



**Dr.WEB**

KATANA

# 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, SplDer Mail, SplDer 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.

**Dr.Web KATANA**  
**Version 1.0**  
**Manuel utilisateur**  
**17/09/2021**

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

<b>1. A propos de</b>	<b>5</b>
1.1. Conventions	5
1.2. Méthode de détection des menaces	5
1.3. Pré-requis système	7
<b>2. Installation, récupération et suppression de Dr.Web KATANA</b>	<b>9</b>
2.1. Première installation	9
2.2. Récupération et suppression de Dr.Web KATANA	12
<b>3. Licence</b>	<b>14</b>
3.1. Méthodes d'activation	15
3.2. Renouveler la licence	15
3.3. Assistant d'enregistrement	16
<b>4. Mise en route</b>	<b>18</b>
<b>5. Outils</b>	<b>19</b>
5.1. Gestionnaire de licences	19
5.2. Gestionnaire de quarantaine	20
5.3. Support	21
5.3.1. Créer un rapport	22
<b>6. Mise à jour</b>	<b>24</b>
<b>7. Configuration</b>	<b>25</b>
7.1. Général	25
7.2. Mise à jour	26
7.3. Autoprotection	27
7.4. Dr.Web Cloud	28
7.5. Protection	29
<b>8. Support technique</b>	<b>34</b>
<b>9. Annexe A. Paramètres de la ligne de commande pour le Module de mise à jour</b>	<b>35</b>




## 1. A propos de

Dr.Web KATANA protège le système contre les menaces avec les méthodes sans signatures : il analyse le comportement des processus, utilise les technologies cloud de détection des menaces et les règles prédéfinies. Le programme est compatible avec les antivirus créés par d'autres concepteurs et peut fonctionner ensemble avec ces antivirus afin de renforcer la protection de l'ordinateur.

### 1.1. Conventions

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.
<b>Enregistrer</b>	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.
C:\Windows\	Noms de fichiers/dossiers ou fragments de programme.
<a href="#">Annexe A</a>	Liens vers les autres chapitres du manuel ou liens vers des ressources externes.

### 1.2. Méthode de détection des menaces

#### Analyse de comportement

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 actions des trojans-encodeurs) ;
- 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 empêche la désactivation du mode sécurisé Windows en bloquant toutes 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.

## Protection contre les exploits

La technologie Dr.Web ShellGuard incluse dans Dr.Web Process Heuristics 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) ;
- 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.

### 1.3. Pré-requis système

Dr.Web peut être utilisé uniquement sur un ordinateur possédant les pré-requis suivants :

Composant	Pré-requis
Processeur	Processeur pleinement compatible i686.
RAM disponible	Au moins 100 Mo.
Espace sur le disque dur	150 Mo pour les composants de Dr.Web. Les fichiers créés pendant l'installation nécessitent encore de l'espace libre.
Système d'exploitation	Pour les plateformes 32-bits : <ul style="list-style-type: none"><li>• Windows XP avec Service Pack 2 ou supérieur,</li><li>• Windows Vista avec Service Pack 2 ou supérieur,</li><li>• Windows 7,</li><li>• Windows 8,</li><li>• Windows 8.1,</li><li>• Windows 10 21H1 ou une version antérieure,</li><li>• Windows Server 2003 avec Service Pack 1,</li><li>• Windows Server 2008.</li></ul> Pour les plateformes 64-bits : <ul style="list-style-type: none"><li>• Windows Vista avec Service Pack 2 ou supérieur,</li><li>• Windows 7,</li><li>• Windows 8,</li><li>• Windows 8.1,</li><li>• Windows 10 21H1 ou une version antérieure,</li><li>• Windows 11,</li></ul>



	<ul style="list-style-type: none"><li>• Windows Server 2008 avec Service Pack 2 ou supérieur,</li><li>• Windows Server 2008 R2,</li><li>• Windows Server 2012,</li><li>• Windows Server 2012 R2,</li><li>• Windows Server 2016,</li><li>• Windows Server 2019.</li></ul> <p>Vous aurez peut-être à télécharger et installer certaines mises à jour de composants système depuis le site Microsoft. Si cela est nécessaire, Dr.Web vous indiquera les composants requis et vous fournira les liens de téléchargement.</p>
Résolution d'écran	Au moins 1024x768.

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 se connecter au service Dr.Web Cloud	sortants	2075 (y compris les ports UDP)

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





## 2. Installation, récupération et suppression de Dr.Web KATANA

Avant d'installer Dr.Web KATANA, consultez les [pré-requis système](#). Il est également recommandé d'effectuer 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 : <https://support.microsoft.com/help/12373/windows-update-faq>) ; si le producteur ne supporte plus le système d'exploitation, il est recommandé de migrer vers une version plus récente du système d'exploitation ;
- analyser le système de fichiers en utilisant les outils système, et en cas d'erreurs détectées, résoudre le problème ;
- fermer toutes les applications en cours.

### 2.1. Première installation

Il existe les modes suivants d'installation du logiciel antivirus Dr.Web :

- en tâche de fond,
- le mode standard.

#### Installation en mode Standard

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

- si vous avez le fichier d'installation (`drweb-1.0-katana.exe`), 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'autodémarrage sera ouverte. Cliquez sur le bouton **Installer**.

