et effraient l'utilisateur afin qu'il effectue des actions qui conduiront à la perte de données. Leur objectif est d'effrayer ou de déranger l'utilisateur.

Dialers

Ce sont les logiciels spécifiques utilisant l'accès à Internet avec l'autorisation de l'utilisateur pour accéder aux sites déterminés. D'habitude, ils possèdent un certificat signé et notifient toutes leurs actions à l'utilisateur.

Riskwares

Ces logiciels ne sont pas créés pour endommager le système, mais à cause de leurs particularités, ils peuvent présenter une menace pour la sécurité du système. Ces logiciels peuvent non seulement endommager les données ou les supprimer par hasard, mais ils peuvent également être utilisés par des hackers ou par d'autres logiciels pirates pour nuire au système. Les logiciels utilisés à distance, d'administration à distance, les serveurs FTP etc. peuvent être considérés comme potentiellement dangereux.

Objets suspects

Ce sont des menaces potentielles détectées à l'aide de l'analyse heuristique. Ces objets peuvent appartenir à un des types de menaces informatiques (même inconnues pour les spécialistes de la sécurité informatique) ou être absolument inoffensifs, en cas de faux positif. En tous cas, il est recommandé de placer les fichiers contenant des objets suspects en quarantaine et envoyer pour analyse aux spécialistes du laboratoire antivirus de Doctor Web.



16.2. Actions appliquées aux menaces détectées

Il existe plusieurs méthodes de neutralisation des menaces. Les produits de Doctor Web combinent ces méthodes pour la protection la plus fiable des ordinateurs et des réseaux en utilisant une configuration conviviale et flexible. Les principales actions de neutralisation des programmes malveillants sont les suivantes :

1. **Désinfecter** : l'action appliquée aux virus, vers et trojans. Ceci implique la suppression du code malveillant des fichiers infectés ou la suppression de copies de programmes malveillants, ainsi que la restauration des objets infectés (c'est-à-dire la restauration de la structure et du fonctionnement de l'objet tels qu'ils étaient avant son infection) si possible. Tous les programmes malveillants ne peuvent être désinfectés. Cependant, les produits de Doctor Web sont basés sur les plus efficaces algorithmes de désinfection et de restauration de fichiers infectés.
2. **Déplacer en quarantaine** : il s'agit de déplacer l'objet malveillant dans un dossier spécial et de l'isoler du reste du système. Cette action est préférable en cas d'impossibilité de désinfecter et pour tous les objets suspects. Il est recommandé d'envoyer des copies de ces fichiers au laboratoire antivirus de Doctor Web afin qu'elles soient analysées.
3. **Supprimer** : l'action efficace de neutralisation des menaces. Elle peut s'appliquer à n'importe quel type d'objet malveillant. Notez que la suppression sera parfois appliquée aux objets pour lesquels la désinfection était sélectionnée. Ceci arrive si l'objet contient uniquement le code malveillant et ne contient pas d'information utile. Par exemple, la désinfection d'un ver d'ordinateur signifie la destruction de toutes ses copies opérationnelles.
4. **Bloquer, renommer** : ces actions peuvent également être utilisées pour neutraliser des programmes malveillants. Cependant, des copies totalement fonctionnelles de ces programmes demeurent dans le système. En utilisant l'action Bloquer, toutes les tentatives d'accès vers ou depuis l'objet malveillant sont bloquées. Le renommage signifie que l'extension du fichier est modifiée, ce qui le rend inopérant.



17. Annexe C. Principes de nomination des menaces

En cas de détection d'un code viral les composants Dr.Web le signalent à l'utilisateur à l'aide des outils de l'interface et inscrivent le nom du virus, attribué par les spécialistes Doctor Web, dans le fichier du rapport. Ces noms sont créés en fonction de certains principes et reflètent un modèle de menace, des catégories d'objets vulnérables, l'environnement de diffusion (OS et applications) et d'autres caractéristiques. Le fait de savoir ces principes peut être utile pour la compréhension du logiciel et les vulnérabilités organisationnelles du système protégé. Vous trouverez ci-dessous le bref exposé de ces principes, la version complète de cette classification qui est mise à jour constamment se trouve sur <https://vms.drweb.com/classification/>.

Dans certains cas, cette classification est conventionnelle, car certains virus possèdent plusieurs caractéristiques en même temps. De plus, elle ne devrait pas être considérée comme exhaustive car de nouveaux types de virus apparaissent constamment et la classification devient de plus en plus précise.

Le nom complet d'un virus se compose de plusieurs éléments, séparés par des points. Certains éléments au début du nom (préfixes) et à la fin du nom (suffixes) sont standards dans la classification.

Préfixes généraux

Préfixes du système d'exploitation

Les préfixes listés ci-dessous sont utilisés pour nommer les virus infectant les fichiers exécutables de certains OS :

- Win : programmes 16-bit Windows 3.1 ;
- Win95 : programmes 32-bit Windows 95, Windows 98, Windows Me ;
- WinNT : programmes 32-bit Windows NT, Windows 2000, Windows XP, Windows Vista ;
- Win32 : programmes 32-bit OS Windows 95, Windows 98, Windows Me et Windows NT, Windows 2000, Windows XP, OS Windows Vista ;
- Win32.NET : programmes Microsoft .NET Framework ;
- OS2 : programmes OS/2 ;
- Unix : programmes dans différents systèmes basés sur UNIX ;
- Linux : programmes Linux ;
- FreeBSD : programmes FreeBSD ;
- SunOS : programmes SunOS (Solaris) ;
- Symbian : programmes Symbian OS (OS mobile).

Notez que certains virus peuvent infecter les programmes d'un système même s'ils sont créés pour fonctionner dans un autre système.