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

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

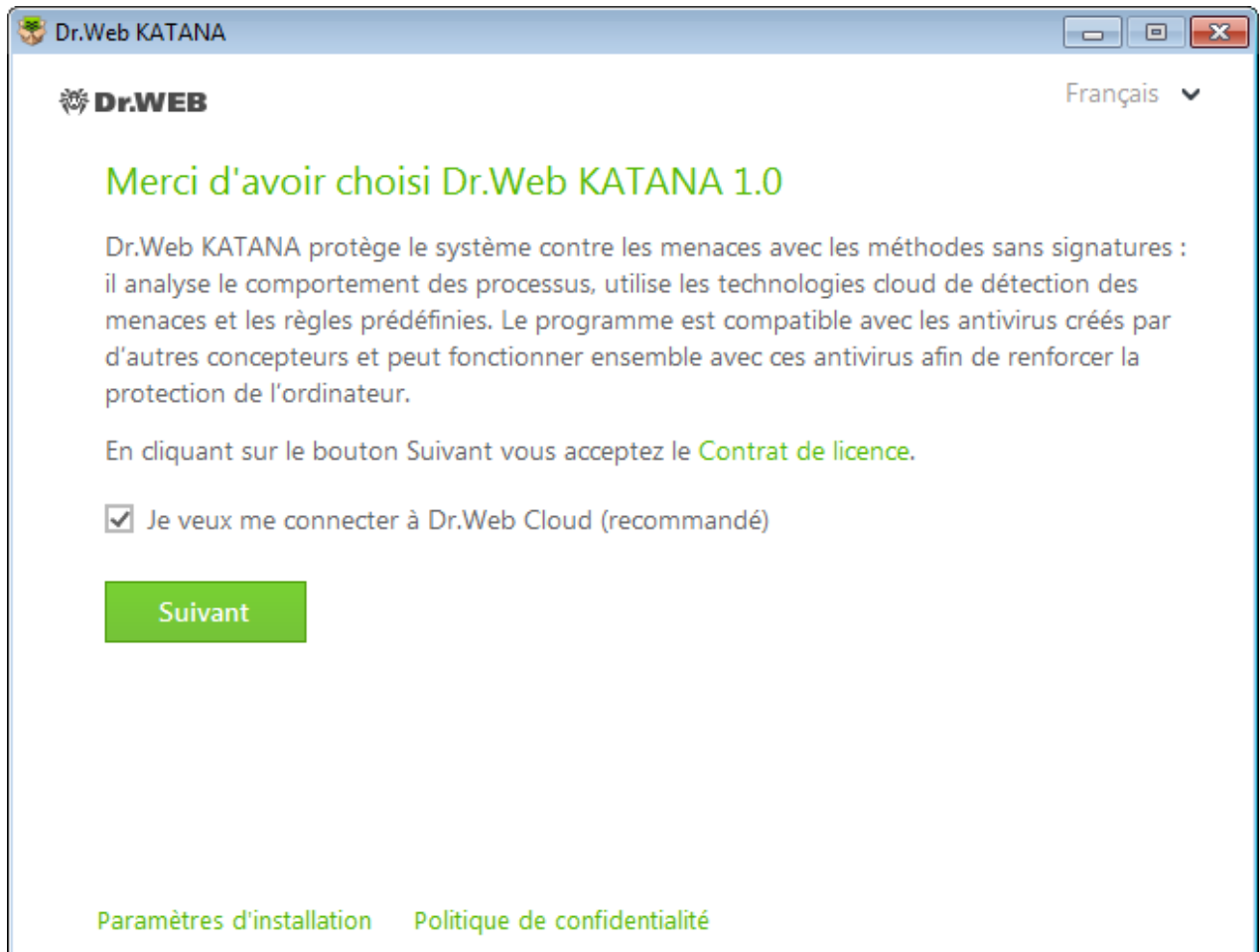
#### Pour installer le programme

1. Si un autre antivirus de Doctor Web 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 d'effectuer l'analyse de données en utilisant les informations virales les plus récentes. Ces informations sont stockées et mises à jour en temps réel sur les serveurs de Doctor Web. L'option est activée par défaut.



**Figure 1. Assistant d'installation**

3. Si vous voulez effectuer l'installation avec les paramètres par défaut, passez à l'étape 4. Pour sélectionner les composants que vous souhaitez installer, spécifiez le chemin d'installation de ces composants et d'autres paramètres, cliquez sur le lien **Paramètres d'installation**. Cette option est destinée aux utilisateurs expérimentés.
  - Dans le premier onglet, vous pouvez modifier le chemin d'installation.
  - Dans le deuxième onglet, 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, cliquez sur **Spécifier le chemin vers le fichier clé valide**. Cliquez sur **Parcourir** et sélectionnez le fichier clé nécessaire dans la fenêtre qui s'ouvre.
- Si vous n'avez pas le fichier clé et que vous souhaitez le recevoir durant l'installation, sélectionnez **Obtenir le fichier clé lors de l'installation** et cliquez sur **Installer**.



Figure 2. Assistant d'enregistrement

## Installation avec les paramètres de ligne de commande

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

Paramètre	Valeur
lang	Langue du produit. La valeur de ce paramètre est le code de la langue au format ISO 639-1, par exemple, /lang fr.
reboot	Redémarre l'ordinateur automatiquement après l'installation complète.



Paramètre	Valeur
silent	Installation en tâche de fond.

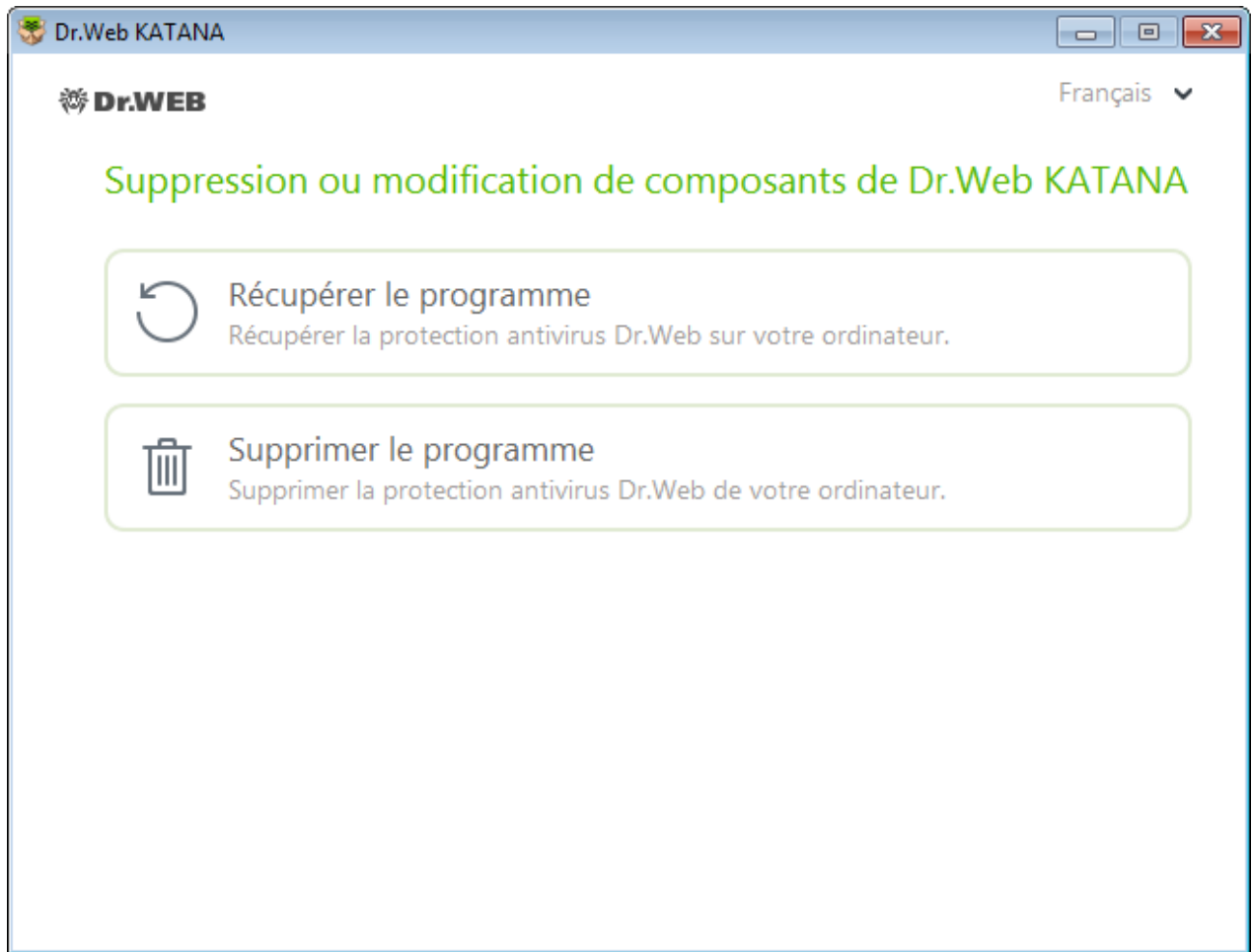
Par exemple, pour lancer une installation de Dr.Web en tâche de fond, exécutez la commande suivante :

```
drweb-1.0-katana.exe /silent yes
```

## 2.2. Récupération et suppression de Dr.Web KATANA

### Récupération ou suppression de Dr.Web avec des outils standard de l'OS Windows

1. Pour supprimer ou récupérer Dr.Web KATANA, lancez l'utilitaire de suppression de logiciels Windows.
2. Dans la liste qui apparaît, sélectionnez la ligne portant le nom du programme.
  - Pour supprimer définitivement le logiciel, cliquez sur **Supprimer** et passez à l'[étape 5](#).
  - Pour restaurer Dr.Web, cliquez sur le bouton **Modifier**. La fenêtre de l'Assistant de récupération/suppression du logiciel va s'ouvrir.



**Figure 3. Assistant de récupération/suppression du logiciel**

3. S'il faut restaurer la protection antivirus sur votre ordinateur, sélectionnez l'élément **Récupérer le programme**. Cette fonction est appliquée au cas où certains composants de Dr.Web seraient endommagés.
4. Pour supprimer tous les composants installés, sélectionnez **Supprimer le programme**.
5. Dans la fenêtre **Paramètres sauvegardés**, cochez les cases contre les éléments à conserver après la suppression du programme. Les objets et les paramètres sauvegardés peuvent être utilisés par le programme lors d'une réinstallation. Cliquez sur **Suivant**.
6. Dans la fenêtre suivante, pour confirmer la désinstallation de Dr.Web saisissez le code affiché, puis cliquez sur **Supprimer le programme**.
7. Redémarrez l'ordinateur pour terminer la suppression.



### 3. Licence

Pour utiliser Dr.Web pendant un long délai, une licence est requise. Vous pouvez acheter une licence avec un produit physique, sur le [site](#) officiel de Doctor Web ou chez les partenaires. Une licence accorde le droit d'utiliser toutes les fonctionnalités du produit durant toute la durée de la licence. Les paramètres du fichier clé sont définis en fonction du Contrat de licence.

Si vous souhaitez tester le produit avant de l'acheter, vous pouvez activer une version d'essai. Cette licence fournit les fonctionnalités complètes des principaux composants, mais la durée de validité est restreinte.



Vous pouvez activer une version d'essai sur le même ordinateur une seule fois par an.

La version d'essai peut être activée pour 1 mois. Dans ce cas, aucun numéro de série ni données d'enregistrement ne sont requis.

#### Fichier clé

Les droits d'utilisation de Dr.Web sont spécifiés dans le fichier spécialisé 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 ;
- période pendant laquelle vous êtes autorisé à utiliser le logiciel ;
- 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. Le 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.



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



Un fichier clé obtenu lors de l'activation de la version d'essai peut être utilisé seulement sur l'ordinateur sur lequel a eu lieu la procédure d'enregistrement.

### 3.1. Méthodes d'activation

Vous pouvez activer la licence par un des moyens suivants :

- en utilisant l'[Assistant d'enregistrement](#) durant l'installation ou plus tard ;
- en obtenant le fichier clé durant l'enregistrement sur le [site](#) de Doctor Web ;
- en indiquant durant l'installation le chemin vers le fichier clé valide sur votre ordinateur ou dans la fenêtre de l'[Assistant d'enregistrement](#).

#### Réactivation de la licence

Vous pourriez avoir à réactiver votre licence ou la version d'essai si vous avez perdu le fichier clé.



Lors de la réactivation de la licence ou de la version d'essai, vous recevez le même fichier clé que durant l'enregistrement antérieur 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 envoyé. Dans ce cas, pour recevoir le 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 du support technique à votre adresse e-mail.

### 3.2. Renouveler la licence

Dans certains cas, par exemple, lorsque la licence expire, vous pouvez avoir besoin de renouveler ou d'étendre votre licence pour Dr.Web. Si c'est le cas, vous devez remplacer le fichier clé actuel. Dr.Web supporte la mise à jour des licences en cours sans arrêter ni réinstaller Dr.Web.



### Pour remplacer le fichier clé


1. Pour remplacer la licence actuelle, utilisez l'[Assistant d'enregistrement](#).
2. Si le fichier clé actuel est invalide, Dr.Web va utiliser automatiquement le nouveau fichier clé.

## 3.3. Assistant d'enregistrement

Le module de gestion SplDer Agent vérifie si vous possédez un [fichier clé](#). Si aucun fichier clé n'est trouvé, vous êtes invité à en obtenir un sur Internet.

Il est possible d'obtenir un fichier clé durant la procédure d'installation. Pour cela, sélectionnez l'option **Obtenir le fichier clé lors de l'installation** [à l'étape 5](#) et l'activation d'une licence ou d'une version démo démarrera.

Vous pouvez également obtenir un fichier clé en lançant l'activation de la licence ou de la version démo après l'installation du produit. Pour cela, utilisez l'une des options suivantes :

- ouvrez le menu de SplDer Agent  dans la zone de notifications Windows et sélectionnez l'élément **Licence** ;
- dans la fenêtre du [Gestionnaire de licences](#), cliquez sur **Obtenir une nouvelle licence** et sélectionnez dans la liste déroulante **via Internet**.

Après le lancement de l'activation, la fenêtre de l'Assistant d'enregistrement s'ouvre.

Pour activer la licence, vous devez indiquer le numéro de série qui vous a été fourni lors de l'achat de Dr.Web.

Pour tester le programme, vous pouvez activer la version d'essai pour 1 mois. Dans ce cas, aucun numéro de série ni données d'enregistrement ne sont requis.

La première fenêtre vous invite à sélectionner une des méthodes d'activation suivantes :

- activer la licence ;
- obtenir une démo ;
- acheter une licence.

Si vous possédez un numéro de série pour l'activation d'une licence, sélectionnez **Activer la licence**. Entrez le numéro de série et cliquez sur **Suivant**. La fenêtre d'[entrée des données d'enregistrement](#) va s'ouvrir.

Si vous n'avez pas de numéro de série et que vous souhaitez tester le produit, activez une version démo pour 1 mois en sélectionnant **Obtenir une démo**. Cliquez sur **Suivant**. Une fenêtre affichant les [résultats de l'activation](#) va s'ouvrir.

Pour acheter une licence dans la boutique en ligne de Doctor Web, sélectionnez **Acheter une licence**.





Si vous possédez déjà un fichier clé valide, sélectionnez **Autres types d'activation**. Dans la fenêtre qui s'ouvre, spécifiez le chemin d'accès au fichier.

### Entrée des données d'enregistrement

Pour enregistrer une licence, entrez vos données personnelles (prénom, nom et adresse e-mail) et sélectionnez le pays dans la liste déroulante. Tous les champs sont obligatoires à remplir.

Cliquez sur **Suivant**.


### Résultats de l'activation

Si la procédure d'activation a été effectuée avec succès, un message le confirmant s'affiche. Cliquez sur **Terminer** pour effectuer la mise à jour des bases virales et des autres fichiers du paquet. D'habitude, cette procédure ne requiert pas l'intervention de l'utilisateur.

Si l'activation a échoué, un message d'erreur s'affiche. Cliquez sur **Paramètres de connexion** pour modifier les paramètres de connexion Internet ou cliquez sur **Recommencer** pour corriger les données incorrectes.






## 4. Mise en route



Lorsque Dr.Web est installé, l'icône du module de gestion SplDer Agent  s'affiche dans la zone de notification Windows :



Si SplDer Agent n'est pas lancé, ouvrez le groupe Dr.Web et sélectionnez SplDer Agent dans le menu Démarrer de Windows.

L'icône de SplDer Agent indique le statut de Dr.Web :

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

Le menu de SplDer Agent  vous offre les outils principaux de gestion et de configuration de Dr.Web. Pour accéder au menu de SplDer Agent, cliquez sur l'icône de SplDer Agent  dans la zone de notifications Windows.