Virus infectant les fichiers MS Office

La liste des préfixes pour les virus qui infectent les objets MS Office (le langage des macros infectées par de tels virus est spécifié) :

- WM : Word Basic (MS Word 6.0-7.0) ;
- XM : VBA3 (MS Excel 5.0-7.0) ;
- W97M : VBA5 (MS Word 8.0), VBA6 (MS Word 9.0) ;
- X97M : VBA5 (MS Word 8.0), VBA6 (MS Word 9.0) ;
- A97M : bases de données de MS Access'97/2000 ;
- PP97M : présentations MS PowerPoint ;
- O97M : VBA5 (MS Office'97), VBA6 (MS Office 2000) ; ce virus infecte les fichiers de plus d'un composant de MS Office.

Préfixes de langage de programmation

Le groupe de préfixes HLL est utilisé pour nommer les virus écrits en langages de programmation de haut niveau comme C, C++, Pascal, Basic et d'autres. On utilise des modificateurs, indiquant l'algorithme de fonctionnement de base, notamment :

- HLLW : vers ;
- HLLM : vers de messagerie ;
- HLL0 : virus qui réécrivent le code du programme victime ;
- HLLP : virus parasites ;
- HLLC : virus compagnon.

Le préfixe suivant se réfère également à un langage de développement :

- Java : virus destinés à la machine virtuelle Java.

Chevaux de Troie

Cheval de Troie : nom général pour désigner différents programmes de Troie (Trojans). Dans de nombreux cas, les préfixes de ce groupe sont utilisés avec le préfixe Trojan.

- PWS : Trojan voleur de mots de passe ;
- Backdoor : Trojan avec la fonction de RAT (Remote Administration Tool – utilitaire d'administration à distance) ;
- IRC : Trojan qui utilise des canaux Internet Relay Chat ;
- DownLoader : Trojan qui télécharge discrètement différents programmes malveillants sur Internet ;
- MulDrop : Trojan qui télécharge discrètement des virus contenus dans son corps ;



- `Proxy` : Trojan qui autorise une tierce personne à travailler anonymement sur Internet via l'ordinateur infecté ;
- `StartPage` (synonyme : `Seeker`) : Trojan qui remplace sans autorisation la page d'accueil du navigateur (page de démarrage) ;
- `Click` : Trojan qui redirige l'utilisateur vers un site spécial (ou des sites) ;
- `KeyLogger` : Trojan spyware qui suit et enregistre des touches saisies ; il peut envoyer les données collectées à un cybercriminel ;
- `AVKill` : stoppe ou supprime les programmes antivirus, pare-feu, etc. ;
- `KillFiles`, `KillDisk`, `DiskEraser` : supprime certains fichiers (des fichiers dans certains répertoires, des fichiers selon certains masques, tous les fichiers sur les disques etc.) ;
- `DelWin` : supprime les fichiers vitaux pour le fonctionnement de l'OS Windows ;
- `FormatC` : formate le disque C : (synonyme : `FormatAll` : formate certains disques ou tous les disques) ;
- `KillMBR` : corrompt ou supprime le contenu du secteur principal d'amorçage (MBR) ;
- `KillCMOS` : corrompt ou supprime la mémoire CMOS.

Outil exploitant les vulnérabilités

- `Exploit` : un outil exploitant les vulnérabilités connues d'un OS ou d'une application pour introduire un code malveillant ou effectuer des actions non autorisées.

Outils d'attaques réseaux

- `Nuke` : outils destinés à attaquer certaines vulnérabilités connues des systèmes d'exploitation afin de provoquer l'arrêt du système attaqué ;
- `DDoS` : programme-agent destiné à provoquer une attaque par déni de service (Distributed Denial of Service) ;
- `FDoS` (synonyme : `Flooder`) : Flooder Denial Of Service – programmes destinés à effectuer des actions malveillantes sur Internet reposant sur l'idée des attaques par déni de service ; contrairement aux DDoS où plusieurs agents sur différents ordinateurs sont utilisés simultanément pour attaquer un système, un programme FDoS opère comme un programme indépendant « autosuffisant ».

Virus-script

Préfixes des virus écrits en différents langages de script :

- `VBS` : Visual Basic Script ;
- `JS` : Java Script ;
- `Wscript` : Visual Basic Script et/ou Java Script ;
- `Perl` : Perl ;
- `PHP` : PHP ;



- `BAT` : langage d'interprète de commande de l'OS MS-DOS.

Programmes malveillants

Préfixes des objets qui ne sont pas des virus, mais des programmes malveillants :

- `Adware` : publicité ;
- `Dialer` : programme dialer (il redirige les appels du modem vers des numéros payants) ;
- `Joke` : canular ;
- `Program` : un programme potentiellement dangereux (riskware) ;
- `Tool` : programme utilisé pour faire du piratage (hacktool).

Divers

Le préfixe `generic` est utilisé, après un autre préfixe décrivant l'environnement ou la méthode de développement, pour nommer un représentant typique de ce type de virus. Un tel virus ne possède aucune caractéristique (comme des séries de texte, des effets spécifiques etc.) qui permettrait de lui donner un nom particulier.

Auparavant le préfixe `Silly` était utilisé avec les modificateurs différents pour nommer les virus simples, sans signe particulier.

Suffixes

Les suffixes sont utilisés pour nommer des objets viraux particuliers :

- `generator` : un objet qui n'est pas un virus, mais un générateur de virus ;
- `based` : un virus développé à l'aide d'un générateur spécifique ou d'un virus modifié. Dans les deux cas, les noms de virus de ce type sont génériques et peuvent définir des centaines voire des milliers de virus ;
- `dropper` : un objet qui n'est pas un virus mais l'installateur du virus indiqué.