**Licence.** Ce lien ouvre le [Gestionnaire de licences](#).

**Mise à jour.** Informations sur le statut des mises à jour des composants. Lance une mise à jour.

**Protection.** Accès rapide à la désactivation et à l'activation de la protection préventive. Chaque activation et désactivation de la protection préventive sont enregistrées dans le journal des événements du système d'exploitation Windows, dans la section **Journaux des applications et des services** → **Doctor Web**.

**Paramètres**  . Ouvre la fenêtre de paramètres.

**Outils**  . Ouvre l'accès aux outils suivants :

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

**Aide**  . Ouvre le présent manuel.

## 5. Outils

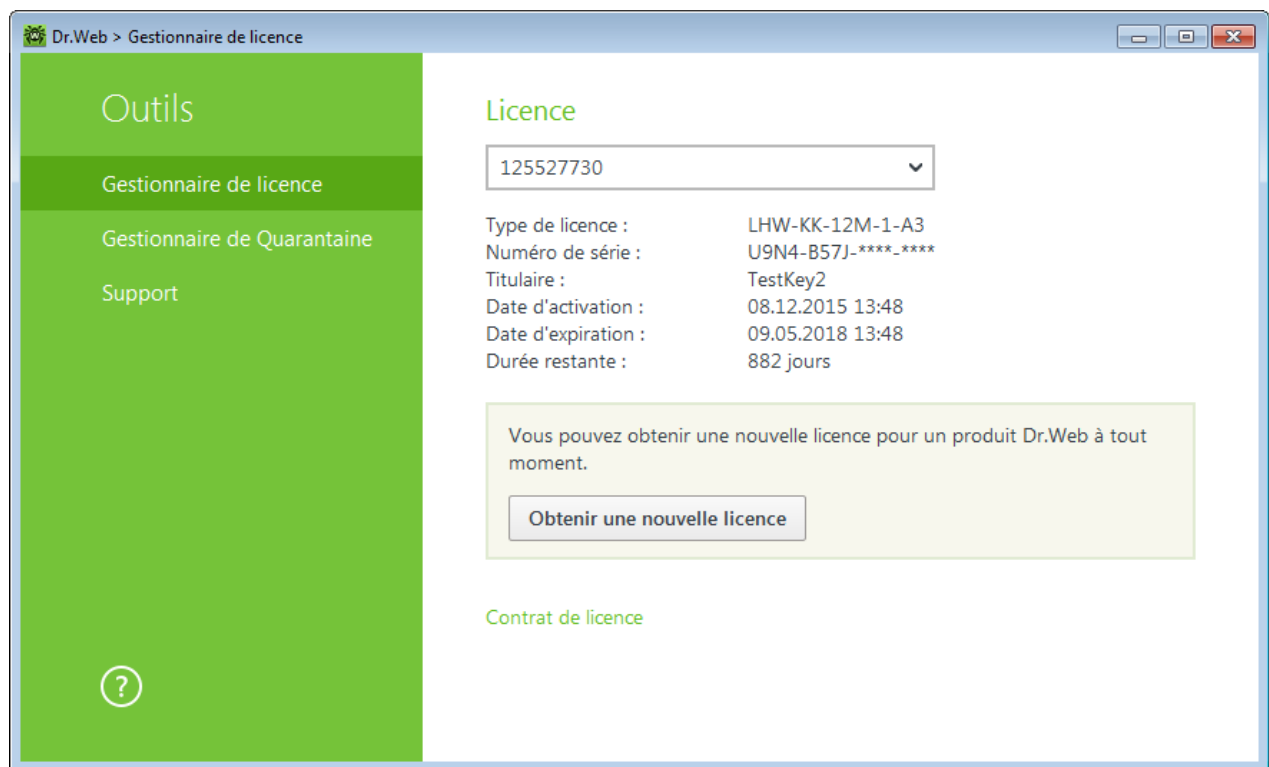
Pour voir les fichiers isolés ou récupérer les fichiers de la quarantaine, sélectionnez l'onglet [Gestionnaire de quarantaine](#).

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

### 5.1. Gestionnaire de licences


Cette fenêtre affiche les informations sur les [licences](#) Dr.Web que vous possédez.

Les informations sur la licence sélectionnée sont affichées dans la partie haute de la fenêtre.



**Figure 4. Informations sur la licence actuelle**

Le bouton **Obtenir une nouvelle licence** ouvre l'[Assistant d'enregistrement](#) grâce auquel vous pouvez activer une nouvelle licence, indiquer un chemin vers un autre fichier clé de licence ou acheter une licence pour tout produit Dr.Web.

Le bouton  permet de supprimer la licence sélectionnée dans la liste.

Pour utiliser Dr.Web, installez le fichier clé Dr.Web dans le système. Si vous avez reçu le fichier clé durant l'installation ou qu'il est inclus au kit de distribution du produit, l'installation du fichier clé démarre automatiquement et ne requiert aucune action supplémentaire.



Par défaut, le fichier clé est placé dans le dossier d'installation de Dr.Web. Le 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.

## 5.2. Gestionnaire de quarantaine

Gestionnaire de quarantaine est un outil permettant de gérer des fichiers isolés. La quarantaine contient les copies de sauvegarde d'objets créées avant leur suppression par Dr.Web. Les logiciels considérés par Dr.Web Process Heuristic comme logiciels modifiant les fichiers utilisateur de façon indésirable (par exemple, les trojans-encodeurs) et les logiciels s'infiltrant dans des processus d'autres applications sont mis en quarantaine.

Objets	Menace	Date d'ajout	Chemin
333.exe	DPH:Trojan.Inject.3	22:34 09.12.2015	C:\test\333.exe
123.exe	DPH:Trojan.Inject.3	22:34 09.12.2015	C:\test\123.exe
Tojan_Inje...	DPH:Trojan.Inject.3	22:33 09.12.2015	C:\test\Tojan_Inject...
444.exe	DPH:Trojan.Inject.3	22:34 09.12.2015	C:\test\444.exe
2222.exe	DPH:Trojan.Inject.3	22:34 09.12.2015	C:\test\2222.exe

Figure 5. Objets en quarantaine

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

- **Objets** : liste de noms des objets placés en quarantaine ;
- **Menace** : type de programme malveillant déterminé par Dr.Web lorsque l'objet est placé en quarantaine ;
- **Date d'ajout** : la date à laquelle l'objet a été déplacé en quarantaine ;
- **Chemin** : chemin d'accès complet au fichier avant qu'il ne soit placé en quarantaine.



## Gestion des objets en quarantaine

Les boutons suivants sont disponibles pour chaque objet :


- **Récupérer** : 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.

- **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 **Supprimer tout** dans la liste déroulante.

## 5.3. Support

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

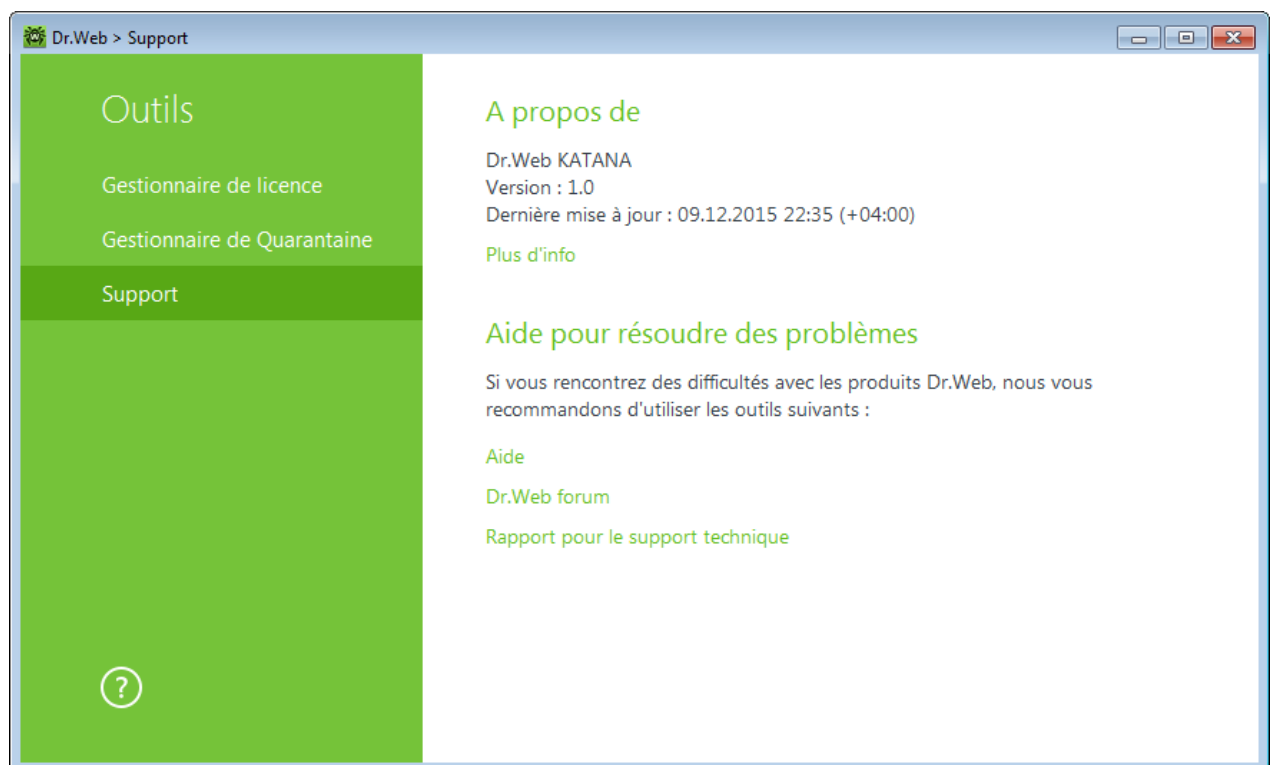


Figure 6. Informations sur la version du produit et support



Si vous avez des questions, utilisez un des outils suivants :

**Aide.** Ce lien ouvre le manuel.

**Forum Dr.Web.** 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 de solution à votre problème, vous pouvez demander une assistance directe du support technique de Doctor Web en remplissant le formulaire dans la section correspondante à la page <https://support.drweb.com/>.

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/>.

### 5.3.1. 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.

Le rapport sera sauvegardé sous forme d'archive dans le répertoire 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,
- informations sur les processus en cours d'exécution,
- informations sur les tâches programmées,
- informations sur les services et les pilotes,
- informations sur le navigateur par défaut,
- informations sur les applications installées,
- informations sur les politiques de restrictions,
- informations sur le fichier HOSTS,
- informations sur les serveurs DNS,
- entrées du journal d'événements,
- liste des répertoires système,
- branches du registre,
- fournisseurs Winsock,
- connexions réseau,
- rapports du débogueur Dr.Watson,



- indice de performances.
2. Informations sur le produit Dr.Web installé :
- type et version du produit Dr.Web installé ;
  - informations sur le contenu des composants installés ; informations sur les modules de Dr.Web ;
  - configuration et paramètres de la configuration du produit Dr.Web ;
  - informations sur la licence ;
  - journal de fonctionnement de Dr.Web.

Les informations sur les produits antivirus Dr.Web se trouvent dans le Journal d'événements du système d'exploitation Windows dans la section **Journaux des applications et des services** → **Doctor Web**.



## 6. Mise à jour

Pour garantir que les algorithmes du logiciel sont à jour, Doctor Web distribue régulièrement des mises à jour par Internet.

### Démarrage 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 à sa sortie.



Pour mettre à jour Dr.Web, l'accès à Internet est requis.

Vous pouvez configurer les paramètres nécessaires à la page **Mise à jour** [des Paramètres principaux](#) de Dr.Web.

### Démarrage d'une mise à jour depuis le module de gestion SpIDer Agent

Dans le [menu](#) SpIDer Agent  sélectionnez l'élément **Mise à jour**. Une fenêtre apparaît et affiche les informations sur la nécessité d'une mise à jour et la date de la dernière mise à jour. Pour démarrer une mise à jour cliquez sur **Mettre à jour**.

### Démarrage d'une mise à jour depuis la ligne de commande

Ouvrez le dossier d'installation de Dr.Web et lancez le fichier `drwupsrv.exe`. La liste des paramètres se trouve dans l'[Annexe A](#).

### Démarrage automatique d'une mise à jour

Lors du démarrage automatique, la mise à jour est effectuée en tâche de fond et le rapport est enregistré dans le fichier `dwupdater.log` situé dans le dossier `%allusersprofile%\Doctor Web\Logs\`.





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.





## 7. Configuration

Pour accéder aux paramètres, ouvrez le menu de SplDer Agent  et lancez **Paramètres** .

### 7.1. Général

Dans cette section, vous pouvez choisir la langue du logiciel, importer et exporter les paramètres de Dr.Web.

#### Langue

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

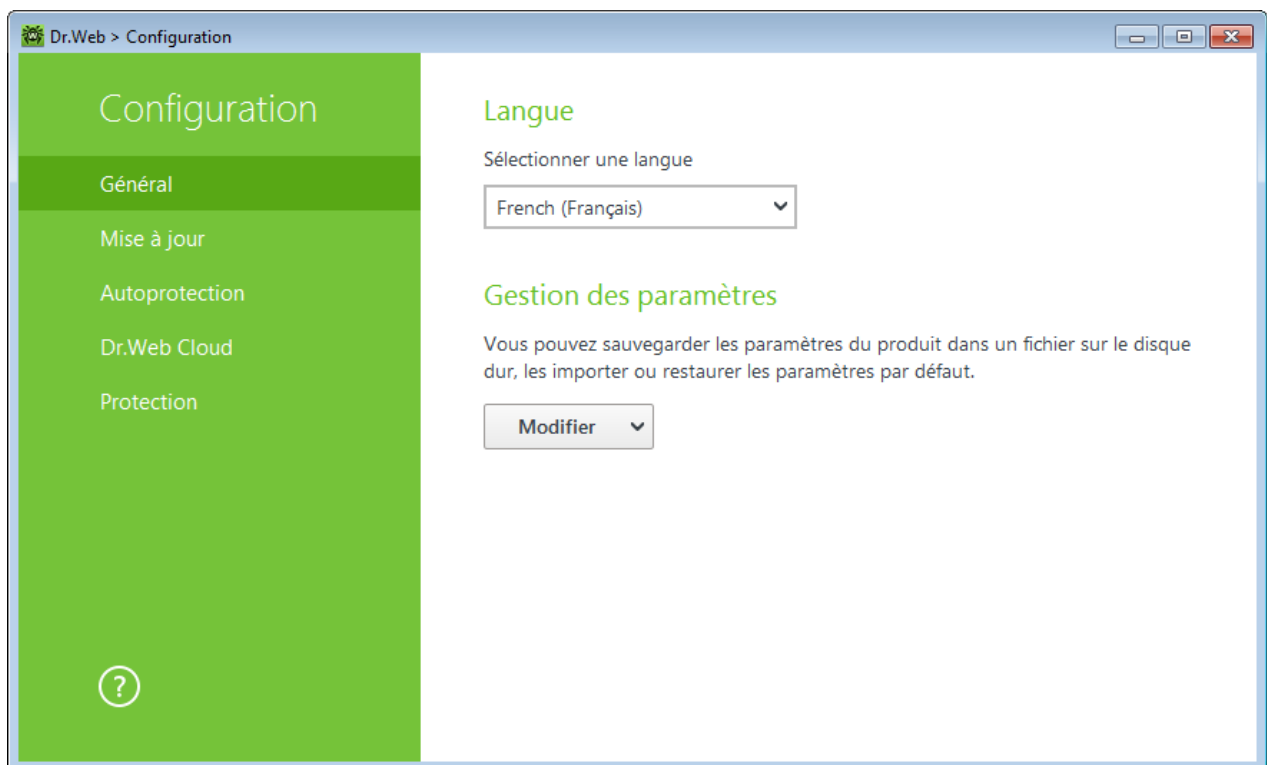


Figure 7. Paramètres principaux

#### Gérer les paramètres

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

Si vous avez déjà configuré le programme sur un autre ordinateur et que vous souhaitez utiliser les mêmes paramètres, 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.

## 7.2. Mise à jour

### Paramètres généraux de mise à jour

**Périodicité des mises à jour.** Indiquez la fréquence de vérification des mises à jour. La valeur par défaut (30 minutes) est optimale pour maintenir à jour les informations sur les menaces.

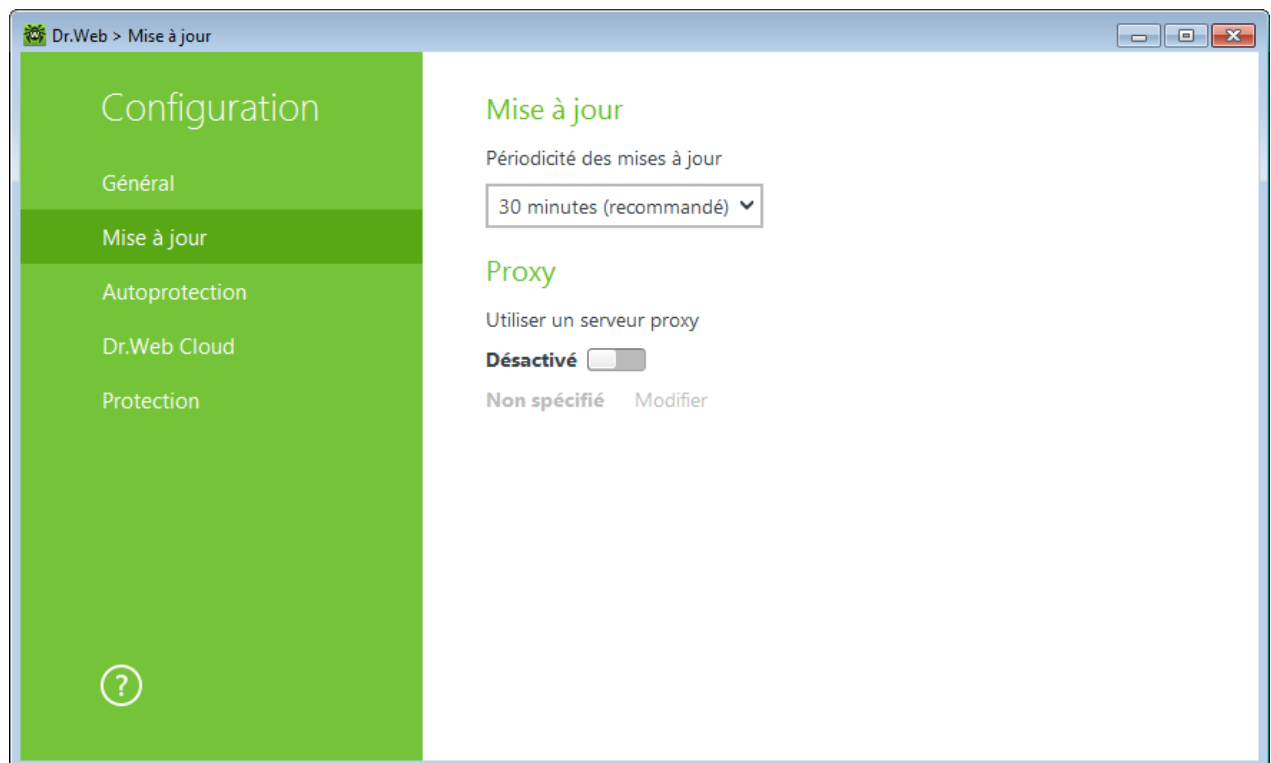


Figure 8. Paramètres de la mise à jour

### Utiliser le serveur proxy

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

Paramètre	Description
Adresse	Spécifiez l'adresse du serveur proxy.
Port	Spécifiez le port du serveur proxy.
Utilisateur	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.



Paramètre	Description
Type d'authentification	Sélectionnez un type d'authentification nécessaire pour se connecter au serveur proxy.

## 7.3. Autoprotection

### Paramètres de l'autoprotection

Sur cette page, vous pouvez configurer les paramètres de protection de Dr.Web lui-même contre des modifications non autorisées par les logiciels anti-antivirus et contre un endommagement accidentel. L'option **Activer l'Autoprotection** permet de protéger les fichiers et les processus de Dr.Web contre un accès non autorisé. Il est recommandé de ne pas désactiver l'autoprotection.

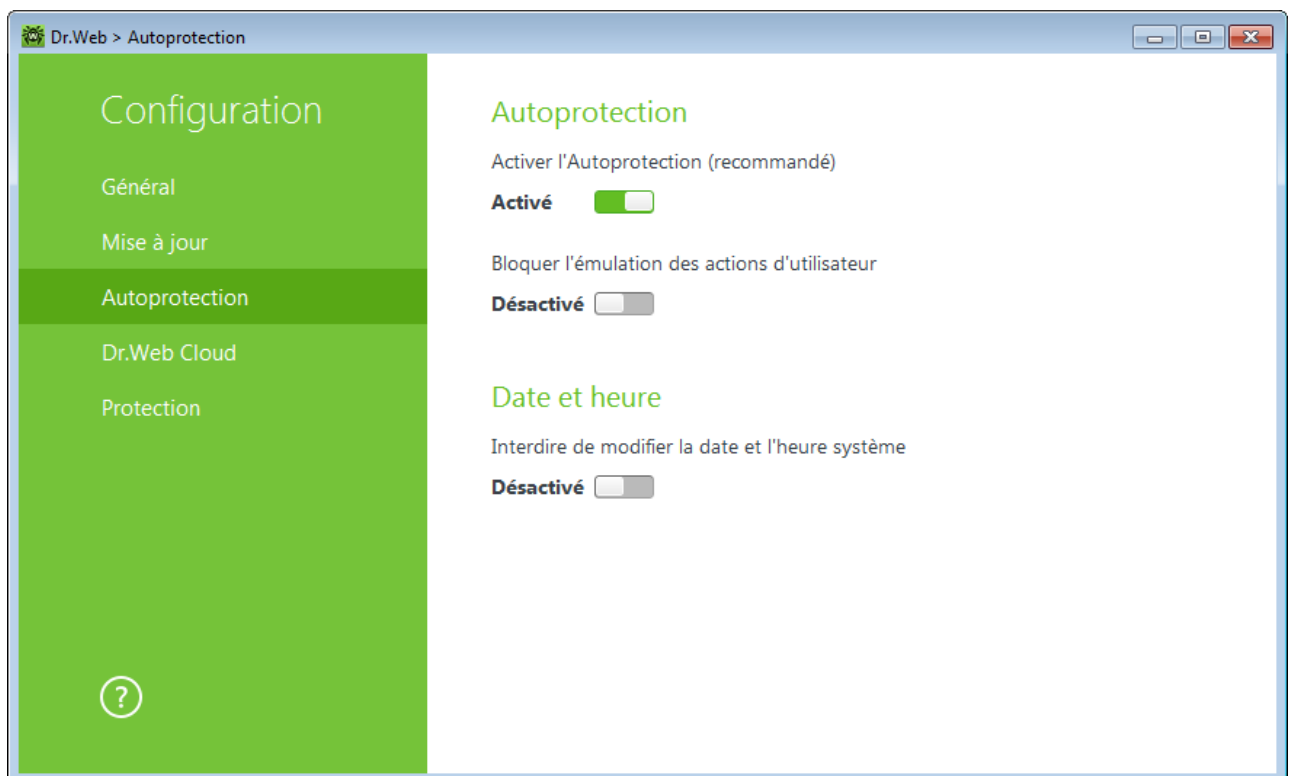


Figure 9. Paramètres de l'Autoprotection Dr.Web



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 toute modification automatique dans le fonctionnement 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.

## Date et heure

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.

## 7.4. 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.

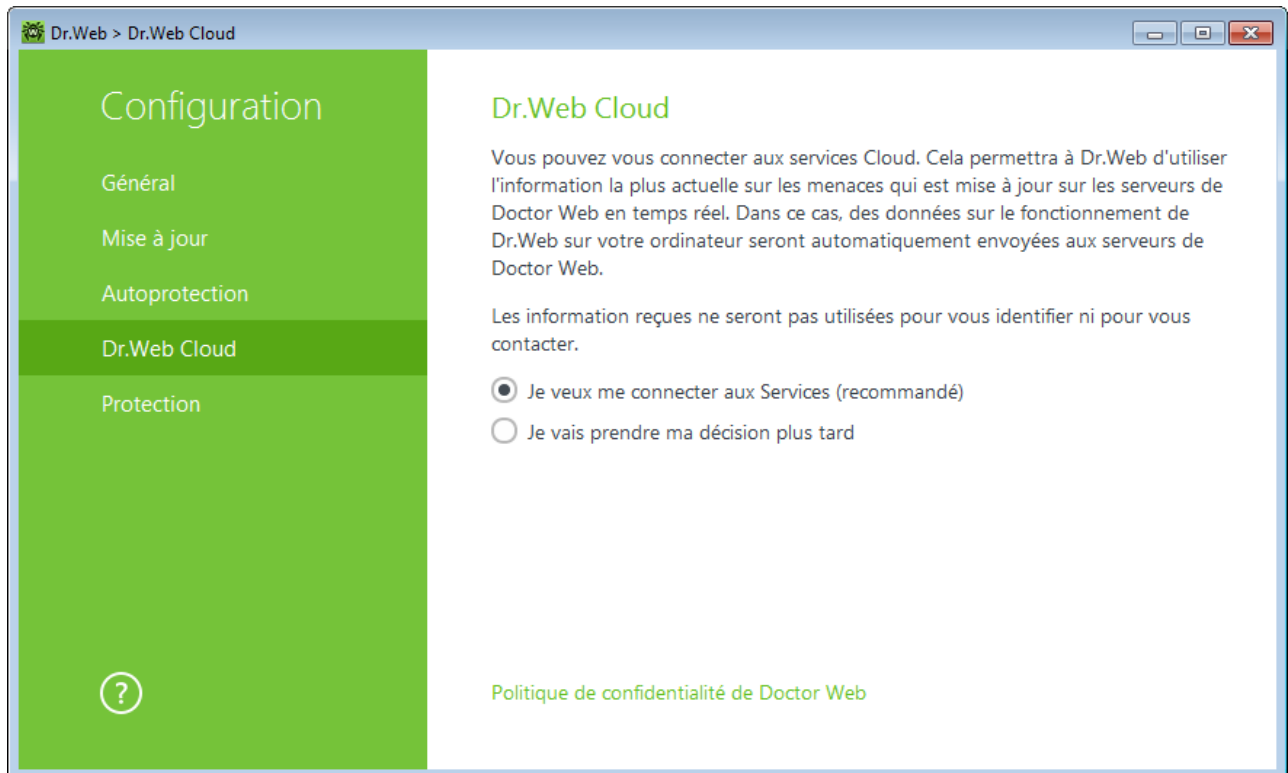


Figure 10. Connexion à Dr.Web Cloud

## 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.



## Programme d'amélioration de la qualité du logiciel

Si vous participez au programme, des données non personnelles sur le fonctionnement de Dr.Web sur votre ordinateur seront périodiquement envoyées sur les serveurs de la société Doctor Web. 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.

## 7.5. Protection

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.

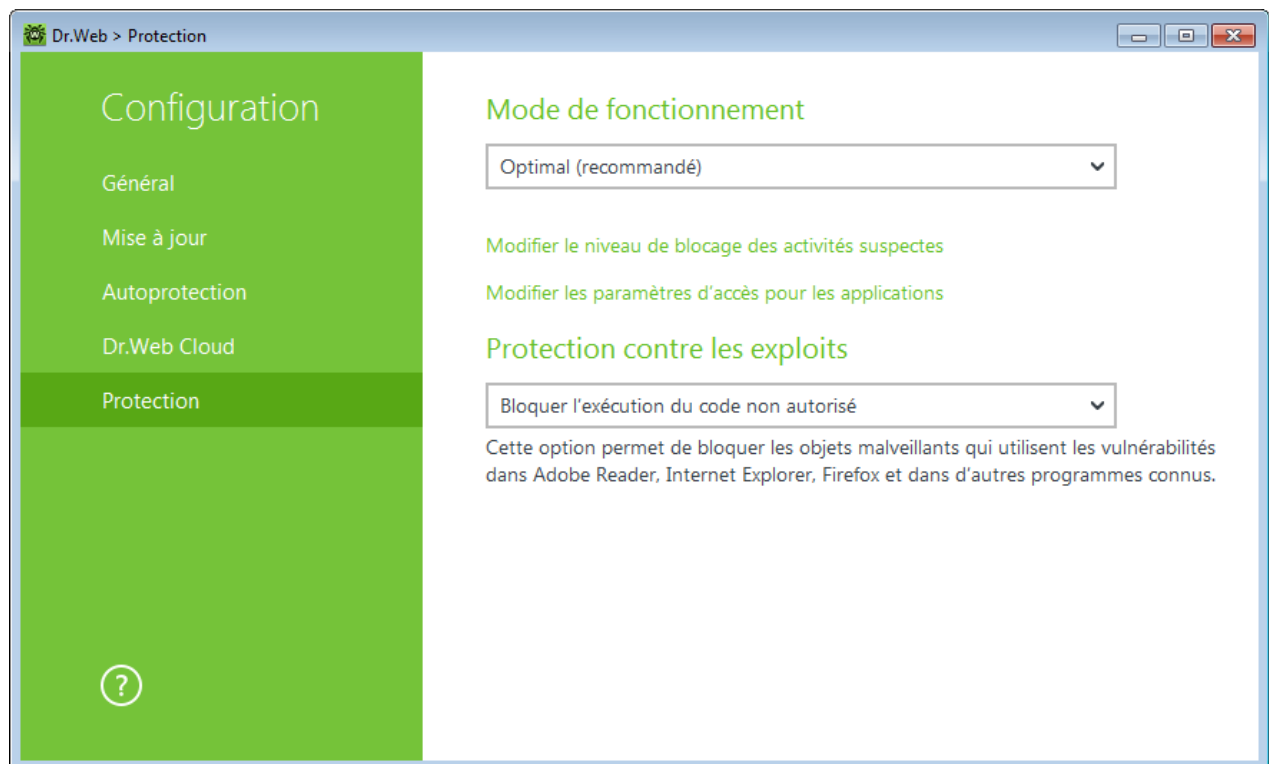



Figure 11. Sélection du mode de Protection

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 les paramètres 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.




### Pour créer 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.

### Pour ajouter une règle

1. Cliquez sur .
2. Dans la fenêtre qui s'affiche, cliquez sur **Parcourir** et spécifiez le chemin d'accès au 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 de la liste, sélectionnez-le et cliquez sur .

### Niveau de la Protection préventive

Dans le mode **Optimal** spécifié par défaut, Dr.Web interdit automatiquement la modification des objets système, dont la modification indiquerait clairement une tentative malveillante d'endommager le système d'exploitation. Il bloque également l'accès bas niveau au disque et protège le fichier HOSTS de toute modification.

S'il existe un risque élevé d'infection de votre ordinateur, vous pouvez augmenter le niveau de protection en choisissant le mode **Moyen**. 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.

Lorsqu'il est nécessaire d'avoir un contrôle total de l'accès aux objets critiques Windows, vous pouvez choisir le mode **Paranoïde**. Dans ce mode, Dr.Web fournit également un contrôle interactif du chargement de pilotes et du démarrage automatique de programmes.

Dans le mode **Utilisateur**, vous pouvez choisir vous-même le niveau de 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 ce qui représente une menace pour la sécurité de l'ordinateur.
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.
Fichier HOSTS	Le système d'exploitation utilise le fichier HOSTS pour faciliter la connexion à Internet. La modification de ce fichier peut 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 pilotes 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"><li>• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options</li></ul> <p>Accès à User Drivers :</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Drivers32</li><li>• Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers</li></ul> <p>Paramètres de Winlogon :</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL</li></ul> <p>Notificateurs Winlogon :</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify</li></ul> <p>Autodémarrage de Windows :</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Windows, Applnit_DLLs, LoadApplnit_DLLs, Load, Run, IconServiceLib</li></ul> <p>Associations de fichiers exécutables :</p> <ul style="list-style-type: none"><li>• Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (clés)</li><li>• Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (clés)</li></ul> <p>Politiques de restriction du démarrage des programmes (SRP) :</p> <ul style="list-style-type: none"><li>• Software\Policies\Microsoft\Windows\Safer</li></ul> <p>Plugin Internet Explorer (objet application d'assistance du navigateur) :</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects</li></ul>



Objet protégé	Description
	<p>Autodémarrage de programmes :</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows\CurrentVersion\Run</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnce</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnceEx</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup</li><li>• Software\Microsoft\Windows\CurrentVersion\RunServices</li><li>• Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</li></ul> <p>Autodémarrage de politiques :</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</li></ul> <p>Configuration du mode sans échec :</p> <ul style="list-style-type: none"><li>• SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal</li><li>• SYSTEM\ControlSetXXX\Control\SafeBoot\Network</li></ul> <p>Paramètres de Session Manager :</p> <ul style="list-style-type: none"><li>• System\ControlSetXXX\Control\Session Manager\SubSystems, Windows</li></ul> <p>Services système :</p> <ul style="list-style-type: none"><li>• System\CurrentControlSet\XXX\Services</li></ul>



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.

## 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 l'action nécessaire.





Niveau de protection	Description
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.



## 8. 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/](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/>.



## 9. Annexe A. Paramètres de la ligne de commande pour le 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 : <code>error</code> (standard), <code>info</code> (élevé), <code>debug</code> (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	Dossier du référentiel, (par défaut <code>&lt;data_dir&gt;/repo</code> ).
-t [ --trace ]	Activer le traçage.
-c [ --command ] arg (=update)	Commande à exécuter : <code>getversions</code> — obtenir les versions, <code>getcomponents</code> — obtenir les composants, <code>update</code> — mise à jour, <code>uninstall</code> — supprimer, <code>exec</code> — exécuter, <code>keyupdate</code> — mettre à jour la clé, <code>download</code> — télécharger.
-z [ --zone ] arg	Liste des zones à utiliser à la place des zones spécifiées dans le fichier de configuration.

### 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 composants à mettre à niveau vers une révision spécifiée. Syntaxe : <code>&lt;name&gt;, &lt;target revision&gt;</code> .
-x [ --selfrestart ] arg (=)yes	Redémarrage après la mise à jour du Module de mise à jour. La valeur par défaut est <code>yes</code> . En cas de valeur <code>no</code> , une notification sur la nécessité de redémarrage sera affichée.



Paramètre	Description
--geo-update	Obtenir une liste des adresses IP <code>update.drweb.com</code> avant la mise à jour.
--type arg (=normal)	Peut prendre l'une des valeurs suivantes : <ul style="list-style-type: none"><li>• <code>reset-all</code> : forcer la mise à jour de tous les composants ;</li><li>• <code>reset-failed</code> : annuler toutes les modifications pour les composants corrompus ;</li><li>• <code>normal-failed</code> : essayer de mettre à niveau les composants y compris ceux qui sont corrompus, vers la dernière version ou vers la version spécifiée ;</li><li>• <code>update-revision</code> : mettre à jour les composants au sein de la révision courante ;</li><li>• <code>normal</code> : mettre à jour tous les composants.</li></ul>
-g [ --proxy ] arg	Serveur proxy pour la mise à jour au format <code>&lt;adresse&gt;: &lt;port&gt;</code> .
-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 : <code>&lt;nom&gt;: &lt;valeur&gt;</code> .
-l [ --progress-to-console ]	Afficher sur la console les informations sur le chargement et l'exécution du script.

### Paramètres spécifiques de la commande d'exécution (exec) :

Paramètre	Description
-s [ --script ] arg	Exécuter le script spécifié.
-f [ --func ] arg	Exécuter la fonction du script.
-p [ --param ] arg	Transmettre les paramètres supplémentaires vers le script. Syntaxe : <code>&lt;nom&gt;: &lt;valeur&gt;</code> .
-l [ --progress-to-console ]	Afficher sur la console des informations sur la progression de l'exécution du script.

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

Paramètre	Description
-s [ --version ] arg	Numéro de version.



Paramètre	Description
-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.
-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 <adresse>: <port>.
-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>&lt;adresse&gt;</i> : <i>&lt;port&gt;</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	Numéro de version.
-p [ --product ] arg	Nom du produit à télécharger.

